Contents

Formaliz. Math. 24 (**1**)

FORMALIZED MATHEMATICS
Vol. 24, No. 1, Pages 1–16, 2016
DOI: 10.1515/forma-2016-0001

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

Modelling Real World Using Stochastic Processes and Filtration

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

Summary. First we give an implementation in Mizar [2] basic important definitions of stochastic finance, i.e. filtration ([9], pp. 183 and 185), adapted stochastic process ([9], p. 185) and predictable stochastic process ([6], p. 224). Second we give some concrete formalization and verification to real world examples.

In article [8] we started to define random variables for a similar presentation to the book [6]. Here we continue this study. Next we define the stochastic process. For further definitions based on stochastic process we implement the definition of filtration.

To get a better understanding we give a real world example and connect the statements to the theorems. Other similar examples are given in [10], pp. 143–159 and in [12], pp. 110–124. First we introduce sets which give informations referring to today (Ω_{now}, Def.6), tomorrow (Ω_{fut_1}, Def.7) and the day after tomorrow (Ω_{fut_2}, Def.8). We give an overview for some events in the σ-algebras $\Omega_{now}, \Omega_{fut1}$ and Ω_{fut2}, see theorems (22) and (23).

The given events are necessary for creating our next functions. The implementations take the form of: $\Omega_{now} \subset \Omega_{fut1} \subset \Omega_{fut2}$ see theorem (24). This tells us growing informations from now to the future 1=now, 2=tomorrow, 3=the day after tomorrow.

We install functions $f : \{1, 2, 3, 4\} \to \mathbb{R}$ as following:
$f_1 : x \to 100, \forall x \in \text{dom } f$, see theorem (36),
$f_2 : x \to 80$, for $x = 1$ or $x = 2$ and
$f_2 : x \to 120$, for $x = 3$ or $x = 4$, see theorem (37),
$f_3 : x \to 60$, for $x = 1$, $f_3 : x \to 80$, for $x = 2$ and
$f_3 : x \to 100$, for $x = 3$, $f_3 : x \to 120$, for $x = 4$ see theorem (38).

These functions are real random variable: f_1 over Ω_{now}, f_2 over Ω_{fut1}, f_3 over Ω_{fut2}, see theorems (46), (43) and (40). We can prove that these functions can be used for giving an example for an adapted stochastic process. See theorem (49).

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

We want to give an interpretation to these functions: suppose you have an equity A which has now $(= w_1)$ the value 100. Tomorrow A changes depending which scenario occurs – e.g. another marketing strategy. In scenario 1 $(= w_{11})$ it has the value 80, in scenario 2 $(= w_{12})$ it has the value 120. The day after tomorrow A changes again. In scenario 1 $(= w_{111})$ it has the value 60, in scenario 2 $(= w_{112})$ the value 80, in scenario 3 $(= w_{121})$ the value 100 and in scenario 4 $(= w_{122})$ it has the value 120. For a visualization refer to the tree:

$$\begin{array}{llllll}
\mathit{Now} & & \mathit{tomorrow} & & \mathit{the\ day\ after\ tomorrow} \\
 & & & & w_{111} = \{1\} \\
 & & w_{11} = \{1,2\} & < & \\
 & & & & w_{112} = \{2\} \\
w_1 = \{1,2,3,4\} & < & & & \\
 & & & & w_{121} = \{3\} \\
 & & w_{12} = \{3,4\} & < & \\
 & & & & w_{122} = \{4\}
\end{array}$$

The sets w_1,w_{11},w_{12},w_{111},w_{112},w_{121},w_{122} which are subsets of $\{1,2,3,4\}$, see (22), tell us which market scenario occurs. The functions tell us the values to the relevant market scenario:

$$\begin{array}{llllll}
\mathit{Now} & & \mathit{tomorrow} & & \mathit{the\ day\ after\ tomorrow} \\
 & & & & f_3(w_i) = 60,\ w_i \text{ in } w_{111} \\
 & & f_2(w_i) = 80 & < & \\
 & & w_i \text{ in } w_{11} & & f_3(w_i) = 80,\ w_i \text{ in } w_{112} \\
f_1(w_i) = 100 & < & & & \\
w_i \text{ in } w_1 & & & & f_3(w_i) = 100,\ w_i \text{ in } w_{121} \\
 & & f_2(w_i) = 120 & < & \\
 & & w_i \text{ in } w_{12} & & f_3(w_i) = 120,\ w_i \text{ in } w_{122}
\end{array}$$

For a better understanding of the definition of the random variable and the relation to the functions refer to [7], p. 20. For the proof of certain sets as σ-fields refer to [7], pp. 10–11 and [9], pp. 1–2.

This article is the next step to the *arbitrage opportunity*. If you use for example a simple probability measure, refer, for example to literature [3], pp. 28–34, [6], p. 6 and p. 232 you can calculate whether an *arbitrage* exists or not. Note, that the example given in literature [3] needs 8 instead of 4 informations as in our model. If we want to code the first 3 given time points into our model we would have the following graph, see theorems (47), (44) and (41):

$$\begin{array}{llllll}
\mathit{Now} & & \mathit{tomorrow} & & \mathit{the\ day\ after\ tomorrow} \\
 & & & & f_3(w_i) = 180,\ w_i \text{ in } w_{111} \\
 & & f_2(w_i) = 150 & < & \\
 & & w_i \text{ in } w_{11} & & f_3(w_i) = 120,\ w_i \text{ in } w_{112} \\
f_1(w_i) = 125 & < & & & \\
w_i \text{ in } w_1 & & & & f_3(w_i) = 120,\ w_i \text{ in } w_{121} \\
 & & f_2(w_i) = 100 & < & \\
 & & w_i \text{ in } w_{12} & & f_3(w_i) = 80,\ w_i \text{ in } w_{122}
\end{array}$$

The function for the "Call-Option" is given in literature [3], p. 28. The function is realized in Def.5. As a background, more examples for using the definition of filtration are given in [9], pp. 185–188.

MSC: 60G05 03B35

Keywords: stochastic process; random variable

MML identifier: FINANCE3, version: 8.1.04 5.36.1267

1. Preliminaries

Now we state the proposition:

(1) Let us consider objects a, b. If $a \neq b$, then $\{a\} \subset \{a, b\}$.

Let I be a non empty subset of $\mathbb{N}$. Observe that $I(\in 2^{\mathbb{R}})$ is non empty.

Let us consider an element T of $\mathbb{N}$. Now we state the propositions:

(2) $\{w$, where w is an element of $\mathbb{N} : w > 0$ and $w \leqslant T\} \subseteq \{w$, where w is an element of $\mathbb{N} : w \leqslant T\}$.

(3) $\{w$, where w is an element of $\mathbb{N} : w \leqslant T\}$ is a non empty subset of $\mathbb{N}$.

(4) If $T > 0$, then $\{w$, where w is an element of $\mathbb{N} : w > 0$ and $w \leqslant T\}$ is a non empty subset of $\mathbb{N}$.

Proof: $\{w$, where w is an element of $\mathbb{N} : w > 0$ and $w \leqslant T\}$ is a subset of $\mathbb{N}$. $1 > 0$ and $1 \leqslant T$ by [1, (24)]. $\square$

Now we state the proposition:

(5) Let us consider a non empty set Ω. Then $\Omega \longmapsto 1$ is a function from Ω into $\mathbb{R}$.

2. Special Random Variables

Now we state the proposition:

(6) Let us consider a natural number d, a sequence φ of real numbers, a non empty set Ω, a σ-field F of subsets of Ω, a non empty set X, a sequence G of X, and an element w of Ω. Then $\{$the portfolio value for future extension of d, φ, F, G and $w\}$ is an event of the Borel sets.

Let d be a natural number, φ be a sequence of real numbers, Ω be a non empty set, F be a σ-field of subsets of Ω, X be a non empty set, G be a sequence of X, and w be an element of Ω. Note that the portfolio value for future extension of d, φ, F, G and w yields an element of $\mathbb{R}$. The $\mathcal{RV}$-portfolio value for future extension of φ, F, G and d yielding a function from Ω into $\mathbb{R}$ is defined by

(Def. 1) for every element w of Ω, $it(w) =$ the portfolio value for future extension of d, φ, F, G and w.

Let us observe that the $\mathcal{RV}$-portfolio value for future extension of φ, F, G and d yields a random variable of F and the Borel sets. Let w be an element of Ω. Let us note that the portfolio value for future of d, φ, F, G and w yields a real number and is defined by the term

(Def. 2) $(\sum_{\alpha=0}^{\kappa}(($the elements of the random variables for the future elements of portfolio value of $(\varphi,F,G,w)) \upharpoonright 1)(\alpha))_{\kappa\in\mathbb{N}}(d-1)$.

Let us note that the portfolio value for future of d, φ, F, G and w yields an element of $\mathbb{R}$. The $\mathcal{RV}$-portfolio value for future of φ, F, G and d yielding a function from Ω into $\mathbb{R}$ is defined by

(Def. 3) for every element w of Ω, $it(w) =$ the portfolio value for future of $d+1$, φ, F, G and w.

Let us note that the $\mathcal{RV}$-portfolio value for future of φ, F, G and d yields a random variable of F and the Borel sets. Now we state the propositions:

(7) Let us consider a natural number d, a sequence φ of real numbers, a non empty set Ω, a σ-field F of subsets of Ω, a non empty set X, a sequence G of X, and an element w of Ω. Then

(i) the portfolio value for future of $d+1$, φ, F, G and $w =$ (the $\mathcal{RV}$-portfolio value for future of φ, F, G and $d)(w)$, and

(ii) $\{$the portfolio value for future of $d+1$, φ, F, G and $w\}$ is an event of the Borel sets.

(8) Let us consider a non empty set Ω, a σ-field F of subsets of Ω, a non empty set X, a sequence G of X, a sequence φ of real numbers, and a natural number d. Then the $\mathcal{RV}$-portfolio value for future extension of φ, F, G and $d+1 =$ (the $\mathcal{RV}$-portfolio value for future of φ, F, G and $d) +$ (the random variables for the future elements of portfolio value of $(\varphi,F,G,0))$.

(9) Let us consider non empty sets Ω, Ω_2, a σ-field Σ of subsets of Ω, a σ-field Σ_2 of subsets of Ω_2, and an element s of Ω_2. Then $\Omega \longmapsto s$ is random variable on Σ and Σ_2.

(10) Let us consider a non empty set Ω, a σ-field Σ of subsets of Ω, a random variable $\mathcal{RV}$ of Σ and the Borel sets, and an element K of $\mathbb{R}$. Then $\mathcal{RV} - (\Omega \longmapsto K)$ is a random variable of Σ and the Borel sets. The theorem is a consequence of (9).

Let Ω be a non empty set, $\mathcal{RV}$ be a function from Ω into $\mathbb{R}$, and w be an element of Ω. The functor Set-Call-Option$(\mathcal{RV}, w)$ yielding an element of $\mathbb{R}$ is defined by the term

(Def. 4) $\begin{cases} \mathcal{RV}(w), & \textbf{if } \mathcal{RV}(w) \geqslant 0, \\ 0, & \textbf{otherwise}. \end{cases}$

Let Σ be a σ-field of subsets of Ω, $\mathcal{RV}$ be a random variable of Σ and the Borel sets, and K be an element of $\mathbb{R}$. The Call-Option on $\mathcal{RV}$ and K yielding a function from Ω into $\mathbb{R}$ is defined by

(Def. 5) for every element w of Ω, if $(\mathcal{RV} - (\Omega \longmapsto K))(w) \geqslant 0$, then $it(w) = (\mathcal{RV} - (\Omega \longmapsto K))(w)$ and if $(\mathcal{RV} - (\Omega \longmapsto K))(w) < 0$, then $it(w) = 0$.

3. Special σ-Fields

Let us consider a sequence A_1 of subsets of $\{1, 2, 3, 4\}$ and a real number w. Now we state the propositions:

(11) Suppose $w = 1$ or $w = 3$. Then suppose for every natural number n, $A_1(n) = \emptyset$ or $A_1(n) = \{1, 2\}$ or $A_1(n) = \{3, 4\}$ or $A_1(n) = \{1, 2, 3, 4\}$. Then $\{w\} \neq \text{Intersection}\, A_1$.

(12) Suppose $w = 2$ or $w = 4$. Then suppose for every natural number n, $A_1(n) = \emptyset$ or $A_1(n) = \{1, 2\}$ or $A_1(n) = \{3, 4\}$ or $A_1(n) = \{1, 2, 3, 4\}$. Then $\{w\} \neq \text{Intersection}\, A_1$.

Now we state the propositions:

(13) Let us consider sets M, A_1, A_2. Suppose $M = \{\emptyset, \{1, 2, 3, 4\}\}$ and A_1, $A_2 \in M$. Then $A_1 \cap A_2 \in M$.

(14) Let us consider a sequence A_1 of subsets of $\{1, 2, 3, 4\}$. Suppose for every natural number n and for every natural number k, $A_1(n) \cap A_1(k) \neq \emptyset$ and $\operatorname{rng} A_1 \subseteq \{\emptyset, \{1, 2\}, \{3, 4\}, \{1, 2, 3, 4\}\}$. Then

(i) $\text{Intersection}\, A_1 = \emptyset$, or

(ii) $\text{Intersection}\, A_1 = \{1, 2\}$, or

(iii) $\text{Intersection}\, A_1 = \{3, 4\}$, or

(iv) $\text{Intersection}\, A_1 = \{1, 2, 3, 4\}$.

PROOF: For every natural number n, $A_1(n) \in \{\emptyset, \{1, 2\}, \{3, 4\}, \{1, 2, 3, 4\}\}$ by [1, (20)], [4, (3)]. For every natural number n, $A_1(n) = \emptyset$ or $A_1(n) = \{1, 2\}$ or $A_1(n) = \{3, 4\}$ or $A_1(n) = \{1, 2, 3, 4\}$. $\square$

Let us consider a sequence A_1 of subsets of $\{1, 2, 3, 4\}$ and a set M. Now we state the propositions:

(15) Suppose $M = \{\emptyset, \{1, 2\}, \{3, 4\}, \{1, 2, 3, 4\}\}$ and $\text{Intersection}\, A_1 = \{1, 2, 3, 4\}$. Then $\text{Intersection}\, A_1 \in M$.

(16) Suppose $M = \{\emptyset, \{1, 2\}, \{3, 4\}, \{1, 2, 3, 4\}\}$ and $\text{Intersection}\, A_1 = \{3, 4\}$. Then $\text{Intersection}\, A_1 \in M$.

(17) Suppose $M = \{\emptyset, \{1, 2\}, \{3, 4\}, \{1, 2, 3, 4\}\}$ and $\text{Intersection}\, A_1 = \{1, 2\}$. Then $\text{Intersection}\, A_1 \in M$.

(18) Suppose $M = \{\emptyset, \{1,2\}, \{3,4\}, \{1,2,3,4\}\}$ and $\mathrm{Intersection}\, A_1 = \emptyset$. Then $\mathrm{Intersection}\, A_1 \in M$.

Now we state the propositions:

(19) Let us consider a set M, and a sequence A_1 of subsets of $\{1,2,3,4\}$. Suppose $\mathrm{rng}\, A_1 \subseteq M$ and $M = \{\emptyset, \{1,2\}, \{3,4\}, \{1,2,3,4\}\}$.
Then $\mathrm{Intersection}\, A_1 \in M$.
PROOF: $\mathrm{Intersection}\, A_1 \in \{\emptyset, \{1,2\}, \{3,4\}, \{1,2,3,4\}\}$ by [11, (13)], (14). $\square$

(20) Let us consider sets M, M_1, and a sequence A_1 of subsets of M_1. Suppose $M_1 = \{1,2,3,4\}$ and $\mathrm{rng}\, A_1 \subseteq M$ and $M = \{\emptyset, \{1,2,3,4\}\}$. If $\mathrm{Intersection}\, A_1 \neq \emptyset$, then $\mathrm{Intersection}\, A_1 \in M$.
PROOF: For every natural number n, $A_1(n) = \emptyset$ or $A_1(n) = \{1,2,3,4\}$ by [1, (20)], [4, (3)]. If there exists a natural number n such that $A_1(n) = \emptyset$, then $\mathrm{Intersection}\, A_1 = \emptyset$ by [11, (13)]. $\mathrm{Intersection}\, A_1 = \{1,2,3,4\}$ by [11, (13)]. $\square$

(21) Let us consider sets M, M_1, and a sequence A_1 of subsets of M_1. Suppose $M_1 = \{1,2,3,4\}$ and $\mathrm{rng}\, A_1 \subseteq M$ and $M = \{\emptyset, \{1,2,3,4\}\}$. Let us consider a natural number k_1, and a natural number k_2. Then $A_1(k_1) \cap A_1(k_2) \in M$.
PROOF: $k_1 \in \mathrm{dom}\, A_1$ by [1, (20)]. $k_2 \in \mathrm{dom}\, A_1$ by [1, (20)]. $A_1(k_1) \cap A_1(k_2) \in M$. $\square$

The functor Ω_{now} yielding a σ-field of subsets of $\{1,2,3,4\}$ is defined by the term

(Def. 6) $\{\emptyset, \{1,2,3,4\}\}$.

The functor Ω_{fut1} yielding a σ-field of subsets of $\{1,2,3,4\}$ is defined by the term

(Def. 7) $\{\emptyset, \{1,2\}, \{3,4\}, \{1,2,3,4\}\}$.

The functor Ω_{fut2} yielding a σ-field of subsets of $\{1,2,3,4\}$ is defined by the term

(Def. 8) $2^{\{1,2,3,4\}}$.

Let us consider a set Ω.

Let us assume that $\Omega = \{1,2,3,4\}$. Now we state the propositions:

(22) (i) $\{1\} \subseteq \Omega$, and
(ii) $\{2\} \subseteq \Omega$, and
(iii) $\{3\} \subseteq \Omega$, and
(iv) $\{4\} \subseteq \Omega$, and
(v) $\{1,2\} \subseteq \Omega$, and
(vi) $\{3,4\} \subseteq \Omega$, and

(vii) $\emptyset \subseteq \Omega \subseteq \Omega$.

(23) (i) Ω, $\emptyset \in \Omega_{now}$, and

(ii) $\{1,2\}$, $\{3,4\}$, Ω, $\emptyset \in \Omega_{fut1}$, and

(iii) Ω, $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\} \in \Omega_{fut2}$.

Now we state the proposition:

(24) $\Omega_{now} \subset \Omega_{fut1} \subset \Omega_{fut2}$.

4. Construction of Filtration and Examples

Now we state the propositions:

(25) There exists a non empty set Ω and there exist σ-fields F_1, F_2, F_3 of subsets of Ω such that $F_1 \subset F_2 \subset F_3$.

(26) There exist non empty sets Ω_1, Ω_2, Ω_3, Ω_4 such that

(i) $\Omega_1 \subset \Omega_2 \subset \Omega_3 \subset \Omega_4$, and

(ii) there exists a σ-field F_1 of subsets of Ω_1 and there exists a σ-field F_2 of subsets of Ω_2 and there exists a σ-field F_3 of subsets of Ω_3 and there exists a σ-field F_4 of subsets of Ω_4 such that $F_1 \subseteq F_2 \subseteq F_3 \subseteq F_4$.

Let I, Ω be non empty sets, Σ be a σ-field of subsets of Ω, M be a many sorted σ-field over I and Σ, and i be an element of I. The functor $\mathcal{M}_{\sigma\text{-field}}(M, i)$ yielding a σ-field of subsets of Ω is defined by the term

(Def. 9) $M(i)$.

Let Ω be a non empty set and I be a non empty subset of $\mathbb{R}$.

A filtration of I and Σ is a many sorted σ-field over I and Σ and is defined by

(Def. 10) for every elements s, t of I such that $s \leqslant t$ holds $it(s)$ is a subset of $it(t)$ and for every element t of I, $it(t) \subseteq \Sigma$.

Let F be a filtration of I and Σ and i be an element of I. The i-$\mathcal{EF}$ of F yielding a σ-field of subsets of Ω is defined by the term

(Def. 11) $F(i)$.

Let k be an element of $\{1, 2, 3\}$. The functor Select12-σ-field(k) yielding a subset of $2^{\{1,2,3,4\}}$ is defined by the term

(Def. 12) $\begin{cases} \Omega_{now}, & \textbf{if } k = 1, \\ \Omega_{fut1}, & \textbf{otherwise}. \end{cases}$

The functor Select123-σ-field(k) yielding a subset of $2^{\{1,2,3,4\}}$ is defined by the term

(Def. 13) $\begin{cases} \text{Select12-}\sigma\text{-field}(k), & \textbf{if } k \leqslant 2, \\ \Omega_{fut2}, & \textbf{otherwise}. \end{cases}$

Now we state the propositions:

(27) Let us consider a σ-field Σ of subsets of $\{1, 2, 3, 4\}$, and a set I. Suppose $I = \{1, 2, 3\}$ and $\Sigma = 2^{\{1,2,3,4\}}$. Then there exists a many sorted σ-field M over I and Σ such that

(i) $M(1) = \Omega_{now}$, and

(ii) $M(2) = \Omega_{fut1}$, and

(iii) $M(3) = \Omega_{fut2}$.

Proof: Define $\mathcal{U}$(element of $\{1, 2, 3\}$) = Select123-σ-field($\$_1$). Consider f_4 being a function from $\{1, 2, 3\}$ into $2^{2^{\{1,2,3,4\}}}$ such that for every element d of $\{1, 2, 3\}$, $f_4(d) = \mathcal{U}(d)$ from [5, Sch. 4]. For every set i such that $i \in I$ holds $f_4(i)$ is a σ-field of subsets of $\{1, 2, 3, 4\}$. $\square$

(28) Let us consider a non empty set Ω, a σ-field Σ of subsets of Ω, and a non empty subset I of $\mathbb{R}$. Suppose $I = \{1, 2, 3\}$ and $\Sigma = 2^{\{1,2,3,4\}}$ and $\Omega = \{1, 2, 3, 4\}$. Then there exists a many sorted σ-field M over I and Σ such that

(i) $M(1) = \Omega_{now}$, and

(ii) $M(2) = \Omega_{fut1}$, and

(iii) $M(3) = \Omega_{fut2}$, and

(iv) M is a filtration of I and Σ.

The theorem is a consequence of (27).

(29) Let us consider a non empty set Ω, a σ-field Σ of subsets of Ω, and a σ-field Σ_2 of subsets of $\{1\}$. Suppose $\Omega = \{1, 2, 3, 4\}$. Then there exists a function X_1 from Ω into $\{1\}$ such that X_1 is random variable of Ω_{now} and Σ_2, random variable of Ω_{fut1} and Σ_2, and random variable of Ω_{fut2} and Σ_2.

(30) Let us consider a non empty set Ω, a σ-field Σ of subsets of Ω, and a non empty subset I of $\mathbb{R}$. Suppose $I = \{1, 2, 3\}$ and $\Sigma = 2^{\{1,2,3,4\}}$ and $\Omega = \{1, 2, 3, 4\}$. Then there exists a many sorted σ-field M over I and Σ such that

(i) $M(1) = \Omega_{now}$, and

(ii) $M(2) = \Omega_{fut1}$, and

(iii) $M(3) = \Omega_{fut2}$, and

(iv) M is a filtration of I and Σ.

The theorem is a consequence of (27).

(31) There exist non empty sets Ω, Ω_2 and there exists a σ-field Σ of subsets of Ω and there exists a σ-field Σ_2 of subsets of Ω_2 and there exists a non empty subset I of $\mathbb{R}$ and there exists a many sorted σ-field Q over I and Σ such that Q is a filtration of I and Σ and there exists a function $\mathcal{RV}$ from Ω into Ω_2 such that for every element i of I, $\mathcal{RV}$ is a random variable of $\mathcal{M}_{\sigma\text{-field}}(Q, i)$ and Σ_2. The theorem is a consequence of (30) and (29).

(32) Let us consider non empty sets Ω, Ω_2, a σ-field Σ of subsets of Ω, a σ-field Σ_2 of subsets of Ω_2, a non empty subset I of $\mathbb{R}$, and a filtration Q of I and Σ. Then there exists a function $\mathcal{RV}$ from Ω into Ω_2 such that for every element i of I, $\mathcal{RV}$ is a random variable of $\mathcal{M}_{\sigma\text{-field}}(Q, i)$ and Σ_2.
PROOF: Consider w being an object such that $w \in \Omega_2$. Set $m_1 = w$. Consider m being a function from Ω into Ω_2 such that $m = \Omega \longmapsto m_1$. For every element i of I, m is a random variable of $\mathcal{M}_{\sigma\text{-field}}(Q, i)$ and Σ_2 by [13, (7)], [11, (5), (4)]. $\square$

5. STOCHASTIC PROCESS: ADAPTED AND PREDICTABLE

Now we state the proposition:

(33) Let us consider a non empty set Ω, a σ-field Σ of subsets of Ω, and a σ-field Σ_2 of subsets of Ω. If $\Sigma_2 \subseteq \Sigma$, then every event of Σ_2 is an event of Σ.

Let Ω, Ω_2 be non empty sets, Σ be a σ-field of subsets of Ω, Σ_2 be a σ-field of subsets of Ω_2, I be a non empty subset of $\mathbb{R}$, and P be a probability on Σ.

A stochastic process of I, Σ, Σ_2 and P is a function from I into the set of random variables on Σ and Σ_2 and is defined by

(Def. 14) for every element k of I, there exists a function $\mathcal{RV}$ from Ω into Ω_2 such that $it(k) = \mathcal{RV}$ and $\mathcal{RV}$ is random variable on Σ and Σ_2.

Let S be a stochastic process of I, Σ, Σ_2 and P and k be an element of I. The k-$\mathcal{RV}$ of S yielding a random variable of Σ and Σ_2 is defined by the term

(Def. 15) $S(k)$.

An adapted stochastic process of I, Σ, Σ_2, P and S is a function from I into the set of random variables on Σ and Σ_2 and is defined by

(Def. 16) there exists a filtration k of I and Σ such that for every element i of I, the i-$\mathcal{RV}$ of S is random variable on the i-$\mathcal{EF}$ of k and Σ_2.

Let I be a non empty subset of $\mathbb{N}$, J be a non empty subset of $\mathbb{N}$, and S be a stochastic process of $J(\in 2^{\mathbb{R}})$, Σ, Σ_2 and P.

A predictable stochastic process of I, J, Σ, Σ_2, P and S is a function from J into the set of random variables on Σ and Σ_2 and is defined by

(Def. 17) there exists a filtration k of $I(\in 2^{\mathbb{R}})$ and Σ such that for every element j of $J(\in 2^{\mathbb{R}})$ for every element i of $I(\in 2^{\mathbb{R}})$ such that $j-1=i$ holds the j-$\mathcal{RV}$ of S is random variable on the i-$\mathcal{EF}$ of k and Σ_2.

Let I be a non empty subset of $\mathbb{R}$, M be a filtration of I and Σ, and S be a stochastic process of I, Σ, Σ_2 and P. We say that S is M-stochastic process w.r.t. filtration if and only if

(Def. 18) for every element i of I, the i-$\mathcal{RV}$ of S is random variable on the i-$\mathcal{EF}$ of M and Σ_2.

Now we state the proposition:

(34) Let us consider non empty sets Ω, Ω_2, a σ-field Σ of subsets of Ω, a σ-field Σ_2 of subsets of Ω_2, a non empty subset I of $\mathbb{R}$, a probability P on Σ, a filtration M of I and Σ, and a stochastic process S of I, Σ, Σ_2 and P. Suppose S is M-stochastic process w.r.t. filtration. Then S is an adapted stochastic process of I, Σ, Σ_2, P and S.

6. Example for a Stochastic Process

Let k_1, k_2 be elements of $\mathbb{R}$, Ω be a non empty set, and k be an element of Ω. The functors: Set1-$\mathcal{RV}(k_1,k_2,k)$ and Set4-$\mathcal{RV}(k_1,k_2,k)$ yielding elements of $\mathbb{R}$ are defined by terms

(Def. 19) $\begin{cases} k_1, & \textbf{if } k=1 \text{ or } k=2, \\ k_2, & \textbf{otherwise}, \end{cases}$

(Def. 20) $\begin{cases} k_1, & \textbf{if } k=3, \\ k_2, & \textbf{otherwise}, \end{cases}$

respectively. Let k_2, k_3, k_4 be elements of $\mathbb{R}$. The functor Set3-$\mathcal{RV}(k_2,k_3,k_4,k)$ yielding an element of $\mathbb{R}$ is defined by the term

(Def. 21) $\begin{cases} k_2, & \textbf{if } k=2, \\ \text{Set4-}\mathcal{RV}(k_3,k_4,k), & \textbf{otherwise}. \end{cases}$

Let k_1, k_2, k_3, k_4 be elements of $\mathbb{R}$. The functor Set2-$\mathcal{RV}(k_1,k_2,k_3,k_4,k)$ yielding an element of $\mathbb{R}$ is defined by the term

(Def. 22) $\begin{cases} k_1, & \textbf{if } k=1, \\ \text{Set3-}\mathcal{RV}(k_2,k_3,k_4,k), & \textbf{otherwise}. \end{cases}$

Now we state the proposition:

(35) Let us consider elements k_1, k_2, k_3, k_4 of $\mathbb{R}$, and a set Ω. Suppose $\Omega = \{1,2,3,4\}$. Then there exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1)=k_1$, and

(ii) $f(2)=k_2$, and

(iii) $f(3) = k_3$, and

(iv) $f(4) = k_4$.

PROOF: Define $\mathcal{U}$(element of Ω) $=$ Set2-$\mathcal{RV}(k_1, k_2, k_3, k_4, \$_1)$. Consider f being a function from Ω into $\mathbb{R}$ such that for every element d of Ω, $f(d) = \mathcal{U}(d)$ from [5, Sch. 4]. $f(1) = k_1$. $f(2) = k_2$. $f(3) = k_3$. $f(4) = k_4$. $\square$

Let us consider a set Ω.

Let us assume that $\Omega = \{1, 2, 3, 4\}$. Now we state the propositions:

(36) There exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = 100$, and

(ii) $f(2) = 100$, and

(iii) $f(3) = 100$, and

(iv) $f(4) = 100$.

The theorem is a consequence of (35).

(37) There exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = 80$, and

(ii) $f(2) = 80$, and

(iii) $f(3) = 120$, and

(iv) $f(4) = 120$.

The theorem is a consequence of (35).

(38) There exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = 60$, and

(ii) $f(2) = 80$, and

(iii) $f(3) = 100$, and

(iv) $f(4) = 120$.

The theorem is a consequence of (35).

(39) Let us consider elements k_1, k_2, k_3, k_4 of $\mathbb{R}$, and a non empty set Ω. Suppose $\Omega = \{1, 2, 3, 4\}$. Let us consider a σ-field Σ of subsets of Ω, a non empty subset I of $\mathbb{R}$, and a filtration M of I and Σ. Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Let us consider an element k of I. Suppose $k = 3$. Then there exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = k_1$, and

(ii) $f(2) = k_2$, and

(iii) $f(3) = k_3$, and

(iv) $f(4) = k_4$, and

(v) f is random variable on the k-$\mathcal{EF}$ of M and the Borel sets.

PROOF: Consider f being a function from Ω into $\mathbb{R}$ such that $f(1) = k_1$ and $f(2) = k_2$ and $f(3) = k_3$ and $f(4) = k_4$. 1, 2, 3, 4 $\in \operatorname{dom} f$. f is random variable on the k-$\mathcal{EF}$ of M and the Borel sets by [4, (1)], [11, (4)]. □

Let us consider a non empty set Ω, a σ-field Σ of subsets of Ω, a non empty subset I of $\mathbb{R}$, a filtration M of I and Σ, and an element k of I.

Let us assume that $\Omega = \{1, 2, 3, 4\}$. Now we state the propositions:

(40) Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Then suppose $k = 3$. Then there exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = 60$, and

(ii) $f(2) = 80$, and

(iii) $f(3) = 100$, and

(iv) $f(4) = 120$, and

(v) f is random variable on the k-$\mathcal{EF}$ of M and the Borel sets.

The theorem is a consequence of (39).

(41) Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Then suppose $k = 3$. Then there exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = 180$, and

(ii) $f(2) = 120$, and

(iii) $f(3) = 120$, and

(iv) $f(4) = 80$, and

(v) f is random variable on the k-$\mathcal{EF}$ of M and the Borel sets.

The theorem is a consequence of (39).

(42) Let us consider elements k_1, k_2 of $\mathbb{R}$, and a non empty set Ω. Suppose $\Omega = \{1, 2, 3, 4\}$. Let us consider a σ-field Σ of subsets of Ω, a non empty subset I of $\mathbb{R}$, and a filtration M of I and Σ. Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Let us consider an element k of I. Suppose $k = 2$. Then there exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = k_1$, and

(ii) $f(2) = k_1$, and

(iii) $f(3) = k_2$, and

(iv) $f(4) = k_2$, and

(v) f is random variable on the k-$\mathcal{EF}$ of M and the Borel sets.

PROOF: Consider f being a function from Ω into $\mathbb{R}$ such that $f(1) = k_1$ and $f(2) = k_1$ and $f(3) = k_2$ and $f(4) = k_2$. Set $i = k$. For every set x, $f^{-1}(x) \in$ the i-$\mathcal{EF}$ of M by [4, (1)]. □

Let us consider a non empty set Ω, a σ-field Σ of subsets of Ω, a non empty subset I of $\mathbb{R}$, a filtration M of I and Σ, and an element k of I.

