FORMALIZED MATHEMATICS
Vol. 25, No. 1, Pages 1–29, 2017
DOI: 10.1515/forma-2017-0001

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

Fubini's Theorem on Measure

Noboru Endou
National Institute of Technology, Gifu College
2236-2 Kamimakuwa, Motosu, Gifu, Japan

Summary. The purpose of this article is to show Fubini's theorem on measure [16], [4], [7], [15], [18]. Some theorems have the possibility of slight generalization, but we have priority to avoid the complexity of the description. First of all, for the product measure constructed in [14], we show some theorems. Then we introduce the section which plays an important role in Fubini's theorem, and prove the relevant proposition. Finally we show Fubini's theorem on measure.

MSC: 28A35 03B35

Keywords: Fubini's theorem; product measure

MML identifier: `MEASUR11`, version: `8.1.05 5.40.1286`

1. Preliminaries

Now we state the propositions:

(1) Let us consider a disjoint valued finite sequence F, and natural numbers n, m. If $n < m$, then $\bigcup \operatorname{rng}(F{\restriction}n)$ misses $F(m)$.

(2) Let us consider a finite sequence F, and natural numbers m, n. Suppose $m \leqslant n$. Then $\operatorname{len}(F{\restriction}m) \leqslant \operatorname{len}(F{\restriction}n)$.

(3) Let us consider a finite sequence F, and a natural number n. Then $\bigcup \operatorname{rng}(F{\restriction}n) \cup F(n+1) = \bigcup \operatorname{rng}(F{\restriction}(n+1))$. The theorem is a consequence of (2).

(4) Let us consider a disjoint valued finite sequence F, and a natural number n. Then $\bigcup (F{\restriction}n)$ misses $F(n+1)$.

(5) Let us consider a set P, and a finite sequence F. Suppose P is $\cup$-closed and $\emptyset \in P$ and for every natural number n such that $n \in \operatorname{dom} F$ holds $F(n) \in P$. Then $\bigcup F \in P$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \bigcup \operatorname{rng}(F{\restriction}\$_1) \in P$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [2, (13)], [3, (59)], [19, (55)], [3, (82)]. For every natural number k, $\mathcal{P}[k]$ from [2, Sch. 2]. $\square$

Let A, X be sets. Observe that the functor $\chi_{A,X}$ yields a function from X into $\overline{\mathbb{R}}$. Let X be a non empty set, S be a σ-field of subsets of X, and F be a finite sequence of elements of S. Let us observe that the functor $\bigcup F$ yields an element of S. Let F be a sequence of S. Let us note that the functor $\bigcup F$ yields an element of S. Let F be a finite sequence of elements of $X \dot{\rightarrow} \overline{\mathbb{R}}$ and x be an element of X. The functor $F \# x$ yielding a finite sequence of elements of $\overline{\mathbb{R}}$ is defined by

(Def. 1) $\operatorname{dom} it = \operatorname{dom} F$ and for every element n of $\mathbb{N}$ such that $n \in \operatorname{dom} it$ holds $it(n) = F(n)(x)$.

Now we state the proposition:

(6) Let us consider a non empty set X, a non empty family S of subsets of X, a finite sequence f of elements of S, and a finite sequence F of elements of $X \dot{\rightarrow} \overline{\mathbb{R}}$. Suppose $\operatorname{dom} f = \operatorname{dom} F$ and f is disjoint valued and for every natural number n such that $n \in \operatorname{dom} F$ holds $F(n) = \chi_{f(n),X}$. Let us consider an element x of X. Then $\chi_{\bigcup f,X}(x) = \sum (F \# x)$.

2. Product Measure and Product σ-measure

Now we state the proposition:

(7) Let us consider non empty sets X_1, X_2, a σ-field S_1 of subsets of X_1, and a σ-field S_2 of subsets of X_2. Then $\sigma(\operatorname{DisUnion} \operatorname{MeasRect}(S_1, S_2)) = \sigma(\operatorname{MeasRect}(S_1, S_2))$.

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. The functor $\operatorname{ProdMeas}(M_1, M_2)$ yielding an induced measure of $\operatorname{MeasRect}(S_1, S_2)$ and $\operatorname{ProdpreMeas}(M_1, M_2)$ is defined by

(Def. 2) for every set E such that $E \in$ the field generated by $\operatorname{MeasRect}(S_1, S_2)$ for every disjoint valued finite sequence F of elements of $\operatorname{MeasRect}(S_1, S_2)$ such that $E = \bigcup F$ holds $it(E) = \sum(\operatorname{ProdpreMeas}(M_1, M_2) \cdot F)$.

The functor $\operatorname{Prod}\sigma\text{-}\operatorname{Meas}(M_1, M_2)$ yielding an induced σ-measure of $\operatorname{MeasRect}(S_1, S_2$ and $\operatorname{ProdMeas}(M_1, M_2)$ is defined by the term

(Def. 3) σ-Meas(the Caratheodory measure determined by $\operatorname{ProdMeas}(M_1, M_2)){\restriction}\sigma(\operatorname{MeasRe}$

Now we state the propositions:

(8) 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 $\mathrm{Prod}\,\sigma\text{-Meas}(M_1, M_2)$ is a σ-measure on $\sigma(\mathrm{MeasRect}(S_1, S_2))$. The theorem is a consequence of (7).

(9) 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 set sequence F_1 of S_1, a set sequence F_2 of S_2, and a natural number n. Then $F_1(n) \times F_2(n)$ is an element of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. The theorem is a consequence of (7).

(10) Let us consider sets X_1, X_2, a sequence F_1 of subsets of X_1, a sequence F_2 of subsets of X_2, and a natural number n. Suppose F_1 is non descending and F_2 is non descending. Then $F_1(n) \times F_2(n) \subseteq F_1(n+1) \times F_2(n+1)$.

(11) 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, an element A of S_1, and an element B of S_2. Then $(\mathrm{ProdMeas}(M_1, M_2))(A \times B) = M_1(A) \cdot M_2(B)$.

(12) 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, a set sequence F_1 of S_1, a set sequence F_2 of S_2, and a natural number n. Then $(\mathrm{ProdMeas}(M_1, M_2))(F_1(n) \times F_2(n)) = M_1(F_1(n)) \cdot M_2(F_2(n))$. The theorem is a consequence of (11).

(13) 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, a finite sequence F_1 of elements of S_1, a finite sequence F_2 of elements of S_2, and a natural number n. Suppose $n \in \mathrm{dom}\, F_1$ and $n \in \mathrm{dom}\, F_2$. Then $(\mathrm{ProdMeas}(M_1, M_2))(F_1(n) \times F_2(n)) = M_1(F_1(n)) \cdot M_2(F_2(n))$.

(14) 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 subset E of $X_1 \times X_2$. Then (the Caratheodory measure determined by $\mathrm{ProdMeas}(M_1, M_2))(E) = \inf \mathrm{Svc}(\mathrm{ProdMeas}(M_1, M_2), E)$.

(15) 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 $\sigma(\mathrm{MeasRect}(S_1, S_2)) \subseteq \sigma$-Field(the Caratheodory measure determined by $\mathrm{ProdMeas}(M_1, M_2)$). The theorem is a consequence of (7).

(16) 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, an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element A of S_1, and an element B of S_2. Suppose $E = A \times B$. Then $(\mathrm{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E) = M_1(A) \cdot M_2(B)$. The theorem is a consequence of (15) and (11).

(17) 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, a set sequence F_1 of S_1, a set sequence F_2 of S_2, and a natural number

n. Then $(\mathrm{Prod}\,\sigma\text{-Meas}(M_1, M_2))(F_1(n) \times F_2(n)) = M_1(F_1(n)) \cdot M_2(F_2(n))$. The theorem is a consequence of (9), (15), and (12).

(18) 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 elements E_1, E_2 of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Suppose E_1 misses E_2. Then $(\mathrm{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E_1 \cup E_2) = (\mathrm{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E_1) + (\mathrm{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E_2)$. The theorem is a consequence of (8).

(19) Let us consider sets X_1, X_2, A, B, a sequence F_1 of subsets of X_1, a sequence F_2 of subsets of X_2, and a sequence F of subsets of $X_1 \times X_2$. Suppose F_1 is non descending and $\lim F_1 = A$ and F_2 is non descending and $\lim F_2 = B$ and for every natural number n, $F(n) = F_1(n) \times F_2(n)$. Then $\lim F = A \times B$. The theorem is a consequence of (10).

3. Sections

Let X be a set, Y be a non empty set, E be a subset of $X \times Y$, and x be a set. The functor $\mathrm{Xsection}(E, x)$ yielding a subset of Y is defined by the term

(Def. 4) $\{y$, where y is an element of Y : $\langle x, y\rangle \in E\}$.

Let X be a non empty set, Y be a set, and y be a set. The functor $\mathrm{Ysection}(E, y)$ yielding a subset of X is defined by the term

(Def. 5) $\{x$, where x is an element of X : $\langle x, y\rangle \in E\}$.

Now we state the propositions:

(20) Let us consider a set X, a non empty set Y, subsets E_1, E_2 of $X \times Y$, and a set p. Suppose $E_1 \subseteq E_2$. Then $\mathrm{Xsection}(E_1, p) \subseteq \mathrm{Xsection}(E_2, p)$.

(21) Let us consider a non empty set X, a set Y, subsets E_1, E_2 of $X \times Y$, and a set p. Suppose $E_1 \subseteq E_2$. Then $\mathrm{Ysection}(E_1, p) \subseteq \mathrm{Ysection}(E_2, p)$.

(22) Let us consider non empty sets X, Y, a subset A of X, a subset B of Y, and a set p. Then

(i) if $p \in A$, then $\mathrm{Xsection}(A \times B, p) = B$, and

(ii) if $p \notin A$, then $\mathrm{Xsection}(A \times B, p) = \emptyset$, and

(iii) if $p \in B$, then $\mathrm{Ysection}(A \times B, p) = A$, and

(iv) if $p \notin B$, then $\mathrm{Ysection}(A \times B, p) = \emptyset$.

(23) Let us consider non empty sets X, Y, a subset E of $X \times Y$, and a set p. Then

(i) if $p \notin X$, then $\mathrm{Xsection}(E, p) = \emptyset$, and

(ii) if $p \notin Y$, then $\mathrm{Ysection}(E, p) = \emptyset$.

(24) Let us consider non empty sets X, Y, and a set p. Then

(i) $\mathrm{Xsection}(\emptyset_{X\times Y}, p) = \emptyset$, and

(ii) $\mathrm{Ysection}(\emptyset_{X\times Y}, p) = \emptyset$, and

(iii) if $p \in X$, then $\mathrm{Xsection}(\Omega_{X\times Y}, p) = Y$, and

(iv) if $p \in Y$, then $\mathrm{Ysection}(\Omega_{X\times Y}, p) = X$.

The theorem is a consequence of (22).

(25) Let us consider non empty sets X, Y, a subset E of $X \times Y$, and a set p. Then

(i) if $p \in X$, then $\mathrm{Xsection}(X \times Y \setminus E, p) = Y \setminus \mathrm{Xsection}(E, p)$, and

(ii) if $p \in Y$, then $\mathrm{Ysection}(X \times Y \setminus E, p) = X \setminus \mathrm{Ysection}(E, p)$.