Let us assume that $\Omega = \{1, 2, 3, 4\}$. Now we state the propositions:

(43) Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Then suppose $k = 2$. Then there exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = 80$, and

(ii) $f(2) = 80$, and

(iii) $f(3) = 120$, and

(iv) $f(4) = 120$, and

(v) f is random variable on the k-$\mathcal{EF}$ of M and the Borel sets.

The theorem is a consequence of (42).

(44) Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Then suppose $k = 2$. Then there exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = 150$, and

(ii) $f(2) = 150$, and

(iii) $f(3) = 100$, and

(iv) $f(4) = 100$, and

(v) f is random variable on the k-$\mathcal{EF}$ of M and the Borel sets.

The theorem is a consequence of (42).

(45) Let us consider an element k_1 of $\mathbb{R}$, and a non empty set Ω. Suppose $\Omega = \{1, 2, 3, 4\}$. Let us consider a σ-field Σ of subsets of Ω, a non empty subset I of $\mathbb{R}$, and a filtration M of I and Σ. Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Let us consider an element k of I. Suppose $k = 1$. Then there exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = k_1$, and

(ii) $f(2) = k_1$, and

(iii) $f(3) = k_1$, and

(iv) $f(4) = k_1$, and

(v) f is random variable on the k-$\mathcal{EF}$ of M and the Borel sets.

PROOF: Consider f being a function from Ω into $\mathbb{R}$ such that $f(1) = k_1$ and $f(2) = k_1$ and $f(3) = k_1$ and $f(4) = k_1$. Set $i = k$. For every set x such that $x \in$ the Borel sets holds $f^{-1}(x) \in$ the i-$\mathcal{EF}$ of M by [4, (1)]. □

Let us consider a non empty set Ω, a σ-field Σ of subsets of Ω, a non empty subset I of $\mathbb{R}$, a filtration M of I and Σ, and an element k of I.

Let us assume that $\Omega = \{1, 2, 3, 4\}$. Now we state the propositions:

(46) Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Then suppose $k = 1$. Then there exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = 100$, and

(ii) $f(2) = 100$, and

(iii) $f(3) = 100$, and

(iv) $f(4) = 100$, and

(v) f is random variable on the k-$\mathcal{EF}$ of M and the Borel sets.

The theorem is a consequence of (45).

(47) Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Then suppose $k = 1$. Then there exists a function f from Ω into $\mathbb{R}$ such that

(i) $f(1) = 125$, and

(ii) $f(2) = 125$, and

(iii) $f(3) = 125$, and

(iv) $f(4) = 125$, and

(v) f is random variable on the k-$\mathcal{EF}$ of M and the Borel sets.

The theorem is a consequence of (45).

Now we state the proposition:

(48) Let us consider a non empty set Ω. Suppose $\Omega = \{1, 2, 3, 4\}$. Let us consider a σ-field Σ of subsets of Ω, and a non empty subset I of $\mathbb{R}$. Suppose $I = \{1, 2, 3\}$ and $\Sigma = 2^{\{1,2,3,4\}}$. Let us consider a filtration M of I and Σ. Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Let us consider a probability P on Σ, and an element i of I. Then there exists a function $\mathcal{RV}$ from Ω into $\mathbb{R}$ such that $\mathcal{RV}$ is random variable on the i-$\mathcal{EF}$ of M and the Borel sets. The theorem is a consequence of (46), (43), and (40).

Let I be a non empty subset of $\mathbb{R}$. Assume $I = \{1, 2, 3\}$. Let i be an element of I. Assume $i = 2$ or $i = 3$. Let Ω be a non empty set. Assume $\Omega = \{1, 2, 3, 4\}$. Let Σ be a σ-field of subsets of Ω. Assume $\Sigma = 2^{\Omega}$. Let f_1 be a function from Ω into $\mathbb{R}$. Assume $f_1(1) = 60$ and $f_1(2) = 80$ and $f_1(3) = 100$ and $f_1(4) = 120$. Let f_2 be a function from Ω into $\mathbb{R}$. Assume $f_2(1) = 80$ and $f_2(2) = 80$ and $f_2(3) = 120$ and $f_2(4) = 120$. Let f_3 be a function from Ω into $\mathbb{R}$. The functor Select12-$\mathcal{RV}(i, \Sigma, f_1, f_2, f_3)$ yielding an element of the set of random variables on Σ and the Borel sets is defined by the term

(Def. 23) $\begin{cases} f_2, & \textbf{if } i = 2, \\ f_1, & \textbf{otherwise}. \end{cases}$

Assume $I = \{1, 2, 3\}$. Assume $\Omega = \{1, 2, 3, 4\}$. Assume $\Sigma = 2^{\Omega}$. Let f_1, f_2 be functions from Ω into $\mathbb{R}$. Assume $f_3(1) = 100$ and $f_3(2) = 100$ and $f_3(3) = 100$ and $f_3(4) = 100$. The functor Select123-$\mathcal{RV}(i, \Sigma, f_1, f_2, f_3)$ yielding an element of the set of random variables on Σ and the Borel sets is defined by the term

(Def. 24) $\begin{cases} \text{Select12-}\mathcal{RV}(i, \Sigma, f_1, f_2, f_3), & \textbf{if } i = 2 \text{ or } i = 3, \\ f_3, & \textbf{otherwise}. \end{cases}$

Now we state the proposition:

(49) Let us consider non empty sets Ω, Ω_2. Suppose $\Omega = \{1, 2, 3, 4\}$. Let us consider a σ-field Σ of subsets of Ω, and a non empty subset I of $\mathbb{R}$. Suppose $I = \{1, 2, 3\}$ and $\Sigma = 2^{\{1,2,3,4\}}$. Let us consider a probability P on Σ, and a filtration M of I and Σ. Suppose $M(1) = \Omega_{now}$ and $M(2) = \Omega_{fut1}$ and $M(3) = \Omega_{fut2}$. Then there exists a stochastic process S of I, Σ, the Borel sets and P such that

(i) for every element k of I, there exists a function $\mathcal{RV}$ from Ω into $\mathbb{R}$ such that $S(k) = \mathcal{RV}$ and $\mathcal{RV}$ is random variable on Σ and the Borel sets and random variable on the k-$\mathcal{EF}$ of M and the Borel sets and there exists a function f from Ω into $\mathbb{R}$ such that if $k = 1$, then $f(1) = 100$ and $f(2) = 100$ and $f(3) = 100$ and $f(4) = 100$ and $S(k) = f$ and there exists a function f from Ω into $\mathbb{R}$ such that if $k = 2$, then $f(1) = 80$ and $f(2) = 80$ and $f(3) = 120$ and $f(4) = 120$ and $S(k) = f$ and there exists a function f from Ω into $\mathbb{R}$ such that if $k = 3$, then $f(1) = 60$ and $f(2) = 80$ and $f(3) = 100$ and $f(4) = 120$ and $S(k) = f$ and S is M-stochastic process w.r.t. filtration, and

(ii) S is an adapted stochastic process of I, Σ, the Borel sets, P and S.

PROOF: Consider f_3 being a function from Ω into $\mathbb{R}$ such that $f_3(1) = 100$ and $f_3(2) = 100$ and $f_3(3) = 100$ and $f_3(4) = 100$. Consider f_2 being a function from Ω into $\mathbb{R}$ such that $f_2(1) = 80$ and $f_2(2) = 80$ and $f_2(3) = 120$ and $f_2(4) = 120$. Consider f_1 being a function from Ω into $\mathbb{R}$ such that $f_1(1) = 60$ and $f_1(2) = 80$ and $f_1(3) = 100$ and $f_1(4) = 120$. Define $\mathcal{U}(\text{element of } I) = \text{Select123-}\mathcal{RV}(\$_1, \Sigma, f_1, f_2, f_3)$. Consider f_4 being a function from I into the set of random variables on Σ and the Borel sets such that for every element d of I, $f_4(d) = \mathcal{U}(d)$ from [5, Sch. 4]. For every element k of I, there exists a function $\mathcal{RV}$ from Ω into $\mathbb{R}$ such that $f_4(k) = \mathcal{RV}$ and $\mathcal{RV}$ is random variable on Σ and the Borel sets. For every element k of I, there exists a function $\mathcal{RV}$ from Ω into $\mathbb{R}$ such that $f_4(k) = \mathcal{RV}$ and $\mathcal{RV}$ is random variable on Σ and the Borel sets and random variable on the k-$\mathcal{EF}$ of M and the Borel sets and there exists a function f from Ω into $\mathbb{R}$ such that if $k = 1$, then $f(1) = 100$ and $f(2) = 100$ and $f(3) = 100$ and $f(4) = 100$ and $f_4(k) = f$ and there exists a function f from Ω into $\mathbb{R}$ such that if $k = 2$, then $f(1) = 80$ and $f(2) = 80$ and $f(3) = 120$ and $f(4) = 120$ and $f_4(k) = f$ and there exists a function f from Ω into $\mathbb{R}$ such that if $k = 3$, then $f(1) = 60$ and $f(2) = 80$ and $f(3) = 100$ and $f(4) = 120$ and $f_4(k) = f$ and f_4 is M-stochastic process w.r.t. filtration and adapted stochastic process of I, Σ, the Borel sets, P and f_4. $\square$

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] Francesca Biagini and Daniel Rost. Money out of nothing? - Prinzipien und Grundlagen der Finanzmathematik. *MATHE-LMU.DE*, LMU-München(25):28–34, 2012.

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

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

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

[7] Hans-Otto Georgii. *Stochastik, Einführung in die Wahrscheinlichkeitstheorie und Statistik*. deGruyter, Berlin, 2nd edition, 2004.

[8] Peter Jaeger. Events of Borel sets, construction of Borel sets and random variables for stochastic finance. *Formalized Mathematics*, 22(**3**):199–204, 2014. doi:10.2478/forma-2014-0022.

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

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

[11] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.

[12] Klaus Sandmann. *Einführung in die Stochastik der Finanzmärkte*. Springer-Verlag, Berlin, Heidelberg, New York, 2 edition, 2001.

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

Received December 30, 2015

FORMALIZED MATHEMATICS
Vol. 24, No. 1, Pages 17–26, 2016
DOI: 10.1515/forma-2016-0002

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

Circumcenter, Circumcircle and Centroid of a Triangle

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

Summary. We introduce, using the Mizar system [1], some basic concepts of Euclidean geometry: the half length and the midpoint of a segment, the perpendicular bisector of a segment, the medians (the cevians that join the vertices of a triangle to the midpoints of the opposite sides) of a triangle.

We prove the existence and uniqueness of the circumcenter of a triangle (the intersection of the three perpendicular bisectors of the sides of the triangle). The extended law of sines and the formula of the radius of the Morley's trisector triangle are formalized [3].

Using the generalized Ceva's Theorem, we prove the existence and uniqueness of the centroid (the common point of the medians [4]) of a triangle.

MSC: 51M04 03B35

Keywords: Euclidean geometry; perpendicular bisector; circumcenter; circumcircle; centroid; extended law of sines

MML identifier: `EUCLID12`, version: `8.1.04 5.36.1267`

1. Preliminaries

From now on n denotes a natural number, λ, λ_2, μ, μ_2 denote real numbers, x_1, x_2 denote elements of $\mathcal{R}^n$, A_1, B_1, C_1 denote points of $\mathcal{E}^n_{\mathrm{T}}$, and a denotes a real number.

Now we state the propositions:

(1) If $A_1 = (1-\lambda)\cdot x_1 + \lambda \cdot x_2$ and $B_1 = (1-\mu)\cdot x_1 + \mu\cdot x_2$, then $B_1 - A_1 = (\mu - \lambda)\cdot(x_2 - x_1)$.

(2) If $|a| = |1-a|$, then $a = \frac{1}{2}$.

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

In the sequel P, A, B denote elements of $\mathcal{R}^n$ and L denotes an element of $\mathrm{Lines}(\mathcal{R}^n)$.

Now we state the propositions:

(3) $\mathrm{Line}(P, P) = \{P\}$.

(4) If $A_1 = A$ and $B_1 = B$, then $\mathrm{Line}(A_1, B_1) = \mathrm{Line}(A, B)$.

(5) If $A_1 \neq C_1$ and $C_1 \in \mathcal{L}(A_1, B_1)$ and A_1, $C_1 \in L$ and L is a line, then $B_1 \in L$. The theorem is a consequence of (4).

Let n be a natural number and S be a subset of $\mathcal{R}^n$. We say that S is a point if and only if

(Def. 1) there exists an element P of $\mathcal{R}^n$ such that $S = \{P\}$.

Now we state the propositions:

(6) (i) L is a line, or

(ii) there exists an element P of $\mathcal{R}^n$ such that $L = \{P\}$.

The theorem is a consequence of (3).

(7) L is a line or a point.

Let us assume that L is a line. Now we state the propositions:

(8) There exists no element P of $\mathcal{R}^n$ such that $L = \{P\}$.

(9) L is not a point.

2. Betweenness

In the sequel A, B, C denote points of $\mathcal{E}^2_{\mathrm{T}}$.

Now we state the propositions:

(10) If $C \in \mathcal{L}(A, B)$, then $|A - B| = |A - C| + |C - B|$.

(11) If $|A - B| = |A - C| + |C - B|$, then $C \in \mathcal{L}(A, B)$. The theorem is a consequence of (10).

(12) Let us consider points p, q_1, q_2 of $\mathcal{E}^2_{\mathrm{T}}$. Then $p \in \mathcal{L}(q_1, q_2)$ if and only if $\rho(q_1, p) + \rho(p, q_2) = \rho(q_1, q_2)$. The theorem is a consequence of (11).

Let us consider elements p, q, r of $\mathcal{E}^2$.

Let us assume that p, q, r are mutually different and $p = A$ and $q = B$ and $r = C$. Now we state the propositions:

(13) $A \in \mathcal{L}(B, C)$ if and only if p is between q and r. The theorem is a consequence of (12) and (11).

(14) $A \in \mathcal{L}(B, C)$ if and only if p is between q and r. The theorem is a consequence of (13).

3. Real Plane

From now on x, y, z, y_1, y_2 denote elements of $\mathcal{R}^2$, L, L_1, L_2 denote elements of Lines($\mathcal{R}^2$), D, E, F denote points of $\mathcal{E}^2_{\mathrm{T}}$, and b, c, d, r, s denote real numbers.

Now we state the propositions:

(15) Let us consider elements O, O_1, O_2 of $\mathcal{R}^2$. Suppose $O = [0,0]$ and $O_1 = [1,0]$ and $O_2 = [0,1]$. Then $\mathcal{R}^2 = \mathrm{Plane}(O, O_1, O_2)$.

(16) $\mathcal{R}^2$ is an element of Planes($\mathcal{R}^2$). The theorem is a consequence of (15).

(17) (i) $[1,0] \neq [0,1]$, and

(ii) $[1,0] \neq [0,0]$, and

(iii) $[0,1] \neq [0,0]$.

(18) There exists x such that $x \notin L$. The theorem is a consequence of (6) and (17).

(19) There exists L such that

(i) L is a point, and

(ii) L misses L_1.

The theorem is a consequence of (18) and (3).

Let us assume that $L_1 \nparallel L_2$. Now we state the propositions:

(20) (i) there exists x such that $L_1 = \{x\}$ or $L_2 = \{x\}$, or

(ii) L_1 is a line and L_2 is a line and there exists x such that $L_1 \cap L_2 = \{x\}$.

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

(21) (i) L_1 is a point, or

(ii) L_2 is a point, or

(iii) L_1 is a line and L_2 is a line and $L_1 \cap L_2$ is a point.

Now we state the proposition:

(22) If $L_1 \cap L_2$ is a point and $A \in L_1 \cap L_2$, then $L_1 \cap L_2 = \{A\}$.

4. The Midpoint of a Segment

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

(Def. 2) $(\frac{1}{2}) \cdot |A - B|$.

Now we state the propositions:

(23) half-length$(A, B) =$ half-length(B, A).

(24) half-length$(A, A) = 0$.

(25) $|A - (\frac{1}{2}) \cdot (A + B)| = (\frac{1}{2}) \cdot |A - B|$.

(26) There exists C such that

(i) $C \in \mathcal{L}(A, B)$, and

(ii) $|A - C| = (\frac{1}{2}) \cdot |A - B|$.

The theorem is a consequence of (25).

(27) If $|A - B| = |A - C|$ and B, $C \in \mathcal{L}(A, D)$, then $B = C$. The theorem is a consequence of (1).

Let A, B be points of $\mathcal{E}^2_{\rm T}$. The functor SegMidpoint(A, B) yielding a point of $\mathcal{E}^2_{\rm T}$ is defined by

(Def. 3) there exists C such that $C \in \mathcal{L}(A, B)$ and $it = C$ and $|A - C| =$ half-length(A, B).

Now we state the propositions:

(28) SegMidpoint$(A, B) \in \mathcal{L}(A, B)$.

(29) SegMidpoint$(A, B) = (\frac{1}{2}) \cdot (A + B)$. The theorem is a consequence of (25).

(30) SegMidpoint$(A, B) =$ SegMidpoint(B, A). The theorem is a consequence of (29).

(31) SegMidpoint$(A, A) = A$. The theorem is a consequence of (29).

(32) If SegMidpoint$(A, B) = A$, then $A = B$. The theorem is a consequence of (29).

(33) If SegMidpoint$(A, B) = B$, then $A = B$. The theorem is a consequence of (30) and (32).

Let us assume that $C \in \mathcal{L}(A, B)$ and $|A - C| = |B - C|$. Now we state the propositions:

(34) half-length$(A, B) = |A - C|$. The theorem is a consequence of (10).

(35) $C =$ SegMidpoint(A, B). The theorem is a consequence of (34).

Now we state the propositions:

(36) $|A -$ SegMidpoint$(A, B)| = |$SegMidpoint$(A, B) - B|$. The theorem is a consequence of (29) and (25).

(37) If $A \neq B$ and r is positive and $r \neq 1$ and $|A - C| = r \cdot |A - B|$, then A, B, C are mutually different.

(38) If $C \in \mathcal{L}(A, B)$ and $|A - C| = (\frac{1}{2}) \cdot |A - B|$, then $|B - C| = (\frac{1}{2}) \cdot |A - B|$. The theorem is a consequence of (10).

5. Perpendicularity

Now we state the propositions:

(39) L_1 and L_2 are coplanar. The theorem is a consequence of (15).

(40) If $L_1 \perp L_2$, then L_1 meets L_2.

(41) If L_1 is a line and L_2 is a line and L_1 misses L_2, then $L_1 \parallel L_2$.

(42) Suppose $L_1 \neq L_2$ and L_1 meets L_2. Then

- (i) there exists x such that $L_1 = \{x\}$ or $L_2 = \{x\}$, or
- (ii) L_1 is a line and L_2 is a line and there exists x such that $L_1 \cap L_2 = \{x\}$.

The theorem is a consequence of (20).

Let us assume that $L_1 \perp L_2$. Now we state the propositions:

(43) There exists x such that $L_1 \cap L_2 = \{x\}$. The theorem is a consequence of (39), (8), and (42).

(44) $L_1 \cap L_2$ is a point.

Now we state the propositions:

(45) If $L_1 \perp L_2$, then $L_1 \nparallel L_2$. The theorem is a consequence of (39).

(46) If L_1 is a line and L_2 is a line and $L_1 \parallel L_2$, then $L_1 \not\perp L_2$.

Now we state the propositions:

(47) If L_1 is a line, then there exists L_2 such that $x \in L_2$ and $L_1 \perp L_2$. The theorem is a consequence of (18).

(48) If $L_1 \perp L_2$ and $L_1 = \mathrm{Line}(A, B)$ and $L_2 = \mathrm{Line}(C, D)$, then $|(B-A, D-C)| = 0$. The theorem is a consequence of (1).

(49) If L is a line and A, $B \in L$ and $A \neq B$, then $L = \mathrm{Line}(A, B)$. The theorem is a consequence of (4).

Let us assume that $L_1 \perp L_2$ and $C \in L_1 \cap L_2$ and $A \in L_1$ and $B \in L_2$ and $A \neq C$ and $B \neq C$. Now we state the propositions:

(50)
- (i) $\measuredangle(A, C, B) = \frac{\pi}{2}$, or
- (ii) $\measuredangle(A, C, B) = \frac{3 \cdot \pi}{2}$.

The theorem is a consequence of (49) and (48).

(51) A, B, C form a triangle.

Proof: $A \notin \mathrm{Line}(B, C)$ by [5, (67)], (43), (49). $\square$

6. The Perpendicular Bisector of a Segment

Now we state the proposition:

(52) Suppose $A \neq B$ and $L_1 = \mathrm{Line}(A, B)$ and $C \in \mathcal{L}(A, B)$ and $|A - C| = (\frac{1}{2}) \cdot |A - B|$. Then there exists L_2 such that

(i) $C \in L_2$, and

(ii) $L_1 \perp L_2$.

The theorem is a consequence of (4) and (47).

Let A, B be elements of $\mathcal{E}^2_{\mathrm{T}}$. Assume $A \neq B$. The functor PerpBisec(A, B) yielding an element of Lines$(\mathcal{R}^2)$ is defined by

(Def. 4) there exist elements L_1, L_2 of Lines$(\mathcal{R}^2)$ such that $it = L_2$ and $L_1 = \mathrm{Line}(A, B)$ and $L_1 \perp L_2$ and $L_1 \cap L_2 = \{\mathrm{SegMidpoint}(A, B)\}$.

Let us assume that $A \neq B$. Now we state the propositions:

(53) PerpBisec(A, B) is a line.

(54) PerpBisec(A, B) = PerpBisec(B, A). The theorem is a consequence of (43), (16), and (30).

(55) Suppose $A \neq B$ and $L_1 = \mathrm{Line}(A, B)$ and $C \in \mathcal{L}(A, B)$ and $|A - C| = (\frac{1}{2}) \cdot |A - B|$ and $C \in L_2$ and $L_1 \perp L_2$ and $D \in L_2$. Then $|D - A| = |D - B|$. The theorem is a consequence of (38), (37), and (50).

(56) If $A \neq B$ and $C \in \mathrm{PerpBisec}(A, B)$, then $|C - A| = |C - B|$. The theorem is a consequence of (28) and (55).

(57) If $C \in \mathrm{Line}(A, B)$ and $|A - C| = |B - C|$, then $C \in \mathcal{L}(A, B)$. The theorem is a consequence of (4), (3), and (2).

(58) If $A \neq B$, then $\mathrm{SegMidpoint}(A, B) \in \mathrm{PerpBisec}(A, B)$.

(59) If $A \neq B$ and $L_1 = \mathrm{Line}(A, B)$ and $L_1 \perp L_2$ and $\mathrm{SegMidpoint}(A, B) \in L_2$, then $L_2 = \mathrm{PerpBisec}(A, B)$. The theorem is a consequence of (16).

(60) If $A \neq B$ and $|C - A| = |C - B|$, then $C \in \mathrm{PerpBisec}(A, B)$. The theorem is a consequence of (47), (43), (50), (57), (35), (58), and (59).

7. The Circumcircle of a Triangle

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

(61) $\mathrm{PerpBisec}(A, B) \cap \mathrm{PerpBisec}(B, C)$ is a point. The theorem is a consequence of (16), (8), and (20).

(62) There exists D such that

(i) $\mathrm{PerpBisec}(A, B) \cap \mathrm{PerpBisec}(B, C) = \{D\}$, and

(ii) $\mathrm{PerpBisec}(B,C) \cap \mathrm{PerpBisec}(C,A) = \{D\}$, and

(iii) $\mathrm{PerpBisec}(C,A) \cap \mathrm{PerpBisec}(A,B) = \{D\}$, and

(iv) $|D - A| = |D - B|$, and

(v) $|D - A| = |D - C|$, and

(vi) $|D - B| = |D - C|$.

The theorem is a consequence of (61), (56), and (60).

Let A, B, C be points of $\mathcal{E}^2_{\mathrm{T}}$. Assume A, B, C form a triangle. The functor Circumcenter $\triangle(A,B,C)$ yielding a point of $\mathcal{E}^2_{\mathrm{T}}$ is defined by

(Def. 5) $\mathrm{PerpBisec}(A,B) \cap \mathrm{PerpBisec}(B,C) = \{it\}$ and $\mathrm{PerpBisec}(B,C) \cap \mathrm{PerpBisec}(C,A) = \{it\}$ and $\mathrm{PerpBisec}(C,A) \cap \mathrm{PerpBisec}(A,B) = \{it\}$.

Assume A, B, C form a triangle. The functor RadCircumCirc $\triangle(A,B,C)$ yielding a real number is defined by the term

(Def. 6) $|\,\mathrm{Circumcenter}\,\triangle(A,B,C) - A|$.

(63) If A, B, C form a triangle, then there exists a and there exists b and there exists r such that A, B, $C \in \mathrm{circle}(a,b,r)$. The theorem is a consequence of (62).

(64) Suppose A, B, C form a triangle and A, B, $C \in \mathrm{circle}(a,b,r)$. Then

(i) $[a,b] = \mathrm{Circumcenter}\,\triangle(A,B,C)$, and

(ii) $r = |\,\mathrm{Circumcenter}\,\triangle(A,B,C) - A|$.

The theorem is a consequence of (60), (22), and (61).

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

(65) $\mathrm{RadCircumCirc}\,\triangle(A,B,C) > 0$. The theorem is a consequence of (63) and (64).

(66) (i) $|\,\mathrm{Circumcenter}\,\triangle(A,B,C) - A| = |\,\mathrm{Circumcenter}\,\triangle(A,B,C) - B|$, and

(ii) $|\,\mathrm{Circumcenter}\,\triangle(A,B,C) - A| = |\,\mathrm{Circumcenter}\,\triangle(A,B,C) - C|$, and

(iii) $|\,\mathrm{Circumcenter}\,\triangle(A,B,C) - B| = |\,\mathrm{Circumcenter}\,\triangle(A,B,C) - C|$.

The theorem is a consequence of (62).

(67) (i) $\mathrm{RadCircumCirc}\,\triangle(A,B,C) = |\,\mathrm{Circumcenter}\,\triangle(A,B,C) - B|$, and

(ii) $\mathrm{RadCircumCirc}\,\triangle(A,B,C) = |\,\mathrm{Circumcenter}\,\triangle(A,B,C) - C|$.

The theorem is a consequence of (66).

(68) If A, B, C form a triangle and A, B, $C \in \mathrm{circle}(a,b,r)$ and A, B, $C \in \mathrm{circle}(c,d,s)$, then $a = c$ and $b = d$ and $r = s$. The theorem is a consequence of (64).

(69) If $r \neq s$, then circle(a, b, r) misses circle(a, b, s).

8. Extended Law of Sines

Now we state the propositions:

(70) Suppose A, B, C form a triangle and A, B, $C \in$ circle(a, b, r) and A, B, D form a triangle and A, B, $D \in$ circle(a, b, r) and $C \neq D$. Then

- (i) $\varnothing_{\lhd}\ (A, B, C) = \varnothing_{\lhd}\ (D, B, C)$, or
- (ii) $\varnothing_{\lhd}\ (A, B, C) = -\varnothing_{\lhd}\ (D, B, C)$.

Proof: D, B, C form a triangle by [6, (20), (11)], [2, (68)], [6, (30)]. □

(71) Suppose A, B, C form a triangle and A, B, $C \in$ circle(a, b, r). Then

- (i) $\varnothing_{\lhd}\ (A, B, C) = 2 \cdot r$, or
- (ii) $\varnothing_{\lhd}\ (A, B, C) = -2 \cdot r$.

The theorem is a consequence of (70).

(72) If A, B, C form a triangle and $0 < \measuredangle(C, B, A) < \pi$, then $\varnothing_{\lhd}\ (A, B, C) > 0$.

(73) If A, B, C form a triangle and $\pi < \measuredangle(C, B, A) < 2 \cdot \pi$, then $\varnothing_{\lhd}\ (A, B, C) < 0$.

(74) Suppose A, B, C form a triangle and $0 < \measuredangle(C, B, A) < \pi$ and A, B, $C \in$ circle(a, b, r). Then $\varnothing_{\lhd}\ (A, B, C) = 2 \cdot r$. The theorem is a consequence of (71) and (72).

(75) Suppose A, B, C form a triangle and $\pi < \measuredangle(C, B, A) < 2 \cdot \pi$ and A, B, $C \in$ circle(a, b, r). Then $\varnothing_{\lhd}\ (A, B, C) = -2 \cdot r$. The theorem is a consequence of (71) and (73).

(76) Suppose A, B, C form a triangle and $0 < \measuredangle(C, B, A) < \pi$ and A, B, $C \in$ circle(a, b, r). Then

- (i) $|A - B| = 2 \cdot r \cdot \sin \measuredangle(A, C, B)$, and
- (ii) $|B - C| = 2 \cdot r \cdot \sin \measuredangle(B, A, C)$, and
- (iii) $|C - A| = 2 \cdot r \cdot \sin \measuredangle(C, B, A)$.

The theorem is a consequence of (74).

(77) Suppose A, B, C form a triangle and $\pi < \measuredangle(C, B, A) < 2 \cdot \pi$ and A, B, $C \in$ circle(a, b, r). Then

- (i) $|A - B| = -2 \cdot r \cdot \sin \measuredangle(A, C, B)$, and
- (ii) $|B - C| = -2 \cdot r \cdot \sin \measuredangle(B, A, C)$, and
- (iii) $|C - A| = -2 \cdot r \cdot \sin \measuredangle(C, B, A)$.

The theorem is a consequence of (75).

(78) Extended law of sines:
Suppose A, B, C form a triangle and $0 < \measuredangle(C, B, A) < \pi$ and A, B, $C \in \mathrm{circle}(a, b, r)$. Then

(i) $\frac{|A-B|}{\sin \measuredangle(A,C,B)} = 2 \cdot r$, and

(ii) $\frac{|B-C|}{\sin \measuredangle(B,A,C)} = 2 \cdot r$, and

(iii) $\frac{|C-A|}{\sin \measuredangle(C,B,A)} = 2 \cdot r$.

The theorem is a consequence of (76).

(79) Suppose A, B, C form a triangle and $\pi < \measuredangle(C, B, A) < 2 \cdot \pi$ and A, B, $C \in \mathrm{circle}(a, b, r)$. Then

(i) $\frac{|A-B|}{\sin \measuredangle(A,C,B)} = -2 \cdot r$, and

(ii) $\frac{|B-C|}{\sin \measuredangle(B,A,C)} = -2 \cdot r$, and

(iii) $\frac{|C-A|}{\sin \measuredangle(C,B,A)} = -2 \cdot r$.

The theorem is a consequence of (77).

9. The Centroid of a Triangle

Now we state the proposition:

(80) Suppose A, B, C form a triangle and $D = (1 - (\frac{1}{2})) \cdot B + (\frac{1}{2}) \cdot C$ and $E = (1 - (\frac{1}{2})) \cdot C + (\frac{1}{2}) \cdot A$ and $F = (1 - (\frac{1}{2})) \cdot A + (\frac{1}{2}) \cdot B$. Then $\mathrm{Line}(A, D)$, $\mathrm{Line}(B, E)$, $\mathrm{Line}(C, F)$ are concurrent.

Let A, B, C be points of $\mathcal{E}^2_{\mathrm{T}}$. The functor $\mathrm{Median}\triangle(A, B, C)$ yielding an element of $\mathrm{Lines}(\mathcal{R}^2)$ is defined by the term

(Def. 7) $\mathrm{Line}(A, \mathrm{SegMidpoint}(B, C))$.

(81) $\mathrm{Median}\triangle(A, A, A) = \{A\}$. The theorem is a consequence of (4), (3), and (31).

(82) $\mathrm{Median}\triangle(A, A, B) = \mathrm{Line}(A, B)$. The theorem is a consequence of (28), (32), (4), (3), and (81).

(83) $\mathrm{Median}\triangle(A, B, A) = \mathrm{Line}(A, B)$. The theorem is a consequence of (28), (33), (4), (3), and (81).

(84) $\mathrm{Median}\triangle(B, A, A) = \mathrm{Line}(A, B)$.

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

(85) $\mathrm{Median}\triangle(A, B, C)$ is a line. The theorem is a consequence of (6) and (28).

(86) There exists D such that

(i) $D \in \mathrm{Median} \triangle(A, B, C)$, and

(ii) $D \in \mathrm{Median} \triangle(B, C, A)$, and

(iii) $D \in \mathrm{Median} \triangle(C, A, B)$.

The theorem is a consequence of (29), (80), and (4).

(87) There exists D such that

(i) $\mathrm{Median} \triangle(A, B, C) \cap \mathrm{Median} \triangle(B, C, A) = \{D\}$, and

(ii) $\mathrm{Median} \triangle(B, C, A) \cap \mathrm{Median} \triangle(C, A, B) = \{D\}$, and

(iii) $\mathrm{Median} \triangle(C, A, B) \cap \mathrm{Median} \triangle(A, B, C) = \{D\}$.

The theorem is a consequence of (86), (4), (85), (28), (32), (5), (8), and (20).

Let A, B, C be points of $\mathcal{E}^2_{\mathrm{T}}$. Assume A, B, C form a triangle. The functor $\mathrm{Centroid} \triangle(A, B, C)$ yielding a point of $\mathcal{E}^2_{\mathrm{T}}$ is defined by

(Def. 8) $\mathrm{Median} \triangle(A, B, C) \cap \mathrm{Median} \triangle(B, C, A) = \{it\}$ and $\mathrm{Median} \triangle(B, C, A) \cap \mathrm{Median} \triangle(C, A, B) = \{it\}$ and $\mathrm{Median} \triangle(C, A, B) \cap \mathrm{Median} \triangle(A, B, C) = \{it\}$.