Let us consider non empty sets X, Y, subsets E_1, E_2 of $X \times Y$, and a set p. Now we state the propositions:

(26) (i) $\mathrm{Xsection}(E_1 \cup E_2, p) = \mathrm{Xsection}(E_1, p) \cup \mathrm{Xsection}(E_2, p)$, and

(ii) $\mathrm{Ysection}(E_1 \cup E_2, p) = \mathrm{Ysection}(E_1, p) \cup \mathrm{Ysection}(E_2, p)$.

(27) (i) $\mathrm{Xsection}(E_1 \cap E_2, p) = \mathrm{Xsection}(E_1, p) \cap \mathrm{Xsection}(E_2, p)$, and

(ii) $\mathrm{Ysection}(E_1 \cap E_2, p) = \mathrm{Ysection}(E_1, p) \cap \mathrm{Ysection}(E_2, p)$.

Now we state the propositions:

(28) Let us consider a set X, a non empty set Y, a finite sequence F of elements of $2^{X\times Y}$, a finite sequence F_4 of elements of 2^Y, and a set p. Suppose $\mathrm{dom}\, F = \mathrm{dom}\, F_4$ and for every natural number n such that $n \in \mathrm{dom}\, F_4$ holds $F_4(n) = \mathrm{Xsection}(F(n), p)$. Then $\mathrm{Xsection}(\bigcup \mathrm{rng}\, F, p) = \bigcup \mathrm{rng}\, F_4$.

(29) Let us consider a non empty set X, a set Y, a finite sequence F of elements of $2^{X\times Y}$, a finite sequence F_3 of elements of 2^X, and a set p. Suppose $\mathrm{dom}\, F = \mathrm{dom}\, F_3$ and for every natural number n such that $n \in \mathrm{dom}\, F_3$ holds $F_3(n) = \mathrm{Ysection}(F(n), p)$. Then $\mathrm{Ysection}(\bigcup \mathrm{rng}\, F, p) = \bigcup \mathrm{rng}\, F_3$.

Let us consider a set X, a non empty set Y, a set p, a sequence F of subsets of $X \times Y$, and a sequence F_4 of subsets of Y. Now we state the propositions:

(30) If for every natural number n, $F_4(n) = \mathrm{Xsection}(F(n), p)$, then $\mathrm{Xsection}(\bigcup \mathrm{rng}\, F, p)$ $\bigcup \mathrm{rng}\, F_4$.

(31) If for every natural number n, $F_4(n) = \mathrm{Xsection}(F(n), p)$, then $\mathrm{Xsection}(\bigcap \mathrm{rng}\, F, p)$ $\bigcap \mathrm{rng}\, F_4$.

Let us consider a non empty set X, a set Y, a set p, a sequence F of subsets of $X \times Y$, and a sequence F_3 of subsets of X. Now we state the propositions:

(32) If for every natural number n, $F_3(n) = \mathrm{Ysection}(F(n), p)$, then $\mathrm{Ysection}(\bigcup \mathrm{rng}\, F, p)$ $\bigcup \mathrm{rng}\, F_3$.

(33) If for every natural number n, $F_3(n) = \text{Ysection}(F(n), p)$, then $\text{Ysection}(\bigcap \text{rng}\, F, p) = \bigcap \text{rng}\, F_3$.

Now we state the propositions:

(34) Let us consider non empty sets X, Y, sets x, y, and a subset E of $X \times Y$. Then

(i) $\chi_{E,X\times Y}(x, y) = \chi_{\text{Xsection}(E,x),Y}(y)$, and

(ii) $\chi_{E,X\times Y}(x, y) = \chi_{\text{Ysection}(E,y),X}(x)$.

(35) Let us consider non empty sets X, Y, subsets E_1, E_2 of $X \times Y$, and a set p. Suppose E_1 misses E_2. Then

(i) $\text{Xsection}(E_1, p)$ misses $\text{Xsection}(E_2, p)$, and

(ii) $\text{Ysection}(E_1, p)$ misses $\text{Ysection}(E_2, p)$.

(36) Let us consider non empty sets X, Y, a disjoint valued finite sequence F of elements of $2^{X\times Y}$, and a set p. Then

(i) there exists a disjoint valued finite sequence F_4 of elements of 2^X such that $\text{dom}\, F = \text{dom}\, F_4$ and for every natural number n such that $n \in \text{dom}\, F_4$ holds $F_4(n) = \text{Ysection}(F(n), p)$, and

(ii) there exists a disjoint valued finite sequence F_3 of elements of 2^Y such that $\text{dom}\, F = \text{dom}\, F_3$ and for every natural number n such that $n \in \text{dom}\, F_3$ holds $F_3(n) = \text{Xsection}(F(n), p)$.

Proof: Define $\{_\infty$(natural number) $= \text{Ysection}(F(\$_1), p)$. Define $\{_\in$(natural number) $= \text{Xsection}(F(\$_1), p)$. There exists a disjoint valued finite sequence F_4 of elements of 2^X such that $\text{dom}\, F = \text{dom}\, F_4$ and for every natural number n such that $n \in \text{dom}\, F_4$ holds $F_4(n) = \text{Ysection}(F(n), p)$ by (35), [19, (29)]. There exists a disjoint valued finite sequence F_3 of elements of 2^Y such that $\text{dom}\, F = \text{dom}\, F_3$ and for every natural number n such that $n \in \text{dom}\, F_3$ holds $F_3(n) = \text{Xsection}(F(n), p)$ by (35), [19, (29)]. $\square$

(37) Let us consider non empty sets X, Y, a disjoint valued sequence F of subsets of $X \times Y$, and a set p. Then

(i) there exists a disjoint valued sequence F_4 of subsets of X such that for every natural number n, $F_4(n) = \text{Ysection}(F(n), p)$, and

(ii) there exists a disjoint valued sequence F_3 of subsets of Y such that for every natural number n, $F_3(n) = \text{Xsection}(F(n), p)$.

Proof: There exists a disjoint valued sequence F_4 of subsets of X such that for every natural number n, $F_4(n) = \text{Ysection}(F(n), p)$. Define $\{$(natural number) $= \text{Xsection}(F(\$_1), p)$. Consider F_3 being a sequence of subsets of Y such that for every element n of $\mathbb{N}$, $F_3(n) = f(n)$ from [11, Sch. 4]. $\square$

(38) Let us consider non empty sets X, Y, sets x, y, and subsets E_1, E_2 of $X \times Y$. Suppose E_1 misses E_2. Then

(i) $\chi_{E_1 \cup E_2, X \times Y}(x, y) = \chi_{\mathrm{Xsection}(E_1, x), Y}(y) + \chi_{\mathrm{Xsection}(E_2, x), Y}(y)$, and

(ii) $\chi_{E_1 \cup E_2, X \times Y}(x, y) = \chi_{\mathrm{Ysection}(E_1, y), X}(x) + \chi_{\mathrm{Ysection}(E_2, y), X}(x)$.

The theorem is a consequence of (35), (34), and (26).

(39) Let us consider a set X, a non empty set Y, a set x, a sequence E of subsets of $X \times Y$, and a sequence G of subsets of Y. Suppose E is non descending and for every natural number n, $G(n) = \mathrm{Xsection}(E(n), x)$. Then G is non descending. The theorem is a consequence of (20).

(40) Let us consider a non empty set X, a set Y, a set x, a sequence E of subsets of $X \times Y$, and a sequence G of subsets of X. Suppose E is non descending and for every natural number n, $G(n) = \mathrm{Ysection}(E(n), x)$. Then G is non descending. The theorem is a consequence of (21).

(41) Let us consider a set X, a non empty set Y, a set x, a sequence E of subsets of $X \times Y$, and a sequence G of subsets of Y. Suppose E is non ascending and for every natural number n, $G(n) = \mathrm{Xsection}(E(n), x)$. Then G is non ascending. The theorem is a consequence of (20).

(42) Let us consider a non empty set X, a set Y, a set x, a sequence E of subsets of $X \times Y$, and a sequence G of subsets of X. Suppose E is non ascending and for every natural number n, $G(n) = \mathrm{Ysection}(E(n), x)$. Then G is non ascending. The theorem is a consequence of (21).

(43) Let us consider a set X, a non empty set Y, a sequence E of subsets of $X \times Y$, and a set x. Suppose E is non descending. Then there exists a sequence G of subsets of Y such that

(i) G is non descending, and

(ii) for every natural number n, $G(n) = \mathrm{Xsection}(E(n), x)$.

PROOF: Define $\mathcal{F}(\text{natural number}) = \mathrm{Xsection}(E(\$_1), x)$. Consider G being a function from $\mathbb{N}$ into 2^Y such that for every element n of $\mathbb{N}$, $G(n) = \mathcal{F}(n)$ from [11, Sch. 4]. For every natural number n, $G(n) = \mathrm{Xsection}(E(n), x)$. $\square$

(44) Let us consider a non empty set X, a set Y, a sequence E of subsets of $X \times Y$, and a set x. Suppose E is non descending. Then there exists a sequence G of subsets of X such that

(i) G is non descending, and

(ii) for every natural number n, $G(n) = \mathrm{Ysection}(E(n), x)$.

PROOF: Define $\mathcal{F}(\text{natural number}) = \mathrm{Ysection}(E(\$_1), x)$. Consider G being a function from $\mathbb{N}$ into 2^X such that for every element n of $\mathbb{N}$, $G(n) =$

$\mathcal{F}(n)$ from [11, Sch. 4]. For every natural number n, $G(n) = \text{Ysection}(E(n), x)$. $\square$

(45) Let us consider a set X, a non empty set Y, a sequence E of subsets of $X \times Y$, and a set x. Suppose E is non ascending. Then there exists a sequence G of subsets of Y such that

(i) G is non ascending, and

(ii) for every natural number n, $G(n) = \text{Xsection}(E(n), x)$.

PROOF: Define $\mathcal{F}(\text{natural number}) = \text{Xsection}(E(\$_1), x)$. Consider G being a function from $\mathbb{N}$ into 2^Y such that for every element n of $\mathbb{N}$, $G(n) = \mathcal{F}(n)$ from [11, Sch. 4]. For every natural number n, $G(n) = \text{Xsection}(E(n), x)$. $\square$

(46) Let us consider a non empty set X, a set Y, a sequence E of subsets of $X \times Y$, and a set x. Suppose E is non ascending. Then there exists a sequence G of subsets of X such that

(i) G is non ascending, and

(ii) for every natural number n, $G(n) = \text{Ysection}(E(n), x)$.

PROOF: Define $\mathcal{F}(\text{natural number}) = \text{Ysection}(E(\$_1), x)$. Consider G being a function from $\mathbb{N}$ into 2^X such that for every element n of $\mathbb{N}$, $G(n) = \mathcal{F}(n)$ from [11, Sch. 4]. For every natural number n, $G(n) = \text{Ysection}(E(n), x)$. $\square$

4. Measurable Sections

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, an element E of $\sigma(\text{MeasRect}(S_1, S_2))$, and a set K. Now we state the propositions:

(47) Suppose $K = \{C$, where C is a subset of $X_1 \times X_2$: for every set $p, \text{Xsection}(C, p) \in S_2\}$. Then

(i) the field generated by $\text{MeasRect}(S_1, S_2) \subseteq K$, and

(ii) K is a σ-field of subsets of $X_1 \times X_2$.