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] Czesław Byliński. Introduction to real linear topological spaces. *Formalized Mathematics*, 13(**1**):99–107, 2005.

[3] H.S.M. Coxeter and S.L. Greitzer. *Geometry Revisited*. The Mathematical Association of America (Inc.), 1967.

[4] Robin Hartshorne. *Geometry: Euclid and beyond*. Springer, 2000.

[5] Akihiro Kubo. Lines on planes in n-dimensional Euclidean spaces. *Formalized Mathematics*, 13(**3**):389–397, 2005.

[6] Marco Riccardi. Heron's formula and Ptolemy's theorem. *Formalized Mathematics*, 16(**2**): 97–101, 2008. doi:10.2478/v10037-008-0014-2.

Received December 30, 2015

FORMALIZED MATHEMATICS
Vol. 24, No. 1, Pages 27–36, 2016
DOI: 10.1515/forma-2016-0003

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

Altitude, Orthocenter of a Triangle and Triangulation

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

Summary. We introduce the altitudes of a triangle (the cevians perpendicular to the opposite sides). Using the generalized Ceva's Theorem, we prove the existence and uniqueness of the orthocenter of a triangle [7]. Finally, we formalize in Mizar [1] some formulas [2] to calculate distance using triangulation.

MSC: 51M04 03B35

Keywords: Euclidean geometry; trigonometry; altitude; orthocenter; triangulation; distance

MML identifier: EUCLID13, version: 8.1.04 5.36.1267

1. Preliminaries

From now on n denotes a natural number, i denotes an integer, r, s, t denote real numbers, A_1, B_1, C_1, D_1 denote points of $\mathcal{E}^n_{\mathrm{T}}$, L_1, L_2 denote elements of $\mathrm{Lines}(\mathcal{R}^n)$, and A, B, C denote points of $\mathcal{E}^2_{\mathrm{T}}$.

Now we state the propositions:

(1) If $0 < i \cdot r < r$, then $i = 1$.

(2) Let us consider an integer i. If $\frac{-3}{2} < i < \frac{1}{2}$, then $i = 0$ or $i = -1$.

(3) Suppose r is not zero and s is not zero and t is not zero. Then $(\frac{-r}{-s}) \cdot (\frac{-t}{-r}) \cdot (\frac{-s}{-t}) = 1$.

(4) If $0 < r < 2 \cdot \pi$, then $\sin(\frac{r}{2}) \neq 0$. The theorem is a consequence of (1).

(5) If $-2 \cdot \pi < r < 0$, then $\sin(\frac{r}{2}) \neq 0$. The theorem is a consequence of (4).

(6) $\tan(2 \cdot \pi - r) = -\tan r$.

(7) If $A_1 \in \mathrm{Line}(B_1, C_1)$ and $A_1 \neq C_1$, then $\mathrm{Line}(B_1, C_1) = \mathrm{Line}(A_1, C_1)$.

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

(8) If $A_1 \neq C_1$ and $A_1 \in \mathrm{Line}(B_1, C_1)$, then $B_1 \in \mathrm{Line}(A_1, C_1)$.

(9) Suppose $A_1 \neq B_1$ and $A_1 \neq C_1$ and $|(A_1 - B_1, A_1 - C_1)| = 0$ and $L_1 = \mathrm{Line}(A_1, B_1)$ and $L_2 = \mathrm{Line}(A_1, C_1)$. Then $L_1 \perp L_2$.

(10) If $B_1 \neq C_1$ and $|(B_1 - A_1, B_1 - C_1)| = 0$, then $A_1 \neq C_1$.

(11) $|(A_1 - B_1, A_1 - C_1)| = |(B_1 - A_1, C_1 - A_1)|$.

(12) Suppose $B_1 \neq C_1$ and $r = -(\frac{|(B_1,C_1)|-|(C_1,C_1)|-|(A_1,B_1)|+|(A_1,C_1)|}{|(B_1-C_1,B_1-C_1)|})$ and $D_1 = r \cdot B_1 + (1-r) \cdot C_1$. Then $|(D_1 - A_1, D_1 - C_1)| = 0$.

(13) If $A_1 \neq B_1$ and $C_1 = r \cdot A_1 + (1-r) \cdot B_1$ and $C_1 = B_1$, then $r = 0$.

(14) (i) $|(B_1, C_1)| - |(C_1, C_1)| - |(A_1, B_1)| + |(A_1, C_1)| = |(C_1 - A_1, B_1 - C_1)|$, and

(ii) $|(B_1 - C_1, B_1 - C_1)| + |(C_1 - A_1, B_1 - C_1)| = |(B_1 - C_1, B_1 - A_1)|$.

(15) $|(A_1 - B_1, A_1 - C_1)| = -|(A_1 - B_1, C_1 - A_1)|$.

(16) $|(B_1 - A_1, C_1 - A_1)| = |(A_1 - B_1, A_1 - C_1)|$.

(17) $|(B_1 - A_1, C_1 - A_1)| = -|(B_1 - A_1, A_1 - C_1)|$. The theorem is a consequence of (16) and (15).

(18) Suppose $B_1 \neq C_1$ and $C_1 \neq A_1$ and $A_1 \neq B_1$ and $|(C_1 - A_1, B_1 - C_1)|$ is not zero and $|(B_1 - C_1, A_1 - B_1)|$ is not zero and $|(C_1 - A_1, A_1 - B_1)|$ is not zero and $r = -(\frac{|(B_1,C_1)|-|(C_1,C_1)|-|(A_1,B_1)|+|(A_1,C_1)|}{|(B_1-C_1,B_1-C_1)|})$ and $s = -(\frac{|(C_1,A_1)|-|(A_1,A_1)|-|(B_1,C_1)|+|(B_1,A_1)|}{|(C_1-A_1,C_1-A_1)|})$ and

$t = -(\frac{|(A_1,B_1)|-|(B_1,B_1)|-|(C_1,A_1)|+|(C_1,B_1)|}{|(A_1-B_1,A_1-B_1)|})$. Then $\frac{(\frac{(\frac{r}{1-r})\cdot s}{1-s})\cdot t}{1-t} = 1$. The theorem is a consequence of (14), (15), and (3).

(19) If $C_1 = r \cdot A_1 + (1-r) \cdot B_1$ and $r = 1$, then $C_1 = A_1$.

(20) If $C_1 = r \cdot A_1 + (1-r) \cdot B_1$ and $r = 0$, then $C_1 = B_1$.

(21) If $|(B_1 - C_1, B_1 - C_1)| = -|(C_1 - A_1, B_1 - C_1)|$, then $|(B_1 - C_1, A_1 - B_1)| = 0$. The theorem is a consequence of (15).

(22) Suppose $B_1 \neq C_1$ and $r = -(\frac{|(B_1,C_1)|-|(C_1,C_1)|-|(A_1,B_1)|+|(A_1,C_1)|}{|(B_1-C_1,B_1-C_1)|})$ and $r = 1$. Then $|(B_1 - C_1, A_1 - B_1)| = 0$. The theorem is a consequence of (14) and (21).

(23) If $A \neq B$ and $A \neq C$, then $|A - B| + |A - C| \neq 0$.

(24) If A, B, C form a triangle, then $A \notin \mathrm{Line}(B, C)$.

(25) If $A \neq B$ and $B \neq C$ and $|(B - A, B - C)| = 0$, then $\measuredangle(A, B, C) = \frac{\pi}{2}$ or $\measuredangle(A, B, C) = (\frac{3}{2}) \cdot \pi$.

(26) If A, B, C form a triangle, then $\sin(\frac{\measuredangle(A,B,C)}{2}) > 0$.

(27) If $\measuredangle(B, A, C) \neq \measuredangle(C, B, A)$, then $\sin(\frac{\measuredangle(B,A,C)-\measuredangle(C,B,A)}{2}) \neq 0$. The theorem is a consequence of (5) and (4).

(28) If A, B, C form a triangle, then $\sin \measuredangle(A,B,C) \neq 0$.

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

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

(30) $\measuredangle(B,A,C) + \measuredangle(C,B,A) = \pi - \measuredangle(A,C,B)$. The theorem is a consequence of (29).

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

(31) $\measuredangle(B,A,C) - \measuredangle(C,B,A) \neq \pi$.

(32) $\measuredangle(B,A,C) - \measuredangle(C,B,A) \neq -\pi$.

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

(33) $(-2) \cdot \pi < \measuredangle(B,A,C) - \measuredangle(C,B,A) < 2 \cdot \pi$.

(34) $-\pi < \frac{\measuredangle(B,A,C) - \measuredangle(C,B,A)}{2} < \pi$. The theorem is a consequence of (33).

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

(35) $-\pi < \measuredangle(B,A,C) - \measuredangle(C,B,A) < \pi$.

(36) $-(\frac{\pi}{2}) < \frac{\measuredangle(B,A,C) - \measuredangle(C,B,A)}{2} < \frac{\pi}{2}$. The theorem is a consequence of (35).

2. Orthocenter

From now on D denotes a point of $\mathcal{E}^2_{\mathrm{T}}$ and a, b, c, d denote real numbers.

Let A, B, C be points of $\mathcal{E}^2_{\mathrm{T}}$. Assume $B \neq C$. The functor $\mathrm{Altit}\,\triangle(A,B,C)$ yielding an element of $\mathrm{Lines}(\mathcal{R}^2)$ is defined by

(Def. 1) there exist elements L_1, L_2 of $\mathrm{Lines}(\mathcal{R}^2)$ such that $it = L_1$ and $L_2 = \mathrm{Line}(B,C)$ and $A \in L_1$ and $L_1 \perp L_2$.

Let us assume that $B \neq C$. Now we state the propositions:

(37) $A \in \mathrm{Altit}\,\triangle(A,B,C)$.

(38) $\mathrm{Altit}\,\triangle(A,B,C)$ is a line.

(39) $\mathrm{Altit}\,\triangle(A,B,C) = \mathrm{Altit}\,\triangle(A,C,B)$.

Now we state the propositions:

(40) If $B \neq C$ and $D \in \mathrm{Altit}\,\triangle(A,B,C)$, then $\mathrm{Altit}\,\triangle(D,B,C) = \mathrm{Altit}\,\triangle(A,B,C)$.

(41) If $B \neq C$ and $D \in \mathrm{Line}(B,C)$ and $D \neq C$, then $\mathrm{Altit}\,\triangle(A,B,C) = \mathrm{Altit}\,\triangle(A,D,C)$. The theorem is a consequence of (7).

Let A, B, C be points of $\mathcal{E}^2_{\mathrm{T}}$. Assume $B \neq C$. The functor $\mathrm{FootAltit}\,\triangle(A,B,C)$ yielding a point of $\mathcal{E}^2_{\mathrm{T}}$ is defined by

(Def. 2) there exists a point P of $\mathcal{E}^2_{\mathrm{T}}$ such that $it = P$ and $\mathrm{Altit}\,\triangle(A,B,C) \cap \mathrm{Line}(B,C) = \{P\}$.

Let us assume that $B \neq C$. Now we state the propositions:

(42) $\mathrm{FootAltit}\,\triangle(A,B,C) = \mathrm{FootAltit}\,\triangle(A,C,B)$. The theorem is a consequence of (39).

(43) (i) $\mathrm{FootAltit}\,\triangle(A,B,C) \in \mathrm{Line}(B,C)$, and

(ii) $\mathrm{FootAltit}\,\triangle(A,B,C) \in \mathrm{Altit}\,\triangle(A,B,C)$.

Now we state the propositions:

(44) If $B \neq C$ and $A \notin \mathrm{Line}(B,C)$, then $\mathrm{Altit}\,\triangle(A,B,C) = \mathrm{Line}(A, \mathrm{FootAltit}\,\triangle(A,B,C))$. The theorem is a consequence of (43).

(45) If $B \neq C$ and $A \in \mathrm{Line}(B,C)$, then $\mathrm{FootAltit}\,\triangle(A,B,C) = A$.

(46) If $B \neq C$ and $\mathrm{FootAltit}\,\triangle(A,B,C) = A$, then $A \in \mathrm{Line}(B,C)$.

Let us assume that $B \neq C$. Now we state the propositions:

(47) $|(A - \mathrm{FootAltit}\,\triangle(A,B,C), B - C)| = 0$. The theorem is a consequence of (44) and (45).

(48) $|(A-\mathrm{FootAltit}\,\triangle(A,B,C), B-\mathrm{FootAltit}\,\triangle(A,B,C))| = 0$. The theorem is a consequence of (43), (44), and (45).

(49) $|(A-\mathrm{FootAltit}\,\triangle(A,B,C), C-\mathrm{FootAltit}\,\triangle(A,B,C))| = 0$. The theorem is a consequence of (42) and (48).

Now we state the propositions:

(50) If $B \neq C$ and $B = \mathrm{FootAltit}\,\triangle(A,B,C)$, then $|(B-A, B-C)| = 0$. The theorem is a consequence of (49), (11), and (43).

(51) If $B \neq C$ and $D \in \mathrm{Line}(B,C)$ and $D \neq C$, then $\mathrm{FootAltit}\,\triangle(A,B,C) = \mathrm{FootAltit}\,\triangle(A,D,C)$. The theorem is a consequence of (7) and (41).

(52) If $B \neq C$ and $|(B-A, B-C)| = 0$, then $B = \mathrm{FootAltit}\,\triangle(A,B,C)$. The theorem is a consequence of (9) and (45).

(53) If $B \neq C$ and $B \neq A$ and $\measuredangle(A,B,C) = \frac{\pi}{2}$, then $\mathrm{FootAltit}\,\triangle(A,B,C) = B$. The theorem is a consequence of (11) and (52).

(54) If A, B, C form a triangle, then $A \neq \mathrm{FootAltit}\,\triangle(A,B,C)$. The theorem is a consequence of (43).

(55) If A, B, C form a triangle and $|(B - A, B - C)| \neq 0$, then $\mathrm{FootAltit}\,\triangle(A,B,C)$, B, A form a triangle.

PROOF: Set $p = \mathrm{FootAltit}\,\triangle(A,B,C)$. Consider P being a point of $\mathcal{E}^2_{\mathrm{T}}$ such that $\mathrm{FootAltit}\,\triangle(A,B,C) = P$ and $\mathrm{Altit}\,\triangle(A,B,C) \cap \mathrm{Line}(B,C) = \{P\}$. Consider L_1, L_2 being elements of $\mathrm{Lines}(\mathcal{R}^2)$ such that $\mathrm{Altit}\,\triangle(A,B,C) = L_1$ and $L_2 = \mathrm{Line}(B,C)$ and $A \in L_1$ and $L_1 \perp L_2$. $P \neq B$. $p \neq A$. p, B, A are mutually different. $P \in \mathrm{Line}(B,C)$. $B, C \in \mathrm{Line}(B,P)$. $\measuredangle(p,B,A) \neq \pi$

by [11, (11)], [12, (12)], (50), (8). $\measuredangle(B, A, p) \neq \pi$ by [11, (11)], [12, (12)]. $\measuredangle(A, p, B) \neq \pi$ by [11, (11)], [12, (12)], (8), (54). $\square$

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

(Def. 3) $|A - \operatorname{FootAltit}\triangle(A, B, C)|$.

Let us assume that $B \neq C$. Now we state the propositions:

(56) $0 \leqslant |\operatorname{Altit}\triangle(A, B, C)|$.

(57) $|\operatorname{Altit}\triangle(A, B, C)| = |\operatorname{Altit}\triangle(A, C, B)|$. The theorem is a consequence of (42).

Now we state the propositions:

(58) If $B \neq C$ and $|(B - A, B - C)| = 0$, then $|\operatorname{FootAltit}\triangle(A, B, C) - A| = |A - B|$. The theorem is a consequence of (52).

(59) Suppose $B \neq C$ and $r = -(\frac{|(B,C)| - |(C,C)| - |(A,B)| + |(A,C)|}{|(B-C,B-C)|})$ and $D = r \cdot B + (1 - r) \cdot C$ and $D \neq C$. Then $D = \operatorname{FootAltit}\triangle(A, B, C)$.
Proof: $|(D - A, D - C)| = 0$. $D = \operatorname{FootAltit}\triangle(A, D, C)$. $D \in \operatorname{Line}(B, C)$ by [6, (4)]. $\square$

(60) Suppose $B \neq C$ and $r = -(\frac{|(B,C)| - |(C,C)| - |(A,B)| + |(A,C)|}{|(B-C,B-C)|})$ and $D = r \cdot B + (1 - r) \cdot C$ and $D = C$. Then $C = \operatorname{FootAltit}\triangle(A, B, C)$. The theorem is a consequence of (13), (14), (15), (52), and (42).

(61) Suppose A, B, C form a triangle and $|(C - A, B - C)|$ is not zero and $|(B - C, A - B)|$ is not zero and $|(C - A, A - B)|$ is not zero. Then $\operatorname{Line}(A, \operatorname{FootAltit}\triangle(A, B, C))$, $\operatorname{Line}(C, \operatorname{FootAltit}\triangle(C, A, B))$, $\operatorname{Line}(B, \operatorname{FootAltit}\triangle(B, C, A))$ are concurrent. The theorem is a consequence of (60), (17), (47), (59), (18), and (22).

(62) If A, B, C form a triangle and $|(C - A, B - C)|$ is zero, then $\operatorname{FootAltit}\triangle(A, B, C) = C$ and $\operatorname{FootAltit}\triangle(B, C, A) = C$. The theorem is a consequence of (15), (52), and (42).

(63) Suppose A, B, C form a triangle and $C \in \operatorname{Altit}\triangle(A, B, C)$ and $C \in \operatorname{Altit}\triangle(B, C, A)$. Then $\operatorname{Altit}\triangle(A, B, C) \cap \operatorname{Altit}\triangle(B, C, A)$ is a point.
Proof: Consider L_1, L_2 being elements of $\operatorname{Lines}(\mathcal{R}^2)$ such that $\operatorname{Altit}\triangle(A, B, C) = L_1$ and $L_2 = \operatorname{Line}(B, C)$ and $A \in L_1$ and $L_1 \perp L_2$. Consider L_3, L_4 being elements of $\operatorname{Lines}(\mathcal{R}^2)$ such that $\operatorname{Altit}\triangle(B, C, A) = L_3$ and $L_4 = \operatorname{Line}(C, A)$ and $B \in L_3$ and $L_3 \perp L_4$. $L_1 \nparallel L_3$ by [9, (41)], [6, (16)], [8, (108)], [12, (13)]. L_1 is not a point and L_3 is not a point. $\square$

(64) Suppose B, C, A form a triangle and $C \in \operatorname{Altit}\triangle(B, C, A)$ and $C \in \operatorname{Altit}\triangle(C, A, B)$. Then $\operatorname{Altit}\triangle(B, C, A) \cap \operatorname{Altit}\triangle(C, A, B)$ is a point.
Proof: Consider L_1, L_2 being elements of $\operatorname{Lines}(\mathcal{R}^2)$ such that

$\operatorname{Altit}\triangle(B,C,A) = L_1$ and $L_2 = \operatorname{Line}(C,A)$ and $B \in L_1$ and $L_1 \perp L_2$. Consider L_3, L_4 being elements of $\operatorname{Lines}(\mathcal{R}^2)$ such that $\operatorname{Altit}\triangle(C,A,B) = L_3$ and $L_4 = \operatorname{Line}(A,B)$ and $C \in L_3$ and $L_3 \perp L_4$. $L_1 \not\parallel L_3$ by [8, (71), (111)], [6, (16)], [9, (41)]. L_1 is not a point and L_3 is not a point. □

(65) Suppose C, A, B form a triangle and $C \in \operatorname{Altit}\triangle(C,A,B)$ and $C \in \operatorname{Altit}\triangle(A,B,C)$. Then $\operatorname{Altit}\triangle(C,A,B) \cap \operatorname{Altit}\triangle(A,B,C)$ is a point.
Proof: Consider L_1, L_2 being elements of $\operatorname{Lines}(\mathcal{R}^2)$ such that $\operatorname{Altit}\triangle(C,A,B) = L_1$ and $L_2 = \operatorname{Line}(A,B)$ and $C \in L_1$ and $L_1 \perp L_2$. Consider L_3, L_4 being elements of $\operatorname{Lines}(\mathcal{R}^2)$ such that $\operatorname{Altit}\triangle(A,B,C) = L_3$ and $L_4 = \operatorname{Line}(B,C)$ and $A \in L_3$ and $L_3 \perp L_4$. $L_1 \not\parallel L_3$ by [8, (71), (111)], [6, (16)], [9, (41)]. L_1 is not a point and L_3 is not a point. □

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

(i) $\operatorname{Altit}\triangle(A,B,C) \cap \operatorname{Altit}\triangle(B,C,A) = \{C\}$, and

(ii) $\operatorname{Altit}\triangle(B,C,A) \cap \operatorname{Altit}\triangle(C,A,B) = \{C\}$, and

(iii) $\operatorname{Altit}\triangle(C,A,B) \cap \operatorname{Altit}\triangle(A,B,C) = \{C\}$.

Proof: $A \notin \operatorname{Line}(B,C)$ and $B \notin \operatorname{Line}(C,A)$. $\operatorname{FootAltit}\triangle(A,B,C) = C$ and $\operatorname{FootAltit}\triangle(B,C,A) = C$. $\operatorname{Altit}\triangle(A,B,C) = \operatorname{Line}(A,C)$ and $\operatorname{Altit}\triangle(B,C,A) = \operatorname{Line}(B,C)$. $C \in \operatorname{Altit}\triangle(C,A,B)$. $\operatorname{Altit}\triangle(A,B,C) \cap \operatorname{Altit}\triangle(B,C,A) = \{C\}$ by [6, (22)], (63). $\operatorname{Altit}\triangle(B,C,A) \cap \operatorname{Altit}\triangle(C,A,B) = \{C\}$ by [12, (15)], (37), (64), [6, (22)]. $\operatorname{Altit}\triangle(C,A,B) \cap \operatorname{Altit}\triangle(A,B,C) = \{C\}$ by [12, (15)], (37), (65), [6, (22)]. □

(67) Suppose A, B, C form a triangle. Then there exists a point P of $\mathcal{E}^2_{\mathrm{T}}$ such that

(i) $\operatorname{Altit}\triangle(A,B,C) \cap \operatorname{Altit}\triangle(B,C,A) = \{P\}$, and

(ii) $\operatorname{Altit}\triangle(B,C,A) \cap \operatorname{Altit}\triangle(C,A,B) = \{P\}$, and

(iii) $\operatorname{Altit}\triangle(C,A,B) \cap \operatorname{Altit}\triangle(A,B,C) = \{P\}$.

The theorem is a consequence of (66), (61), (24), (44), and (38).

Let A, B, C be points of $\mathcal{E}^2_{\mathrm{T}}$. Assume A, B, C form a triangle. The functor $\operatorname{Orthocenter}\triangle(A,B,C)$ yielding a point of $\mathcal{E}^2_{\mathrm{T}}$ is defined by

(Def. 4) $\operatorname{Altit}\triangle(A,B,C) \cap \operatorname{Altit}\triangle(B,C,A) = \{it\}$ and $\operatorname{Altit}\triangle(B,C,A) \cap \operatorname{Altit}\triangle(C,A,B) = \{it\}$ and $\operatorname{Altit}\triangle(C,A,B) \cap \operatorname{Altit}\triangle(A,B,C) = \{it\}$.

3. Triangulation

Let us assume that $B \neq A$. Now we state the propositions:

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

(69) $\sin(\frac{\measuredangle(B,A,C)+\measuredangle(C,B,A)}{2}) \cdot \cos(\frac{\measuredangle(B,A,C)-\measuredangle(C,B,A)}{2}) \cdot (|C-B|-|C-A|) = \sin(\frac{\measuredangle(B,A,C)-\measuredangle(C,B,A)}{2}) \cdot \cos(\frac{\measuredangle(B,A,C)+\measuredangle(C,B,A)}{2}) \cdot (|C-B|+|C-A|)$. The theorem is a consequence of (68).

Now we state the proposition:

(70) Suppose A, B, C form a triangle and $\measuredangle(B,A,C) - \measuredangle(C,B,A) \neq \pi$ and $\measuredangle(B,A,C) - \measuredangle(C,B,A) \neq -\pi$. Then $\cos(\frac{\measuredangle(B,A,C)-\measuredangle(C,B,A)}{2}) \neq 0$. The theorem is a consequence of (2).

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

(71) $\tan(\frac{\measuredangle(B,A,C)-\measuredangle(C,B,A)}{2}) = \cot(\frac{\measuredangle(A,C,B)}{2}) \cdot (\frac{|C-B|-|C-A|}{|C-B|+|C-A|})$.
PROOF: $\measuredangle(B,A,C) - \measuredangle(C,B,A) \neq \pi$ and $\measuredangle(B,A,C) - \measuredangle(C,B,A) \neq -\pi$. Set $\alpha = \frac{\measuredangle(B,A,C)-\measuredangle(C,B,A)}{2}$. Set $\beta = \frac{\measuredangle(B,A,C)+\measuredangle(C,B,A)}{2}$. $\measuredangle(A,C,B) = \pi - (\measuredangle(C,B,A)+\measuredangle(B,A,C))$. Set $\alpha_1 = \frac{\measuredangle(A,C,B)}{2}$. $\sin\alpha_1 \neq 0$. $|C-B|+|C-A| \neq 0$ by [11, (42)]. $\sin\beta \cdot \cos\alpha \cdot (|C-B|-|C-A|) = \sin\alpha \cdot \cos\beta \cdot (|C-B|+|C-A|)$. $(|C-B|-|C-A|) \cdot \cos\alpha_1 \cdot 1 = (|C-B|+|C-A|) \cdot \sin\alpha_1 \cdot (\frac{\sin\alpha}{\cos\alpha})$. $\square$

(72) $\frac{\measuredangle(B,A,C)-\measuredangle(C,B,A)}{2} = \arctan(\cot(\frac{\measuredangle(A,C,B)}{2}) \cdot (\frac{|C-B|-|C-A|}{|C-B|+|C-A|}))$. The theorem is a consequence of (71) and (36).

(73) $\measuredangle(B,A,C) - \measuredangle(C,B,A) = 2 \cdot \arctan(\cot(\frac{\measuredangle(A,C,B)}{2}) \cdot (\frac{|C-B|-|C-A|}{|C-B|+|C-A|}))$. The theorem is a consequence of (72).

(74) (i) $\measuredangle(B,A,C) = \arctan(\cot(\frac{\measuredangle(A,C,B)}{2}) \cdot (\frac{|C-B|-|C-A|}{|C-B|+|C-A|})) + (\frac{\pi}{2}) - (\frac{\measuredangle(A,C,B)}{2})$, and

(ii) $\measuredangle(C,B,A) = (\frac{\pi}{2}) - (\frac{\measuredangle(A,C,B)}{2}) - \arctan(\cot(\frac{\measuredangle(A,C,B)}{2}) \cdot (\frac{|C-B|-|C-A|}{|C-B|+|C-A|}))$.

The theorem is a consequence of (73) and (30).

(75) $|B-C| = \frac{|A-B| \cdot \sin\measuredangle(B,A,C)}{\sin(\measuredangle(B,A,C)+\measuredangle(C,B,A))}$.
PROOF: $|B-C| = \frac{|A-B| \cdot \sin\measuredangle(B,A,C)}{\sin\measuredangle(A,C,B)}$ by [11, (6), (43)], (28). $\measuredangle(A,C,B) = \pi - (\measuredangle(C,B,A) + \measuredangle(B,A,C))$. $\square$

(76) $|A-C| = \frac{|A-B| \cdot \sin\measuredangle(C,B,A)}{\sin(\measuredangle(B,A,C)+\measuredangle(C,B,A))}$.
PROOF: $|A-C| = \frac{|A-B| \cdot \sin\measuredangle(C,B,A)}{\sin\measuredangle(A,C,B)}$ by [11, (6)], (28). $\measuredangle(A,C,B) = \pi - (\measuredangle(C,B,A) + \measuredangle(B,A,C))$ by [11, (20)], [10, (47)]. $\square$

Now we state the propositions:

(77) Suppose A, C, B form a triangle and $\measuredangle(C,A,B) = \frac{\pi}{2}$.
Then $|\operatorname{Altit}\triangle(C,A,B)| = |A-B| \cdot \tan\measuredangle(A,B,C)$. The theorem is a consequence of (11) and (58).

(78) Suppose A, B, C form a triangle and $\measuredangle(C,A,B) = (\frac{3}{2}) \cdot \pi$.

Then $|\operatorname{Altit}\triangle(C,A,B)| = |A-B| \cdot \tan\measuredangle(C,B,A)$. The theorem is a consequence of (11) and (58).

(79) Suppose A, C, B form a triangle and $|(A-C,A-B)| = 0$. Then $|\operatorname{Altit}\triangle(C,A,B)| = |A-B| \cdot |\tan\measuredangle(A,B,C)|$. The theorem is a consequence of (11), (77), (56), (6), and (78).

(80) Suppose $B \neq C$ and $\operatorname{FootAltit}\triangle(A,B,C)$, B, A form a triangle. Then

  (i) $|A-B| \cdot \sin\measuredangle(A,B,\operatorname{FootAltit}\triangle(A,B,C)) = |\operatorname{FootAltit}\triangle(A,B,C) - A|$, or

  (ii) $|A-B| \cdot (-\sin\measuredangle(A,B,\operatorname{FootAltit}\triangle(A,B,C))) = |\operatorname{FootAltit}\triangle(A,B,C) - A|$.

The theorem is a consequence of (48).

(81) Suppose A, B, C form a triangle and $|(B-A,B-C)| \neq 0$. Then

  (i) $|A-B| \cdot \sin\measuredangle(A,B,\operatorname{FootAltit}\triangle(A,B,C)) = |\operatorname{FootAltit}\triangle(A,B,C) - A|$, or

  (ii) $|A-B| \cdot (-\sin\measuredangle(A,B,\operatorname{FootAltit}\triangle(A,B,C))) = |\operatorname{FootAltit}\triangle(A,B,C) - A|$.

The theorem is a consequence of (80) and (55).

(82) Suppose A, C, B form a triangle and $\measuredangle(A,C,B) < \pi$ and $|(A-C,A-B)| \neq 0$. Then $|\operatorname{Altit}\triangle(C,A,B)| = |A-B| \cdot |(\frac{\sin\measuredangle(C,B,A)}{\sin(\measuredangle(B,A,C)+\measuredangle(C,B,A))}) \cdot \sin\measuredangle(C,A,\operatorname{FootAltit}\triangle(C,A,B))|$. The theorem is a consequence of (76), (55), and (80).

(83) Suppose $0 < \measuredangle(B,A,D) < \pi$ and $0 < \measuredangle(D,A,C) < \pi$ and D, A, C are mutually different and B, A, D are mutually different. Then $\measuredangle(A,C,D) + \measuredangle(D,B,A) = 2 \cdot \pi - (\measuredangle(B,A,C) + \measuredangle(A,D,B) + \measuredangle(C,D,A))$.
PROOF: $\measuredangle(B,A,D) + \measuredangle(D,A,C) = \measuredangle(B,A,C)$ by [5, (2)], [11, (4)]. $\measuredangle(A,C,D) = \pi - (\measuredangle(C,D,A) + \measuredangle(D,A,C))$ by [10, (47)]. $\measuredangle(D,B,A) = \pi - (\measuredangle(A,D,B) + \measuredangle(B,A,D))$ by [10, (47)]. $\square$

(84) Suppose A, C, B form a triangle and $\measuredangle(A,C,B) < \pi$ and A, D, B form a triangle and $\measuredangle(A,D,B) < \pi$ and $a = \measuredangle(C,B,A)$ and $b = \measuredangle(B,A,C)$ and $c = \measuredangle(D,B,A)$ and $d = \measuredangle(C,A,D)$. Then $|D-C|^{\mathbf{2}} = |A-B|^{\mathbf{2}} \cdot ((\frac{\sin a}{\sin(a+b)})^{\mathbf{2}} + (\frac{\sin c}{\sin(b+d+c)})^{\mathbf{2}} - 2 \cdot (\frac{\sin a}{\sin(b+a)}) \cdot (\frac{\sin c}{\sin(b+d+c)}) \cdot \cos d)$.
PROOF: Set $e = b+d$. $\sin(e+c) = \sin(\measuredangle(B,A,D) + \measuredangle(D,B,A))$ by [14, (79)]. $\square$

(85) Suppose $\sin(2 \cdot s) \cdot \cos d = \cos(2 \cdot t)$. Then $(r \cdot \cos s)^{\mathbf{2}} + (r \cdot \sin s)^{\mathbf{2}} - 2 \cdot (r \cdot \cos s) \cdot (r \cdot \sin s) \cdot \cos d = 2 \cdot r^{\mathbf{2}} \cdot (\sin t)^{\mathbf{2}}$.

(86) Let us consider real numbers R, ϑ. Suppose $D \neq C$ and $0 \leqslant R$ and A, C, B form a triangle and $\measuredangle(A,C,B) < \pi$ and A, D, B form a triangle

and $\measuredangle(A,D,B) < \pi$ and $a = \measuredangle(C,B,A)$ and $b = \measuredangle(B,A,C)$ and $c = \measuredangle(D,B,A)$ and $d = \measuredangle(C,A,D)$ and $R \cdot \cos s = \frac{\sin a}{\sin(a+b)}$ and $R \cdot \sin s = \frac{\sin c}{\sin(b+d+c)}$ and $0 < \vartheta < \pi$ and $\sin(2 \cdot s) \cdot \cos d = \cos(2 \cdot \vartheta)$. Then $|D - C| = |A - B| \cdot \sqrt{2} \cdot R \cdot \sin \vartheta$.

Proof: $|D-C|^{\mathbf{2}} = |A-B|^{\mathbf{2}} \cdot ((R \cdot \cos s)^{\mathbf{2}} + (R \cdot \sin s)^{\mathbf{2}} - 2 \cdot (R \cdot \cos s) \cdot (R \cdot \sin s) \cdot \cos d)$. $|D - C| \neq -|A - B| \cdot \sqrt{2} \cdot R \cdot \sin \vartheta$ by [13, (25)], [11, (42)]. □

(87) Suppose A, C, B form a triangle and $\measuredangle(A,C,B) < \pi$ and D, A, C form a triangle and $\measuredangle(A,D,C) = \frac{\pi}{2}$. Then $|D - C| = (\frac{|A-B| \cdot \sin \measuredangle(C,B,A)}{\sin(\measuredangle(B,A,C) + \measuredangle(C,B,A))}) \cdot \sin \measuredangle(C,A,D)$. The theorem is a consequence of (76).

(88) Suppose B, C, A form a triangle and $\measuredangle(B,C,A) < \pi$ and D, C, A form a triangle and $\measuredangle(C,D,A) = \frac{\pi}{2}$. Then $|D - C| = (\frac{|A-B| \cdot \sin \measuredangle(A,B,C)}{\sin(\measuredangle(A,B,C) + \measuredangle(C,A,B))}) \cdot \sin \measuredangle(D,A,C)$. The theorem is a consequence of (75).

(89) Suppose A, C, B form a triangle and $\measuredangle(A,C,B) < \pi$ and D, A, C form a triangle and $\measuredangle(A,D,C) = \frac{\pi}{2}$ and $A \in \mathcal{L}(B,D)$ and $A \neq D$. Then $|D-C| = (\frac{|A-B| \cdot \sin \measuredangle(C,B,A)}{\sin(\measuredangle(C,A,D) - \measuredangle(C,B,A))}) \cdot \sin \measuredangle(C,A,D)$. The theorem is a consequence of (87).

(90) Suppose B, C, A form a triangle and $\measuredangle(B,C,A) < \pi$ and D, C, A form a triangle and $\measuredangle(C,D,A) = \frac{\pi}{2}$ and $A \in \mathcal{L}(D,B)$ and $A \neq D$. Then $|D - C| = (\frac{|A-B| \cdot \sin \measuredangle(A,B,C)}{\sin(\measuredangle(D,A,C) - \measuredangle(A,B,C))}) \cdot \sin \measuredangle(D,A,C)$.

Proof: $\sin(\measuredangle(C,A,B) + \measuredangle(A,B,C)) = \sin(\measuredangle(D,A,C) - \measuredangle(A,B,C))$ by [4, (1)], [3, (8)]. □

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] R. Campbell. *La trigonométrie*. Que sais-je? Presses universitaires de France, 1956.

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

[4] Roland Coghetto. Some facts about trigonometry and Euclidean geometry. *Formalized Mathematics*, 22(**4**):313–319, 2014. doi:10.2478/forma-2014-0031.

[5] Roland Coghetto. Morley's trisector theorem. *Formalized Mathematics*, 23(**2**):75–79, 2015. doi:10.1515/forma-2015-0007.

[6] Roland Coghetto. Circumcenter, circumcircle and centroid of a triangle. *Formalized Mathematics*, 24(**1**):17–26, 2016. doi:10.1515/forma-2016-0002.

[7] H.S.M. Coxeter and S.L. Greitzer. *Geometry Revisited.* The Mathematical Association of America (Inc.), 1967.

[8] Akihiro Kubo. Lines on planes in n-dimensional Euclidean spaces. *Formalized Mathematics*, 13(**3**):389–397, 2005.

[9] Akihiro Kubo. Lines in n-dimensional Euclidean spaces. *Formalized Mathematics*, 11(**4**): 371–376, 2003.

[10] Akihiro Kubo and Yatsuka Nakamura. Angle and triangle in Euclidean topological space. *Formalized Mathematics*, 11(**3**):281–287, 2003.

[11] Marco Riccardi. Heron's formula and Ptolemy's theorem. *Formalized Mathematics*, 16 (**2**):97–101, 2008. doi:10.2478/v10037-008-0014-2.

[12] Boris A. Shminke. Routh's, Menelaus' and generalized Ceva's theorems. *Formalized Mathematics*, 20(**2**):157–159, 2012. doi:10.2478/v10037-012-0018-9.

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

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

Received December 30, 2015

FORMALIZED MATHEMATICS
Vol. 24, No. 1, Pages 37–47, 2016
DOI: 10.1515/forma-2016-0004

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

Divisible $\mathbb{Z}$-modules

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

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize the definition of divisible $\mathbb{Z}$-module and its properties in the Mizar system [3]. We formally prove that any non-trivial divisible $\mathbb{Z}$-modules are not finitely-generated. We introduce a divisible $\mathbb{Z}$-module, equivalent to a vector space of a torsion-free $\mathbb{Z}$-module with a coefficient ring $\mathbb{Q}$. $\mathbb{Z}$-modules are important for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm [15], cryptographic systems with lattices [16] and coding theory [8].

MSC: 15A03 16D20 13C13 03B35

Keywords: divisible vector; divisible $\mathbb{Z}$-module

MML identifier: ZMODUL08, version: 8.1.04 5.36.1267

1. Divisible Module

Let a, b be elements of $\mathbb{F}_{\mathbb{Q}}$ and x, y be rational numbers. We identify $x + y$ with $a + b$. We identify $x \cdot y$ with $a \cdot b$. Let V be a $\mathbb{Z}$-module and v be a vector of V. We say that v is divisible if and only if

(Def. 1) for every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ there exists a vector u of V such that $a \cdot u = v$.

Let us observe that 0_V is divisible and there exists a vector of V which is divisible.

Now we state the propositions:

(1) Let us consider a $\mathbb{Z}$-module V, and divisible vectors v, u of V. Then $v+u$ is divisible.

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

(2) Let us consider a $\mathbb{Z}$-module V, and a divisible vector v of V. Then $-v$ is divisible.

PROOF: For every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ there exists a vector w of V such that $-v = a \cdot w$ by [9, (6)]. □

(3) Let us consider a $\mathbb{Z}$-module V, a divisible vector v of V, and an element i of $\mathbb{Z}^{\mathrm{R}}$. Then $i \cdot v$ is divisible.

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

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

Observe that $\mathbf{0}_V$ is divisible and $\mathbb{Z}$-module$\mathbb{Q}$ is divisible and there exists a $\mathbb{Z}$-module which is divisible.

Let V be a $\mathbb{Z}$-module. Let us note that there exists a submodule of V which is divisible and there exists a divisible $\mathbb{Z}$-module which is non finitely generated.

Now we state the propositions:

(4) (The left integer multiplication of $\mathbb{F}_{\mathbb{Q}}$)$\restriction(\mathbb{Z} \times \mathbb{Z}) =$ the left integer multiplication of $\mathbb{Z}^{\mathrm{R}}$.

PROOF: Set $a =$ (the left integer multiplication of $\mathbb{F}_{\mathbb{Q}}$)$\restriction(\mathbb{Z} \times \mathbb{Z})$. For every object z such that $z \in \operatorname{dom} a$ holds $a(z) =$ (the left integer multiplication of $\mathbb{Z}^{\mathrm{R}}$)(z) by [5, (49)], [13, (15)], [12, (14)]. □

(5) $\langle$the carrier of $\mathbb{Z}^{\mathrm{R}}$, the addition of $\mathbb{Z}^{\mathrm{R}}$, the zero of $\mathbb{Z}^{\mathrm{R}}$, the left integer multiplication of $\mathbb{Z}^{\mathrm{R}}\rangle$ is a submodule of $\mathbb{Z}$-module$\mathbb{Q}$. The theorem is a consequence of (4).

(6) Let us consider a divisible $\mathbb{Z}$-module V, and a submodule W of V. Then $\mathbb{Z}$-ModuleQuot(V, W) is divisible.

Let us note that there exists a divisible $\mathbb{Z}$-module which is non trivial.

Now we state the proposition:

(7) Let us consider a $\mathbb{Z}$-module V. Then V is divisible if and only if Ω_V is divisible.

Let us consider a $\mathbb{Z}$-module V and a vector v of V. Now we state the propositions:

(8) If v is not torsion, then $\operatorname{Lin}(\{v\})$ is not divisible.

(9) If v is torsion and $v \neq 0_V$, then $\operatorname{Lin}(\{v\})$ is not divisible.

Let V be a non trivial $\mathbb{Z}$-module and v be a non zero vector of V. Observe that $\operatorname{Lin}(\{v\})$ is non divisible and there exists a submodule of V which is non divisible.

Now we state the propositions:

(10) Every non trivial, finitely generated, torsion-free $\mathbb{Z}$-module is not divisible.

Proof: Consider I being a finite subset of V such that I is a basis of V. Consider v being an object such that $v \in I$. v is not divisible by [9, (92)], [12, (19)], [19, (15)], [9, (9)]. $\square$

(11) Let us consider a non trivial, finitely generated, torsion $\mathbb{Z}$-module V. Then there exists an element i of $\mathbb{Z}^{\mathrm{R}}$ such that

(i) $i \neq 0$, and

(ii) for every vector v of V, $i \cdot v = 0_V$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite subset I of V such that $\overline{\overline{I}} = \$_1$ there exists an element i of $\mathbb{Z}^{\mathrm{R}}$ such that $i \neq 0$ and for every vector v of V such that $v \in \mathrm{Lin}(I)$ holds $i \cdot v = 0_V$. $\mathcal{P}[0]$ by [10, (67)], [9, (1)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [7, (40)], [10, (72)], [1, (44)], [7, (31)]. For every natural number n, $\mathcal{P}[n]$ from [2, Sch. 2]. Consider I being a finite subset of V such that $\mathrm{Lin}(I) =$ the vector space structure of V. Consider i being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $i \neq 0$ and for every vector v of V such that $v \in \mathrm{Lin}(I)$ holds $i \cdot v = 0_V$. For every vector v of V, $i \cdot v = 0_V$. $\square$

(12) Let us consider a non trivial, finitely generated, torsion $\mathbb{Z}$-module V, and an element i of $\mathbb{Z}^{\mathrm{R}}$. Suppose $i \neq 0$ and for every vector v of V, $i \cdot v = 0_V$. Then V is not divisible.

(13) Every non trivial, finitely generated, torsion $\mathbb{Z}$-module is not divisible. The theorem is a consequence of (11) and (12).

One can verify that there exists a non trivial, finitely generated, torsion $\mathbb{Z}$-module which is non divisible.

Now we state the proposition:

(14) Every non trivial, finitely generated $\mathbb{Z}$-module is not divisible. The theorem is a consequence of (13), (6), and (10).

Let us note that every non trivial, divisible $\mathbb{Z}$-module is non finitely generated.

Let V be a non trivial, non divisible $\mathbb{Z}$-module. One can verify that there exists a non zero vector of V which is non divisible.

Let V be a non trivial, finite rank, free $\mathbb{Z}$-module. Observe that $\operatorname{rank} V$ is non zero.

Now we state the propositions:

(15) Let us consider a non trivial, free $\mathbb{Z}$-module V, a non zero vector v of V, and a basis I of V. Then there exists a linear combination L of I and there exists a vector u of V such that $v = \sum L$ and $u \in I$ and $L(u) \neq 0$.
Proof: Consider L being a linear combination of I such that $v = \sum L$. The support of $L \neq \emptyset$ by [10, (23)]. Consider u_1 being an object such that

$u_1 \in$ the support of L. Consider u being a vector of V such that $u = u_1$ and $L(u) \neq 0$. □

(16) Let us consider a non trivial, free $\mathbb{Z}$-module V. Then every non zero vector of V is not divisible. The theorem is a consequence of (15).

Let us observe that every non trivial, free $\mathbb{Z}$-module is non divisible.

Let us consider a non trivial, free $\mathbb{Z}$-module V and a non zero vector v of V. Now we state the propositions:

(17) There exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that

(i) $a \in \mathbb{N}$, and

(ii) for every element b of $\mathbb{Z}^{\mathrm{R}}$ and for every vector u of V such that $b > a$ holds $v \neq b \cdot u$.

PROOF: Set $I =$ the basis of V. Consider L being a linear combination of I, w being a vector of V such that $v = \sum L$ and $w \in I$ and $L(w) \neq 0$. Reconsider $a = |L(w)|$ as an element of $\mathbb{Z}^{\mathrm{R}}$. For every element b of $\mathbb{Z}^{\mathrm{R}}$ and for every vector u of V such that $b > a$ holds $v \neq b \cdot u$ by [10, (64), (31), (53)], [11, (3)]. □

(18) There exists an element a of $\mathbb{Z}^{\mathrm{R}}$ and there exists a vector u of V such that $a \in \mathbb{N}$ and $a \neq 0$ and $v = a \cdot u$ and for every element b of $\mathbb{Z}^{\mathrm{R}}$ and for every vector w of V such that $b > a$ holds $v \neq b \cdot w$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ there exists a vector u of V and there exists an element k of $\mathbb{Z}^{\mathrm{R}}$ such that $k = \$_1$ and $v = k \cdot u$. Consider a being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $a \in \mathbb{N}$ and for every element b of $\mathbb{Z}^{\mathrm{R}}$ and for every vector u of V such that $b > a$ holds $v \neq b \cdot u$. There exists a natural number k such that $\mathcal{P}[k]$. Consider a_0 being a natural number such that $\mathcal{P}[a_0]$ and for every natural number n such that $\mathcal{P}[n]$ holds $n \leqslant a_0$ from [2, Sch. 6]. Reconsider $a = a_0$ as an element of $\mathbb{Z}^{\mathrm{R}}$. Consider u being a vector of V such that $v = a \cdot u$. $a \neq 0$ by [9, (1)]. For every element b of $\mathbb{Z}^{\mathrm{R}}$ and for every vector w of V such that $b > a$ holds $v \neq b \cdot w$ by [18, (3)]. □

2. Divisible Module for Torsion-free $\mathbb{Z}$-module

Let V be a torsion-free $\mathbb{Z}$-module. The functor Embedding(V) yielding a strict $\mathbb{Z}$-module is defined by

(Def. 3) the carrier of $it = \operatorname{rng} \mathrm{MorphsZQ}(V)$ and the zero of $it = \mathrm{zeroCoset}(V)$ and the addition of $it = \mathrm{addCoset}(V) \restriction \operatorname{rng} \mathrm{MorphsZQ}(V)$ and the left multiplication of $it = \mathrm{lmultCoset}(V) \restriction (\mathbb{Z} \times \operatorname{rng} \mathrm{MorphsZQ}(V))$.

Let us consider a torsion-free $\mathbb{Z}$-module V. Now we state the propositions:

(19) (i) every vector of Embedding(V) is a vector of $\mathbb{Z}$-MQVectSp(V), and

(ii) $0_{\mathrm{Embedding}(V)} = 0_{\mathbb{Z}\text{-}\mathrm{MQVectSp}(V)}$, and

(iii) for every vectors x, y of Embedding(V) and for every vectors v, w of $\mathbb{Z}$-MQVectSp(V) such that $x = v$ and $y = w$ holds $x + y = v + w$, and

(iv) for every element i of $\mathbb{Z}^{\mathrm{R}}$ and for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector x of Embedding(V) and for every vector v of $\mathbb{Z}$-MQVectSp(V) such that $i = j$ and $x = v$ holds $i \cdot x = j \cdot v$.

PROOF: Set $Z = \mathbb{Z}$-MQVectSp(V). Set $E =$ Embedding(V). For every vectors x, y of E and for every vectors v, w of Z such that $x = v$ and $y = w$ holds $x + y = v + w$ by [5, (49)]. For every element i of $\mathbb{Z}^{\mathrm{R}}$ and for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector x of E and for every vector v of Z such that $i = j$ and $x = v$ holds $i \cdot x = j \cdot v$ by [5, (49)]. $\square$

(20) (i) for every vectors v, w of $\mathbb{Z}$-MQVectSp(V) such that $v, w \in$ Embedding(V) holds $v + w \in$ Embedding(V), and

(ii) for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector v of $\mathbb{Z}$-MQVectSp(V) such that $j \in \mathbb{Z}$ and $v \in$ Embedding(V) holds $j \cdot v \in$ Embedding(V).

The theorem is a consequence of (19).

(21) There exists a linear transformation T from V to Embedding(V) such that

(i) T is bijective, and

(ii) $T =$ MorphsZQ(V), and

(iii) for every vector v of V, $T(v) = [\langle v, 1\rangle]_{\mathrm{EQRZM}(V)}$.

The theorem is a consequence of (19).

Now we state the proposition:

(22) Let us consider a torsion-free $\mathbb{Z}$-module V, and a vector v_1 of Embedding(V). Then there exists a vector v of V such that $(\mathrm{MorphsZQ}(V))(v) = v_1$. The theorem is a consequence of (21).

Let V be a torsion-free $\mathbb{Z}$-module. The functor DivisibleMod(V) yielding a strict $\mathbb{Z}$-module is defined by

(Def. 4) the carrier of *it* = Classes EQRZM(V) and the zero of *it* = zeroCoset(V) and the addition of *it* = addCoset(V) and the left multiplication of *it* = lmultCoset$(V) \restriction (\mathbb{Z} \times \mathrm{Classes\,EQRZM}(V))$.

Now we state the proposition:

(23) Let us consider a torsion-free $\mathbb{Z}$-module V, a vector v of DivisibleMod(V), and an element a of $\mathbb{Z}^{\mathrm{R}}$. Suppose $a \neq 0$. Then there exists a vector u of DivisibleMod(V) such that $a \cdot u = v$.

PROOF: For every vector v of DivisibleMod(V) and for every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0$ there exists a vector u of DivisibleMod(V) such that $a \cdot u = v$ by [5, (49)], [7, (87)]. □

Let V be a torsion-free $\mathbb{Z}$-module. Let us observe that DivisibleMod(V) is divisible.

Now we state the proposition:

(24) Let us consider a torsion-free $\mathbb{Z}$-module V. Then Embedding(V) is a submodule of DivisibleMod(V).

PROOF: Set $E =$ Embedding(V). Set $D =$ DivisibleMod(V). For every object x such that $x \in$ the carrier of E holds $x \in$ the carrier of D by [6, (11), (5)]. The left multiplication of $E =$ (the left multiplication of D)$\restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}$) $\times$ rng MorphsZQ(V)) by [20, (74)], [7, (96)]. □

Let V be a finitely generated, torsion-free $\mathbb{Z}$-module. One can check that Embedding(V) is finitely generated.

Let V be a non trivial, torsion-free $\mathbb{Z}$-module. Observe that Embedding(V) is non trivial.

Let G be a field, V be a vector space over G, W be a subset of V, and a be an element of G. The functor $a \cdot W$ yielding a subset of V is defined by the term

(Def. 5) $\{a \cdot u$, where u is a vector of $V : u \in W\}$.

Let V be a torsion-free $\mathbb{Z}$-module and r be an element of $\mathbb{F}_{\mathbb{Q}}$. The functor Embedding(r, V) yielding a strict $\mathbb{Z}$-module is defined by

(Def. 6) the carrier of *it* $= r \cdot$rng MorphsZQ(V) and the zero of *it* $=$ zeroCoset(V) and the addition of *it* $=$ addCoset(V) $\restriction$ ($r \cdot$rng MorphsZQ(V)) and the left multiplication of *it* $=$
lmultCoset(V)$\restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}$) $\times$ ($r \cdot$ rng MorphsZQ(V))).

Let us consider a torsion-free $\mathbb{Z}$-module V and an element r of $\mathbb{F}_{\mathbb{Q}}$. Now we state the propositions:

(25) (i) every vector of Embedding(r, V) is a vector of $\mathbb{Z}$-MQVectSp(V), and

(ii) $0_{\mathrm{Embedding}(r,V)} = 0_{\mathbb{Z}\text{-MQVectSp}(V)}$, and

(iii) for every vectors x, y of Embedding(r, V) and for every vectors v, w of $\mathbb{Z}$-MQVectSp(V) such that $x = v$ and $y = w$ holds $x + y = v + w$, and

(iv) for every element i of $\mathbb{Z}^{\mathrm{R}}$ and for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector x of Embedding(r, V) and for every vector v of $\mathbb{Z}$-MQVectSp(V) such that $i = j$ and $x = v$ holds $i \cdot x = j \cdot v$.

PROOF: Set $Z = \mathbb{Z}$-MQVectSp(V). Set $E =$ Embedding(r, V). For every vectors x, y of E and for every vectors v, w of Z such that $x = v$ and

$y = w$ holds $x + y = v + w$ by [5, (49)]. For every element i of $\mathbb{Z}^{\mathrm{R}}$ and for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector x of E and for every vector v of Z such that $i = j$ and $x = v$ holds $i \cdot x = j \cdot v$ by [5, (49)]. □

(26) (i) for every vectors v, w of $\mathbb{Z}$-MQVectSp(V) such that v, $w \in$ Embedding(r, V) holds $v + w \in$ Embedding(r, V), and

(ii) for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector v of $\mathbb{Z}$-MQVectSp(V) such that $j \in \mathbb{Z}$ and $v \in$ Embedding(r, V) holds $j \cdot v \in$ Embedding(r, V).

The theorem is a consequence of (25).

(27) Suppose $r \neq 0_{\mathbb{F}_{\mathbb{Q}}}$. Then there exists a linear transformation T from Embedding(V) to Embedding(r, V) such that

(i) for every element v of $\mathbb{Z}$-MQVectSp(V) such that $v \in$ Embedding(V) holds $T(v) = r \cdot v$, and

(ii) T is bijective.

Proof: Set $Z = \mathbb{Z}$-MQVectSp(V). Define $\mathcal{F}$(vector of Z) $= r \cdot \$_1$. Consider T being a function from the carrier of Z into the carrier of Z such that for every element x of the carrier of Z, $T(x) = \mathcal{F}(x)$ from [6, Sch. 4]. Set $T_0 = T \restriction$(the carrier of Embedding(V)). For every object y, $y \in \operatorname{rng} T_0$ iff $y \in$ the carrier of Embedding(r, V) by [5, (49)]. T_0 is additive by (19), (20), [5, (49)], (25). For every element x of Embedding(V) and for every element i of $\mathbb{Z}^{\mathrm{R}}$, $T_0(i \cdot x) = i \cdot T_0(x)$ by (19), (20), [5, (49)], (25). For every element v of $\mathbb{Z}$-MQVectSp(V) such that $v \in$ Embedding(V) holds $T_0(v) = r \cdot v$ by [5, (49)]. For every objects x_1, x_2 such that x_1, $x_2 \in$ the carrier of Embedding(V) and $T_0(x_1) = T_0(x_2)$ holds $x_1 = x_2$ by [14, (20)]. □

Now we state the propositions:

(28) Let us consider a torsion-free $\mathbb{Z}$-module V, and a vector v of V. Then $[\langle v, 1\rangle]_{\mathrm{EQRZM}(V)} \in$ Embedding(V).

(29) Let us consider a torsion-free $\mathbb{Z}$-module V, and a vector v of DivisibleMod (V). Then there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that

(i) $a \neq 0$, and

(ii) $a \cdot v \in$ Embedding(V).

The theorem is a consequence of (28).

Let V be a torsion-free $\mathbb{Z}$-module. One can check that DivisibleMod(V) is torsion-free and Embedding(V) is torsion-free.

Let V be a free $\mathbb{Z}$-module. Let us note that Embedding(V) is free.

Let us consider a torsion-free $\mathbb{Z}$-module V. Now we state the propositions:

(30) (i) every vector of $\mathbb{Z}$-MQVectSp(V) is a vector of DivisibleMod(V), and

(ii) every vector of DivisibleMod(V) is a vector of $\mathbb{Z}$-MQVectSp(V), and

(iii) $0_{\mathrm{DivisibleMod}(V)} = 0_{\mathbb{Z}\text{-MQVectSp}(V)}$.

(31) (i) for every vectors x, y of DivisibleMod(V) and for every vectors v, u of $\mathbb{Z}$-MQVectSp(V) such that $x = v$ and $y = u$ holds $x+y = v+u$, and

(ii) for every vector z of DivisibleMod(V) and for every vector w of $\mathbb{Z}$-MQVectSp(V) and for every element a of $\mathbb{Z}^{\mathrm{R}}$ and for every element a_1 of $\mathbb{F}_{\mathbb{Q}}$ such that $z = w$ and $a = a_1$ holds $a \cdot z = a_1 \cdot w$, and

(iii) for every vector z of DivisibleMod(V) and for every vector w of $\mathbb{Z}$-MQVectSp(V) and for every element a_1 of $\mathbb{F}_{\mathbb{Q}}$ and for every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0$ and $a_1 = a$ and $a \cdot z = a_1 \cdot w$ holds $z = w$, and

(iv) for every vector x of DivisibleMod(V) and for every vector v of $\mathbb{Z}$-MQVectSp(V) and for every element r of $\mathbb{F}_{\mathbb{Q}}$ and for every elements m, n of $\mathbb{Z}^{\mathrm{R}}$ and for every integers m_1, n_1 such that $m = m_1$ and $n = n_1$ and $x = v$ and $r \neq 0_{\mathbb{F}_{\mathbb{Q}}}$ and $n \neq 0$ and $r = \frac{m_1}{n_1}$ there exists a vector y of DivisibleMod(V) such that $x = n \cdot y$ and $r \cdot v = m \cdot y$.

PROOF: For every vector z of DivisibleMod(V) and for every vector w of $\mathbb{Z}$-MQVectSp(V) and for every element a of $\mathbb{Z}^{\mathrm{R}}$ and for every element a_1 of $\mathbb{F}_{\mathbb{Q}}$ such that $z = w$ and $a = a_1$ holds $a \cdot z = a_1 \cdot w$ by [5, (49)], [7, (87)]. For every vector z of DivisibleMod(V) and for every vector w of $\mathbb{Z}$-MQVectSp(V) and for every element a_1 of $\mathbb{F}_{\mathbb{Q}}$ and for every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0$ and $a_1 = a$ and $a \cdot z = a_1 \cdot w$ holds $z = w$ by (30), [9, (8)], [19, (15), (21)]. For every vector x of DivisibleMod(V) and for every vector v of $\mathbb{Z}$-MQVectSp(V) and for every element r of $\mathbb{F}_{\mathbb{Q}}$ and for every elements m, n of $\mathbb{Z}^{\mathrm{R}}$ and for every integers m_1, n_1 such that $m = m_1$ and $n = n_1$ and $x = v$ and $r \neq 0_{\mathbb{F}_{\mathbb{Q}}}$ and $n \neq 0$ and $r = \frac{m_1}{n_1}$ there exists a vector y of DivisibleMod(V) such that $x = n \cdot y$ and $r \cdot v = m \cdot y$. $\square$

Now we state the proposition:

(32) Let us consider a torsion-free $\mathbb{Z}$-module V, and an element r of $\mathbb{F}_{\mathbb{Q}}$. Then Embedding(r, V) is a submodule of DivisibleMod(V). The theorem is a consequence of (25) and (30).

Let V be a finitely generated, torsion-free $\mathbb{Z}$-module and r be an element of $\mathbb{F}_{\mathbb{Q}}$. Observe that Embedding(r, V) is finitely generated.

Let V be a non trivial, torsion-free $\mathbb{Z}$-module and r be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. One can verify that Embedding(r, V) is non trivial.

Let V be a torsion-free $\mathbb{Z}$-module and r be an element of $\mathbb{F}_{\mathbb{Q}}$. Observe that Embedding(r, V) is torsion-free.

Let V be a free $\mathbb{Z}$-module and r be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. One can check that $\mathrm{Embedding}(r, V)$ is free.

Now we state the propositions:

(33) Let us consider a non trivial, free $\mathbb{Z}$-module V, and a vector v of $\mathrm{DivisibleMod}(V)$. Then there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that

(i) $a \in \mathbb{N}$, and

(ii) $a \neq 0$, and

(iii) $a \cdot v \in \mathrm{Embedding}(V)$, and

(iv) for every element b of $\mathbb{Z}^{\mathrm{R}}$ such that $b \in \mathbb{N}$ and $b < a$ and $b \neq 0$ holds $b \cdot v \notin \mathrm{Embedding}(V)$.

PROOF: Consider a_1 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $a_1 \neq 0$ and $a_1 \cdot v \in \mathrm{Embedding}(V)$. $|a_1| \cdot v \in \mathrm{Embedding}(V)$ by (24), [9, (16), (30)]. Define $\mathcal{P}[\text{natural number}] \equiv$ there exists an element n of $\mathbb{Z}^{\mathrm{R}}$ such that $n = \$_1$ and $n \in \mathbb{N}$ and $n \neq 0$ and $n \cdot v \in \mathrm{Embedding}(V)$. There exists a natural number k such that $\mathcal{P}[k]$ and for every natural number n such that $\mathcal{P}[n]$ holds $k \leqslant n$ from [2, Sch. 5]. Consider a_0 being a natural number such that $\mathcal{P}[a_0]$ and for every natural number b_0 such that $\mathcal{P}[b_0]$ holds $a_0 \leqslant b_0$. $\square$

(34) Let us consider a finite rank, free $\mathbb{Z}$-module V. Then $\mathrm{rank}\,\mathrm{Embedding}(V) = \mathrm{rank}\,V$. The theorem is a consequence of (21).

Let us consider a finite rank, free $\mathbb{Z}$-module V and a non zero element r of $\mathbb{F}_{\mathbb{Q}}$. Now we state the propositions:

(35) $\mathrm{rank}\,\mathrm{Embedding}(r, V) = \mathrm{rank}\,\mathrm{Embedding}(V)$. The theorem is a consequence of (27).

(36) $\mathrm{rank}\,\mathrm{Embedding}(r, V) = \mathrm{rank}\,V$. The theorem is a consequence of (35) and (34).

Observe that every non trivial, torsion-free $\mathbb{Z}$-module is infinite.

Now we state the propositions:

(37) Let us consider a $\mathbb{Z}$-module V. Then there exists a subset A of V such that

(i) A is linearly independent, and

(ii) for every vector v of V, there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \in \mathbb{N}$ and $a > 0$ and $a \cdot v \in \mathrm{Lin}(A)$.

PROOF: Consider A being a subset of V such that $\emptyset \subseteq A$ and A is linearly independent and for every vector v of V, there exists an element a_1 of $\mathbb{Z}^{\mathrm{R}}$ such that $a_1 \neq 0$ and $a_1 \cdot v \in \mathrm{Lin}(A)$. For every vector v of V, there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \in \mathbb{N}$ and $a > 0$ and $a \cdot v \in \mathrm{Lin}(A)$ by [17, (2)], [4, (46)], [18, (3)], [9, (16), (38)]. □

(38) Let us consider a non trivial, torsion-free $\mathbb{Z}$-module V, a non zero vector v of V, a subset A of V, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Suppose $a \in \mathbb{N}$ and A is linearly independent and $a > 0$ and $a \cdot v \in \mathrm{Lin}(A)$. Then there exists a linear combination L of A and there exists a vector u of V such that $a \cdot v = \sum L$ and $u \in A$ and $L(u) \neq 0$.

Proof: Consider L being a linear combination of A such that $a \cdot v = \sum L$. The support of $L \neq \emptyset$ by [10, (23)]. Consider u_1 being an object such that $u_1 \in$ the support of L. Consider u being a vector of V such that $u = u_1$ and $L(u) \neq 0$. □

(39) Let us consider a torsion-free $\mathbb{Z}$-module V, a non zero integer i, and non zero elements r_1, r_2 of $\mathbb{F}_{\mathbb{Q}}$. Suppose $r_2 = \frac{r_1}{i}$. Then $\mathrm{Embedding}(r_1, V)$ is a submodule of $\mathrm{Embedding}(r_2, V)$.

Proof: For every vector x of $\mathrm{DivisibleMod}(V)$ such that $x \in \mathrm{Embedding}(r_1, V)$ holds $x \in \mathrm{Embedding}(r_2, V)$ by (27), [6, (11)], (19), [6, (5)]. $\mathrm{Embedding}(r_1, V)$ is a submodule of $\mathrm{DivisibleMod}(V)$ and $\mathrm{Embedding}(r_2, V)$ is a submodule of $\mathrm{DivisibleMod}(V)$. □

(40) Let us consider a finite rank, free $\mathbb{Z}$-module V, and a submodule Z of $\mathrm{DivisibleMod}(V)$. Then Z is finitely generated if and only if there exists a non zero element r of $\mathbb{F}_{\mathbb{Q}}$ such that Z is a submodule of $\mathrm{Embedding}(r, V)$. The theorem is a consequence of (32), (29), (19), (27), (31), and (39).

References

[1] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.

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

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

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

[8] Wolfgang Ebeling. *Lattices and Codes.* Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.

[9] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.

[10] 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.

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

[12] Yuichi Futa, Hiroyuki Okazaki, Kazuhisa Nakasho, and Yasunari Shidama. Torsion $\mathbb{Z}$-module and torsion-free $\mathbb{Z}$-module. *Formalized Mathematics*, 22(**4**):277–289, 2014. doi:10.2478/forma-2014-0028.

[13] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Torsion part of $\mathbb{Z}$-module. *Formalized Mathematics*, 23(**4**):297–307, 2015. doi:10.1515/forma-2015-0024.