PROOF: For every set x, $\text{Xsection}(\emptyset_{X_1 \times X_2}, x) \in S_2$ by (24), [5, (7)]. For every subset C of $X_1 \times X_2$ such that $C \in K$ holds $C^{\text{c}} \in K$ by [17, (5), (6)], (25), (23). $\square$

(48) Suppose $K = \{C$, where C is a subset of $X_1 \times X_2$: for every set $p, \text{Ysection}(C, p) \in S_1\}$. Then

(i) the field generated by $\text{MeasRect}(S_1, S_2) \subseteq K$, and

(ii) K is a σ-field of subsets of $X_1 \times X_2$.

PROOF: For every set y, $\mathrm{Ysection}(\emptyset_{X_1 \times X_2}, y) \in S_1$ by (24), [5, (7)]. For every subset C of $X_1 \times X_2$ such that $C \in K$ holds $C^{\mathrm{c}} \in K$ by [17, (5), (6)], (25), (23). □

Now we state the proposition:

(49) 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, and an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Then

(i) for every set p, $\mathrm{Xsection}(E, p) \in S_2$, and

(ii) for every set p, $\mathrm{Ysection}(E, p) \in S_1$.

The theorem is a consequence of (47) and (48).

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, E be an element of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, and x be a set. The functor $\boxed{\mathrm{MeasurableXsection}(E, x)}$ yielding an element of S_2 is defined by the term

(Def. 6) $\mathrm{Xsection}(E, x)$.

Let y be a set. The functor $\boxed{\mathrm{MeasurableYsection}(E, y)}$ yielding an element of S_1 is defined by the term

(Def. 7) $\mathrm{Ysection}(E, y)$.

Now we state the propositions:

(50) 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 finite sequence F of elements of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, a finite sequence F_4 of elements of S_2, and a set p. Suppose $\mathrm{dom}\, F = \mathrm{dom}\, F_4$ and for every natural number n such that $n \in \mathrm{dom}\, F_4$ holds $F_4(n) = \mathrm{MeasurableXsection}(F(n), p)$. Then $\mathrm{MeasurableXsection}(\bigcup F, p) = \bigcup F_4$. The theorem is a consequence of (28).

(51) 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 finite sequence F of elements of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, a finite sequence F_3 of elements of S_1, and a set p. Suppose $\mathrm{dom}\, F = \mathrm{dom}\, F_3$ and for every natural number n such that $n \in \mathrm{dom}\, F_3$ holds $F_3(n) = \mathrm{MeasurableYsection}(F(n), p)$. Then $\mathrm{MeasurableYsection}(\bigcup F, p) = \bigcup F_3$. The theorem is a consequence of (29).

(52) 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, an element A of S_1, an element B of S_2, and an element x of X_1. Then $M_2(B) \cdot \chi_{A, X_1}(x) = \int \mathrm{curry}(\chi_{A \times B, X_1 \times X_2}, x)\, \mathrm{d}M_2$.

PROOF: For every element y of X_2, $(\mathrm{curry}(\chi_{A \times B, X_1 \times X_2}, x))(y) = \chi_{A, X_1}(x) \cdot \chi_{B, X_2}(y)$ by [**?** , (2)]. □

(53) 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, an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element A of S_1, an element B of S_2, and an element x of X_1. Suppose $E = A \times B$. Then $M_2(\mathrm{MeasurableXsection}(E, x)) = M_2(B) \cdot \chi_{A,X_1}(x)$. The theorem is a consequence of (22).

(54) 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, an element A of S_1, an element B of S_2, and an element y of X_2. Then $M_1(A) \cdot \chi_{B,X_2}(y) = \int \mathrm{curry}'(\chi_{A\times B, X_1 \times X_2}, y)\, \mathrm{d}M_1$.
PROOF: For every element x of X_1, $(\mathrm{curry}'(\chi_{A\times B,X_1\times X_2}, y))(x) = \chi_{A,X_1}(x) \cdot \chi_{B,X_2}(y)$ by [**?** , (2)]. $\square$

(55) 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, an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element A of S_1, an element B of S_2, and an element y of X_2. Suppose $E = A \times B$. Then $M_1(\mathrm{MeasurableYsection}(E, y)) = M_1(A) \cdot \chi_{B,X_2}(y)$. The theorem is a consequence of (22).

5. Finite Sequence of Functions

Let X, Y be non empty sets, G be a non empty set of functions from X to Y, F be a finite sequence of elements of G, and n be a natural number. Observe that the functor F_n yields an element of G. Let X be a set and F be a finite sequence of elements of $\overline{\mathbb{R}}^X$. We say that $\boxed{F \text{ is (without } +\infty\text{)-valued}}$ if and only if

(Def. 8) for every natural number n such that $n \in \mathrm{dom}\, F$ holds $F(n)$ is without $+\infty$.

We say that $\boxed{F \text{ is (without } -\infty\text{)-valued}}$ if and only if

(Def. 9) for every natural number n such that $n \in \mathrm{dom}\, F$ holds $F(n)$ is without $-\infty$.

Now we state the proposition:

(56) Let us consider a non empty set X. Then

(i) $\langle X \longmapsto 0 \rangle$ is a finite sequence of elements of $\overline{\mathbb{R}}^X$, and

(ii) for every natural number n such that $n \in \mathrm{dom}\langle X \longmapsto 0\rangle$ holds $\langle X \longmapsto 0\rangle(n)$ is without $+\infty$, and

(iii) for every natural number n such that $n \in \mathrm{dom}\langle X \longmapsto 0\rangle$ holds $\langle X \longmapsto 0\rangle(n)$ is without $-\infty$.

Let X be a non empty set. One can verify that there exists a finite sequence of elements of $\overline{\mathbb{R}}^X$ which is (without $+\infty$)-valued and (without $-\infty$)-valued.

Now we state the propositions:

(57) Let us consider a non empty set X, a (without $+\infty$)-valued finite sequence F of elements of $\overline{\mathbb{R}}^X$, and a natural number n. If $n \in \operatorname{dom} F$, then $(F_n)^{-1}(\{+\infty\}) = \emptyset$.

(58) Let us consider a non empty set X, a (without $-\infty$)-valued finite sequence F of elements of $\overline{\mathbb{R}}^X$, and a natural number n. If $n \in \operatorname{dom} F$, then $(F_n)^{-1}(\{-\infty\}) = \emptyset$.

(59) Let us consider a non empty set X, and a finite sequence F of elements of $\overline{\mathbb{R}}^X$. Suppose F is (without $+\infty$)-valued or (without $-\infty$)-valued. Let us consider natural numbers n, m. If $n, m \in \operatorname{dom} F$, then $\operatorname{dom}(F_n + F_m) = X$. The theorem is a consequence of (57) and (58).

Let X be a non empty set and F be a finite sequence of elements of $\overline{\mathbb{R}}^X$. We say that F is summable if and only if

(Def. 10) F is (without $+\infty$)-valued or (without $-\infty$)-valued.

Observe that there exists a finite sequence of elements of $\overline{\mathbb{R}}^X$ which is summable.

Let F be a summable finite sequence of elements of $\overline{\mathbb{R}}^X$. The functor $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}$ yielding a finite sequence of elements of $\overline{\mathbb{R}}^X$ is defined by

(Def. 11) $\operatorname{len} F = \operatorname{len} it$ and $F(1) = it(1)$ and for every natural number n such that $1 \leqslant n < \operatorname{len} F$ holds $it(n+1) = it_n + F_{n+1}$.

One can check that every finite sequence of elements of $\overline{\mathbb{R}}^X$ which is (without $+\infty$)-valued is also summable and every finite sequence of elements of $\overline{\mathbb{R}}^X$ which is (without $-\infty$)-valued is also summable.

Now we state the propositions:

(60) Let us consider a non empty set X, and a (without $+\infty$)-valued finite sequence F of elements of $\overline{\mathbb{R}}^X$. Then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}$ is (without $+\infty$)-valued.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \in \operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}$, then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(\$_1)$ is without $+\infty$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [19, (29)], [2, (14)], [19, (25)], [2, (13)]. For every natural number n, $\mathcal{P}[n]$ from [2, Sch. 2]. □

(61) Let us consider a non empty set X, and a (without $-\infty$)-valued finite sequence F of elements of $\overline{\mathbb{R}}^X$. Then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}$ is (without $-\infty$)-valued.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \in \operatorname{dom}(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}$, then

$(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(\$_1)$ is without $-\infty$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [19, (29)], [2, (14)], [19, (25)], [2, (13)]. For every natural number n, $\mathcal{P}[n]$ from [2, Sch. 2]. $\square$

(62) Let us consider a non empty set X, a set A, an extended real e, and a function f from X into $\overline{\mathbb{R}}$. Suppose for every element x of X, $f(x) = e \cdot \chi_{A,X}(x)$. Then

(i) if $e = +\infty$, then $f = \overline{\chi}_{A,X}$, and

(ii) if $e = -\infty$, then $f = -\overline{\chi}_{A,X}$, and

(iii) if $e \neq +\infty$ and $e \neq -\infty$, then there exists a real number r such that $r = e$ and $f = r \cdot \chi_{A,X}$.

(63) Let us consider a non empty set X, a σ-field S of subsets of X, a partial function f from X to $\overline{\mathbb{R}}$, and an element A of S. Suppose f is measurable on A and $A \subseteq \operatorname{dom} f$. Then $-f$ is measurable on A.

Let X be a non empty set and f be a without $-\infty$ partial function from X to $\overline{\mathbb{R}}$. Observe that $-f$ is without $+\infty$.

Let f be a without $+\infty$ partial function from X to $\overline{\mathbb{R}}$. One can check that $-f$ is without $-\infty$.

Let f_1, f_2 be without $+\infty$ partial functions from X to $\overline{\mathbb{R}}$. Let us note that the functor $f_1 + f_2$ yields a without $+\infty$ partial function from X to $\overline{\mathbb{R}}$. Let f_1, f_2 be without $-\infty$ partial functions from X to $\overline{\mathbb{R}}$. Note that the functor $f_1 + f_2$ yields a without $-\infty$ partial function from X to $\overline{\mathbb{R}}$. Let f_1 be a without $+\infty$ partial function from X to $\overline{\mathbb{R}}$ and f_2 be a without $-\infty$ partial function from X to $\overline{\mathbb{R}}$. One can verify that the functor $f_1 - f_2$ yields a without $+\infty$ partial function from X to $\overline{\mathbb{R}}$. Let f_1 be a without $-\infty$ partial function from X to $\overline{\mathbb{R}}$ and f_2 be a without $+\infty$ partial function from X to $\overline{\mathbb{R}}$. Observe that the functor $f_1 - f_2$ yields a without $-\infty$ partial function from X to $\overline{\mathbb{R}}$. Now we state the propositions:

(64) Let us consider a non empty set X, and partial functions f, g from X to $\overline{\mathbb{R}}$. Then

(i) $-(f + g) = -f + -g$, and

(ii) $-(f - g) = -f + g$, and

(iii) $-(f - g) = g - f$, and

(iv) $-(-f + g) = f - g$, and

(v) $-(-f + g) = f + -g$.

(65) Let us consider a non empty set X, a σ-field S of subsets of X, without $+\infty$ partial functions f, g from X to $\overline{\mathbb{R}}$, and an element A of S. Suppose f is measurable on A and g is measurable on A and $A \subseteq \operatorname{dom}(f + g)$. Then $f + g$ is measurable on A. The theorem is a consequence of (63) and (64).

(66) Let us consider a non empty set X, a σ-field S of subsets of X, an element A of S, a without $+\infty$ partial function f from X to $\overline{\mathbb{R}}$, and a without $-\infty$ partial function g from X to $\overline{\mathbb{R}}$. Suppose f is measurable on A and g is measurable on A and $A \subseteq \mathrm{dom}(f-g)$. Then $f-g$ is measurable on A. The theorem is a consequence of (63) and (64).

(67) Let us consider a non empty set X, a σ-field S of subsets of X, an element A of S, a without $-\infty$ partial function f from X to $\overline{\mathbb{R}}$, and a without $+\infty$ partial function g from X to $\overline{\mathbb{R}}$. Suppose f is measurable on A and g is measurable on A and $A \subseteq \mathrm{dom}(f-g)$. Then $f-g$ is measurable on A. The theorem is a consequence of (64), (63), and (65).

(68) Let us consider a non empty set X, a σ-field S of subsets of X, an element P of S, and a summable finite sequence F of elements of $\overline{\mathbb{R}}^X$. Suppose for every natural number n such that $n \in \mathrm{dom}\, F$ holds F_n is measurable on P. Let us consider a natural number n. Suppose $n \in \mathrm{dom}\, F$. Then $((\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}})_n$ is measurable on P. The theorem is a consequence of (60), (65), and (61).

6. Some Properties of Integral

Now we state the propositions:

(69) 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, an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element A of S_1, an element B of S_2, an element x of X_1, and an element y of X_2. Suppose $E = A \times B$. Then

(i) $\int \mathrm{curry}(\chi_{E, X_1 \times X_2}, x)\, \mathrm{d}M_2 = M_2(\mathrm{MeasurableXsection}(E, x)) \cdot \chi_{A, X_1}(x)$, and

(ii) $\int \mathrm{curry}'(\chi_{E, X_1 \times X_2}, y)\, \mathrm{d}M_1 = M_1(\mathrm{MeasurableYsection}(E, y)) \cdot \chi_{B, X_2}(y)$.

The theorem is a consequence of (52), (53), (54), and (55).

(70) 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, and an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Suppose $E \in$ the field generated by $\mathrm{MeasRect}(S_1, S_2)$. Then there exists a disjoint valued finite sequence f of elements of $\mathrm{MeasRect}(S_1, S_2)$ and there exists a finite sequence A of elements of S_1 and there exists a finite sequence B of elements of S_2 such that $\mathrm{len}\, f = \mathrm{len}\, A$ and $\mathrm{len}\, f = \mathrm{len}\, B$ and $E = \bigcup f$ and for every natural number n such that $n \in \mathrm{dom}\, f$ holds $\pi_1(f(n)) = A(n)$ and $\pi_2(f(n)) = B(n)$ and for every natural number n

and for every sets x, y such that $n \in \operatorname{dom} f$ and $x \in X_1$ and $y \in X_2$ holds $\chi_{f(n),X_1 \times X_2}(x,y) = \chi_{A(n),X_1}(x) \cdot \chi_{B(n),X_2}(y)$.
PROOF: Consider E_1 being a subset of $X_1 \times X_2$ such that $E = E_1$ and there exists a disjoint valued finite sequence f of elements of $\mathrm{MeasRect}(S_1, S_2)$ such that $E_1 = \bigcup f$. Consider f being a disjoint valued finite sequence of elements of $\mathrm{MeasRect}(S_1, S_2)$ such that $E_1 = \bigcup f$. Define $\mathcal{S}[\text{natural number, object}] \equiv \$_2 = \pi_1(f(\$_1))$. For every natural number i such that $i \in \operatorname{Seg} \operatorname{len} f$ there exists an element A_1 of S_1 such that $\mathcal{S}[i, A_1]$ by [12, (4)], [1, (9)], [5, (7)]. Consider A being a finite sequence of elements of S_1 such that $\operatorname{dom} A = \operatorname{Seg} \operatorname{len} f$ and for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} f$ holds $\mathcal{S}[i, A(i)]$ from [3, Sch. 5]. Define $\mathcal{T}[\text{natural number, object}] \equiv \$_2 = \pi_2(f(\$_1))$. For every natural number i such that $i \in \operatorname{Seg} \operatorname{len} f$ there exists an element B_1 of S_2 such that $\mathcal{T}[i, B_1]$ by [12, (4)], [1, (9)], [5, (7)]. Consider B being a finite sequence of elements of S_2 such that $\operatorname{dom} B = \operatorname{Seg} \operatorname{len} f$ and for every natural number i such that $i \in \operatorname{Seg} \operatorname{len} f$ holds $\mathcal{T}[i, B(i)]$ from [3, Sch. 5]. For every natural number n such that $n \in \operatorname{dom} f$ holds $\pi_1(f(n)) = A(n)$ and $\pi_2(f(n)) = B(n)$. Consider A_2 being an element of S_1, B_2 being an element of S_2 such that $f(n) = A_2 \times B_2$. $\square$

(71) 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, an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element x of X_1, an element y of X_2, an element U of S_1, and an element V of S_2. Then

(i) $M_1(\mathrm{MeasurableYsection}(E, y) \cap U) = \int \mathrm{curry}'(\chi_{E \cap (U \times X_2), X_1 \times X_2}, y)\, \mathrm{d}M_1$, and

(ii) $M_2(\mathrm{MeasurableXsection}(E, x) \cap V) = \int \mathrm{curry}(\chi_{E \cap (X_1 \times V), X_1 \times X_2}, x)\, \mathrm{d}M_2$.

The theorem is a consequence of (34), (27), and (22).

(72) 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, an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element x of X_1, and an element y of X_2. Then

(i) $M_1(\mathrm{MeasurableYsection}(E, y)) = \int \mathrm{curry}'(\chi_{E, X_1 \times X_2}, y)\, \mathrm{d}M_1$, and

(ii) $M_2(\mathrm{MeasurableXsection}(E, x)) = \int \mathrm{curry}(\chi_{E, X_1 \times X_2}, x)\, \mathrm{d}M_2$.

The theorem is a consequence of (71).

(73) 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 disjoint valued finite sequence f of elements of $\mathrm{MeasRect}(S_1, S_2)$, an element x of X_1, a natural number n, an element E_2 of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element A_2 of S_1, and

an element B_2 of S_2. Suppose $n \in \mathrm{dom}\, f$ and $f(n) = E_2$ and $E_2 = A_2 \times B_2$. Then $\int \mathrm{curry}(\chi_{f(n),X_1 \times X_2}, x)\, \mathrm{d}M_2 = M_2(\mathrm{MeasurableXsection}(E_2, x)) \cdot \chi_{A_2,X_1}(x)$.

(74) 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, and an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Suppose $E \in$ the field generated by $\mathrm{MeasRect}(S_1, S_2)$ and $E \neq \emptyset$. Then there exists a disjoint valued finite sequence f of elements of $\mathrm{MeasRect}(S_1, S_2)$ and there exists a finite sequence A of elements of S_1 and there exists a finite sequence B of elements of S_2 and there exists a summable finite sequence X_3 of elements of $\overline{\mathbb{R}}^{X_1 \times X_2}$ such that $E = \bigcup f$ and $\mathrm{len}\, f \in \mathrm{dom}\, f$ and $\mathrm{len}\, f = \mathrm{len}\, A$ and $\mathrm{len}\, f = \mathrm{len}\, B$ and $\mathrm{len}\, f = \mathrm{len}\, X_3$ and for every natural number n such that $n \in \mathrm{dom}\, f$ holds $f(n) = A(n) \times B(n)$ and for every natural number n such that $n \in \mathrm{dom}\, X_3$ holds $X_3(n) = \chi_{f(n),X_1 \times X_2}$ and $(\sum_{\alpha=0}^{\kappa} X_3(\alpha))_{\kappa \in \mathbb{N}}(\mathrm{len}\, X_3) = \chi_{E,X_1 \times X_2}$ and for every natural number n and for every sets x, y such that $n \in \mathrm{dom}\, X_3$ and $x \in X_1$ and $y \in X_2$ holds $X_3(n)(x, y) = \chi_{A(n),X_1}(x) \cdot \chi_{B(n),X_2}(y)$ and for every element x of X_1, $\mathrm{curry}(\chi_{E,X_1 \times X_2}, x) = \mathrm{curry}(((\sum_{\alpha=0}^{\kappa} X_3(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, X_3}, x)$ and for every element y of X_2, $\mathrm{curry}'(\chi_{E,X_1 \times X_2}, y) = \mathrm{curry}'(((\sum_{\alpha=0}^{\kappa} X_3(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, X_3}, y)$.
PROOF: Consider f being a disjoint valued finite sequence of elements of $\mathrm{MeasRect}(S_1, S_2)$, A being a finite sequence of elements of S_1, B being a finite sequence of elements of S_2 such that $\mathrm{len}\, f = \mathrm{len}\, A$ and $\mathrm{len}\, f = \mathrm{len}\, B$ and $E = \bigcup f$ and for every natural number n such that $n \in \mathrm{dom}\, f$ holds $\pi_1(f(n)) = A(n)$ and $\pi_2(f(n)) = B(n)$ and for every natural number n and for every sets x, y such that $n \in \mathrm{dom}\, f$ and $x \in X_1$ and $y \in X_2$ holds $\chi_{f(n),X_1 \times X_2}(x, y) = \chi_{A(n),X_1}(x) \cdot \chi_{B(n),X_2}(y)$. Define $\mathcal{F}(\text{set}) = \chi_{f(\$_1),X_1 \times X_2}$. Consider X_3 being a finite sequence such that $\mathrm{len}\, X_3 = \mathrm{len}\, f$ and for every natural number n such that $n \in \mathrm{dom}\, X_3$ holds $X_3(n) = \mathcal{F}(n)$ from [3, Sch. 2]. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \in \mathrm{dom}\, f$, then $(\sum_{\alpha=0}^{\kappa} X_3(\alpha))_{\kappa \in \mathbb{N}}(\$_1) = \chi_{\bigcup(f \restriction \$_1),X_1 \times X_2}$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [9, (20)], [3, (39)], [13, (25)], [2, (14)]. For every natural number n, $\mathcal{P}[n]$ from [2, Sch. 2]. For every natural number n such that $n \in \mathrm{dom}\, f$ holds $f(n) = A(n) \times B(n)$ by [12, (4)], [13, (90)], [1, (9)]. For every natural number n and for every sets x, y such that $n \in \mathrm{dom}\, X_3$ and $x \in X_1$ and $y \in X_2$ holds $X_3(n)(x, y) = \chi_{A(n),X_1}(x) \cdot \chi_{B(n),X_2}(y)$. For every element x of X_1, $\mathrm{curry}(\chi_{E,X_1 \times X_2}, x) = \mathrm{curry}(((\sum_{\alpha=0}^{\kappa} X_3(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, X_3}, x)$. $\square$