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

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

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

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

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

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

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

Received December 30, 2015

FORMALIZED MATHEMATICS
Vol. 24, No. 1, Pages 49–68, 2016
DOI: 10.1515/forma-2016-0005

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

Lattice of $\mathbb{Z}$-module

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

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize the definition of lattice of $\mathbb{Z}$-module and its properties in the Mizar system [5]. We formally prove that scalar products in lattices are bilinear forms over the field of real numbers $\mathbb{R}$. We also formalize the definitions of positive definite and integral lattices and their properties. Lattice of $\mathbb{Z}$-module is necessary for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm [14], and cryptographic systems with lattices [15] and coding theory [9].

MSC: 15A03 15A63 11E39 03B35

Keywords: $\mathbb{Z}$-lattice; Gram matrix; integral $\mathbb{Z}$-lattice; positive definite $\mathbb{Z}$-lattice

MML identifier: ZMODLAT1, version: 8.1.04 5.36.1267

1. Definition of Lattices of $\mathbb{Z}$-module

Now we state the proposition:

(1) Let us consider non empty sets D, E, natural numbers n, m, and a matrix M over D of dimension $n \times m$. Suppose for every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of M holds $M_{i,j} \in E$. Then M is a matrix over E of dimension $n \times m$.

Let a, b be elements of $\mathbb{F}_{\mathbb{Q}}$ and x, y be rational numbers. We identify $x + y$ with $a + b$ and $x \cdot y$ with $a \cdot b$. Let F be a 1-sorted structure. We consider structures of $\mathbb{Z}$-lattice over F which extend vector space structures over F and are systems

$$\langle \text{a carrier, an addition, a zero, a left multiplication,}$$

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

a scalar product$\rangle$

where the carrier is a set, the addition is a binary operation on the carrier, the zero is an element of the carrier, the left multiplication is a function from (the carrier of F) $\times$ (the carrier) into the carrier, the scalar product is a function from (the carrier) $\times$ (the carrier) into the carrier of $\mathbb{R}_{\mathrm{F}}$.

Note that there exists a structure of $\mathbb{Z}$-lattice over F which is strict and non empty.

Let D be a non empty set, Z be an element of D, a be a binary operation on D, m be a function from (the carrier of F) $\times$ D into D, and s be a function from $D \times D$ into the carrier of $\mathbb{R}_{\mathrm{F}}$. One can check that $\langle D, a, Z, m, s\rangle$ is non empty.

Let X be a non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ and x, y be vectors of X. The functor $\langle x,\, y\rangle$ yielding an element of $\mathbb{R}_{\mathrm{F}}$ is defined by the term

(Def. 1) (the scalar product of X)$(\langle x,\, y\rangle)$.

Let x be a vector of X. The functor $\|x\|$ yielding an element of $\mathbb{R}_{\mathrm{F}}$ is defined by the term

(Def. 2) $\langle x,\, x\rangle$.

Let X be a non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$. We say that X is $\mathbb{Z}$-lattice-like if and only if

(Def. 3) for every vector x of X such that for every vector y of X, $\langle x, y\rangle = 0$ holds $x = 0_X$ and for every vectors x, y of X, $\langle x, y\rangle = \langle y, x\rangle$ and for every vectors x, y, z of X and for every element a of $\mathbb{Z}^{\mathrm{R}}$, $\langle x+y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$ and $\langle a \cdot x, y\rangle = a \cdot \langle x, y\rangle$.

Let V be a $\mathbb{Z}$-module and s be a function from (the carrier of V)$\times$(the carrier of V) into the carrier of $\mathbb{R}_{\mathrm{F}}$. The functor $\mathrm{GenLat}(V, s)$ yielding a non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ is defined by the term

(Def. 4) $\langle$the carrier of V, the addition of V, 0_V, the left multiplication of V, $s\rangle$.

Let us note that there exists a non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ which is vector distributive, scalar distributive, scalar associative, scalar unital, Abelian, add-associative, right zeroed, right complementable, and strict.

Let V be a $\mathbb{Z}$-module and s be a function from (the carrier of V)$\times$(the carrier of V) into the carrier of $\mathbb{R}_{\mathrm{F}}$. One can verify that $\mathrm{GenLat}(V, s)$ is Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, and scalar unital.

Let us consider a $\mathbb{Z}$-module V and a function s from (the carrier of V) $\times$ (the carrier of V) into the carrier of $\mathbb{R}_{\mathrm{F}}$. Now we state the propositions:

(2) $\mathrm{GenLat}(V, s)$ is a submodule of V.

(3) V is a submodule of $\mathrm{GenLat}(V, s)$.

Note that there exists an Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ which is free.

Let V be a free $\mathbb{Z}$-module and s be a function from (the carrier of V) $\times$ (the carrier of V) into the carrier of $\mathbb{R}_{\mathrm{F}}$. Let us observe that $\mathrm{GenLat}(V, s)$ is free and there exists an Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ which is torsion-free.

Now we state the proposition:

(4) Let us consider a finite rank, free $\mathbb{Z}$-module V, and a function s from (the carrier of V) $\times$ (the carrier of V) into the carrier of $\mathbb{R}_{\mathrm{F}}$.
Then $\mathrm{GenLat}(V, s)$ is finite rank. The theorem is a consequence of (2).

Let us note that there exists a free, Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ which is finite rank.

Let V be a finite rank, free $\mathbb{Z}$-module and s be a function from (the carrier of V) $\times$ (the carrier of V) into the carrier of $\mathbb{R}_{\mathrm{F}}$. Let us note that $\mathrm{GenLat}(V, s)$ is finite rank.

Now we state the proposition:

(5) Let us consider a finite rank, free $\mathbb{Z}$-module V, and a function f from (the carrier of $\mathbf{0}_V$) $\times$ (the carrier of $\mathbf{0}_V$) into the carrier of $\mathbb{R}_{\mathrm{F}}$. Suppose $f =$ (the carrier of $\mathbf{0}_V$) $\times$ (the carrier of $\mathbf{0}_V$) $\longmapsto 0_{\mathbb{R}_{\mathrm{F}}}$. Then $\mathrm{GenLat}(\mathbf{0}_V, f)$ is $\mathbb{Z}$-lattice-like.

Proof: Set $X = \mathrm{GenLat}(\mathbf{0}_V, f)$. For every vector x of X such that for every vector y of X, $\langle x, y \rangle = 0$ holds $x = 0_X$ by [10, (26)]. For every vectors x, y, z of X and for every element a of $\mathbb{Z}^{\mathrm{R}}$, $\langle x, y \rangle = \langle y, x \rangle$ and $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$ and $\langle a \cdot x, y \rangle = a \cdot \langle x, y \rangle$ by [16, (7)], [8, (87)]. $\square$

Note that there exists a non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ which is $\mathbb{Z}$-lattice-like and there exists a finite rank, free, Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ which is $\mathbb{Z}$-lattice-like.

There exists a finite rank, free, $\mathbb{Z}$-lattice-like, Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ which is strict.

A $\mathbb{Z}$-lattice is a finite rank, free, $\mathbb{Z}$-lattice-like, Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$. Now we state the proposition:

(6) Let us consider a non trivial, torsion-free $\mathbb{Z}$-module V, a submodule Z of V, a non zero vector v of V, and a function f from (the carrier of Z) $\times$ (the carrier of Z) into the carrier of $\mathbb{R}_{\mathrm{F}}$. Suppose $Z = \mathrm{Lin}(\{v\})$ and for every vectors v_1, v_2 of Z and for every elements a, b of $\mathbb{Z}^{\mathrm{R}}$ such that $v_1 = a \cdot v$ and $v_2 = b \cdot v$ holds $f(v_1, v_2) = a \cdot b$. Then $\mathrm{GenLat}(Z, f)$ is $\mathbb{Z}$-lattice-like.

PROOF: Set $L = \mathrm{GenLat}(Z, f)$. L is $\mathbb{Z}$-lattice-like by [10, (26)], [12, (19)], [10, (1)], [12, (21)]. $\square$

Observe that there exists a $\mathbb{Z}$-lattice which is non trivial.

Let V be a torsion-free $\mathbb{Z}$-module. Let us observe that $\mathbb{Z}$-MQVectSp(V) is scalar distributive, vector distributive, scalar associative, scalar unital, add-associative, right zeroed, right complementable, and Abelian as a non empty vector space structure over $\mathbb{F}_{\mathbb{Q}}$.

Now we state the propositions:

(7) Let us consider a $\mathbb{Z}$-lattice L, and vectors v, u of L. Then

(i) $\langle v, -u \rangle = -\langle v, u \rangle$, and

(ii) $\langle -v, u \rangle = -\langle v, u \rangle$.

(8) Let us consider a $\mathbb{Z}$-lattice L, and vectors v, u, w of L. Then $\langle v, u+w \rangle = \langle v, u \rangle + \langle v, w \rangle$.

(9) Let us consider a $\mathbb{Z}$-lattice L, vectors v, u of L, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Then $\langle v, a \cdot u \rangle = a \cdot \langle v, u \rangle$.

(10) Let us consider a $\mathbb{Z}$-lattice L, vectors v, u, w of L, and elements a, b of $\mathbb{Z}^{\mathrm{R}}$. Then

(i) $\langle a \cdot v + b \cdot u, w \rangle = a \cdot \langle v, w \rangle + b \cdot \langle u, w \rangle$, and

(ii) $\langle v, a \cdot u + b \cdot w \rangle = a \cdot \langle v, u \rangle + b \cdot \langle v, w \rangle$.

The theorem is a consequence of (8) and (9).

(11) Let us consider a $\mathbb{Z}$-lattice L, and vectors v, u, w of L. Then

(i) $\langle v - u, w \rangle = \langle v, w \rangle - \langle u, w \rangle$, and

(ii) $\langle v, u - w \rangle = \langle v, u \rangle - \langle v, w \rangle$.

The theorem is a consequence of (8) and (9).

(12) Let us consider a $\mathbb{Z}$-lattice L, and a vector v of L. Then

(i) $\langle v, 0_L \rangle = 0$, and

(ii) $\langle 0_L, v \rangle = 0$.

The theorem is a consequence of (11).

Let X be a $\mathbb{Z}$-lattice. We say that X is integral if and only if

(Def. 5) for every vectors v, u of X, $\langle v, u\rangle \in \mathbb{Z}$.

Observe that there exists a $\mathbb{Z}$-lattice which is integral.

Let L be an integral $\mathbb{Z}$-lattice and v, u be vectors of L. Let us observe that $\langle v,\ u\rangle$is integer.

Let v be a vector of L. Let us note that $\|v\|$ is integer.

Now we state the propositions:

(13) 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 $\langle v, u\rangle \in \mathbb{Z}$. Let us consider a vector v of L. If $v \in \mathrm{Lin}(I)$, then $\langle v, u\rangle \in \mathbb{Z}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ 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 $\langle v, u\rangle \in \mathbb{Z}$ for every vector v of L such that $v \in \mathrm{Lin}(I)$ holds $\langle v, u\rangle \in \mathbb{Z}$. $\mathcal{P}[0]$ by [11, (67)], (12). For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [8, (40)], [11, (72)], [1, (44)], [8, (31)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(14) 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 $\langle v, u\rangle \in \mathbb{Z}$. Let us consider vectors v, u of L. Then $\langle v, u\rangle \in \mathbb{Z}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ 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 $\langle v, u\rangle \in \mathbb{Z}$ for every vectors v, u of L such that v, $u \in \mathrm{Lin}(I)$ holds $\langle v, u\rangle \in \mathbb{Z}$. $\mathcal{P}[0]$ by [11, (67)], (12). For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [8, (40)], [11, (72)], [1, (44)], [8, (31)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(15) 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 $\langle v, u\rangle \in \mathbb{Z}$. Then L is integral.

Let X be a $\mathbb{Z}$-lattice. We say that X is positive definite if and only if

(Def. 6) for every vector v of X such that $v \neq 0_X$ holds $\|v\| > 0$.

Let us observe that there exists a $\mathbb{Z}$-lattice which is non trivial, integral, and positive definite.

Let us consider a positive definite $\mathbb{Z}$-lattice L and a vector v of L. Now we state the propositions:

(16) $\|v\| = 0$ if and only if $v = 0_L$.

(17) $\|v\| \geqslant 0$. The theorem is a consequence of (12).

Let X be an integral $\mathbb{Z}$-lattice. We say that X is even if and only if

(Def. 7) for every vector v of X, $\|v\|$ is even.

One can verify that there exists an integral $\mathbb{Z}$-lattice which is even.

Let L be a $\mathbb{Z}$-lattice. We introduce the notation $\dim(L)$ as a synonym of $\operatorname{rank} L$.

Let v, u be vectors of L. We say that v, u are orthogonal if and only if

(Def. 8) $\langle v, u\rangle = 0$.

Let us note that the predicate is symmetric.

Let us consider a $\mathbb{Z}$-lattice L and vectors v, u of L.

Let us assume that v, u are orthogonal. Now we state the propositions:

(18) (i) v, $-u$ are orthogonal, and

(ii) $-v$, u are orthogonal, and

(iii) $-v$, $-u$ are orthogonal.

The theorem is a consequence of (7).

(19) $\|v + u\| = \|v\| + \|u\|$. The theorem is a consequence of (8).

(20) $\|v - u\| = \|v\| + \|u\|$. The theorem is a consequence of (11).

Let L be a $\mathbb{Z}$-lattice.

A $\mathbb{Z}$-sublattice of L is a $\mathbb{Z}$-lattice and is defined by

(Def. 9) the carrier of *it* $\subseteq$ the carrier of L and $0_{it} = 0_L$ and the addition of *it* = (the addition of L) $\restriction$ (the carrier of *it*) and the left multiplication of *it* = (the left multiplication of L)$\restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}$) $\times$ (the carrier of *it*)) and the scalar product of *it* = (the scalar product of L) $\restriction$ (the carrier of *it*).

Now we state the propositions:

(21) Let us consider a $\mathbb{Z}$-lattice L. Then every $\mathbb{Z}$-sublattice of L is a submodule of L.

(22) Let us consider an object x, a $\mathbb{Z}$-lattice L, and $\mathbb{Z}$-sublattices L_1, L_2 of L. Suppose $x \in L_1$ and L_1 is a $\mathbb{Z}$-sublattice of L_2. Then $x \in L_2$. The theorem is a consequence of (21).

(23) Let us consider an object x, a $\mathbb{Z}$-lattice L, and a $\mathbb{Z}$-sublattice L_1 of L. If $x \in L_1$, then $x \in L$. The theorem is a consequence of (21).

(24) Let us consider a $\mathbb{Z}$-lattice L, and a $\mathbb{Z}$-sublattice L_1 of L. Then every vector of L_1 is a vector of L. The theorem is a consequence of (21).

(25) Let us consider a $\mathbb{Z}$-lattice L, and $\mathbb{Z}$-sublattices L_1, L_2 of L. Then $0_{L_1} = 0_{L_2}$.

(26) Let us consider a $\mathbb{Z}$-lattice L, a $\mathbb{Z}$-sublattice L_1 of L, vectors v_1, v_2 of L, and vectors w_1, w_2 of L_1. If $w_1 = v_1$ and $w_2 = v_2$, then $w_1 + w_2 = v_1 + v_2$. The theorem is a consequence of (21).

(27) Let us consider a $\mathbb{Z}$-lattice L, a $\mathbb{Z}$-sublattice L_1 of L, a vector v of L, a vector w of L_1, and an element a of $\mathbb{Z}^{\mathrm{R}}$. If $w = v$, then $a \cdot w = a \cdot v$. The theorem is a consequence of (21).

(28) Let us consider a $\mathbb{Z}$-lattice L, a $\mathbb{Z}$-sublattice L_1 of L, a vector v of L, and a vector w of L_1. If $w = v$, then $-w = -v$. The theorem is a consequence of (21).

(29) Let us consider a $\mathbb{Z}$-lattice L, a $\mathbb{Z}$-sublattice L_1 of L, vectors v_1, v_2 of L, and vectors w_1, w_2 of L_1. If $w_1 = v_1$ and $w_2 = v_2$, then $w_1 - w_2 = v_1 - v_2$. The theorem is a consequence of (21).

(30) Let us consider a $\mathbb{Z}$-lattice L, and a $\mathbb{Z}$-sublattice L_1 of L. Then $0_L \in L_1$. The theorem is a consequence of (21).

(31) Let us consider a $\mathbb{Z}$-lattice L, and $\mathbb{Z}$-sublattices L_1, L_2 of L. Then $0_{L_1} \in L_2$. The theorem is a consequence of (21).

(32) Let us consider a $\mathbb{Z}$-lattice L, and a $\mathbb{Z}$-sublattice L_1 of L. Then $0_{L_1} \in L$. The theorem is a consequence of (21).

(33) Let us consider a $\mathbb{Z}$-lattice L, a $\mathbb{Z}$-sublattice L_1 of L, and vectors v_1, v_2 of L. If v_1, $v_2 \in L_1$, then $v_1 + v_2 \in L_1$. The theorem is a consequence of (21).

(34) Let us consider a $\mathbb{Z}$-lattice L, a $\mathbb{Z}$-sublattice L_1 of L, a vector v of L, and an element a of $\mathbb{Z}^{\mathrm{R}}$. If $v \in L_1$, then $a \cdot v \in L_1$. The theorem is a consequence of (21).

(35) Let us consider a $\mathbb{Z}$-lattice L, a $\mathbb{Z}$-sublattice L_1 of L, and a vector v of L. If $v \in L_1$, then $-v \in L_1$. The theorem is a consequence of (21).

(36) Let us consider a $\mathbb{Z}$-lattice L, a $\mathbb{Z}$-sublattice L_1 of L, and vectors v_1, v_2 of L. If v_1, $v_2 \in L_1$, then $v_1 - v_2 \in L_1$. The theorem is a consequence of (21).

(37) Let us consider a positive definite $\mathbb{Z}$-lattice L, a non empty set A, an element z of A, a binary operation a on A, a function m from (the carrier of $\mathbb{Z}^{\mathrm{R}}) \times A$ into A, and a function s from $A \times A$ into the carrier of $\mathbb{R}_{\mathrm{F}}$. Suppose A is a linearly closed subset of L and $z = 0_L$ and $a =$ (the addition of $L) \restriction A$ and $m =$ (the left multiplication of $L) \restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}) \times A$) and $s =$ (the scalar product of $L) \restriction A$. Then $\langle A, a, z, m, s \rangle$ is a $\mathbb{Z}$-sublattice of L.

PROOF: Set $L_1 = \langle A, a, z, m, s \rangle$. Set $V_1 = \langle A, a, z, m \rangle$. L_1 is a submodule of V_1. L_1 is $\mathbb{Z}$-lattice-like by [10, (25)], [7, (49)], [10, (28), (29)]. $\square$

(38) Let us consider a $\mathbb{Z}$-lattice L, a $\mathbb{Z}$-sublattice L_1 of L, vectors w_1, w_2 of L_1, and vectors v_1, v_2 of L. Suppose $w_1 = v_1$ and $w_2 = v_2$. Then $\langle w_1, w_2 \rangle = \langle v_1, v_2 \rangle$.

Let L be an integral $\mathbb{Z}$-lattice. Note that every $\mathbb{Z}$-sublattice of L is integral.

Let L be a positive definite $\mathbb{Z}$-lattice. Let us observe that every $\mathbb{Z}$-sublattice of L is positive definite.

Let V, W be vector space structures over $\mathbb{Z}^{\mathrm{R}}$.

An $\mathbb{R}$-form of V and W is a function from (the carrier of V) $\times$ (the carrier of W) into the carrier of $\mathbb{R}_{\mathrm{F}}$. The functor NulFrForm(V, W) yielding an $\mathbb{R}$-form of V and W is defined by the term

(Def. 10) (the carrier of V) $\times$ (the carrier of W) $\longmapsto 0_{\mathbb{R}_{\mathrm{F}}}$.

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathrm{R}}$ and f, g be $\mathbb{R}$-forms of V and W. The functor $f+g$ yielding an $\mathbb{R}$-form of V and W is defined by

(Def. 11) for every vector v of V and for every vector w of W, $it(v,w) = f(v,w) + g(v,w)$.

Let f be an $\mathbb{R}$-form of V and W and a be an element of $\mathbb{R}_{\mathrm{F}}$. The functor $a \cdot f$ yielding an $\mathbb{R}$-form of V and W is defined by

(Def. 12) for every vector v of V and for every vector w of W, $it(v,w) = a \cdot f(v,w)$.

The functor $-f$ yielding an $\mathbb{R}$-form of V and W is defined by

(Def. 13) for every vector v of V and for every vector w of W, $it(v,w) = -f(v,w)$.

One can verify that the functor $-f$ is defined by the term

(Def. 14) $(-1_{\mathbb{R}_{\mathrm{F}}}) \cdot f$.

Let f, g be $\mathbb{R}$-forms of V and W. The functor $f-g$ yielding an $\mathbb{R}$-form of V and W is defined by the term

(Def. 15) $f + -g$.

Observe that the functor $f-g$ is defined by

(Def. 16) for every vector v of V and for every vector w of W, $it(v,w) = f(v,w) - g(v,w)$.

Let us note that the functor $f+g$ is commutative.

Now we state the propositions:

(39) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and an $\mathbb{R}$-form f of V and W. Then $f + \mathrm{NulFrForm}(V, W) = f$.

(40) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and $\mathbb{R}$-forms f, g, h of V and W. Then $(f+g)+h = f+(g+h)$.

(41) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and an $\mathbb{R}$-form f of V and W. Then $f - f = \mathrm{NulFrForm}(V, W)$.

(42) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, an element a of $\mathbb{R}_{\mathrm{F}}$, and $\mathbb{R}$-forms f, g of V and W. Then $a \cdot (f+g) = a \cdot f + a \cdot g$.

Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, elements a, b of $\mathbb{R}_{\mathrm{F}}$, and an $\mathbb{R}$-form f of V and W. Now we state the propositions:

(43) $(a+b) \cdot f = a \cdot f + b \cdot f$.

(44) $(a \cdot b) \cdot f = a \cdot (b \cdot f)$.

(45) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and an $\mathbb{R}$-form f of V and W. Then $1_{\mathbb{R}_{\mathrm{F}}} \cdot f = f$.

Let V be a vector space structure over $\mathbb{Z}^{\mathrm{R}}$.

An $\mathbb{R}$-functional of V is a function from the carrier of V into the carrier of $\mathbb{R}_{\mathrm{F}}$. Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$ and f, g be $\mathbb{R}$-functionals of V. The functor $f+g$ yielding an $\mathbb{R}$-functional of V is defined by

(Def. 17) for every element x of V, $it(x) = f(x) + g(x)$.

Let f be an $\mathbb{R}$-functional of V. The functor $-f$ yielding an $\mathbb{R}$-functional of V is defined by

(Def. 18) for every element x of V, $it(x) = -f(x)$.

Let f, g be $\mathbb{R}$-functionals of V. The functor $f-g$ yielding an $\mathbb{R}$-functional of V is defined by the term

(Def. 19) $f + -g$.

Let v be an element of $\mathbb{R}_{\mathrm{F}}$ and f be an $\mathbb{R}$-functional of V. The functor $v \cdot f$ yielding an $\mathbb{R}$-functional of V is defined by

(Def. 20) for every element x of V, $it(x) = v \cdot f(x)$.

Let V be a vector space structure over $\mathbb{Z}^{\mathrm{R}}$. The functor 0FrFunctional(V) yielding an $\mathbb{R}$-functional of V is defined by the term

(Def. 21) $\Omega_V \longmapsto 0_{\mathbb{R}_{\mathrm{F}}}$.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$ and F be an $\mathbb{R}$-functional of V. We say that F is homogeneous if and only if

(Def. 22) for every vector x of V and for every scalar r of V, $F(r \cdot x) = r \cdot F(x)$.

We say that F is 0-preserving if and only if

(Def. 23) $F(0_V) = 0_{\mathbb{R}_{\mathrm{F}}}$.

Let V be a $\mathbb{Z}$-module. Note that every $\mathbb{R}$-functional of V which is homogeneous is also 0-preserving.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$. One can verify that 0FrFunctional(V) is additive and 0FrFunctional(V) is homogeneous and 0FrFunctional(V) is 0-preserving and there exists an $\mathbb{R}$-functional of V which is additive, homogeneous, and 0-preserving.

Now we state the propositions:

(46) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathrm{R}}$, and $\mathbb{R}$-functionals f, g of V. Then $f + g = g + f$.

(47) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathrm{R}}$, and $\mathbb{R}$-functionals f, g, h of V. Then $(f+g)+h = f+(g+h)$.

(48) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathrm{R}}$, and an element x of V. Then $(0\mathrm{FrFunctional}(V))(x) = 0_{\mathbb{R}_{\mathrm{F}}}$.

Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathrm{R}}$ and an $\mathbb{R}$-functional f of V. Now we state the propositions:

(49) $f + 0\mathrm{FrFunctional}(V) = f$.

(50) $f - f = 0\mathrm{FrFunctional}(V)$.

(51) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathrm{R}}$, an element r of $\mathbb{R}_{\mathrm{F}}$, and $\mathbb{R}$-functionals f, g of V. Then $r \cdot (f+g) = r \cdot f + r \cdot g$.

Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathrm{R}}$, elements r, s of $\mathbb{R}_{\mathrm{F}}$, and an $\mathbb{R}$-functional f of V. Now we state the propositions:

(52) $(r+s) \cdot f = r \cdot f + s \cdot f$.

(53) $(r \cdot s) \cdot f = r \cdot (s \cdot f)$.

(54) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathrm{R}}$, and an $\mathbb{R}$-functional f of V. Then $1_{\mathbb{R}_{\mathrm{F}}} \cdot f = f$.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$ and f, g be additive $\mathbb{R}$-functionals of V. Observe that $f+g$ is additive.

Let f be an additive $\mathbb{R}$-functional of V. One can check that $-f$ is additive.

Let v be an element of $\mathbb{R}_{\mathrm{F}}$. Let us note that $v \cdot f$ is additive.

Let f, g be homogeneous $\mathbb{R}$-functionals of V. Let us observe that $f+g$ is homogeneous.

Let f be a homogeneous $\mathbb{R}$-functional of V. Note that $-f$ is homogeneous.

Let v be an element of $\mathbb{R}_{\mathrm{F}}$. Observe that $v \cdot f$ is homogeneous.

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathrm{R}}$, f be an $\mathbb{R}$-form of V and W, and v be a vector of V. The functor $\mathrm{FrFunctionalFAF}(f, v)$ yielding an $\mathbb{R}$-functional of W is defined by the term

(Def. 24) $(\mathrm{curry}\, f)(v)$.

Let w be a vector of W. The functor $\mathrm{FrFunctionalSAF}(f, w)$ yielding an $\mathbb{R}$-functional of V is defined by the term

(Def. 25) $(\mathrm{curry}'\, f)(w)$.

Now we state the propositions:

(55) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, an $\mathbb{R}$-form f of V and W, and a vector v of V. Then

(i) $\mathrm{dom}\, \mathrm{FrFunctionalFAF}(f, v) =$ the carrier of W, and

(ii) $\mathrm{rng}\, \mathrm{FrFunctionalFAF}(f, v) \subseteq$ the carrier of $\mathbb{R}_{\mathrm{F}}$, and

(iii) for every vector w of W, $(\mathrm{FrFunctionalFAF}(f, v))(w) = f(v, w)$.

(56) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, an $\mathbb{R}$-form f of V and W, and a vector w of W. Then

(i) $\mathrm{dom}\,\mathrm{FrFunctionalSAF}(f, w) =$ the carrier of V, and

(ii) $\mathrm{rng}\,\mathrm{FrFunctionalSAF}(f, w) \subseteq$ the carrier of $\mathbb{R}_{\rm F}$, and

(iii) for every vector v of V, $(\mathrm{FrFunctionalSAF}(f, w))(v) = f(v, w)$.

(57) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\rm R}$, and an element x of V. Then $(0\mathrm{FrFunctional}(V))(x) = 0_{\mathbb{R}_{\rm F}}$.

(58) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, and a vector v of V. Then $\mathrm{FrFunctionalFAF}(\mathrm{NulFrForm}(V, W), v) = 0\mathrm{FrFunctional}(W)$. The theorem is a consequence of (55).

(59) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, and a vector w of W. Then $\mathrm{FrFunctionalSAF}(\mathrm{NulFrForm}(V, W), w) = 0\mathrm{FrFunctional}(V)$. The theorem is a consequence of (56).

(60) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, $\mathbb{R}$-forms f, g of V and W, and a vector w of W. Then $\mathrm{FrFunctionalSAF}(f + g, w) = \mathrm{FrFunctionalSAF}(f, w) + \mathrm{FrFunctionalSAF}(g, w)$. The theorem is a consequence of (56).

(61) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, $\mathbb{R}$-forms f, g of V and W, and a vector v of V. Then $\mathrm{FrFunctionalFAF}(f + g, v) = \mathrm{FrFunctionalFAF}(f, v) + \mathrm{FrFunctionalFAF}(g, v)$. The theorem is a consequence of (55).

(62) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, an $\mathbb{R}$-form f of V and W, an element a of $\mathbb{R}_{\rm F}$, and a vector w of W. Then $\mathrm{FrFunctionalSAF}(a \cdot f, w) = a \cdot \mathrm{FrFunctionalSAF}(f, w)$. The theorem is a consequence of (56).

(63) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, an $\mathbb{R}$-form f of V and W, an element a of $\mathbb{R}_{\rm F}$, and a vector v of V. Then $\mathrm{FrFunctionalFAF}(a \cdot f, v) = a \cdot \mathrm{FrFunctionalFAF}(f, v)$. The theorem is a consequence of (55).

(64) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, an $\mathbb{R}$-form f of V and W, and a vector w of W. Then $\mathrm{FrFunctionalSAF}(-f, w) = -\mathrm{FrFunctionalSAF}(f, w)$. The theorem is a consequence of (56).

(65) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, an $\mathbb{R}$-form f of V and W, and a vector v of V. Then $\mathrm{FrFunctionalFAF}(-f, v) = -\mathrm{FrFunctionalFAF}(f, v)$. The theorem is a consequence of (55).

(66) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, $\mathbb{R}$-forms f, g of V and W, and a vector w of W. Then $\mathrm{FrFunctionalSAF}(f -$

$g, w) = \mathrm{FrFunctionalSAF}(f, w) - \mathrm{FrFunctionalSAF}(g, w)$. The theorem is a consequence of (56).

(67) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, $\mathbb{R}$-forms f, g of V and W, and a vector v of V. Then $\mathrm{FrFunctionalFAF}(f - g, v) = \mathrm{FrFunctionalFAF}(f, v) - \mathrm{FrFunctionalFAF}(g, v)$. The theorem is a consequence of (55).

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathrm{R}}$, f be an $\mathbb{R}$-functional of V, and g be an $\mathbb{R}$-functional of W. The functor $\mathrm{FrFormFunctional}(f, g)$ yielding an $\mathbb{R}$-form of V and W is defined by

(Def. 26) for every vector v of V and for every vector w of W, $it(v, w) = f(v) \cdot g(w)$.

(68) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, an $\mathbb{R}$-functional f of V, a vector v of V, and a vector w of W.
Then $(\mathrm{FrFormFunctional}(f, 0\mathrm{FrFunctional}(W)))(v, w) = 0_{\mathbb{Z}^{\mathrm{R}}}$.

(69) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, an $\mathbb{R}$-functional g of W, a vector v of V, and a vector w of W.
Then $(\mathrm{FrFormFunctional}(0\mathrm{FrFunctional}(V), g))(v, w) = 0_{\mathbb{Z}^{\mathrm{R}}}$.

(70) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and an $\mathbb{R}$-functional f of V. Then $\mathrm{FrFormFunctional}(f, 0\mathrm{FrFunctional}(W)) = \mathrm{NulFrForm}(V, W)$. The theorem is a consequence of (68).

(71) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and an $\mathbb{R}$-functional g of W. Then $\mathrm{FrFormFunctional}(0\mathrm{FrFunctional}(V), g) = \mathrm{NulFrForm}(V, W)$. The theorem is a consequence of (69).

(72) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, an $\mathbb{R}$-functional f of V, an $\mathbb{R}$-functional g of W, and a vector v of V. Then $\mathrm{FrFunctionalFAF}(\mathrm{FrFormFunctional}(f, g), v) = f(v) \cdot g$. The theorem is a consequence of (55).

(73) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, an $\mathbb{R}$-functional f of V, an $\mathbb{R}$-functional g of W, and a vector w of W. Then $\mathrm{FrFunctionalSAF}(\mathrm{FrFormFunctional}(f, g), w) = g(w) \cdot f$. The theorem is a consequence of (56).

2. Bilinear Forms over Field of Reals and Their Properties

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathrm{R}}$ and f be an $\mathbb{R}$-form of V and W. We say that f is additive w.r.t. second argument if and only if

(Def. 27) for every vector v of V, $\mathrm{FrFunctionalFAF}(f, v)$ is additive.

We say that f is additive w.r.t. first argument if and only if

(Def. 28) for every vector w of W, $\mathrm{FrFunctionalSAF}(f, w)$ is additive.

We say that f is homogeneous w.r.t. second argument if and only if

(Def. 29) for every vector v of V, $\mathrm{FrFunctionalFAF}(f, v)$ is homogeneous.

We say that f is homogeneous w.r.t. first argument if and only if

(Def. 30) for every vector w of W, $\mathrm{FrFunctionalSAF}(f, w)$ is homogeneous.

Observe that $\mathrm{NulFrForm}(V, W)$ is additive w.r.t. second argument and

$\mathrm{NulFrForm}(V, W)$ is additive w.r.t. first argument and there exists an $\mathbb{R}$-form of V and W which is additive w.r.t. second argument and additive w.r.t. first argument and $\mathrm{NulFrForm}(V, W)$ is homogeneous w.r.t. second argument and $\mathrm{NulFrForm}(V, W)$ is homogeneous w.r.t. first argument.