(75) 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, and a finite sequence F of elements of $\mathrm{MeasRect}(S_1, S_2)$. Then $\bigcup F \in \sigma(\mathrm{MeasRect}(S_1, S_2))$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant \mathrm{len}\, F$, then $\bigcup \mathrm{rng}(F \restriction \$_1) \in$

$\sigma(\mathrm{MeasRect}(S_1, S_2))$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [2, (11)], [19, (25)], [8, (11)], [3, (59)]. For every natural number k, $\mathcal{P}[k]$ from [2, Sch. 2]. $\square$

(76) 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 an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Suppose $E \in$ the field generated by $\mathrm{MeasRect}(S_1, S_2)$ and $E \neq \emptyset$. Then there exists a disjoint valued finite sequence F of elements of $\mathrm{MeasRect}(S_1, S_2)$ and there exists a finite sequence A of elements of S_1 and there exists a finite sequence B of elements of S_2 and there exists a summable finite sequence C of elements of $\overline{\mathbb{R}}^{X_1 \times X_2}$ and there exists a summable finite sequence I of elements of $\overline{\mathbb{R}}^{X_1}$ and there exists a summable finite sequence J of elements of $\overline{\mathbb{R}}^{X_2}$ such that $E = \bigcup F$ and $\mathrm{len}\, F \in \mathrm{dom}\, F$ and $\mathrm{len}\, F = \mathrm{len}\, A$ and $\mathrm{len}\, F = \mathrm{len}\, B$ and $\mathrm{len}\, F = \mathrm{len}\, C$ and $\mathrm{len}\, F = \mathrm{len}\, I$ and $\mathrm{len}\, F = \mathrm{len}\, J$ and for every natural number n such that $n \in \mathrm{dom}\, C$ holds $C(n) = \chi_{F(n), X_1 \times X_2}$ and $((\sum_{\alpha=0}^{\kappa} C(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, C} = \chi_{E, X_1 \times X_2}$ and for every element x of X_1 and for every natural number n such that $n \in \mathrm{dom}\, I$ holds $I(n)(x) = \int \mathrm{curry}(C_n, x)\, \mathrm{d}M_2$ and for every natural number n and for every element P of S_1 such that $n \in \mathrm{dom}\, I$ holds I_n is measurable on P and for every element x of X_1, $\int \mathrm{curry}(((\sum_{\alpha=0}^{\kappa} C(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, C}, x)\, \mathrm{d}M_2 = ((\sum_{\alpha=0}^{\kappa} I(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, I}(x)$ and for every element y of X_2 and for every natural number n such that $n \in \mathrm{dom}\, J$ holds $J(n)(y) = \int \mathrm{curry}'(C_n, y)\, \mathrm{d}M_1$ and for every natural number n and for every element P of S_2 such that $n \in \mathrm{dom}\, J$ holds J_n is measurable on P and for every element y of X_2, $\int \mathrm{curry}'(((\sum_{\alpha=0}^{\kappa} C(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, C}, y)\, \mathrm{d}M_1 = ((\sum_{\alpha=0}^{\kappa} J(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, J}(y)$.

Proof: Consider F being a disjoint valued finite sequence of elements of $\mathrm{MeasRect}(S_1, S_2)$, A being a finite sequence of elements of S_1, B being a finite sequence of elements of S_2, C being a summable finite sequence of elements of $\overline{\mathbb{R}}^{X_1 \times X_2}$ such that $E = \bigcup F$ and $\mathrm{len}\, F \in \mathrm{dom}\, F$ and $\mathrm{len}\, F = \mathrm{len}\, A$ and $\mathrm{len}\, F = \mathrm{len}\, B$ and $\mathrm{len}\, F = \mathrm{len}\, C$ and for every natural number n such that $n \in \mathrm{dom}\, F$ holds $F(n) = A(n) \times B(n)$ and for every natural number n such that $n \in \mathrm{dom}\, C$ holds $C(n) = \chi_{F(n), X_1 \times X_2}$ and $(\sum_{\alpha=0}^{\kappa} C(\alpha))_{\kappa \in \mathbb{N}}(\mathrm{len}\, C) = \chi_{E, X_1 \times X_2}$ and for every natural number n and for every sets x, y such that $n \in \mathrm{dom}\, C$ and $x \in X_1$ and $y \in X_2$ holds $C(n)(x, y) = \chi_{A(n), X_1}(x) \cdot \chi_{B(n), X_2}(y)$ and for every element x of X_1, $\mathrm{curry}(\chi_{E, X_1 \times X_2}, x) = \mathrm{curry}(((\sum_{\alpha=0}^{\kappa} C(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, C}, x)$ and for every element y of X_2, $\mathrm{curry}'(\chi_{E, X_1 \times X_2}, y) = \mathrm{curry}'(((\sum_{\alpha=0}^{\kappa} C(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, C}, y)$. Define $\mathcal{S}[\text{natural number}, \text{object}] \equiv$ there exists a function f from X_1 into $\overline{\mathbb{R}}$ such that $f = \$_2$ and for every element x of X_1, $f(x) = \int \mathrm{curry}(C_{\$_1}, x)\, \mathrm{d}M_2$. For every natural number n such that $n \in \mathrm{Seg}\, \mathrm{len}\, F$ there exists an object z such that $\mathcal{S}[n, z]$. Consider I being a finite sequence such that $\mathrm{dom}\, I = \mathrm{Seg}\,\mathrm{len}\, F$ and for every natural number n such that $n \in \mathrm{Seg}\,\mathrm{len}\, F$ holds $\mathcal{S}[n, I(n)]$ from [3, Sch. 1]. For every element x of X_1 and for every natural number n such that $n \in \mathrm{dom}\, I$ holds $I(n)(x) = \int \mathrm{curry}(C_n, x)\, \mathrm{d}M_2$ by [12, (4)]. Define $\mathcal{T}[\text{natural number}, \text{object}] \equiv$ there exists a function f from X_2 into $\overline{\mathbb{R}}$ such that $f = \$_2$ and for every element x of X_2, $f(x) = \int \mathrm{curry}'(C_{\$_1}, x)\, \mathrm{d}M_1$. For every natural number n such that $n \in \mathrm{Seg}\,\mathrm{len}\, F$ there exists an object z such that $\mathcal{T}[n, z]$. Consider J being a finite sequence such that $\mathrm{dom}\, J = \mathrm{Seg}\,\mathrm{len}\, F$ and for every natural number n such that $n \in \mathrm{Seg}\,\mathrm{len}\, F$ holds $\mathcal{T}[n, J(n)]$ from [3, Sch. 1]. For every element x of X_2 and for every natural number n such that $n \in \mathrm{dom}\, J$ holds $J(n)(x) = \int \mathrm{curry}'(C_n, x)\, \mathrm{d}M_1$ by [12, (4)]. For every natural number n and for every element P of S_1 such that $n \in \mathrm{dom}\, I$ holds I_n is measurable on P by [12, (4)], (69), (22), [? , (32)]. For every element x of X_1, $\int \mathrm{curry}(((\sum_{\alpha=0}^{\kappa} C(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, C}, x)\, \mathrm{d}M_2 = ((\sum_{\alpha=0}^{\kappa} I(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, I}(x)$ by [19, (24), (25)], [2, (13)], [9, (20)]. For every natural number n and for every element P of S_2 such that $n \in \mathrm{dom}\, J$ holds J_n is measurable on P by [12, (4)], (69), (22), [? , (32)]. For every element x of X_2, $\int \mathrm{curry}'(((\sum_{\alpha=0}^{\kappa} C(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, C}, x)\, \mathrm{d}M_1 = ((\sum_{\alpha=0}^{\kappa} J(\alpha))_{\kappa \in \mathbb{N}})_{\mathrm{len}\, J}(x)$ by [19, (24), (25)], [2, (13)], [9, (20)]. $\square$

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, F be a set sequence of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, and n be a natural number. One can verify that the functor $F(n)$ yields an element of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Let F be a function from $\mathbb{N} \times \sigma(\mathrm{MeasRect}(S_1, S_2))$ into $\sigma(\mathrm{MeasRect}(S_1, S_2))$, n be an element of $\mathbb{N}$, and E be an element of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Let us observe that the functor $F(n, E)$ yields an element of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Now we state the propositions:

(77) 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, an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, and an element V of S_2. Suppose $E \in$ the field generated by $\mathrm{MeasRect}(S_1, S_2)$. Then there exists a function F from X_1 into $\overline{\mathbb{R}}$ such that

(i) for every element x of X_1, $F(x) = M_2(\mathrm{MeasurableXsection}(E, x) \cap V)$, and

(ii) for every element P of S_1, F is measurable on P.

The theorem is a consequence of (22), (27), (24), (76), (71), and (68).

(78) 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, an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, and an element V of S_1.

Suppose $E \in$ the field generated by $\text{MeasRect}(S_1, S_2)$. Then there exists a function F from X_2 into $\overline{\mathbb{R}}$ such that

(i) for every element x of X_2, $F(x) = M_1(\text{MeasurableYsection}(E, x) \cap V)$, and

(ii) for every element P of S_2, F is measurable on P.

The theorem is a consequence of (22), (27), (24), (76), (71), and (68).

(79) 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, and an element E of $\sigma(\text{MeasRect}(S_1, S_2))$. Suppose $E \in$ the field generated by $\text{MeasRect}(S_1, S_2)$. Let us consider an element B of S_2. Then $E \in \{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2))$: there exists a function F from X_1 into $\overline{\mathbb{R}}$ such that for every element x of $X_1, F(x) = M_2(\text{MeasurableXsection}(E, x) \cap B)$ and for every element V of S_1, F is measurable on $V\}$. The theorem is a consequence of (77).

(80) 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 an element E of $\sigma(\text{MeasRect}(S_1, S_2))$. Suppose $E \in$ the field generated by $\text{MeasRect}(S_1, S_2)$. Let us consider an element B of S_1. Then $E \in \{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2))$: there exists a function F from X_2 into $\overline{\mathbb{R}}$ such that for every element x of $X_2, F(x) = M_1(\text{MeasurableYsection}(E, x) \cap B)$ and for every element V of S_2, F is measurable on $V\}$. The theorem is a consequence of (78).

(81) 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, and an element B of S_2. Then the field generated by $\text{MeasRect}(S_1, S_2) \subseteq \{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2))$: there exists a function F from X_1 into $\overline{\mathbb{R}}$ such that for every element x of $X_1, F(x) = M_2(\text{MeasurableXsection}(E, x) \cap B)$ and for every element V of S_1, F is measurable on $V\}$. The theorem is a consequence of (7) and (79).

(82) 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 an element B of S_1. Then the field generated by $\text{MeasRect}(S_1, S_2) \subseteq \{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2))$: there exists a function F from X_2 into $\overline{\mathbb{R}}$ such that for every element y of $X_2, F(y) = M_1(\text{MeasurableYsection}(E, y) \cap B)$ and for every element V of S_2, F is measurable on $V\}$. The theorem is a consequence of (7) and (80).

7. σ-finite Measure

Let X be a non empty set, S be a σ-field of subsets of X, and M be a σ-measure on S. We say that M is σ-finite if and only if

(Def. 12) there exists a set sequence E of S such that for every natural number n, $M(E(n)) < +\infty$ and $\bigcup E = X$.

Now we state the propositions:

(83) Let us consider a non empty set X, a σ-field S of subsets of X, and a σ-measure M on S. Then M is σ-finite if and only if there exists a set sequence F of S such that F is non descending and for every natural number n, $M(F(n)) < +\infty$ and $\lim F = X$.

(84) Let us consider a set X, a semialgebra S of sets of X, a pre-measure P of S, and an induced measure M of S and P. Then $M =$ (the Caratheodory measure determined by $M)\restriction$(the field generated by S).

8. Fubini's Theorem on Measure

Now we state the propositions:

(85) 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, and an element B of S_2. Suppose $M_2(B) < +\infty$. Then $\{E$, where E is an element of $\sigma(\mathrm{MeasRect}(S_1, S_2))$: there exists a function F from X_1 into $\overline{\mathbb{R}}$ such that for every element x of X_1, $F(x) = M_2(\mathrm{MeasurableXsection}(E, x) \cap B)$ and for every element V of S_1, F is measurable on $V\}$ is a monotone class of $X_1 \times X_2$.

PROOF: Set $Z = \{E$, where E is an element of $\sigma(\mathrm{MeasRect}(S_1, S_2))$: there exists a function F from X_1 into $\overline{\mathbb{R}}$ such that for every element x of $X_1, F(x) = M_2(\mathrm{MeasurableXsection}(E, x) \cap B)$ and for every element V of S_1, F is measurable on $V\}$. For every sequence A_1 of subsets of $X_1 \times X_2$ such that A_1 is monotone and $\mathrm{rng}\, A_1 \subseteq Z$ holds $\lim A_1 \in Z$ by [10, (3)], [5, (35)], [21, (63)], [12, (45)]. $\square$

(86) 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 an element B of S_1. Suppose $M_1(B) < +\infty$. Then $\{E$, where E is an element of $\sigma(\mathrm{MeasRect}(S_1, S_2))$: there exists a function F from X_2 into $\overline{\mathbb{R}}$ such that for every element y of X_2, $F(y) = M_1(\mathrm{MeasurableYsection}(E, y) \cap B)$ and for every element V of S_2, F is measurable on $V\}$ is a monotone class of $X_1 \times X_2$.

PROOF: Set $Z = \{E$, where E is an element of $\sigma(\mathrm{MeasRect}(S_1, S_2))$: there exists a function F from X_2 into $\overline{\mathbb{R}}$ such that for every element y of $X_2, F(y) = M_1(\mathrm{MeasurableYsection}(E, y) \cap B)$ and for every element V

of S_2, F is measurable on $V\}$. For every sequence A_1 of subsets of $X_1 \times X_2$ such that A_1 is monotone and $\operatorname{rng} A_1 \subseteq Z$ holds $\lim A_1 \in Z$ by [10, (3)], [5, (35)], [21, (63)], [12, (45)]. $\square$

(87) Let us consider a non empty set X, a field F of subsets of X, and a sequence L of subsets of X. Suppose $\operatorname{rng} L$ is a monotone class of X and $F \subseteq \operatorname{rng} L$. Then

(i) $\sigma(F) = \text{monotone-class}(F)$, and

(ii) $\sigma(F) \subseteq \operatorname{rng} L$.

(88) Let us consider a non empty set X, a field F of subsets of X, and a family K of subsets of X. Suppose K is a monotone class of X and $F \subseteq K$. Then

(i) $\sigma(F) = \text{monotone-class}(F)$, and

(ii) $\sigma(F) \subseteq K$.

(89) 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, and an element B of S_2. Suppose $M_2(B) < +\infty$. Then $\sigma(\text{MeasRect}(S_1, S_2)) \subseteq \{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2))$: there exists a function F from X_1 into $\overline{\mathbb{R}}$ such that for every element x of $X_1, F(x) = M_2(\text{MeasurableXsection}(E, x) \cap B)$ and for every element V of S_1, F is measurable on $V\}$. The theorem is a consequence of (85), (81), (7), and (88).

(90) 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 an element B of S_1. Suppose $M_1(B) < +\infty$. Then $\sigma(\text{MeasRect}(S_1, S_2)) \subseteq \{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2))$: there exists a function F from X_2 into $\overline{\mathbb{R}}$ such that for every element y of $X_2, F(y) = M_1(\text{MeasurableYsection}(E, y) \cap B)$ and for every element V of S_2, F is measurable on $V\}$. The theorem is a consequence of (86), (82), (7), and (88).

(91) 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, and an element E of $\sigma(\text{MeasRect}(S_1, S_2))$. Suppose M_2 is σ-finite. Then there exists a function F from X_1 into $\overline{\mathbb{R}}$ such that

(i) for every element x of X_1, $F(x) = M_2(\text{MeasurableXsection}(E, x))$, and

(ii) for every element V of S_1, F is measurable on V.

PROOF: Consider B being a set sequence of S_2 such that B is non descending and for every natural number n, $M_2(B(n)) < +\infty$ and $\lim B = X_2$. Define $\mathcal{P}[\text{natural number}, \text{object}] \equiv$ there exists a function f_1 from X_1 into $\overline{\mathbb{R}}$ such that $\$_2 = f_1$ and for every element x of X_1, $f_1(x) =$

$M_2(\text{MeasurableXsection}(E, x) \cap B(\$_1))$ and for every element V of S_1, f_1 is measurable on V. For every element n of $\mathbb{N}$, there exists an element f of $X_1 \dot{\rightarrow} \overline{\mathbb{R}}$ such that $\mathcal{P}[n, f]$ by (89), [12, (45)]. Consider f being a function from $\mathbb{N}$ into $X_1 \dot{\rightarrow} \overline{\mathbb{R}}$ such that for every element n of $\mathbb{N}$, $\mathcal{P}[n, f(n)]$ from [11, Sch. 3]. For every natural number n, $f(n)$ is a function from X_1 into $\overline{\mathbb{R}}$ and for every element x of X_1, $f(n)(x) = M_2(\text{MeasurableXsection}(E, x) \cap B(n))$ and for every element V of S_1, $f(n)$ is measurable on V. For every natural numbers n, m, $\text{dom}(f(n)) = \text{dom}(f(m))$. For every element x of X_1 such that $x \in X_1$ holds $f \# x$ is convergent by [5, (11), (31)], [20, (7), (37)]. Reconsider $F = \lim f$ as a function from X_1 into $\overline{\mathbb{R}}$. For every element x of X_1, $F(x) = M_2(\text{MeasurableXsection}(E, x))$ by [21, (80)], [22, (92)], (49), [5, (11)]. □

(92) 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 an element E of $\sigma(\text{MeasRect}(S_1, S_2))$. Suppose M_1 is σ-finite. Then there exists a function F from X_2 into $\overline{\mathbb{R}}$ such that

(i) for every element y of X_2, $F(y) = M_1(\text{MeasurableYsection}(E, y))$, and

(ii) for every element V of S_2, F is measurable on V.

PROOF: Consider B being a set sequence of S_1 such that B is non descending and for every natural number n, $M_1(B(n)) < +\infty$ and $\lim B = X_1$. Define $\mathcal{P}[\text{natural number}, \text{object}] \equiv$ there exists a function f_1 from X_2 into $\overline{\mathbb{R}}$ such that $\$_2 = f_1$ and for every element y of X_2, $f_1(y) = M_1(\text{MeasurableYsection}(E, y) \cap B(\$_1))$ and for every element V of S_2, f_1 is measurable on V. For every element n of $\mathbb{N}$, there exists an element f of $X_2 \dot{\rightarrow} \overline{\mathbb{R}}$ such that $\mathcal{P}[n, f]$ by (90), [12, (45)]. Consider f being a function from $\mathbb{N}$ into $X_2 \dot{\rightarrow} \overline{\mathbb{R}}$ such that for every element n of $\mathbb{N}$, $\mathcal{P}[n, f(n)]$ from [11, Sch. 3]. For every natural number n, $f(n)$ is a function from X_2 into $\overline{\mathbb{R}}$ and for every element y of X_2, $f(n)(y) = M_1(\text{MeasurableYsection}(E, y) \cap B(n))$ and for every element V of S_2, $f(n)$ is measurable on V. For every natural numbers n, m, $\text{dom}(f(n)) = \text{dom}(f(m))$. For every element y of X_2 such that $y \in X_2$ holds $f \# y$ is convergent by [5, (11), (31)], [20, (7), (37)]. Reconsider $F = \lim f$ as a function from X_2 into $\overline{\mathbb{R}}$. For every element y of X_2, $F(y) = M_1(\text{MeasurableYsection}(E, y))$ by [21, (80)], [22, (92)], (49), [5, (11)]. □

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_2 be a σ-measure on S_2, and E be an element of $\sigma(\text{MeasRect}(S_1, S_2))$. Assume M_2 is σ-finite. The functor $\boxed{\text{Yvol}(E, M_2)}$ yielding a non-negative function from X_1 into $\overline{\mathbb{R}}$ is defined by

(Def. 13) for every element x of X_1, $it(x) = M_2(\mathrm{MeasurableXsection}(E, x))$ and for every element V of S_1, it is measurable on V.

Let M_1 be a σ-measure on S_1. Assume M_1 is σ-finite. The functor $\boxed{\mathrm{Xvol}(E, M_1)}$ yielding a non-negative function from X_2 into $\overline{\mathbb{R}}$ is defined by

(Def. 14) for every element y of X_2, $it(y) = M_1(\mathrm{MeasurableYsection}(E, y))$ and for every element V of S_2, it is measurable on V.

Now we state the propositions:

(93) 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, and elements E_1, E_2 of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Suppose M_2 is σ-finite and E_1 misses E_2. Then $\mathrm{Yvol}(E_1 \cup E_2, M_2) = \mathrm{Yvol}(E_1, M_2) + \mathrm{Yvol}(E_2, M_2)$.
PROOF: For every element x of X_1 such that $x \in \mathrm{dom}\,\mathrm{Yvol}(E_1 \cup E_2, M_2)$ holds $(\mathrm{Yvol}(E_1 \cup E_2, M_2))(x) = (\mathrm{Yvol}(E_1, M_2) + \mathrm{Yvol}(E_2, M_2))(x)$ by (26), (35), [5, (30)]. $\square$

(94) 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 elements E_1, E_2 of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Suppose M_1 is σ-finite and E_1 misses E_2. Then $\mathrm{Xvol}(E_1 \cup E_2, M_1) = \mathrm{Xvol}(E_1, M_1) + \mathrm{Xvol}(E_2, M_1)$.
PROOF: For every element x of X_2 such that $x \in \mathrm{dom}\,\mathrm{Xvol}(E_1 \cup E_2, M_1)$ holds $(\mathrm{Xvol}(E_1 \cup E_2, M_1))(x) = (\mathrm{Xvol}(E_1, M_1) + \mathrm{Xvol}(E_2, M_1))(x)$ by (26), (35), [5, (30)]. $\square$

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 elements E_1, E_2 of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Now we state the propositions:

(95) Suppose M_2 is σ-finite and E_1 misses E_2. Then $\int \mathrm{Yvol}(E_1 \cup E_2, M_2)\,\mathrm{d}M_1 = \int \mathrm{Yvol}(E_1, M_2)\,\mathrm{d}M_1 + \int \mathrm{Yvol}(E_2, M_2)\,\mathrm{d}M_1$. The theorem is a consequence of (93).