There exists an $\mathbb{R}$-form of V and W which is additive w.r.t. second argument, homogeneous w.r.t. second argument, additive w.r.t. first argument, and homogeneous w.r.t. first argument.

An $\mathbb{R}$-bilinear form of V and W is an additive w.r.t. first argument, homogeneous w.r.t. first argument, additive w.r.t. second argument, homogeneous w.r.t. second argument $\mathbb{R}$-form of V and W. Let f be an additive w.r.t. second argument $\mathbb{R}$-form of V and W and v be a vector of V. One can check that $\mathrm{FrFunctionalFAF}(f, v)$ is additive.

Let f be an additive w.r.t. first argument $\mathbb{R}$-form of V and W and w be a vector of W. Observe that $\mathrm{FrFunctionalSAF}(f, w)$ is additive.

Let f be a homogeneous w.r.t. second argument $\mathbb{R}$-form of V and W and v be a vector of V. One can check that $\mathrm{FrFunctionalFAF}(f, v)$ is homogeneous.

Let f be a homogeneous w.r.t. first argument $\mathbb{R}$-form of V and W and w be a vector of W. Observe that $\mathrm{FrFunctionalSAF}(f, w)$ is homogeneous.

Let f be an $\mathbb{R}$-functional of V and g be an additive $\mathbb{R}$-functional of W. Observe that $\mathrm{FrFormFunctional}(f, g)$ is additive w.r.t. second argument.

Let f be an additive $\mathbb{R}$-functional of V and g be an $\mathbb{R}$-functional of W. One can check that $\mathrm{FrFormFunctional}(f, g)$ is additive w.r.t. first argument.

Let f be an $\mathbb{R}$-functional of V and g be a homogeneous $\mathbb{R}$-functional of W. Observe that $\mathrm{FrFormFunctional}(f, g)$ is homogeneous w.r.t. second argument.

Let f be a homogeneous $\mathbb{R}$-functional of V and g be an $\mathbb{R}$-functional of W. One can check that $\mathrm{FrFormFunctional}(f, g)$ is homogeneous w.r.t. first argument.

Let V be a non trivial vector space structure over $\mathbb{Z}^{\mathrm{R}}$, W be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$, and f be an $\mathbb{R}$-functional of V. One can verify that $\mathrm{FrFormFunctional}(f, g)$ is non trivial and $\mathrm{FrFormFunctional}(f, g)$ is non trivial.

Let F be an $\mathbb{R}$-functional of V. We say that F is 0-preserving if and only if

(Def. 31) $F(0_V) = 0_{\mathbb{R}_{\mathrm{F}}}$.

Let V be a $\mathbb{Z}$-module. One can check that every $\mathbb{R}$-functional of V which is homogeneous is also 0-preserving.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$. Let us observe that $0\mathrm{FrFunctional}(V)$ is 0-preserving and there exists an $\mathbb{R}$-functional of V which is additive, homogeneous, and 0-preserving.

Let V be a non trivial, free $\mathbb{Z}$-module. Note that there exists an $\mathbb{R}$-functional of V which is additive, homogeneous, non constant, and non trivial.

(74) Let us consider a non trivial, free $\mathbb{Z}$-module V, and a non constant, 0-preserving $\mathbb{R}$-functional f of V. Then there exists a vector v of V such that

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

(ii) $f(v) \neq 0_{\mathbb{R}_{\mathrm{F}}}$.

Let V, W be non trivial, free $\mathbb{Z}$-modules, f be a non constant, 0-preserving $\mathbb{R}$-functional of V, and g be a non constant, 0-preserving $\mathbb{R}$-functional of W. Note that $\mathrm{FrFormFunctional}(f, g)$ is non constant.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$.

An $\mathbb{R}$-linear functional of V is an additive, homogeneous $\mathbb{R}$-functional of V. Let V, W be non trivial, free $\mathbb{Z}$-modules. Observe that there exists an $\mathbb{R}$-form of V and W which is non trivial, non constant, additive w.r.t. second argument, homogeneous w.r.t. second argument, additive w.r.t. first argument, and homogeneous w.r.t. first argument.

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathrm{R}}$ and f, g be additive w.r.t. first argument $\mathbb{R}$-forms of V and W. Let us observe that $f + g$ is additive w.r.t. first argument. Let f, g be additive w.r.t. second argument $\mathbb{R}$-forms of V and W. One can check that $f + g$ is additive w.r.t. second argument.

Let f be an additive w.r.t. first argument $\mathbb{R}$-form of V and W and a be an element of $\mathbb{R}_{\mathrm{F}}$. Let us observe that $a \cdot f$ is additive w.r.t. first argument.

Let f be an additive w.r.t. second argument $\mathbb{R}$-form of V and W. Note that $a \cdot f$ is additive w.r.t. second argument.

Let f be an additive w.r.t. first argument $\mathbb{R}$-form of V and W. Let us observe that $-f$ is additive w.r.t. first argument.

Let f be an additive w.r.t. second argument $\mathbb{R}$-form of V and W. Let us observe that $-f$ is additive w.r.t. second argument.

Let f, g be additive w.r.t. first argument $\mathbb{R}$-forms of V and W. Observe that $f - g$ is additive w.r.t. first argument.

Let f, g be additive w.r.t. second argument $\mathbb{R}$-forms of V and W. One can check that $f - g$ is additive w.r.t. second argument.

Let f, g be homogeneous w.r.t. first argument $\mathbb{R}$-forms of V and W. Observe that $f + g$ is homogeneous w.r.t. first argument.

Let f, g be homogeneous w.r.t. second argument $\mathbb{R}$-forms of V and W. One can verify that $f+g$ is homogeneous w.r.t. second argument.

Let f be a homogeneous w.r.t. first argument $\mathbb{R}$-form of V and W and a be an element of $\mathbb{R}_{\rm F}$. Observe that $a \cdot f$ is homogeneous w.r.t. first argument.

Let f be a homogeneous w.r.t. second argument $\mathbb{R}$-form of V and W. One can check that $a \cdot f$ is homogeneous w.r.t. second argument.

Let f be a homogeneous w.r.t. first argument $\mathbb{R}$-form of V and W. Observe that $-f$ is homogeneous w.r.t. first argument. Let f be a homogeneous w.r.t. second argument $\mathbb{R}$-form of V and W. Observe that $-f$ is homogeneous w.r.t. second argument.

Let f, g be homogeneous w.r.t. first argument $\mathbb{R}$-forms of V and W. Let us note that $f-g$ is homogeneous w.r.t. first argument.

Let f, g be homogeneous w.r.t. second argument $\mathbb{R}$-forms of V and W. One can verify that $f-g$ is homogeneous w.r.t. second argument.

(75) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, vectors v, u of V, a vector w of W, and an $\mathbb{R}$-form f of V and W. If f is additive w.r.t. first argument, then $f(v+u,w) = f(v,w)+f(u,w)$. The theorem is a consequence of (56).

(76) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, a vector v of V, vectors u, w of W, and an $\mathbb{R}$-form f of V and W. If f is additive w.r.t. second argument, then $f(v,u+w) = f(v,u)+f(v,w)$. The theorem is a consequence of (55).

(77) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, vectors v, u of V, vectors w, t of W, and an additive w.r.t. first argument, additive w.r.t. second argument $\mathbb{R}$-form f of V and W. Then $f(v+u,w+t) = f(v,w)+f(v,t)+(f(u,w)+f(u,t))$. The theorem is a consequence of (75) and (76).

(78) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, an additive w.r.t. second argument $\mathbb{R}$-form f of V and W, and a vector v of V. Then $f(v,0_W) = 0_{\mathbb{Z}^{\rm R}}$. The theorem is a consequence of (76).

(79) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, an additive w.r.t. first argument $\mathbb{R}$-form f of V and W, and a vector w of W. Then $f(0_V,w) = 0_{\mathbb{Z}^{\rm R}}$. The theorem is a consequence of (75).

Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, a vector v of V, a vector w of W, an element a of $\mathbb{Z}^{\rm R}$, and an $\mathbb{R}$-form f of V and W. Now we state the propositions:

(80) If f is homogeneous w.r.t. first argument, then $f(a \cdot v,w) = a \cdot f(v,w)$.

The theorem is a consequence of (56).

(81) If f is homogeneous w.r.t. second argument, then $f(v, a \cdot w) = a \cdot f(v, w)$. The theorem is a consequence of (55).

(82) Let us consider add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, a homogeneous w.r.t. first argument $\mathbb{R}$-form f of V and W, and a vector w of W. Then $f(0_V, w) = 0_{\mathbb{R}_{\rm F}}$. The theorem is a consequence of (80).

(83) Let us consider add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, a homogeneous w.r.t. second argument $\mathbb{R}$-form f of V and W, and a vector v of V. Then $f(v, 0_W) = 0_{\mathbb{R}_{\rm F}}$. The theorem is a consequence of (81).

(84) Let us consider $\mathbb{Z}$-modules V, W, vectors v, u of V, a vector w of W, and an additive w.r.t. first argument, homogeneous w.r.t. first argument $\mathbb{R}$-form f of V and W. Then $f(v-u, w) = f(v, w) - f(u, w)$. The theorem is a consequence of (75) and (80).

(85) Let us consider $\mathbb{Z}$-modules V, W, a vector v of V, vectors w, t of W, and an additive w.r.t. second argument, homogeneous w.r.t. second argument $\mathbb{R}$-form f of V and W. Then $f(v, w-t) = f(v, w) - f(v, t)$. The theorem is a consequence of (76) and (81).

(86) Let us consider $\mathbb{Z}$-modules V, W, vectors v, u of V, vectors w, t of W, and an $\mathbb{R}$-bilinear form f of V and W. Then $f(v-u, w-t) = f(v, w) - f(v, t) - (f(u, w) - f(u, t))$. The theorem is a consequence of (84) and (85).

(87) Let us consider add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, vectors v, u of V, vectors w, t of W, elements a, b of $\mathbb{Z}^{\rm R}$, and an $\mathbb{R}$-bilinear form f of V and W. Then $f(v+a \cdot u, w+b \cdot t) = f(v, w) + b \cdot f(v, t) + (a \cdot f(u, w) + a \cdot (b \cdot f(u, t)))$. The theorem is a consequence of (77), (81), and (80).

(88) Let us consider $\mathbb{Z}$-modules V, W, vectors v, u of V, vectors w, t of W, elements a, b of $\mathbb{Z}^{\rm R}$, and an $\mathbb{R}$-bilinear form f of V and W. Then $f(v - a \cdot u, w - b \cdot t) = f(v, w) - b \cdot f(v, t) - (a \cdot f(u, w) - a \cdot (b \cdot f(u, t)))$. The theorem is a consequence of (86), (81), and (80).

(89) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\rm R}$, and an $\mathbb{R}$-form f of V and W. Suppose f is additive w.r.t. second argument or additive w.r.t. first argument. Then f is constant if and only if for every vector v of V and for every vector w of W, $f(v, w) = 0_{\mathbb{Z}^{\rm R}}$. The theorem is a consequence of (78) and (79).

3. Matrices of Bilinear Form over Field of Real Numbers

Let V_1, V_2 be finite rank, free $\mathbb{Z}$-modules, b_1 be an ordered basis of V_1, b_2 be an ordered basis of V_2, and f be an $\mathbb{R}$-bilinear form of V_1 and V_2. The functor $\mathrm{Bilinear}(f, b_1, b_2)$ yielding a matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension $\mathrm{len}\, b_1 \times \mathrm{len}\, b_2$ is defined by

(Def. 32) for every natural numbers i, j such that $i \in \mathrm{dom}\, b_1$ and $j \in \mathrm{dom}\, b_2$ holds $it_{i,j} = f({b_1}_i, {b_2}_j)$.

Now we state the propositions:

(90) Let us consider a finite rank, free $\mathbb{Z}$-module V, an $\mathbb{R}$-linear functional F of V, a finite sequence y of elements of V, a finite sequence x of elements of $\mathbb{Z}^{\mathrm{R}}$, and finite sequences X, Y of elements of $\mathbb{R}_{\mathrm{F}}$. Suppose $X = x$ and $\mathrm{len}\, y = \mathrm{len}\, x$ and $\mathrm{len}\, X = \mathrm{len}\, Y$ and for every natural number k such that $k \in \mathrm{Seg}\, \mathrm{len}\, x$ holds $Y(k) = F(y_k)$. Then $X \cdot Y = F(\sum \mathrm{lmlt}(x, y))$.

PROOF: Define $\mathcal{P}[\text{finite sequence of elements of } V] \equiv$ for every finite sequence x of elements of $\mathbb{Z}^{\mathrm{R}}$ for every finite sequences X, Y of elements of $\mathbb{R}_{\mathrm{F}}$ such that $X = x$ and $\mathrm{len}\, \$_1 = \mathrm{len}\, x$ and $\mathrm{len}\, X = \mathrm{len}\, Y$ and for every natural number k such that $k \in \mathrm{Seg}\, \mathrm{len}\, x$ holds $Y(k) = F(\$_{1k})$ holds $X \cdot Y = F(\sum \mathrm{lmlt}(x, \$_1))$. For every finite sequence y of elements of V and for every element w of V such that $\mathcal{P}[y]$ holds $\mathcal{P}[y \frown \langle w \rangle]$ by [4, (22), (39), (59)], [3, (11)]. $\mathcal{P}[\varepsilon_\alpha]$, where α is the carrier of V by [17, (43)]. For every finite sequence p of elements of V, $\mathcal{P}[p]$ from [6, Sch. 2]. $\square$

(91) Let us consider finite rank, free $\mathbb{Z}$-modules V_1, V_2, an ordered basis b_2 of V_2, an ordered basis b_3 of V_2, an $\mathbb{R}$-bilinear form f of V_1 and V_2, a vector v_1 of V_1, a vector v_2 of V_2, and finite sequences X, Y of elements of $\mathbb{R}_{\mathrm{F}}$. Suppose $\mathrm{len}\, X = \mathrm{len}\, b_2$ and $\mathrm{len}\, Y = \mathrm{len}\, b_2$ and for every natural number k such that $k \in \mathrm{Seg}\, \mathrm{len}\, b_2$ holds $Y(k) = f(v_1, {b_2}_k)$ and $X = v_2 \rightarrow b_2$. Then $Y \cdot X = f(v_1, v_2)$. The theorem is a consequence of (55) and (90).

(92) Let us consider finite rank, free $\mathbb{Z}$-modules V_1, V_2, an ordered basis b_1 of V_1, an $\mathbb{R}$-bilinear form f of V_1 and V_2, a vector v_1 of V_1, a vector v_2 of V_2, and finite sequences X, Y of elements of $\mathbb{R}_{\mathrm{F}}$. Suppose $\mathrm{len}\, X = \mathrm{len}\, b_1$ and $\mathrm{len}\, Y = \mathrm{len}\, b_1$ and for every natural number k such that $k \in \mathrm{Seg}\, \mathrm{len}\, b_1$ holds $Y(k) = f({b_1}_k, v_2)$ and $X = v_1 \rightarrow b_1$. Then $X \cdot Y = f(v_1, v_2)$. The theorem is a consequence of (56) and (90).

(93) Every matrix over $\mathbb{Z}^{\mathrm{R}}$ is a matrix over $\mathbb{R}_{\mathrm{F}}$.

Let M be a matrix over $\mathbb{Z}^{\mathrm{R}}$. The functor $\mathbb{Z}2\mathbb{R}(M)$ yielding a matrix over $\mathbb{R}_{\mathrm{F}}$ is defined by the term

(Def. 33) M.

Let n, m be natural numbers and M be a matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension $n \times m$. Note that the functor $\mathbb{Z}2\mathbb{R}(M)$ yields a matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension $n \times m$. Let n be a natural number and M be a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension n. Let us note that the functor $\mathbb{Z}2\mathbb{R}(M)$ yields a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension n. Now we state the propositions:

(94) Let us consider natural numbers m, l, n, a matrix S over $\mathbb{Z}^{\mathrm{R}}$ of dimension $l \times m$, a matrix T over $\mathbb{Z}^{\mathrm{R}}$ of dimension $m \times n$, a matrix S_1 over $\mathbb{R}_{\mathrm{F}}$ of dimension $l \times m$, and a matrix T_1 over $\mathbb{R}_{\mathrm{F}}$ of dimension $m \times n$. If $S = S_1$ and $T = T_1$ and $0 < l$ and $0 < m$, then $S \cdot T = S_1 \cdot T_1$.

Proof: Reconsider $S_3 = S \cdot T$ as a matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension $l \times n$. Reconsider $S_2 = S_1 \cdot T_1$ as a matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension $l \times n$. For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of S_3 holds $S_{3i,j} = S_{2i,j}$ by [8, (87)], [13, (2), (3), (37)]. $\square$

(95) Let us consider a natural number n. Then $I^{n \times n}_{\mathbb{Z}^{\mathrm{R}}} = I^{n \times n}_{\mathbb{R}_{\mathrm{F}}}$.

(96) Let us consider finite rank, free $\mathbb{Z}$-modules V_1, V_2, an ordered basis b_1 of V_1, an ordered basis b_2 of V_2, an ordered basis b_3 of V_2, and an $\mathbb{R}$-bilinear form f of V_1 and V_2. Suppose $0 < \operatorname{rank} V_1$. Then $\mathrm{Bilinear}(f, b_1, b_3) = \mathrm{Bilinear}(f, b_1, b_2) \cdot (\mathbb{Z}2\mathbb{R}(\mathrm{AutMt}(\mathrm{id}_{V_2}, b_3, b_2)))^{\mathrm{T}}$.

Proof: Set $n = \operatorname{len} b_2$. Reconsider $I_2 = \mathrm{AutMt}(\mathrm{id}_{V_2}, b_3, b_2)$ as a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension n. Reconsider $M_1 = \mathbb{Z}2\mathbb{R}({I_2}^{\mathrm{T}})$ as a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension n. Set $M_2 = \mathrm{Bilinear}(f, b_1, b_2) \cdot M_1$. For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of $\mathrm{Bilinear}(f, b_1, b_3)$ holds $(\mathrm{Bilinear}(f, b_1, b_3))_{i,j} = M_{2i,j}$ by [8, (87)], [13, (1)], (91). $\square$

(97) Let us consider finite rank, free $\mathbb{Z}$-modules V_1, V_2, an ordered basis b_1 of V_1, an ordered basis b_2 of V_2, an ordered basis b_3 of V_1, and an $\mathbb{R}$-bilinear form f of V_1 and V_2. Suppose $0 < \operatorname{rank} V_1$. Then $\mathrm{Bilinear}(f, b_3, b_2) = \mathbb{Z}2\mathbb{R}(\mathrm{AutMt}(\mathrm{id}_{V_1}, b_3, b_1)) \cdot \mathrm{Bilinear}(f, b_1, b_2)$.

Proof: Set $n = \operatorname{len} b_3$. Reconsider $I_2 = \mathrm{AutMt}(\mathrm{id}_{V_1}, b_3, b_1)$ as a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension n. Reconsider $M_1 = \mathbb{Z}2\mathbb{R}(I_2)$ as a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension n. Set $M_2 = M_1 \cdot \mathrm{Bilinear}(f, b_1, b_2)$. For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of $\mathrm{Bilinear}(f, b_3, b_2)$ holds $(\mathrm{Bilinear}(f, b_3, b_2))_{i,j} = M_{2i,j}$ by [8, (87)], [4, (1)], [13, (1)], (92). $\square$

(98) Let us consider a finite rank, free $\mathbb{Z}$-module V, ordered bases b_1, b_2 of V, and an $\mathbb{R}$-bilinear form f of V and V. Suppose $0 < \operatorname{rank} V$. Then $\mathrm{Bilinear}(f, b_2, b_2) = \mathbb{Z}2\mathbb{R}(\mathrm{AutMt}(\mathrm{id}_V, b_2, b_1)) \cdot \mathrm{Bilinear}(f, b_1, b_1) \cdot (\mathbb{Z}2\mathbb{R}(\mathrm{AutMt}(\mathrm{id}_V, b_2, b_1)))^{\mathrm{T}}$. The theorem is a consequence of (97) and (96).

Let us consider a finite rank, free $\mathbb{Z}$-module V, ordered bases b_1, b_2 of V, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $\operatorname{rank} V$.

Let us assume that $M = \mathrm{AutMt}(\mathrm{id}_V, b_1, b_2)$. Now we state the propositions:

(99) (i) $\operatorname{Det} M = 1$ and $\operatorname{Det} M^{\mathrm{T}} = 1$, or

(ii) $\operatorname{Det} M = -1$ and $\operatorname{Det} M^{\mathrm{T}} = -1$.

The theorem is a consequence of (94) and (95).

(100) $|\operatorname{Det} M| = 1$. The theorem is a consequence of (99).

Let us consider a finite rank, free $\mathbb{Z}$-module V, ordered bases b_1, b_2 of V, and an $\mathbb{R}$-bilinear form f of V and V. Now we state the propositions:

(101) $\operatorname{Det} \operatorname{Bilinear}(f, b_2, b_2) = \operatorname{Det} \operatorname{Bilinear}(f, b_1, b_1)$. The theorem is a consequence of (98) and (99).

(102) $|\operatorname{Det} \operatorname{Bilinear}(f, b_2, b_2)| = |\operatorname{Det} \operatorname{Bilinear}(f, b_1, b_1)|$.

Let V be a finite rank, free $\mathbb{Z}$-module, f be an $\mathbb{R}$-bilinear form of V and V, and b be an ordered basis of V. The functor $\operatorname{GramMatrix}(f, b)$ yielding a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension $\operatorname{rank} V$ is defined by the term

(Def. 34) $\operatorname{Bilinear}(f, b, b)$.

The functor $\operatorname{GramDet}(f)$ yielding an element of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 35) for every ordered basis b of V, $it = \operatorname{Det} \operatorname{GramMatrix}(f, b)$.

Let L be a $\mathbb{Z}$-lattice. The functor InnerProduct L yielding an $\mathbb{R}$-form of L and L is defined by the term

(Def. 36) the scalar product of L.

One can check that InnerProduct L is additive w.r.t. first argument, homogeneous w.r.t. first argument, additive w.r.t. second argument, and homogeneous w.r.t. second argument.

Let b be an ordered basis of L. The functor $\operatorname{GramMatrix}(b)$ yielding a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension $\dim(L)$ is defined by the term

(Def. 37) $\operatorname{GramMatrix}(\operatorname{InnerProduct} L, b)$.

The functor $\operatorname{GramDet}(L)$ yielding an element of $\mathbb{R}_{\mathrm{F}}$ is defined by the term

(Def. 38) $\operatorname{GramDet}(\operatorname{InnerProduct} L)$.

(103) Let us consider an integral $\mathbb{Z}$-lattice L. Then InnerProduct L is a bilinear form of L, L.

PROOF: For every object z such that $z \in$ (the carrier of L) $\times$ (the carrier of L) holds $(\operatorname{InnerProduct} L)(z) \in$ the carrier of $\mathbb{Z}^{\mathrm{R}}$. Reconsider $f =$ InnerProduct L as a form of L, L. For every vector v of L, $f(\cdot, v)$ is additive by [2, (70)], (8). For every vector v of L, $f(\cdot, v)$ is homogeneous by [2, (70)], (9). For every vector v of L, $f(v, \cdot)$ is additive by [2, (69)], (8). For every vector v of L, $f(v, \cdot)$ is homogeneous by [2, (69)], (9). $\square$

(104) Let us consider an integral $\mathbb{Z}$-lattice L, and an ordered basis b of L. Then $\operatorname{GramMatrix}(b)$ is a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension $\dim(L)$.

Proof: For every natural numbers i, j such that $\langle i, j\rangle \in$ the indices of GramMatrix(b) holds $(\text{GramMatrix}(b))_{i,j} \in$ the carrier of $\mathbb{Z}^{\mathrm{R}}$ by [8, (87)]. $\square$

Let L be an integral $\mathbb{Z}$-lattice. Note that GramDet(L) is integer.

References

[1] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.

[2] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(**3**): 537–541, 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. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[9] Wolfgang Ebeling. *Lattices and Codes*. Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.

[10] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.

[11] 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.

[12] Yuichi Futa, Hiroyuki Okazaki, Kazuhisa Nakasho, and Yasunari Shidama. Torsion $\mathbb{Z}$-module and torsion-free $\mathbb{Z}$-module. *Formalized Mathematics*, 22(**4**):277–289, 2014. doi:10.2478/forma-2014-0028.

[13] 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.

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

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

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

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

Received December 30, 2015

FORMALIZED MATHEMATICS
Vol. 24, No. 1, Pages 69–79, 2016
DOI: 10.1515/forma-2016-0006

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

Product Pre-Measure

Noboru Endou
Gifu National College of Technology
Gifu, Japan

Summary. In this article we formalize in Mizar [5] product pre-measure on product sets of measurable sets. Although there are some approaches to construct product measure [22], [6], [9], [21], [25], we start it from σ-measure because existence of σ-measure on any semialgebras has been proved in [15]. In this approach, we use some theorems for integrals.

MSC: 28A35 03B35

Keywords: product measure; pre-measure

MML identifier: `MEASUR10`, version: `8.1.04 5.36.1267`

1. Preliminaries

Now we state the proposition:

(1) Let us consider non empty sets A, A_1, A_2, B, B_1, B_2. Then $A_1 \times B_1$ misses $A_2 \times B_2$ and $A \times B = A_1 \times B_1 \cup A_2 \times B_2$ if and only if A_1 misses A_2 and $A = A_1 \cup A_2$ and $B = B_1$ and $B = B_2$ or B_1 misses B_2 and $B = B_1 \cup B_2$ and $A = A_1$ and $A = A_2$.

Let C, D be non empty sets, F be a sequence of D^C, and n be a natural number. One can check that the functor $F(n)$ yields a function from C into D.

(2) Let us consider sets X, Y, A, B, and objects x, y. Suppose $x \in X$ and $y \in Y$. Then $\chi_{A,X}(x) \cdot \chi_{B,Y}(y) = \chi_{A \times B, X \times Y}(x, y)$.

Let A, B be sets. One can verify that $\chi_{A,B}$ is non-negative.

(3) Let us consider a non empty set X, a semialgebra S of sets of X, a pre-measure P of S, an induced measure m of S and P, and an induced σ-measure M of S and m. Then $\mathrm{COM}(M)$ is complete on $\mathrm{COM}(\sigma(\text{the field generated by } S), M)$.

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

The functor $\text{Intervals}_{\mathbb{R}}$ yielding a semialgebra of sets of $\mathbb{R}$ is defined by the term

(Def. 1) the set of all I where I is an interval.

Now we state the propositions:

(4) $\text{Halflines} \subseteq \text{Intervals}_{\mathbb{R}}$.

(5) Let us consider a subset I of $\mathbb{R}$. If I is an interval, then $I \in$ the Borel sets.

(6) (i) $\sigma(\text{Intervals}_{\mathbb{R}}) =$ the Borel sets, and

(ii) σ(the field generated by $\text{Intervals}_{\mathbb{R}}$) $=$ the Borel sets.

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

2. Family of Semialgebras, Fields and Measures

Now we state the propositions:

(7) Let us consider sets X_1, X_2, a non empty family S_1 of subsets of X_1, and a non empty family S_2 of subsets of X_2. Then the set of all $a \times b$ where a is an element of S_1, b is an element of S_2 is a non empty family of subsets of $X_1 \times X_2$.

(8) Let us consider sets X, Y, a family M of subsets of X with the empty element, and a family N of subsets of Y with the empty element. Then the set of all $A \times B$ where A is an element of M, B is an element of N is a family of subsets of $X \times Y$ with the empty element. The theorem is a consequence of (7).

(9) Let us consider a set X, and disjoint valued finite sequences O, T of elements of X. Suppose $\bigcup \text{rng}\, O$ misses $\bigcup \text{rng}\, T$. Then $O \frown T$ is a disjoint valued finite sequence of elements of X.

(10) Let us consider sets X_1, X_2, a semiring S_1 of X_1, and a semiring S_2 of X_2. Then the set of all $A \times B$ where A is an element of S_1, B is an element of S_2 is a semiring of $X_1 \times X_2$.

(11) Let us consider sets X_1, X_2, a semialgebra S_1 of sets of X_1, and a semialgebra S_2 of sets of X_2. Then the set of all $A \times B$ where A is an element of S_1, B is an element of S_2 is a semialgebra of sets of $X_1 \times X_2$. The theorem is a consequence of (10).

(12) Let us consider sets X_1, X_2, a field O of subsets of X_1, and a field T of subsets of X_2. Then the set of all $A \times B$ where A is an element of O, B is an element of T is a semialgebra of sets of $X_1 \times X_2$. The theorem is a consequence of (11).

Let n be a non zero natural number and X be a non-empty, n-element finite sequence.

A family of semialgebras of X is an n-element finite sequence and is defined by

(Def. 2) for every natural number i such that $i \in \operatorname{Seg} n$ holds $it(i)$ is a semialgebra of sets of $X(i)$.

Let us observe that a family of semialgebras of X is a $\cap$-closed yielding family of semirings of X. Now we state the proposition:

(13) Let us consider a non zero natural number n, a non-empty, n-element finite sequence X, a family S of semialgebras of X, and a natural number i. If $i \in \operatorname{Seg} n$, then $X(i) \in S(i)$.

Let us consider a non-empty, 1-element finite sequence X and a family S of semialgebras of X. Now we state the propositions:

(14) the set of all $\prod\langle s\rangle$ where s is an element of $S(1)$ is a semialgebra of sets of the set of all $\langle x\rangle$ where x is an element of $X(1)$. The theorem is a consequence of (13).

(15) SemiringProduct(S) is a semialgebra of sets of $\prod X$. The theorem is a consequence of (14).

(16) Let us consider sets X_1, X_2, a semialgebra S_1 of sets of X_1, and a semialgebra S_2 of sets of X_2. Then the set of all $s_1 \times s_2$ where s_1 is an element of S_1, s_2 is an element of S_2 is a semialgebra of sets of $X_1 \times X_2$.

(17) Let us consider a non zero natural number n, a non-empty, n-element finite sequence X, and a family S of semialgebras of X. Then SemiringProduct (S) is a semialgebra of sets of $\prod X$.

Proof: Define $\mathcal{P}$[non zero natural number] $\equiv$ for every non-empty, $\$_1$-element finite sequence X for every family S of semialgebras of X, SemiringProduct(S) is a semialgebra of sets of $\prod X$. $\mathcal{P}[1]$. For every non zero natural number k, $\mathcal{P}[k]$ from [3, Sch. 10]. $\square$

(18) Let us consider a non zero natural number n, a non-empty, n-element finite sequence X_8, a non-empty, 1-element finite sequence X_1, a family S_4 of semialgebras of X_8, and a family S_1 of semialgebras of X_1. Then SemiringProduct($S_4 \frown S_1$) is a semialgebra of sets of $\prod(X_8 \frown X_1)$. The theorem is a consequence of (17), (16), and (13).

Let n be a non zero natural number and X be a non-empty, n-element finite sequence.

A family of fields of X is an n-element finite sequence and is defined by

(Def. 3) for every natural number i such that $i \in \operatorname{Seg} n$ holds $it(i)$ is a field of subsets of $X(i)$.

Let S be a family of fields of X and i be a natural number. Assume $i \in \operatorname{Seg} n$. Observe that the functor $S(i)$ yields a field of subsets of $X(i)$.

Observe that a family of fields of X is a family of semialgebras of X.

Let us consider a non-empty, 1-element finite sequence X and a family S of fields of X. Now we state the propositions:

(19) the set of all $\prod\langle s\rangle$ where s is an element of $S(1)$ is a field of subsets of the set of all $\langle x\rangle$ where x is an element of $X(1)$. The theorem is a consequence of (14).

(20) SemiringProduct(S) is a field of subsets of $\prod X$. The theorem is a consequence of (19).

Let n be a non zero natural number, X be a non-empty, n-element finite sequence, and S be a family of fields of X.

A family of measures of S is an n-element finite sequence and is defined by

(Def. 4) for every natural number i such that $i \in \operatorname{Seg} n$ holds $it(i)$ is a measure on $S(i)$.

3. Product of Two Measures

Let X_1, X_2 be sets, S_1 be a field of subsets of X_1, and S_2 be a field of subsets of X_2. The functor MeasRect(S_1, S_2) yielding a semialgebra of sets of $X_1 \times X_2$ is defined by the term

(Def. 5) the set of all $A \times B$ where A is an element of S_1, B is an element of S_2.

Now we state the proposition:

(21) Let us consider a set X, and a field F of subsets of X. Then there exists a semialgebra S of sets of X such that

(i) $F = S$, and

(ii) $F =$ the field generated by S.

Let X_1, X_2 be sets, S_1 be a field of subsets of X_1, S_2 be a field of subsets of X_2, m_1 be a measure on S_1, and m_2 be a measure on S_2. The functor ProdpreMeas(m_1, m_2) yielding a non-negative, zeroed function from MeasRect (S_1, S_2) into $\overline{\mathbb{R}}$ is defined by

(Def. 6) for every element C of MeasRect(S_1, S_2), there exists an element A of S_1 and there exists an element B of S_2 such that $C = A \times B$ and $it(C) = m_1(A) \cdot m_2(B)$.

Now we state the propositions:

(22) Let us consider sets X_1, X_2, a field S_1 of subsets of X_1, a field S_2 of subsets of X_2, a measure m_1 on S_1, a measure m_2 on S_2, and sets A, B.

Suppose $A \in S_1$ and $B \in S_2$. Then $(\mathrm{ProdpreMeas}(m_1, m_2))(A \times B) = m_1(A) \cdot m_2(B)$.