(96) Suppose M_1 is σ-finite and E_1 misses E_2. Then $\int \mathrm{Xvol}(E_1 \cup E_2, M_1)\,\mathrm{d}M_2 = \int \mathrm{Xvol}(E_1, M_1)\,\mathrm{d}M_2 + \int \mathrm{Xvol}(E_2, M_1)\,\mathrm{d}M_2$. The theorem is a consequence of (94).

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, an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element A of S_1, and an element B of S_2. Now we state the propositions:

(97) Suppose $E = A \times B$ and M_2 is σ-finite. Then

(i) if $M_2(B) = +\infty$, then $\mathrm{Yvol}(E, M_2) = \overline{\chi}_{A, X_1}$, and

(ii) if $M_2(B) \neq +\infty$, then there exists a real number r such that $r = M_2(B)$ and $\mathrm{Yvol}(E, M_2) = r \cdot \chi_{A, X_1}$.

The theorem is a consequence of (53).

(98) Suppose $E = A \times B$ and M_1 is σ-finite. Then

(i) if $M_1(A) = +\infty$, then $\mathrm{Xvol}(E, M_1) = \overline{\chi}_{B,X_2}$, and

(ii) if $M_1(A) \neq +\infty$, then there exists a real number r such that $r = M_1(A)$ and $\mathrm{Xvol}(E, M_1) = r \cdot \chi_{B,X_2}$.

The theorem is a consequence of (55).

Now we state the proposition:

(99) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, an element A of S, and a real number r. If $r \geqslant 0$, then $\int r \cdot \chi_{A,X}\,\mathrm{d}M = r \cdot M(A)$.

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, a finite sequence F of elements of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, and a natural number n. Now we state the propositions:

(100) Suppose M_2 is σ-finite and F is a finite sequence of elements of $\mathrm{MeasRect}(S_1, S_2)$. Then $(\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(F(n)) = \int \mathrm{Yvol}(F(n), M_2)\,\mathrm{d}M_1$. The theorem is a consequence of (16), (97), and (99).

(101) Suppose M_1 is σ-finite and F is a finite sequence of elements of $\mathrm{MeasRect}(S_1, S_2)$. Then $(\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(F(n)) = \int \mathrm{Xvol}(F(n), M_1)\,\mathrm{d}M_2$. The theorem is a consequence of (16), (98), and (99).

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, a disjoint valued finite sequence F of elements of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, and a natural number n. Now we state the propositions:

(102) Suppose M_2 is σ-finite and F is a finite sequence of elements of $\mathrm{MeasRect}(S_1, S_2)$. Then $(\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(\bigcup F) = \int \mathrm{Yvol}(\bigcup F, M_2)\,\mathrm{d}M_1$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(\bigcup(F \restriction \$_1)) = \int \mathrm{Yvol}(\bigcup(F \restriction \$_1), M_2)\,\mathrm{d}M_1$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [2, (13)], [3, (59)], [19, (55)], [3, (82)]. For every natural number k, $\mathcal{P}[k]$ from [2, Sch. 2]. □

(103) Suppose M_1 is σ-finite and F is a finite sequence of elements of $\mathrm{MeasRect}(S_1, S_2)$. Then $(\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(\bigcup F) = \int \mathrm{Xvol}(\bigcup F, M_1)\,\mathrm{d}M_2$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(\bigcup(F \restriction \$_1)) = \int \mathrm{Xvol}(\bigcup(F \restriction \$_1), M_1)\,\mathrm{d}M_2$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [2, (13)], [3, (59)], [19, (55)], [3, (82)]. For every natural number k, $\mathcal{P}[k]$ from [2, Sch. 2]. □

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, an element

E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element V of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element A of S_1, and an element B of S_2. Now we state the propositions:

(104) Suppose $E \in$ the field generated by $\mathrm{MeasRect}(S_1, S_2)$ and M_2 is σ-finite. Then suppose $V = A \times B$. Then $E \in \{E$, where E is an element of $\sigma(\mathrm{MeasRect}(S_1, S_2)) : \int \mathrm{Yvol}(E \cap V, M_2)\,\mathrm{d}M_1 = (\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(E \cap V)\}$. The theorem is a consequence of (102).

(105) Suppose $E \in$ the field generated by $\mathrm{MeasRect}(S_1, S_2)$ and M_1 is σ-finite. Then suppose $V = A \times B$. Then $E \in \{E$, where E is an element of $\sigma(\mathrm{MeasRect}(S_1, S_2)) : \int \mathrm{Xvol}(E \cap V, M_1)\,\mathrm{d}M_2 = (\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(E \cap V)\}$. The theorem is a consequence of (103).

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, an element V of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, an element A of S_1, and an element B of S_2. Now we state the propositions:

(106) Suppose M_2 is σ-finite and $V = A \times B$. Then the field generated by $\mathrm{MeasRect}(S_1, S_2) \subseteq \{E$, where E is an element of $\sigma(\mathrm{MeasRect}(S_1, S_2)) : \int \mathrm{Yvol}(E \cap V, M_2)\,\mathrm{d}M_1 = (\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(E \cap V)\}$. The theorem is a consequence of (7) and (104).

(107) Suppose M_1 is σ-finite and $V = A \times B$. Then the field generated by $\mathrm{MeasRect}(S_1, S_2) \subseteq \{E$, where E is an element of $\sigma(\mathrm{MeasRect}(S_1, S_2)) : \int \mathrm{Xvol}(E \cap V, M_1)\,\mathrm{d}M_2 = (\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(E \cap V)\}$. The theorem is a consequence of (7) and (105).

Now we state the propositions:

(108) 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, elements E, V of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, a set sequence P of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, and an element x of X_1. Suppose P is non descending and $\lim P = E$. Then there exists a sequence K of subsets of S_2 such that

(i) K is non descending, and

(ii) for every natural number n, $K(n) = \mathrm{MeasurableXsection}(P(n), x) \cap \mathrm{MeasurableXsection}(V, x)$, and

(iii) $\lim K = \mathrm{MeasurableXsection}(E, x) \cap \mathrm{MeasurableXsection}(V, x)$.

The theorem is a consequence of (43), (49), and (30).

(109) 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, elements E, V of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, a set sequence P of $\sigma(\mathrm{MeasRect}(S_1, S_2))$, and an element y of X_2. Suppose P is non descending and $\lim P = E$. Then there exists a sequence K of subsets of S_1 such that

(i) K is non descending, and

(ii) for every natural number n, $K(n) = \text{MeasurableYsection}(P(n), y) \cap \text{MeasurableYsection}(V, y)$, and

(iii) $\lim K = \text{MeasurableYsection}(E, y) \cap \text{MeasurableYsection}(V, y)$.

The theorem is a consequence of (44), (49), and (32).

(110) 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, elements E, V of $\sigma(\text{MeasRect}(S_1, S_2))$, a set sequence P of $\sigma(\text{MeasRect}(S_1, S_2))$, and an element x of X_1. Suppose P is non ascending and $\lim P = E$. Then there exists a sequence K of subsets of S_2 such that

(i) K is non ascending, and

(ii) for every natural number n, $K(n) = \text{MeasurableXsection}(P(n), x) \cap \text{MeasurableXsection}(V, x)$, and

(iii) $\lim K = \text{MeasurableXsection}(E, x) \cap \text{MeasurableXsection}(V, x)$.

The theorem is a consequence of (45), (49), and (31).

(111) 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, elements E, V of $\sigma(\text{MeasRect}(S_1, S_2))$, a set sequence P of $\sigma(\text{MeasRect}(S_1, S_2))$, and an element y of X_2. Suppose P is non ascending and $\lim P = E$. Then there exists a sequence K of subsets of S_1 such that

(i) K is non ascending, and

(ii) for every natural number n, $K(n) = \text{MeasurableYsection}(P(n), y) \cap \text{MeasurableYsection}(V, y)$, and

(iii) $\lim K = \text{MeasurableYsection}(E, y) \cap \text{MeasurableYsection}(V, y)$.

The theorem is a consequence of (46), (49), and (33).

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, an element V of $\sigma(\text{MeasRect}(S_1, S_2))$, an element A of S_1, and an element B of S_2. Now we state the propositions:

(112) Suppose M_2 is σ-finite and $V = A \times B$ and $(\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(V) < +\infty$ and $M_2(B) < +\infty$. Then $\{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2))$: $\int \text{Yvol}(E \cap V, M_2)\,\mathrm{d}M_1 = (\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E \cap V)\}$ is a monotone class of $X_1 \times X_2$.

PROOF: Set $Z = \{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2))$: $\int \text{Yvol}(E \cap V, M_2)\,\mathrm{d}M_1 = (\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E \cap V)\}$. For every sequence A_1 of subsets of $X_1 \times X_2$ such that A_1 is monotone and $\text{rng}\, A_1 \subseteq Z$ holds $\lim A_1 \in Z$ by [10, (3)], [5, (35)], [21, (63)], [12, (45)]. $\square$

(113) Suppose M_1 is σ-finite and $V = A \times B$ and $(\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(V) < +\infty$ and $M_1(A) < +\infty$. Then $\{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2)) : \int \text{Xvol}(E \cap V, M_1)\, \mathrm{d}M_2 = (\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E \cap V)\}$ is a monotone class of $X_1 \times X_2$.

PROOF: Set $Z = \{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2)) : \int \text{Xvol}(E \cap V, M_1)\, \mathrm{d}M_2 = (\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E \cap V)\}$. For every sequence A_1 of subsets of $X_1 \times X_2$ such that A_1 is monotone and $\operatorname{rng} A_1 \subseteq Z$ holds $\lim A_1 \in Z$ by [10, (3)], [5, (35)], [21, (63)], [12, (45)]. □

(114) Suppose M_2 is σ-finite and $V = A \times B$ and $(\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(V) < +\infty$ and $M_2(B) < +\infty$. Then $\sigma(\text{MeasRect}(S_1, S_2)) \subseteq \{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2)) : \int \text{Yvol}(E \cap V, M_2)\, \mathrm{d}M_1 = (\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E \cap V)\}$. The theorem is a consequence of (112), (106), (7), and (88).

(115) Suppose M_1 is σ-finite and $V = A \times B$ and $(\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(V) < +\infty$ and $M_1(A) < +\infty$. Then $\sigma(\text{MeasRect}(S_1, S_2)) \subseteq \{E$, where E is an element of $\sigma(\text{MeasRect}(S_1, S_2)) : \int \text{Xvol}(E \cap V, M_1)\, \mathrm{d}M_2 = (\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E \cap V)\}$. The theorem is a consequence of (113), (107), (7), and (88).

Now we state the proposition:

(116) Let us consider sets X, Y, a sequence A of subsets of X, a sequence B of subsets of Y, and a sequence C of subsets of $X \times Y$. Suppose A is non descending and B is non descending and for every natural number n, $C(n) = A(n) \times B(n)$. Then

(i) C is non descending and convergent, and

(ii) $\bigcup C = \bigcup A \times \bigcup B$.