(23) Let us consider sets X_1, X_2, a non empty family S_1 of subsets of X_1, a non empty family S_2 of subsets of X_2, a non empty family S of subsets of $X_1 \times X_2$, and a finite sequence H of elements of S. Suppose $S =$ the set of all $A \times B$ where A is an element of S_1, B is an element of S_2. Then there exists a finite sequence F of elements of S_1 and there exists a finite sequence G of elements of S_2 such that $\mathrm{len}\, H = \mathrm{len}\, F$ and $\mathrm{len}\, H = \mathrm{len}\, G$ and for every natural number k such that $k \in \mathrm{dom}\, H$ and $H(k) \neq \emptyset$ holds $H(k) = F(k) \times G(k)$.

PROOF: For every natural number k such that $k \in \mathrm{dom}\, H$ there exists an element A of S_1 and there exists an element B of S_2 such that $H(k) = A \times B$. Define $\mathcal{P}[\text{natural number}, \text{set}] \equiv$ there exists an element B of S_2 such that $H(\$_1) = \$_2 \times B$. Consider F being a finite sequence of elements of S_1 such that $\mathrm{dom}\, F = \mathrm{Seg}\, \mathrm{len}\, H$ and for every natural number k such that $k \in \mathrm{Seg}\, \mathrm{len}\, H$ holds $\mathcal{P}[k, F(k)]$ from [4, Sch. 5]. Define $\mathcal{Q}[\text{natural number}, \text{set}] \equiv$ there exists an element A of S_1 such that $H(\$_1) = A \times \$_2$. For every natural number k such that $k \in \mathrm{Seg}\, \mathrm{len}\, H$ there exists an element B of S_2 such that $\mathcal{Q}[k, B]$. Consider G being a finite sequence of elements of S_2 such that $\mathrm{dom}\, G = \mathrm{Seg}\, \mathrm{len}\, H$ and for every natural number k such that $k \in \mathrm{Seg}\, \mathrm{len}\, H$ holds $\mathcal{Q}[k, G(k)]$ from [4, Sch. 5]. $\square$

(24) Let us consider a set X, a non empty, semi-diff-closed, $\cap$-closed family S of subsets of X, and elements E_1, E_2 of S. Then there exist disjoint valued finite sequences O, T, F of elements of S such that

(i) $\bigcup \mathrm{rng}\, O = E_1 \setminus E_2$, and

(ii) $\bigcup \mathrm{rng}\, T = E_2 \setminus E_1$, and

(iii) $\bigcup \mathrm{rng}\, F = E_1 \cap E_2$, and

(iv) $(O \frown T) \frown F$ is a disjoint valued finite sequence of elements of S.

The theorem is a consequence of (9).

(25) Let us consider sets X_1, X_2, a field S_1 of subsets of X_1, a field S_2 of subsets of X_2, a measure m_1 on S_1, a measure m_2 on S_2, and elements E_1, E_2 of $\mathrm{MeasRect}(S_1, S_2)$. Suppose E_1 misses E_2 and $E_1 \cup E_2 \in \mathrm{MeasRect}(S_1, S_2)$. Then $(\mathrm{ProdpreMeas}(m_1, m_2))(E_1 \cup E_2) = (\mathrm{ProdpreMeas}(m_1, m_2))(E_1) + (\mathrm{ProdpreMeas}(m_1, m_2))(E_2)$. The theorem is a consequence of (1) and (22).

(26) Let us consider a non empty set X, a non empty family S of subsets of X, a function f from $\mathbb{N}$ into S, and a sequence F of partial functions from X into $\overline{\mathbb{R}}$. Suppose f is disjoint valued and for every natural number

n, $F(n) = \chi_{f(n),X}$. Let us consider an object x. Suppose $x \in X$. Then $\chi_{\bigcup f,X}(x) = (\lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}})(x)$.

(27) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a partial function f from X to $\overline{\mathbb{R}}$, and a real number r. Suppose $\operatorname{dom} f \in S$ and $0 \leqslant r$ and for every object x such that $x \in \operatorname{dom} f$ holds $f(x) = r$. Then $\int f \, \mathrm{d}M = r \cdot M(\operatorname{dom} f)$.

Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, a partial function f from X to $\overline{\mathbb{R}}$, and an element A of S. Now we state the propositions:

(28) Suppose there exists an element E of S such that $E = \operatorname{dom} f$ and f is measurable on E and for every object x such that $x \in \operatorname{dom} f \setminus A$ holds $f(x) = 0$ and f is non-negative. Then $\int f \, \mathrm{d}M = \int f {\restriction} A \, \mathrm{d}M$. The theorem is a consequence of (27).

(29) If f is integrable on M and for every object x such that $x \in \operatorname{dom} f \setminus A$ holds $f(x) = 0$, then $\int f \, \mathrm{d}M = \int f {\restriction} A \, \mathrm{d}M$. The theorem is a consequence of (27).

(30) Let us consider non empty sets X_1, X_2, a σ-field S_1 of subsets of X_1, a σ-field S_2 of subsets of X_2, a σ-measure M_2 on S_2, a function D from $\mathbb{N}$ into S_1, a function E from $\mathbb{N}$ into S_2, an element A of S_1, an element B of S_2, a sequence F of partial functions from X_2 into $\overline{\mathbb{R}}$, a sequence R of $\mathbb{R}^{X_1}$, and an element x of X_1. Suppose for every natural number n, $R(n) = \chi_{D(n),X_1}$ and for every natural number n, $F(n) = R(n)(x) \cdot \chi_{E(n),X_2}$ and for every natural number n, $E(n) \subseteq B$. Then there exists a sequence I of extended reals such that

(i) for every natural number n, $I(n) = M_2(E(n)) \cdot \chi_{D(n),X_1}(x)$, and

(ii) I is summable, and

(iii) $\int \lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}} \, \mathrm{d}M_2 = \sum I$.

Proof: For every natural number n, $\operatorname{dom}(F(n)) = X_2$. Reconsider $S_3 = X_2$ as an element of S_2. For every natural number n and for every set y such that $y \in E(n)$ holds $F(n)(y) = 0$ or $F(n)(y) = 1$ by [10, (3)], [18, (1)], [12, (39)]. For every natural number n and for every set y such that $y \notin E(n)$ holds $F(n)(y) = 0$. For every natural number n, $F(n)$ is non-negative and $F(n)$ is measurable on B by [8, (51)], [17, (37)], [18, (29)]. For every element y of X_2 such that $y \in B$ holds $F\#y$ is summable by [8, (51), (39)], [19, (16)], [29, (37)].

Consider I being a sequence of extended reals such that for every natural number n, $I(n) = \int F(n){\restriction}B \, \mathrm{d}M_2$ and I is summable and $\int \lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}{\restriction}B \, \mathrm{d}M_2 = \sum I$. For every natural number n, $I(n) =$

$M_2(E(n)) \cdot \chi_{D(n),X_1}(x)$ by [28, (61)], [10, (47), (49)], [18, (29)]. For every natural number n, $F(n)$ is measurable on S_3 by [18, (29)], [17, (37)]. For every natural number n, $F(n)$ is without $-\infty$. For every element y of X_2 such that $y \in S_3$ holds $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}} \# y$ is convergent by [19, (38)]. For every object y such that $y \in \operatorname{dom} \lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}} \setminus B$ holds $(\lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}})(y) = 0$ by [19, (43)], [16, (52)]. For every object y such that $y \in \operatorname{dom} \lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}$ holds $(\lim(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}})(y) \geqslant 0$ by [19, (36)], [8, (51)], [19, (10), (38)]. □

(31) Let us consider a non empty set X, a σ-field S of subsets of X, an element A of S, and an extended real number p. Then $X \longmapsto p$ is measurable on A.
Proof: For every real number r, $A \cap \text{GTE-dom}(X \longmapsto p, r) \in S$ by [26, (7)], [7, (7)]. □

Let A, X be sets. The functor $\overline{\chi}_{A,X}$ yielding a function from X into $\overline{\mathbb{R}}$ is defined by

(Def. 7) for every object x such that $x \in X$ holds if $x \in A$, then $it(x) = +\infty$ and if $x \notin A$, then $it(x) = 0$.

Now we state the proposition:

(32) Let us consider a non empty set X, a σ-field S of subsets of X, and elements A, B of S. Then $\overline{\chi}_{A,X}$ is measurable on B.

Let X, A be sets. Let us observe that $\overline{\chi}_{A,X}$ is non-negative.

(33) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, and an element A of S. Then
 (i) if $M(A) \neq 0$, then $\int \overline{\chi}_{A,X} \, \mathrm{d}M = +\infty$, and
 (ii) if $M(A) = 0$, then $\int \overline{\chi}_{A,X} \, \mathrm{d}M = 0$.

Proof: Reconsider $X_3 = X$ as an element of S. Reconsider $X_2 = X_3 \setminus A$ as an element of S. Reconsider $F = \overline{\chi}_{A,X} \restriction A$ as a partial function from X to $\overline{\mathbb{R}}$. Reconsider $O = \overline{\chi}_{A,X} \restriction X_2$ as a partial function from X to $\overline{\mathbb{R}}$. Reconsider $T = \overline{\chi}_{A,X} \restriction (X_2 \cup A)$ as a partial function from X to $\overline{\mathbb{R}}$. $\int F \, \mathrm{d}M = 0$. O is measurable on X_2. For every element x of X such that $x \in \operatorname{dom}(\overline{\chi}_{A,X} \restriction X_2)$ holds $(\overline{\chi}_{A,X} \restriction X_2)(x) = 0$ by [10, (47)]. $\int T \, \mathrm{d}M = \int O \, \mathrm{d}M + 0$. □

(34) Let us consider non empty sets X_1, X_2, a σ-field S_1 of subsets of X_1, a σ-field S_2 of subsets of X_2, a σ-measure M_1 on S_1, a σ-measure M_2 on S_2, and a disjoint valued function K from $\mathbb{N}$ into $\operatorname{MeasRect}(S_1, S_2)$. Suppose $\bigcup K \in \operatorname{MeasRect}(S_1, S_2)$. Then $(\operatorname{ProdpreMeas}(M_1, M_2))(\bigcup K) = \sum(\operatorname{ProdpreMeas}(M_1, M_2) \cdot K)$.
Proof: Consider A being an element of S_1, B being an element of S_2 such that $\bigcup K = A \times B$. Consider P being an element of S_1, Q being an element of S_2 such that $\bigcup K = P \times Q$ and $(\operatorname{ProdpreMeas}(M_1, M_2))(\bigcup K) = M_1(P) \cdot$

$M_2(Q)$. Define $\mathcal{F}(\text{object}) = \chi_{K(\$_1),X_1 \times X_2}$. Consider X_6 being a sequence of partial functions from $X_1 \times X_2$ into $\overline{\mathbb{R}}$ such that for every natural number n, $X_6(n) = \mathcal{F}(n)$ from [24, Sch. 1]. Define $\mathcal{P}[\text{natural number}, \text{object}] \equiv \$_2 = \pi_1(K(\$_1))$. For every element i of $\mathbb{N}$, there exists an element A of S_1 such that $\mathcal{P}[i, A]$ by [2, (9)], [7, (7)]. Consider D being a function from $\mathbb{N}$ into S_1 such that for every element i of $\mathbb{N}$, $\mathcal{P}[i, D(i)]$ from [11, Sch. 3]. Define $\mathcal{Q}[\text{natural number}, \text{object}] \equiv \$_2 = \pi_2(K(\$_1))$. For every element i of $\mathbb{N}$, there exists an element B of S_2 such that $\mathcal{Q}[i, B]$ by [2, (9)], [7, (7)].

Consider E being a function from $\mathbb{N}$ into S_2 such that for every element i of $\mathbb{N}$, $\mathcal{Q}[i, E(i)]$ from [11, Sch. 3]. Define $\mathcal{O}(\text{object}) = \chi_{D(\$_1),X_1}$. Consider X_7 being a sequence of partial functions from X_1 into $\overline{\mathbb{R}}$ such that for every natural number n, $X_7(n) = \mathcal{O}(n)$ from [24, Sch. 1]. Define $\mathcal{T}(\text{object}) = \chi_{E(\$_1),X_2}$. Consider X_4 being a sequence of partial functions from X_2 into $\overline{\mathbb{R}}$ such that for every natural number n, $X_4(n) = \mathcal{T}(n)$ from [24, Sch. 1]. For every natural number n and for every objects x, y such that $x \in X_1$ and $y \in X_2$ holds $X_6(n)(x, y) = X_7(n)(x) \cdot X_4(n)(y)$ by [14, (87)], [2, (9)], (2). $(\text{ProdpreMeas}(M_1, M_2))(\bigcup K) = M_1(A) \cdot M_2(B)$ by [14, (110)]. Reconsider $C_1 = \chi_{A \times B, X_1 \times X_2}$ as a function from $X_1 \times X_2$ into $\overline{\mathbb{R}}$. For every element x of X_1, $M_2(B) \cdot \chi_{A,X_1}(x) = \int \text{curry}(C_1, x)\, \mathrm{d}M_2$ by (2), [13, (5)], [19, (14)], [23, (4)]. For every object n such that $n \in \mathbb{N}$ holds $X_7(n) \in \mathbb{R}^{X_1}$ by [12, (39)]. Reconsider $R_1 = X_7$ as a sequence of $\mathbb{R}^{X_1}$. For every natural number n, $D(n) \subseteq A$ and $E(n) \subseteq B$ by [2, (10)], [1, (1)]. For every element x of X_1, there exists a sequence X_5 of partial functions from X_2 into $\overline{\mathbb{R}}$ and there exists a sequence I of extended reals such that for every natural number n, $X_5(n) = R_1(n)(x) \cdot \chi_{E(n),X_2}$ and for every natural number n, $I(n) = M_2(E(n)) \cdot \chi_{D(n),X_1}(x)$ and I is summable and $\int \lim(\sum_{\alpha=0}^{\kappa} X_5(\alpha))_{\kappa \in \mathbb{N}}\, \mathrm{d}M_2 = \sum I$ by [13, (45)], (30).

Reconsider $L_1 = \lim(\sum_{\alpha=0}^{\kappa} X_6(\alpha))_{\kappa \in \mathbb{N}}$ as a function from $X_1 \times X_2$ into $\overline{\mathbb{R}}$. For every element x of X_1 and for every element y of X_2, $(\text{curry}(C_1, x))(y) = (\text{curry}(L_1, x))(y)$. For every element x of X_1, $\text{curry}(C_1, x) = \text{curry}(L_1, x)$. For every element x of X_1, $M_2(B) \cdot \chi_{A,X_1}(x) = \int \text{curry}(L_1, x)\, \mathrm{d}M_2$. For every element x of X_1, there exists a sequence I of extended reals such that for every natural number n, $I(n) = M_2(E(n)) \cdot \chi_{D(n),X_1}(x)$ and $M_2(B) \cdot \chi_{A,X_1}(x) = \sum I$ by [8, (51)], [19, (38), (29), (30)]. Define $\mathcal{R}[\text{natural number}, \text{object}] \equiv$ if $M_2(E(\$_1)) = +\infty$, then $\$_2 = \overline{\chi}_{D(\$_1),X_1}$ and if $M_2(E(\$_1)) \neq +\infty$, then there exists a real number m_2 such that $m_2 = M_2(E(\$_1))$ and $\$_2 = m_2 \cdot \chi_{D(\$_1),X_1}$. For every element n of $\mathbb{N}$, there exists an element y of $X_1 \dot{\to} \overline{\mathbb{R}}$ such that $\mathcal{R}[n, y]$ by [13, (45)], [8, (51)]. Consider F_1 being a function from $\mathbb{N}$ into $X_1 \dot{\to} \overline{\mathbb{R}}$ such that for every element n of $\mathbb{N}$, $\mathcal{R}[n, F_1(n)]$ from [11, Sch. 3]. For every natural number

n, $\mathrm{dom}(F_1(n)) = X_1$. For every natural number n, $F_1(n)$ is non-negative by [8, (51)]. For every natural numbers n, m, $\mathrm{dom}(F_1(n)) = \mathrm{dom}(F_1(m))$.

Reconsider $X_3 = X_1$ as an element of S_1. For every natural number n, $F_1(n)$ is non-negative and $F_1(n)$ is measurable on A and $F_1(n)$ is measurable on X_3 by (32), [18, (29)], [17, (37)]. For every element x of X_1 such that $x \in A$ holds $F_1\#x$ is summable by [8, (51), (39)], [20, (2)]. Consider J being a sequence of extended reals such that for every natural number n, $J(n) = \int F_1(n)\restriction A \,\mathrm{d}M_1$ and J is summable and $\int \lim(\sum_{\alpha=0}^{\kappa} F_1(\alpha))_{\kappa\in\mathbb{N}}\restriction A \,\mathrm{d}M_1 = \sum J$. For every natural number n, $J(n) = \int F_1(n)\,\mathrm{d}M_1$. Reconsider $X_3 = X_1$ as an element of S_1. For every element n of $\mathbb{N}$, $J(n) = (\mathrm{ProdpreMeas}(M_1, M_2)\cdot K)(n)$ by (33), [8, (51)], [18, (29)], [16, (86), (88)]. For every element x of X_1, $(\lim(\sum_{\alpha=0}^{\kappa} F_1(\alpha))_{\kappa\in\mathbb{N}})(x) \geqslant 0$ by [19, (38)], [29, (37), (23)], [8, (51)]. For every natural number n, $F_1(n)$ is measurable on X_3 and $F_1(n)$ is without $-\infty$. For every object x such that $x \in \mathrm{dom}\lim(\sum_{\alpha=0}^{\kappa} F_1(\alpha))_{\kappa\in\mathbb{N}} \setminus A$ holds $(\lim(\sum_{\alpha=0}^{\kappa} F_1(\alpha))_{\kappa\in\mathbb{N}})(x) = 0$ by [19, (30), (32)], [16, (52)]. $\int \lim(\sum_{\alpha=0}^{\kappa} F_1(\alpha))_{\kappa\in\mathbb{N}}\,\mathrm{d}M_1 =$ $\int \lim(\sum_{\alpha=0}^{\kappa} F_1(\alpha))_{\kappa\in\mathbb{N}}\restriction A\,\mathrm{d}M_1$. $\int \lim(\sum_{\alpha=0}^{\kappa} F_1(\alpha))_{\kappa\in\mathbb{N}}\,\mathrm{d}M_1 = M_1(A)\cdot M_2(B)$ by [11, (63)], [19, (30), (32)], [8, (51)]. $\square$

(35) Let us consider a without $-\infty$ finite sequence f of elements of $\overline{\mathbb{R}}$, and a without $-\infty$ sequence s of extended reals. Suppose for every object n such that $n \in \mathrm{dom}\, f$ holds $f(n) = s(n)$.
Then $\sum f + s(0) = (\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}(\mathrm{len}\, f)$.
PROOF: Consider F being a sequence of $\overline{\mathbb{R}}$ such that $\sum f = F(\mathrm{len}\, f)$ and $F(0) = 0$ and for every natural number i such that $i < \mathrm{len}\, f$ holds $F(i+1) = F(i) + f(i+1)$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant \mathrm{len}\, f$, then $F(\$_1) + s(0) = (\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}(\$_1)$ and $F(\$_1) \neq -\infty$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [3, (11)], [27, (25)], [16, (10)], [3, (13)]. For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 2]. $\square$

(36) Let us consider a non-negative finite sequence f of elements of $\overline{\mathbb{R}}$, and a sequence s of extended reals. Suppose for every object n such that $n \in \mathrm{dom}\, f$ holds $f(n) = s(n)$ and for every element n of $\mathbb{N}$ such that $n \notin \mathrm{dom}\, f$ holds $s(n) = 0$. Then

(i) $\sum f = \sum s$, and

(ii) $\sum f = \overline{\sum} s$.

PROOF: For every object n such that $n \in \mathrm{dom}\, s$ holds $0 \leqslant s(n)$ by [8, (51)]. $\sum f + s(0) = (\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}(\mathrm{len}\, f)$. Define $\mathcal{P}[\text{natural number}] \equiv$ $(\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}}(\mathrm{len}\, f) = ((\sum_{\alpha=0}^{\kappa} s(\alpha))_{\kappa\in\mathbb{N}} \uparrow \mathrm{len}\, f)(\$_1)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [27, (25)]. For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 2]. $\square$

(37) Let us consider non empty sets X_1, X_2, a σ-field S_1 of subsets of X_1, a σ-field S_2 of subsets of X_2, a σ-measure M_1 on S_1, a σ-measure M_2 on S_2, and a disjoint valued finite sequence F of elements of $\mathrm{MeasRect}(S_1, S_2)$. Suppose $\bigcup F \in \mathrm{MeasRect}(S_1, S_2)$. Then $(\mathrm{ProdpreMeas}(M_1, M_2))(\bigcup F) = \sum(\mathrm{ProdpreMeas}(M_1, M_2) \cdot F)$.

Proof: Set $S = \mathrm{MeasRect}(S_1, S_2)$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ if $\$_1 \in \mathrm{dom}\, F$, then $\$_2 = F(\$_1)$ and if $\$_1 \notin \mathrm{dom}\, F$, then $\$_2 = \emptyset$. For every element n of $\mathbb{N}$, there exists an element y of S such that $\mathcal{P}[n, y]$ by [10, (3)]. Consider G being a function from $\mathbb{N}$ into S such that for every element n of $\mathbb{N}$, $\mathcal{P}[n, G(n)]$ from [11, Sch. 3]. For every object x such that $x \notin \mathrm{dom}\, F$ holds $G(x) = \emptyset$. For every objects x, y such that $x \neq y$ holds $G(x)$ misses $G(y)$. $(\mathrm{ProdpreMeas}(M_1, M_2))(\bigcup F) = \overline{\sum}(\mathrm{ProdpreMeas}(M_1, M_2) \cdot G)$. For every object n such that $n \in \mathrm{dom}(\mathrm{ProdpreMeas}(M_1, M_2) \cdot F)$ holds $(\mathrm{ProdpreMeas}(M_1, M_2) \cdot F)(n) = (\mathrm{ProdpreMeas}(M_1, M_2) \cdot G)(n)$ by [10, (11), (12), (13)]. For every element n of $\mathbb{N}$ such that $n \notin \mathrm{dom}(\mathrm{ProdpreMeas}(M_1, M_2) \cdot F)$ holds $(\mathrm{ProdpreMeas}(M_1, M_2) \cdot G)(n) = 0$ by [10, (3), (11), (13)]. $\square$

(38) Let us consider non empty sets X_1, X_2, a σ-field S_1 of subsets of X_1, a σ-field S_2 of subsets of X_2, a σ-measure M_1 on S_1, and a σ-measure M_2 on S_2. Then $\mathrm{ProdpreMeas}(M_1, M_2)$ is a pre-measure of $\mathrm{MeasRect}(S_1, S_2)$. The theorem is a consequence of (37) and (34).

Let X_1, X_2 be non empty sets, S_1 be a σ-field of subsets of X_1, S_2 be a σ-field of subsets of X_2, M_1 be a σ-measure on S_1, and M_2 be a σ-measure on S_2. Let us observe that the functor $\mathrm{ProdpreMeas}(M_1, M_2)$ yields a pre-measure of $\mathrm{MeasRect}(S_1, S_2)$.

References

[1] Grzegorz Bancerek. Towards the construction of a model of Mizar concepts. *Formalized Mathematics*, 16(**2**):207–230, 2008. doi:10.2478/v10037-008-0027-x.

[2] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(**3**):537–541, 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] Heinz Bauer. *Measure and Integration Theory*. Walter de Gruyter Inc.

[7] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

[8] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.
[9] Vladimir Igorevich Bogachev and Maria Aparecida Soares Ruas. *Measure theory*, volume 1. Springer, 2007.
[10] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[11] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[12] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.
[13] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[14] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[15] Noboru Endou. Construction of measure from semialgebra of sets. *Formalized Mathematics*, 23(**4**):309–323, 2015. doi:10.1515/forma-2015-0025.
[16] Noboru Endou and Yasunari Shidama. Integral of measurable function. *Formalized Mathematics*, 14(**2**):53–70, 2006. doi:10.2478/v10037-006-0008-x.
[17] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definitions and basic properties of measurable functions. *Formalized Mathematics*, 9(**3**):495–500, 2001.
[18] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. The measurability of extended real valued functions. *Formalized Mathematics*, 9(**3**):525–529, 2001.
[19] Noboru Endou, Keiko Narita, and Yasunari Shidama. The Lebesgue monotone convergence theorem. *Formalized Mathematics*, 16(**2**):167–175, 2008. doi:10.2478/v10037-008-0023-1.
[20] Noboru Endou, Hiroyuki Okazaki, and Yasunari Shidama. Hopf extension theorem of measure. *Formalized Mathematics*, 17(**2**):157–162, 2009. doi:10.2478/v10037-009-0018-6.
[21] Gerald B. Folland. *Real Analysis: Modern Techniques and Their Applications*. Wiley, 2 edition, 1999.
[22] P. R. Halmos. *Measure Theory*. Springer-Verlag, 1974.
[23] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.
[24] Beata Perkowska. Functional sequence from a domain to a domain. *Formalized Mathematics*, 3(**1**):17–21, 1992.
[25] M.M. Rao. *Measure Theory and Integration*. Marcel Dekker, 2nd edition, 2004.
[26] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.
[27] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
[28] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[29] Hiroshi Yamazaki, Noboru Endou, Yasunari Shidama, and Hiroyuki Okazaki. Inferior limit, superior limit and convergence of sequences of extended real numbers. *Formalized Mathematics*, 15(**4**):231–236, 2007. doi:10.2478/v10037-007-0026-3.

Received December 31, 2015

FORMALIZED MATHEMATICS
Vol. 24, No. 1, Pages 81–94, 2016
DOI: 10.1515/forma-2016-0007

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

Conservation Rules of Direct Sum Decomposition of Groups

Kazuhisa Nakasho
Shinshu University
Nagano, Japan

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, conservation rules of the direct sum decomposition of groups are mainly discussed. In the first section, we prepare miscellaneous definitions and theorems for further formalization in Mizar [5]. In the next three sections, we formalized the fact that the property of direct sum decomposition is preserved against the substitutions of the subscript set, flattening of direct sum, and layering of direct sum, respectively. We referred to [14], [13] [6] and [11] in the formalization.

MSC: 20E34 03B35

Keywords: group theory; direct sum decomposition

MML identifier: GROUP_21, version: 8.1.04 5.36.1267

1. Preliminaries

Let I, J be non empty sets, a be a function from I into J, and F be a multiplicative magma family of J. Observe that the functor $F \cdot a$ yields a multiplicative magma family of I. Let F be a group family of J. Let us observe that the functor $F \cdot a$ yields a group family of I. Let G be a group and F be a subgroup family of J and G. The functor $F \cdot a$ yielding a subgroup family of I and G is defined by the term

(Def. 1) $F \cdot a$.

The scheme *Sch1* deals with a set $\mathcal{A}$ and a 1-sorted structure $\mathcal{B}$ and a unary functor $\mathcal{F}$ yielding a set and states that

(Sch. 1) There exists a function f such that $\mathrm{dom}\, f = \mathcal{A}$ and for every element x of $\mathcal{B}$ such that $x \in \mathcal{A}$ holds $f(x) = \mathcal{F}(x)$.

Let I be a set. Let us note that there exists a many sorted set indexed by I which is non-empty and disjoint valued.

Now we state the propositions:

(1) Let us consider a non-empty, disjoint valued function f. If $\bigcup f$ is finite, then $\mathrm{dom}\, f$ is finite.
PROOF: For every objects x, y such that $x, y \in \mathrm{dom}\, f$ and $f(x) = f(y)$ holds $x = y$ by [7, (3)]. □

(2) Let us consider non empty sets X, Y, sets X_0, Y_0, and a function f from X into Y. Suppose f is bijective and $\mathrm{rng}(f \restriction X_0) = Y_0$. Then $(f \restriction X_0)^{-1} = f^{-1} \restriction Y_0$.
PROOF: For every object x such that $x \in \mathrm{dom}(f^{-1} \restriction Y_0)$ holds $(f^{-1} \restriction Y_0)(x) = (f \restriction X_0)^{-1}(x)$ by [18, (62)], [7, (49), (33)], [18, (59)]. □

2. Conservation Rule of Direct Sum Decomposition for Substitution of Subscript Set

Now we state the proposition:

(3) Let us consider non empty sets I, J, a function a from I into J, a multiplicative magma family F of J, and an element x of $\prod F$. Then $x \cdot a \in \prod (F \cdot a)$.
PROOF: Reconsider $y = x \cdot a$ as a many sorted set indexed by I. Reconsider $z =$ the support of $F \cdot a$ as a many sorted set indexed by I. For every object i such that $i \in I$ holds $y(i) \in z(i)$ by [7, (13)]. □

Let I, J be non empty sets, a be a function from I into J, and F be a multiplicative magma family of J. The functor $\mathrm{Trans}\prod(F, a)$ yielding a function from $\prod F$ into $\prod (F \cdot a)$ is defined by

(Def. 2) for every element x of $\prod F$, $it(x) = x \cdot a$.

Now we state the proposition:

(4) Let us consider non empty sets I, J, a function a from I into J, and a multiplicative magma family F of J. Then $\mathrm{Trans}\prod(F, a)$ is multiplicative.
PROOF: Reconsider $f = \mathrm{Trans}\prod(F, a)$ as a function from $\prod F$ into $\prod (F \cdot a)$. For every elements x, y of $\prod F$, $f(x \cdot y) = f(x) \cdot f(y)$ by (3), [7, (13)], [10, (1)], [18, (27)]. □

Let I, J be non empty sets, a be a function from I into J, and F be a group family of J. Let us observe that the functor $\mathrm{Trans}\prod(F, a)$ yields a homomorphism from $\prod F$ to $\prod(F \cdot a)$. Now we state the propositions:

(5) Let us consider non empty sets I, J, a function a from I into J, a multiplicative magma family F of J, and an element y of $\prod(F \cdot a)$. If a is bijective, then $y \cdot a^{-1} \in \prod F$.

Proof: Set $x = y \cdot a^{-1}$. For every object j such that $j \in J$ holds $x(j) \in$ (the support of F)(j) by [7, (32), (13)]. □

(6) Let us consider non empty sets I, J, a function a from I into J, and functions x, y. Suppose $\operatorname{dom} x = I$ and $\operatorname{dom} y = J$ and a is bijective. Then $x = y \cdot a$ if and only if $y = x \cdot a^{-1}$.

(7) Let us consider non empty sets I, J, a multiplicative magma family F of J, and a function a from I into J. Suppose a is bijective. Then

(i) $\operatorname{dom} \mathrm{Trans}\prod(F, a) = \Omega_{\prod F}$, and

(ii) $\operatorname{rng} \mathrm{Trans}\prod(F, a) = \Omega_{\prod(F \cdot a)}$.

The theorem is a consequence of (5) and (6).

(8) Let us consider non empty sets I, J, a function a from I into J, and a multiplicative magma family F of J. If a is bijective, then $\mathrm{Trans}\prod(F, a)$ is bijective.

Proof: Reconsider $f = \mathrm{Trans}\prod(F, a)$ as a function from $\prod F$ into $\prod(F \cdot a)$. $\operatorname{dom} f = \Omega_{\prod F}$ and $\operatorname{rng} f = \Omega_{\prod(F \cdot a)}$. For every objects x, y such that x, $y \in \operatorname{dom} f$ and $f(x) = f(y)$ holds $x = y$ by [7, (86)]. □

Let us consider non empty sets I, J, a function a from I into J, a group family F of J, and a function x. Now we state the propositions:

(9) If a is one-to-one, then $a^{\circ}(\mathrm{support}(x \cdot a, F \cdot a)) \subseteq \mathrm{support}(x, F)$.

Proof: For every object j such that $j \in a^{\circ}(\mathrm{support}(x \cdot a, F \cdot a))$ holds $j \in \mathrm{support}(x, F)$ by [7, (13)]. □

(10) If a is onto, then $\mathrm{support}(x, F) \subseteq a^{\circ}(\mathrm{support}(x \cdot a, F \cdot a))$.

Proof: For every object j such that $j \in \mathrm{support}(x, F)$ holds $j \in a^{\circ}(\mathrm{support}(x \cdot a, F \cdot a))$ by [8, (11)], [7, (13)]. □

(11) If a is one-to-one, then if $x \in \operatorname{sum} F$, then $x \cdot a \in \operatorname{sum}(F \cdot a)$. The theorem is a consequence of (3) and (9).

(12) If a is bijective, then $x \in \operatorname{sum} F$ iff $x \cdot a \in \operatorname{sum}(F \cdot a)$ and $\operatorname{dom} x = J$. The theorem is a consequence of (11).

Let I, J be non empty sets, a be a function from I into J, and F be a group family of J. Assume a is bijective. The functor $\mathrm{Trans}\sum(F, a)$ yielding a function from $\operatorname{sum} F$ into $\operatorname{sum}(F \cdot a)$ is defined by the term

(Def. 3) $\mathrm{Trans}\prod(F, a) \restriction \mathrm{sum}\, F$.

Now we state the proposition:

(13) Let us consider groups G, H, a subgroup H_0 of H, and a homomorphism f from G to H. Suppose $\mathrm{rng}\, f \subseteq \Omega_{H_0}$. Then f is a homomorphism from G to H_0.

PROOF: Reconsider $g = f$ as a function from G into H_0. For every elements a, b of G, $g(a \cdot b) = g(a) \cdot g(b)$ by [16, (43)]. □

Let I, J be non empty sets, a be a function from I into J, and F be a group family of J. Assume a is bijective. Let us observe that the functor $\mathrm{Trans}\sum(F, a)$ yields a homomorphism from $\mathrm{sum}\, F$ to $\mathrm{sum}(F \cdot a)$. Now we state the propositions:

(14) Let us consider non empty sets I, J, a function a from I into J, and a group family F of J. If a is bijective, then $\mathrm{Trans}\sum(F, a)$ is bijective.

PROOF: Reconsider $f = \mathrm{Trans}\prod(F, a)$ as a homomorphism from $\prod F$ to $\prod(F \cdot a)$. Reconsider $g = \mathrm{Trans}\sum(F, a)$ as a homomorphism from $\mathrm{sum}\, F$ to $\mathrm{sum}(F \cdot a)$. f is bijective. For every object y such that $y \in \Omega_{\mathrm{sum}(F \cdot a)}$ holds $y \in \mathrm{rng}\, g$ by [16, (42)], (5), (6), (12). □

(15) Let us consider a group G, non empty sets I, J, a direct sum components F of G and J, and a function a from I into J. If a is bijective, then $F \cdot a$ is a direct sum components of G and I. The theorem is a consequence of (14).

(16) Let us consider a non empty set I, and a group G. Then every internal direct sum components of G and I is a subgroup family of I and G.

(17) Let us consider non empty sets I, J, a group G, a function x from I into G, a function y from J into G, and a function a from I into J. Suppose a is onto and $x = y \cdot a$. Then $\mathrm{support}\, y = a^{\circ}(\mathrm{support}\, x)$.

(18) Let us consider non empty sets I, J, a commutative group G, a finite-support function x from I into G, a finite-support function y from J into G, and a function a from I into J. If a is bijective and $x = y \cdot a$, then $\prod x = \prod y$.

PROOF: Reconsider $S_1 = \mathrm{support}\, x$ as a finite set. Reconsider $S_2 = \mathrm{support}\, y$ as a finite set. Reconsider $s_1 = \mathrm{CFS}(S_1)$ as a finite sequence of elements of S_1. Reconsider $s_2 = \mathrm{CFS}(S_2)$ as a finite sequence of elements of S_2. Reconsider $x_1 = x \restriction S_1$ as a function from S_1 into G. Consider x_2 being a finite sequence of elements of G such that $\prod x_1 = \prod x_2$ and $x_2 = x_1 \cdot s_1$. Reconsider $y_1 = y \restriction S_2$ as a function from S_2 into G. Consider y_2 being a finite sequence of elements of G such that $\prod y_1 = \prod y_2$ and $y_2 = y_1 \cdot s_2$. $S_2 = a^{\circ} S_1$. $\overline{\overline{S_1}} = \overline{\overline{S_2}}$ by [1, (66)], [8, (25)], [17, (63)], [8, (17), (29)]. Reconsider $n = \overline{\overline{S_1}}$ as a natural number. Reconsider $a_1 = a \restriction S_1$ as a function from S_1 into J. Reconsider $a_2 = {s_2}^{-1}$ as a function from S_2 into $\mathrm{Seg}\, n$.

Reconsider $p = a_2 \cdot a_1 \cdot s_1$ as a function. If S_2 is not empty, then $x_2 = y_2 \cdot p$ by [18, (27)], [7, (3), (12), (47)]. □

(19) Let us consider non empty sets I, J, a group G, a finite-support function x from I into G, a finite-support function y from J into G, and a function a from I into J. Suppose a is bijective and $x = y \cdot a$ and for every elements i, j of I, $x(i) \cdot x(j) = x(j) \cdot x(i)$. Then $\prod x = \prod y$. The theorem is a consequence of (18).

(20) Let us consider a group G, non empty sets I, J, an internal direct sum components F of G and J, and a function a from I into J. Suppose a is bijective. Then $F \cdot a$ is an internal direct sum components of G and I.
Proof: Reconsider $E = F \cdot a$ as a direct sum components of G and I. For every element i of I, $E(i)$ is a subgroup of G by [7, (13)]. There exists a homomorphism h from $\operatorname{sum} E$ to G such that h is bijective and for every finite-support function x from I into G such that $x \in \operatorname{sum} E$ holds $h(x) = \prod x$ by (14), [17, (62), (63)], [12, (25)]. □

3. Conservation Rule of Direct Sum Decomposition for Flattening

Let I be a non empty set and J be a many sorted set indexed by I.

A J-indexed family of multiplicative magma families is a many sorted set indexed by I and is defined by

(Def. 4) for every element i of I, $it(i)$ is a multiplicative magma family of $J(i)$.

A J-indexed family of group families is a J-indexed family of multiplicative magma families and is defined by

(Def. 5) for every element i of I, $it(i)$ is a group family of $J(i)$.

Let N be a J-indexed family of multiplicative magma families and i be an element of I. One can verify that the functor $N(i)$ yields a multiplicative magma family of $J(i)$. Let N be a J-indexed family of group families. Observe that the functor $N(i)$ yields a group family of $J(i)$. Let J be a disjoint valued many sorted set indexed by I and F be a J-indexed family of group families. One can verify that the functor $\bigcup F$ yields a group family of $\bigcup J$. Now we state the proposition:

(21) Let us consider a non empty set I, a disjoint valued many sorted set J indexed by I, a J-indexed family of group families F, an element j of I, and an object i. If $i \in J(j)$, then $(\bigcup F)(i) = F(j)(i)$.

Let I be a non empty set, J be a many sorted set indexed by I, and F be a J-indexed family of multiplicative magma families. The functor $\operatorname{ProdBundle}(F)$ yielding a multiplicative magma family of I is defined by

(Def. 6) for every element i of I, $it(i) = \prod(F(i))$.

Let F be a J-indexed family of group families.

Note that the functor ProdBundle(F) yields a group family of I. The functor SumBundle(F) yielding a group family of I is defined by

(Def. 7) for every element i of I, $it(i) = \mathrm{sum}(F(i))$.

Let F be a J-indexed family of multiplicative magma families. The functor $\mathrm{d}\prod F$ yielding a multiplicative magma is defined by the term

(Def. 8) $\prod \mathrm{ProdBundle}(F)$.

Let J be a non-empty many sorted set indexed by I. One can check that $\mathrm{d}\prod F$ is non empty and constituted functions.

Let F be a J-indexed family of group families. Observe that $\mathrm{d}\prod F$ is group-like and associative.

The functor $\mathrm{d}\sum F$ yielding a group is defined by the term

(Def. 9) $\mathrm{sum}\,\mathrm{SumBundle}(F)$.

Note that $\mathrm{d}\sum F$ is non empty and constituted functions.

Let us consider a non empty set I and group families F_1, F_2 of I.

Let us assume that for every element i of I, $F_1(i)$ is a subgroup of $F_2(i)$. Now we state the propositions:

(22) $\prod F_1$ is a subgroup of $\prod F_2$.

PROOF: For every object x such that $x \in \Omega_{\prod F_1}$ holds $x \in \Omega_{\prod F_2}$. Reconsider $f_2 =$ (the multiplication of $\prod F_2$) $\restriction \Omega_{\prod F_1}$ as a function from $\Omega_{\prod F_1} \times \Omega_{\prod F_1}$ into $\Omega_{\prod F_2}$. Reconsider $f_1 =$ the multiplication of $\prod F_1$ as a function from $\Omega_{\prod F_1} \times \Omega_{\prod F_1}$ into $\Omega_{\prod F_2}$. For every sets x, y such that $x, y \in \Omega_{\prod F_1}$ holds $f_1(x, y) = f_2(x, y)$ by [10, (1)], [16, (43)], [7, (49)], [9, (87)]. $\square$

(23) $\mathrm{sum}\,F_1$ is a subgroup of $\mathrm{sum}\,F_2$.

PROOF: For every object x such that $x \in \Omega_{\mathrm{sum}\,F_1}$ holds $x \in \Omega_{\mathrm{sum}\,F_2}$ by [16, (40)], (22), [16, (42), (44)]. $\prod F_1$ is a subgroup of $\prod F_2$. $\square$

(24) Let us consider a non empty set I, a non-empty many sorted set J indexed by I, and a J-indexed family of group families F. Then $\mathrm{d}\sum F$ is a subgroup of $\mathrm{d}\prod F$. The theorem is a consequence of (22).

Let I be a non empty set, J be a non-empty, disjoint valued many sorted set indexed by I, and F be a J-indexed family of group families. One can verify that the functor $\mathrm{d}\sum F$ yields a subgroup of $\mathrm{d}\prod F$. The functor dProd2Prod(F) yielding a homomorphism from $\mathrm{d}\prod F$ to $\prod \bigcup F$ is defined by

(Def. 10) for every element x of $\mathrm{d}\prod F$ and for every element i of I, $x(i) = it(x) \restriction J(i)$.

Now we state the proposition:

(25) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, a J-indexed family of group families F, an element y of $\prod \bigcup F$, and an element i of I. Then $y \restriction J(i) \in \prod(F(i))$.
PROOF: Set $x = y \restriction J(i)$. Set $z =$ the support of $F(i)$. For every object j such that $j \in J(i)$ holds $x(j) \in z(j)$ by [7, (49), (1)]. $\square$

Let I be a non empty set, J be a non-empty, disjoint valued many sorted set indexed by I, and F be a J-indexed family of group families. Note that $\mathrm{dProd2Prod}(F)$ is bijective.

The functor $\mathrm{Prod2dProd}(F)$ yielding a homomorphism from $\prod \bigcup F$ to $\mathrm{d}\prod F$ is defined by the term

(Def. 11) $(\mathrm{dProd2Prod}(F))^{-1}$.

Now we state the proposition:

(26) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, a J-indexed family of group families F, an element x of $\prod \bigcup F$, and an element i of I. Then $x \restriction J(i) = (\mathrm{Prod2dProd}(F))(x)(i)$.

Let I be a non empty set, J be a non-empty, disjoint valued many sorted set indexed by I, and F be a J-indexed family of group families. Note that $\mathrm{Prod2dProd}(F)$ is bijective.

(27) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, and a J-indexed family of group families F. Then $\mathrm{Prod2dProd}(F) = (\mathrm{dProd2Prod}(F))^{-1}$.

Let I be a non empty set, J be a non-empty, disjoint valued many sorted set indexed by I, F be a J-indexed family of group families, and x be a function. The functor $\mathrm{rsupport}(x, F)$ yielding a disjoint valued many sorted set indexed by I is defined by

(Def. 12) for every element i of I, $it(i) = \mathrm{support}(x \restriction J(i), F(i))$.

Now we state the propositions:

(28) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, a J-indexed family of group families F, and a function x. Then $\mathrm{support}(x, \bigcup F) = \bigcup \mathrm{rsupport}(x, F)$.
PROOF: Set $y = \mathrm{rsupport}(x, F)$. For every object j, $j \in \mathrm{support}(x, \bigcup F)$ iff $j \in \bigcup y$ by (21), [7, (49), (3)], [9, (74)]. $\square$

(29) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, a J-indexed family of group families F, and functions x, y, z. Suppose $z \in \mathrm{d}\prod F$ and $x = (\mathrm{dProd2Prod}(F))(z)$. Then

(i) $\mathrm{rsupport}(x, F) \restriction \mathrm{support}(z, \mathrm{SumBundle}(F))$ is a non-empty, disjoint valued many sorted set indexed by $\mathrm{support}(z, \mathrm{SumBundle}(F))$, and

(ii) $\mathrm{support}(x, \bigcup F) = \bigcup(\mathrm{rsupport}(x, F) \restriction \mathrm{support}(z, \mathrm{SumBundle}(F)))$.

PROOF: Set $s_1 = \mathrm{rsupport}(x, F)$. Set $s_2 = \mathrm{support}(z, \mathrm{SumBundle}(F))$. Set $f = s_1 \restriction s_2$. For every objects s, t such that $s \neq t$ holds $f(s)$ misses $f(t)$ by [7, (47)]. $\emptyset \notin \mathrm{rng}\, f$ by [7, (47)], [10, (5)], [16, (44)]. $\mathrm{support}(x, \bigcup F) = \bigcup s_1$. For every object k such that $k \in \mathrm{support}(x, \bigcup F)$ holds $k \in \bigcup(s_1 \restriction s_2)$ by [10, (6)], [16, (44)], [18, (57)], [7, (47), (3)]. □

(30) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, a J-indexed family of group families F, and a function y. Suppose $y \in \mathrm{sum} \bigcup F$. Then there exists a function x such that

(i) $y = (\mathrm{dProd2Prod}(F))(x)$, and

(ii) $x \in \mathrm{d}\sum F$.

PROOF: Consider x being an element of $\Omega_{\mathrm{d}\prod F}$ such that $y = (\mathrm{dProd2Prod}(F))(x)$. Set $s_1 = \mathrm{rsupport}(y, F)$. $\mathrm{support}(y, \bigcup F) = \bigcup s_1$. For every element i of I, $x(i) \in (\mathrm{SumBundle}(F))(i)$ by [7, (3)], [9, (74)], [12, (8)]. Set $S = \mathrm{SumBundle}(F)$. Reconsider $W =$ the support of S as a many sorted set indexed by I. For every object i such that $i \in I$ holds $x(i) \in W(i)$. Reconsider $s_2 = s_1 \restriction \mathrm{support}(x, \mathrm{SumBundle}(F))$ as a non-empty, disjoint valued many sorted set indexed by $\mathrm{support}(x, \mathrm{SumBundle}(F))$. $\bigcup s_2$ is finite. $\mathrm{dom}\, s_2$ is finite. □

(31) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, a J-indexed family of group families F, and functions x, y. Suppose x, $x \in \mathrm{d}\sum F$. Then $(\mathrm{dProd2Prod}(F))(x) \in \mathrm{sum} \bigcup F$.
PROOF: Reconsider $y = (\mathrm{dProd2Prod}(F))(x)$ as an element of $\prod \bigcup F$. Set $s_1 = \mathrm{rsupport}(y, F)$. Reconsider $s_2 = s_1 \restriction \mathrm{support}(x, \mathrm{SumBundle}(F))$ as a non-empty, disjoint valued many sorted set indexed by $\mathrm{support}(x, \mathrm{SumBundle}(F))$. For every object i such that $i \in \mathrm{dom}\, s_2$ holds $s_2(i)$ is finite by [16, (40)], [7, (49)]. $\mathrm{support}(y, \bigcup F)$ is finite. □

(32) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, and a J-indexed family of group families F. Then $\mathrm{rng}(\mathrm{dProd2Prod}(F) \restriction \mathrm{d}\sum F) = \Omega_{\mathrm{sum} \bigcup F}$.
PROOF: For every object y, $y \in \mathrm{rng}(\mathrm{dProd2Prod}(F) \restriction \Omega_{\mathrm{d}\sum F})$ iff $y \in \Omega_{\mathrm{sum} \bigcup F}$ by [18, (61)], (31), [7, (47)], (30). □

Let I be a non empty set, J be a non-empty, disjoint valued many sorted set indexed by I, and F be a J-indexed family of group families. The functor $\mathrm{dSum2Sum}(F)$ yielding a homomorphism from $\mathrm{d}\sum F$ to $\mathrm{sum} \bigcup F$ is defined by the term

(Def. 13) $\mathrm{dProd2Prod}(F) \restriction \mathrm{d}\sum F$.

One can verify that $\mathrm{dSum2Sum}(F)$ is bijective.

The functor Sum2dSum(F) yielding a homomorphism from sum $\bigcup F$ to d$\sum F$ is defined by the term

(Def. 14) $(\mathrm{dSum2Sum}(F))^{-1}$.

Now we state the proposition:

(33) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, and a J-indexed family of group families F. Then Sum2dSum(F) = Prod2dProd(F)$\restriction$sum $\bigcup F$. The theorem is a consequence of (2).

Let I be a non empty set, J be a non-empty, disjoint valued many sorted set indexed by I, and F be a J-indexed family of group families. One can check that Sum2dSum(F) is bijective.

Now we state the proposition:

(34) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, and a J-indexed family of group families F. Then dSum2Sum(F) = $(\mathrm{Sum2dSum}(F))^{-1}$.

Let I be a non empty set, G be a group, and F be an internal direct sum components of G and I. The functor InterHom(F) yielding a homomorphism from sum F to G is defined by

(Def. 15) *it* is bijective and for every finite-support function x from I into G such that $x \in$ sum F holds $it(x) = \prod x$.

Let J be a non-empty, disjoint valued many sorted set indexed by I, M be a direct sum components of G and I, N be a J-indexed family of group families, and h be a many sorted set indexed by I. Assume for every element i of I, there exists a homomorphism h_0 from (SumBundle(N))(i) to $M(i)$ such that $h_0 = h(i)$ and h_0 is bijective. The functor ProdHom(G, M, N, h) yielding a homomorphism from d$\sum N$ to sum M is defined by

(Def. 16) it = SumMap(SumBundle(N), M, h) and *it* is bijective.

Now we state the propositions:

(35) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, a group G, a direct sum components M of G and I, and a J-indexed family of group families N. Suppose for every element i of I, $N(i)$ is a direct sum components of $M(i)$ and $J(i)$. Then $\bigcup N$ is a direct sum components of G and $\bigcup J$.

PROOF: Consider f_2 being a homomorphism from sum M to G such that f_2 is bijective. Define $\mathcal{P}(\text{object}) = \Omega_{\mathrm{sum}(N(\$_1(\in I)))}$. Consider D_2 being a function such that dom $D_2 = I$ and for every object i such that $i \in I$ holds $D_2(i) = \mathcal{P}(i)$ from [7, Sch. 3]. Define $\mathcal{Q}(\text{object}) = \Omega_{M(\$_1(\in I))}$. Consider R_1 being a function such that dom $R_1 = I$ and for every object i such that $i \in I$ holds $R_1(i) = \mathcal{Q}(i)$ from [7, Sch. 3]. Define $\mathcal{R}[\text{object}, \text{object}] \equiv$ there exists a homomorphism f_3 from $\text{sum}(N(\$_1(\in I)))$ to $M(\$_1(\in I))$ such that $f_3 = \$_2$ and f_3 is bijective. For every element i of I, there exists an element y of $\bigcup D_2 \dot{\to} \bigcup R_1$ such that $\mathcal{R}[i, y]$ by [7, (3)], [9, (74)]. Consider f_1 being a function from I into $\bigcup D_2 \dot{\to} \bigcup R_1$ such that for every element i of I, $\mathcal{R}[i, f_1(i)]$ from [8, Sch. 3]. For every element i of I, there exists a homomorphism h_0 from $(\text{SumBundle}(N))(i)$ to $M(i)$ such that $h_0 = f_1(i)$ and h_0 is bijective. $\square$

(36) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, a group G, an internal direct sum components M of G and I, and a J-indexed family of group families N. Suppose for every element i of I, $N(i)$ is an internal direct sum components of $M(i)$ and $J(i)$. Then $\bigcup N$ is an internal direct sum components of G and $\bigcup J$.
PROOF: Consider f_3 being a homomorphism from $\text{sum}\, M$ to G such that f_3 is bijective and for every finite-support function x from I into G such that $x \in \text{sum}\, M$ holds $f_3(x) = \prod x$. Define $\mathcal{Q}[\text{object}, \text{object}] \equiv$ there exists an internal direct sum components N_1 of $M(\$_1(\in I))$ and $J(\$_1(\in I))$ such that $N_1 = N(\$_1)$ and $\$_2 = \text{InterHom}(N_1)$. For every object x such that $x \in I$ there exists an object y such that $\mathcal{Q}[x, y]$. Consider f_1 being a function such that $\text{dom}\, f_1 = I$ and for every object i such that $i \in I$ holds $\mathcal{Q}[i, f_1(i)]$ from [7, Sch. 2]. Set $f_2 = \text{ProdHom}(G, M, N, f_1)$. For every element i of I, there exists a homomorphism h_0 from $(\text{SumBundle}(N))(i)$ to $M(i)$ such that $h_0 = f_1(i)$ and h_0 is bijective and for every finite-support function x from $J(i)$ into $M(i)$ such that $x \in (\text{SumBundle}(N))(i)$ holds $h_0(x) = \prod x$. For every element i of I, there exists a homomorphism h_0 from $(\text{SumBundle}(N))(i)$ to $M(i)$ such that $h_0 = f_1(i)$ and h_0 is bijective. Reconsider $h = f_3 \cdot f_2 \cdot \text{Sum2dSum}(N)$ as a homomorphism from $\text{sum} \bigcup N$ to G. Reconsider $U_2 = \bigcup J$ as a non empty set. Reconsider $U_3 = \bigcup N$ as a direct sum components of G and U_2. For every object j such that $j \in U_2$ holds $U_3(j)$ is a subgroup of G by (21), [16, (56)]. For every finite-support function x from U_2 into G such that $x \in \text{sum}\, U_3$ holds $h(x) = \prod x$ by [16, (42), (40)], [7, (13)], [8, (5), (15)]. $\square$

4. Conservation Rule of Direct Sum Decomposition for Layering

Now we state the propositions:

(37) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, a group G, a group family M of I, and a J-indexed family of group families N. Suppose $\bigcup N$ is a direct sum components of G and $\bigcup J$ and for every element i of I, $N(i)$ is a direct sum

components of $M(i)$ and $J(i)$. Then M is a direct sum components of G and I.

PROOF: Set $U_3 = \bigcup N$. Consider f_4 being a homomorphism from sum U_3 to G such that f_4 is bijective. Define $\mathcal{P}(\text{object}) =$ the carrier of sum$(N(\$_1(\in I)))$. Consider D_2 being a function such that $\operatorname{dom} D_2 = I$ and for every object i such that $i \in I$ holds $D_2(i) = \mathcal{P}(i)$ from [7, Sch. 3]. Define $\mathcal{Q}(\text{object}) =$ the carrier of $M(\$_1(\in I))$. Consider R_1 being a function such that $\operatorname{dom} R_1 = I$ and for every object i such that $i \in I$ holds $R_1(i) = \mathcal{Q}(i)$ from [7, Sch. 3]. Define $\mathcal{R}[\text{object}, \text{object}] \equiv$ there exists a homomorphism f_3 from $M(\$_1(\in I))$ to sum$(N(\$_1(\in I)))$ such that $f_3 = \$_2$ and f_3 is bijective. For every element i of I, there exists an element y of $\bigcup R_1 \dot{\rightarrow} \bigcup D_2$ such that $\mathcal{R}[i, y]$ by [17, (62), (63)], [7, (3)], [9, (74)]. Consider f_1 being a function from I into $\bigcup R_1 \dot{\rightarrow} \bigcup D_2$ such that for every element i of I, $\mathcal{R}[i, f_1(i)]$ from [8, Sch. 3]. For every element i of I, there exists a homomorphism h_0 from $M(i)$ to $(\text{SumBundle}(N))(i)$ such that $h_0 = f_1(i)$ and h_0 is bijective. $\square$

(38) Let us consider a non empty set I, a non-empty, disjoint valued many sorted set J indexed by I, a group G, a subgroup family M of I and G, and a J-indexed family of group families N. Suppose $\bigcup N$ is an internal direct sum components of G and $\bigcup J$ and for every element i of I, $N(i)$ is an internal direct sum components of $M(i)$ and $J(i)$. Then M is an internal direct sum components of G and I.

PROOF: Reconsider $U_2 = \bigcup J$ as a non empty set. Consider f_4 being a homomorphism from sum $\bigcup N$ to G such that f_4 is bijective and for every finite-support function x from U_2 into G such that $x \in$ sum $\bigcup N$ holds $f_4(x) = \prod x$. Define $\mathcal{Q}[\text{object}, \text{object}] \equiv$ there exists an internal direct sum components N_1 of $M(\$_1(\in I))$ and $J(\$_1(\in I))$ such that $N_1 = N(\$_1)$ and $\$_2 = (\text{InterHom}(N_1))^{-1}$. For every object x such that $x \in I$ there exists an object y such that $\mathcal{Q}[x, y]$.

Consider f_1 being a function such that $\operatorname{dom} f_1 = I$ and for every object i such that $i \in I$ holds $\mathcal{Q}[i, f_1(i)]$ from [7, Sch. 2]. Reconsider $f_3 = \text{SumMap}(M, (\text{SumBundle}(N)), f_1)$ as a homomorphism from sum M to $\text{d}\sum N$. For every element i of I, there exists a homomorphism h_0 from $M(i)$ to $(\text{SumBundle}(N))(i)$ such that $h_0 = f_1(i)$ and h_0 is bijective by [17, (62), (63)]. Reconsider $h = f_4 \cdot \text{dSum2Sum}(N) \cdot f_3$ as a homomorphism from sum M to G. For every element i of I, there exists a homomorphism h_0 from $(\text{SumBundle}(N))(i)$ to $M(i)$ such that $h_0{}^{-1} = f_1(i)$ and h_0 is bijective and for every finite-support function x from $J(i)$ into $M(i)$ such that $x \in (\text{SumBundle}(N))(i)$ holds $h_0(x) = \prod x$. For every element i of I, there exists a homomorphism h_0 from $(\text{SumBundle}(N))(i)$ to $M(i)$ such that ${h_0}^{-1} = f_1(i)$ and h_0 is bijective. For every finite-support function x from I into G such that $x \in \operatorname{sum} M$ holds $h(x) = \prod x$ by [16, (40)], [7, (13)], [8, (5), (15)]. □

(39) Let us consider a non empty set I_2, and a group family F_2 of I_2. Suppose for every element i of I_2, $\overline{\overline{F_2(i)}} = 1$. Then $\overline{\overline{\alpha}} = 1$, where α is the carrier of $\operatorname{sum} F_2$.

PROOF: For every object x such that $x \in \Omega_{\operatorname{sum} F_2}$ holds $x = \mathbf{1}_{\operatorname{sum} F_2}$ by [16, (42)], [1, (30)], [2, (102)], [10, (5)]. □

(40) Let us consider a non empty set I, a group G, and a finite-support function x from I into G. Suppose for every object i such that $i \in I$ holds $x(i) = \mathbf{1}_G$. Then $\prod x = \mathbf{1}_G$.

(41) Let us consider a non empty set I, a group G, a finite-support function x from I into G, and an element a of G. If $I = \{1, 2\}$ and $x = \langle a, \mathbf{1}_G\rangle$, then $\prod x = a$.

PROOF: Reconsider $i_1 = 1$ as an element of I. Set $y = (I \longmapsto \mathbf{1}_G) +\cdot (i_1, a)$. For every object i such that $i \in \operatorname{dom} x$ holds $x(i) = y(i)$ by [3, (44)], [4, (31), (32)], [15, (7)]. □

(42) Let us consider a group G, non empty sets I_1, I_2, a direct sum components F_1 of G and I_1, and a group family F_2 of I_2. Suppose I_1 misses I_2 and for every element i of I_2, $\overline{\overline{F_2(i)}} = 1$. Then $F_1 +\cdot F_2$ is a direct sum components of G and $I_1 \cup I_2$.

PROOF: Reconsider $I = \{1, 2\}$ as a non empty set. Set $J = \{\langle 1, I_1\rangle, \langle 2, I_2\rangle\}$. For every objects x, y_1, y_2 such that $\langle x, y_1\rangle$, $\langle x, y_2\rangle \in J$ holds $y_1 = y_2$. $\emptyset \notin \operatorname{rng} J$. For every objects i, j such that $i \neq j$ holds $J(i)$ misses $J(j)$. Reconsider $M = \langle \operatorname{sum} F_1, \operatorname{sum} F_2\rangle$ as a group family of I. $\overline{\overline{\Omega_{\operatorname{sum} F_2}}} = 1$. Consider w being an object such that $\{w\} = \Omega_{\operatorname{sum} F_2}$. For every functions x, y such that $x, y \in \Omega_{\prod M}$ and $x(1) = y(1)$ holds $x = y$ by [12, (5)], [3, (44)].

Consider h_1 being a homomorphism from $\operatorname{sum} F_1$ to G such that h_1 is bijective. Set $C_1 =$ the carrier of $\prod M$. Set $C_2 =$ the carrier of G. Define $\mathcal{P}[\text{element of } C_1, \text{element of } C_2] \equiv \$_2 = h_1(\$_1(1))$. For every element x of C_1, there exists an element y of C_2 such that $\mathcal{P}[x, y]$ by [12, (5)], [3, (44)], [8, (5)]. Consider h being a function from C_1 into C_2 such that for every element x of C_1, $\mathcal{P}[x, h(x)]$ from [8, Sch. 3]. For every objects x_1, x_2 such that $x_1, x_2 \in C_1$ and $h(x_1) = h(x_2)$ holds $x_1 = x_2$ by [12, (5)], [3, (44)], [8, (19)]. For every object y such that $y \in C_2$ there exists an object x such that $x \in C_1$ and $y = h(x)$ by [8, (11)], [3, (44)]. For every elements a, b of C_1, $h(a \cdot b) = h(a) \cdot h(b)$ by [3, (44)], [12, (5)], [10, (1)]. Reconsider $M = \langle \operatorname{sum} F_1, \operatorname{sum} F_2\rangle$ as a direct sum components of G and I. Set $N = \langle F_1, F_2 \rangle$. For every element i of I, $N(i)$ is a group family of $J(i)$ by [3, (44)]. For every element i of I, $N(i)$ is a direct sum components of $M(i)$ and $J(i)$ by [3, (44)]. For every object x such that $x \in \operatorname{dom} F_1 \cup \operatorname{dom} F_2$ holds if $x \in \operatorname{dom} F_2$, then $(\bigcup N)(x) = F_2(x)$ and if $x \notin \operatorname{dom} F_2$, then $(\bigcup N)(x) = F_1(x)$ by (21), [3, (44)]. $\square$

(43) Let us consider a group G, non empty sets I_1, I_2, an internal direct sum components F_1 of G and I_1, and a subgroup family F_2 of I_2 and G. Suppose I_1 misses I_2 and $F_2 = I_2 \longmapsto \{\mathbf{1}\}_G$. Then $F_1 {+\cdot} F_2$ is an internal direct sum components of G and $I_1 \cup I_2$.

PROOF: Reconsider $I = \{1, 2\}$ as a non empty set. Set $J = \{\langle 1, I_1 \rangle, \langle 2, I_2 \rangle\}$. For every objects x, y_1, y_2 such that $\langle x, y_1 \rangle$, $\langle x, y_2 \rangle \in J$ holds $y_1 = y_2$. $\emptyset \notin \operatorname{rng} J$. For every objects i, j such that $i \neq j$ holds $J(i)$ misses $J(j)$. Reconsider $M = \langle G, \{\mathbf{1}\}_G \rangle$ as a group family of I. For every functions x, y such that x, $y \in \Omega_{\prod M}$ and $x(1) = y(1)$ holds $x = y$ by [12, (5)], [3, (44)]. Set $h_1 = \mathrm{id}_{(\text{the carrier of } G)}$. Set $C_1 =$ the carrier of $\prod M$. Set $C_2 =$ the carrier of G. Define $\mathcal{P}[\text{element of } C_1, \text{element of } C_2] \equiv \$_2 = h_1(\$_1(1))$. For every element x of C_1, there exists an element y of C_2 such that $\mathcal{P}[x, y]$ by [12, (5)], [3, (44)], [8, (5)]. Consider h being a function from C_1 into C_2 such that for every element x of C_1, $\mathcal{P}[x, h(x)]$ from [8, Sch. 3]. For every objects x_1, x_2 such that x_1, $x_2 \in C_1$ and $h(x_1) = h(x_2)$ holds $x_1 = x_2$ by [12, (5)], [3, (44)], [8, (19)]. For every object y such that $y \in C_2$ there exists an object x such that $x \in C_1$ and $y = h(x)$ by [8, (11)], [3, (44)]. For every elements a, b of C_1, $h(a \cdot b) = h(a) \cdot h(b)$ by [3, (44)], [12, (5)], [10, (1)].

Reconsider $M = \langle G, \{\mathbf{1}\}_G \rangle$ as a direct sum components of G and I. For every element i of I, $M(i)$ is a subgroup of G by [3, (44)], [16, (54)]. For every finite-support function x from I into G such that $x \in \operatorname{sum} M$ holds $h(x) = \prod x$ by [10, (9)], [3, (44)], (41). Set $N = \langle F_1, F_2 \rangle$. For every element i of I, $N(i)$ is a group family of $J(i)$ by [3, (44)]. For every element i of I, $N(i)$ is an internal direct sum components of $M(i)$ and $J(i)$ by [3, (44)], [15, (7)], [1, (30)], (39). For every object x such that $x \in \operatorname{dom} F_1 \cup \operatorname{dom} F_2$ holds if $x \in \operatorname{dom} F_2$, then $(\bigcup N)(x) = F_2(x)$ and if $x \notin \operatorname{dom} F_2$, then $(\bigcup N)(x) = F_1(x)$ by (21), [3, (44)]. $\square$

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

[4] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized*

Mathematics, 5(**4**):485–492, 1996.

[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] Nicolas Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3.* Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1989.

[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] Artur Korniłowicz. The product of the families of the groups. *Formalized Mathematics*, 7(**1**):127–134, 1998.

[11] Serge Lang. *Algebra*. Springer, 3rd edition, 2005.

[12] Kazuhisa Nakasho, Hiroshi Yamazaki, Hiroyuki Okazaki, and Yasunari Shidama. Definition and properties of direct sum decomposition of groups. *Formalized Mathematics*, 23 (**1**):15–27, 2015. doi:10.2478/forma-2015-0002.

[13] D. Robinson. *A Course in the Theory of Groups*. Springer New York, 2012.

[14] J.J. Rotman. *An Introduction to the Theory of Groups*. Springer, 1995.

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

[16] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**): 855–864, 1990.

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

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

Received December 31, 2015