PROOF: For every natural numbers n, m such that $n \leqslant m$ holds $C(n) \subseteq C(m)$ by [13, (96)]. □

Now we state the proposition:

(117) FUBINI'S THEOREM:

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 an element E of $\sigma(\text{MeasRect}(S_1, S_2))$. Suppose M_1 is σ-finite and M_2 is σ-finite. Then $\int \text{Yvol}(E, M_2)\, \mathrm{d}M_1 = (\text{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E)$.

PROOF: Consider A being a set sequence of S_1 such that A is non descending and for every natural number n, $M_1(A(n)) < +\infty$ and $\lim A = X_1$. Consider B being a set sequence of S_2 such that B is non descending and for every natural number n, $M_2(B(n)) < +\infty$ and $\lim B = X_2$. Define $\mathcal{C}(\text{element of } \mathbb{N}) = A(\$_1) \times B(\$_1)$. Consider C being a function from $\mathbb{N}$ into $2^{X_1 \times X_2}$ such that for every element n of $\mathbb{N}$, $C(n) = \mathcal{C}(n)$ from [11, Sch. 4]. For every natural number n, $C(n) = A(n) \times$

$B(n)$. For every natural number n, $C(n) \in \sigma(\mathrm{MeasRect}(S_1, S_2))$. For every natural numbers n, m such that $n \leqslant m$ holds $C(n) \subseteq C(m)$ by [13, (96)]. For every natural number n, $(\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(C(n)) < +\infty$ by (16), [6, (51)]. Set $C_1 = E \cap C$. For every object n such that $n \in \mathbb{N}$ holds $C_1(n) \in \sigma(\mathrm{MeasRect}(S_1, S_2))$. For every natural number n, $\int \mathrm{Yvol}(E \cap C(n), M_2)\,\mathrm{d}M_1 = (\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(E \cap C(n))$. Define $\mathcal{P}[\text{element of } \mathbb{N}, \text{object}] \equiv \$_2 = \mathrm{Yvol}(E \cap C(\$_1), M_2)$. For every element n of $\mathbb{N}$, there exists an element f of $X_1 \dot{\rightarrow} \overline{\mathbb{R}}$ such that $\mathcal{P}[n, f]$ by [12, (45)]. Consider F being a function from $\mathbb{N}$ into $X_1 \dot{\rightarrow} \overline{\mathbb{R}}$ such that for every element n of $\mathbb{N}$, $\mathcal{P}[n, F(n)]$ from [11, Sch. 3]. For every natural number n, $F(n) = \mathrm{Yvol}(E \cap C(n), M_2)$. Reconsider $X_3 = X_1$ as an element of S_1. For every natural number n and for every element x of X_1, $(F\#x)(n) = (\mathrm{Yvol}(E \cap C(n), M_2))(x)$. For every natural numbers n, m, $\mathrm{dom}(F(n)) = \mathrm{dom}(F(m))$. For every natural number n, $F(n)$ is measurable on X_3. For every natural numbers n, m such that $n \leqslant m$ for every element x of X_1 such that $x \in X_3$ holds $F(n)(x) \leqslant F(m)(x)$ by (20), [5, (31)]. For every element x of X_1 such that $x \in X_3$ holds $F\#x$ is convergent by [20, (7), (37)]. Consider I being a sequence of extended reals such that for every natural number n, $I(n) = \int F(n)\,\mathrm{d}M_1$ and I is convergent and $\int \lim F\,\mathrm{d}M_1 = \lim I$. For every element x of X_1 such that $x \in \mathrm{dom} \lim F$ holds $(\lim F)(x) = (\mathrm{Yvol}(E, M_2))(x)$ by (116), (108), (27), [10, (13)]. Set $J = E \cap C$. For every object n such that $n \in \mathbb{N}$ holds $J(n) \in \sigma(\mathrm{MeasRect}(S_1, S_2))$. $\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2)$ is a σ-measure on $\sigma(\mathrm{MeasRect}(S_1, S_2))$. For every element n of $\mathbb{N}$, $I(n) = (\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2)_* J)(n)$ by [10, (13)]. $\square$

Now we state the proposition:

(118) FUBINI'S THEOREM:

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 an element E of $\sigma(\mathrm{MeasRect}(S_1, S_2))$. Suppose M_1 is σ-finite and M_2 is σ-finite. Then $\int \mathrm{Xvol}(E, M_1)\,\mathrm{d}M_2 = (\mathrm{Prod}\,\sigma\text{-}\mathrm{Meas}(M_1, M_2))(E)$.

PROOF: Consider A being a set sequence of S_1 such that A is non descending and for every natural number n, $M_1(A(n)) < +\infty$ and $\lim A = X_1$. Consider B being a set sequence of S_2 such that B is non descending and for every natural number n, $M_2(B(n)) < +\infty$ and $\lim B = X_2$. Define $\mathcal{C}(\text{element of } \mathbb{N}) = A(\$_1) \times B(\$_1)$. Consider C being a function from $\mathbb{N}$ into $2^{X_1 \times X_2}$ such that for every element n of $\mathbb{N}$, $C(n) = \mathcal{C}(n)$ from [11, Sch. 4]. For every natural number n, $C(n) = A(n) \times B(n)$. For every natural number n, $C(n) \in \sigma(\mathrm{MeasRect}(S_1, S_2))$. For every natural numbers n, m such that $n \leqslant m$ holds $C(n) \subseteq C(m)$ by

[13, (96)]. For every natural number n, $(\mathrm{Prod}\,\sigma\text{-Meas}(M_1, M_2))(C(n)) < +\infty$ by (16), [6, (51)]. Set $C_1 = E \cap C$. For every object n such that $n \in \mathbb{N}$ holds $C_1(n) \in \sigma(\mathrm{MeasRect}(S_1, S_2))$. For every natural number n, $\int \mathrm{Xvol}(E \cap C(n), M_1)\, \mathrm{d}M_2 = (\mathrm{Prod}\,\sigma\text{-Meas}(M_1, M_2))(E \cap C(n))$. Define $\mathcal{P}[\text{element of } \mathbb{N}, \text{object}] \equiv \$_2 = \mathrm{Xvol}(E \cap C(\$_1), M_1)$. For every element n of $\mathbb{N}$, there exists an element f of $X_2 \dot{\rightarrow} \overline{\mathbb{R}}$ such that $\mathcal{P}[n, f]$ by [12, (45)]. Consider F being a function from $\mathbb{N}$ into $X_2 \dot{\rightarrow} \overline{\mathbb{R}}$ such that for every element n of $\mathbb{N}$, $\mathcal{P}[n, F(n)]$ from [11, Sch. 3]. For every natural number n, $F(n) = \mathrm{Xvol}(E \cap C(n), M_1)$. Reconsider $X_3 = X_2$ as an element of S_2. For every natural number n and for every element x of X_2, $(F\#x)(n) = (\mathrm{Xvol}(E \cap C(n), M_1))(x)$. For every natural numbers n, m, $\mathrm{dom}(F(n)) = \mathrm{dom}(F(m))$. For every natural number n, $F(n)$ is measurable on X_3. For every natural numbers n, m such that $n \leqslant m$ for every element x of X_2 such that $x \in X_3$ holds $F(n)(x) \leqslant F(m)(x)$ by (21), [5, (31)]. For every element x of X_2 such that $x \in X_3$ holds $F\#x$ is convergent by [20, (7), (37)]. Consider I being a sequence of extended reals such that for every natural number n, $I(n) = \int F(n)\, \mathrm{d}M_2$ and I is convergent and $\int \lim F\, \mathrm{d}M_2 = \lim I$. For every element x of X_2 such that $x \in \mathrm{dom} \lim F$ holds $(\lim F)(x) = (\mathrm{Xvol}(E, M_1))(x)$ by (116), (109), (27), [10, (13)]. Set $J = E \cap C$. For every object n such that $n \in \mathbb{N}$ holds $J(n) \in \sigma(\mathrm{MeasRect}(S_1, S_2))$. $\mathrm{Prod}\,\sigma\text{-Meas}(M_1, M_2)$ is a σ-measure on $\sigma(\mathrm{MeasRect}(S_1, S_2))$. For every element n of $\mathbb{N}$, $I(n) = (\mathrm{Prod}\,\sigma\text{-Meas}(M_1, M_2)_* J)(n)$ by [10, (13)]. $\square$

References

[1] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(**3**): 537–541, 1990.

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

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

[4] Heinz Bauer. *Measure and Integration Theory.* Walter de Gruyter Inc., 2002.

[5] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

[6] Józef Białas. Series of positive real numbers. Measure theory. *Formalized Mathematics*, 2(**1**):173–183, 1991.

[7] Vladimir Igorevich Bogachev and Maria Aparecida Soares Ruas. *Measure theory*, volume 1. Springer, 2007.

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

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

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

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

[14] Noboru Endou. Product pre-measure. *Formalized Mathematics*, 24(**1**):69–79, 2016. doi:10.1515/forma-2016-0006.

[15] Gerald B. Folland. *Real Analysis: Modern Techniques and Their Applications*. Wiley, 2nd edition, 1999.

[16] P. R. Halmos. *Measure Theory*. Springer-Verlag, 1974.

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

[18] M.M. Rao. *Measure Theory and Integration*. Marcel Dekker, 2nd edition, 2004.

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

[20] 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.

[21] Bo Zhang, Hiroshi Yamazaki, and Yatsuka Nakamura. Limit of sequence of subsets. *Formalized Mathematics*, 13(**2**):347–352, 2005.

[22] Bo Zhang, Hiroshi Yamazaki, and Yatsuka Nakamura. Some equations related to the limit of sequence of subsets. *Formalized Mathematics*, 13(**3**):407–412, 2005.

Received February 23, 2017

FORMALIZED MATHEMATICS
Vol. 25, No. 1, Pages 31–37, 2017
DOI: 10.1515/forma-2017-0002

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

Differentiability of Polynomials over Reals

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Summary. In this article, we formalize in the Mizar system [3] the notion of the derivative of polynomials over the field of real numbers [4]. To define it, we use the derivative of functions between reals and reals [9].

MSC: 26A24 03B35

Keywords: differentiation of real polynomials; derivative of real polynomials

MML identifier: POLYDIFF, version: 8.1.05 5.40.1286

1. Preliminaries

From now on c denotes a complex, r denotes a real number, m, n denote natural numbers, and f denotes a complex-valued function.

Now we state the propositions:

(1) $0 + f = f$.

(2) $f - 0 = f$.

Let f be a complex-valued function. Observe that $0 + f$ reduces to f and $f - 0$ reduces to f.

Now we state the propositions:

(3) $c + f = (\operatorname{dom} f \longmapsto c) + f$.

(4) $f - c = f - (\operatorname{dom} f \longmapsto c)$.

(5) $c \cdot f = (\operatorname{dom} f \longmapsto c) \cdot f$.

(6) $f + (\operatorname{dom} f \longmapsto 0) = f$. The theorem is a consequence of (3).

(7) $f - (\operatorname{dom} f \longmapsto 0) = f$. The theorem is a consequence of (4).

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

(8) $\square^0 = \mathbb{R} \longmapsto 1$.
PROOF: Reconsider $s = 1$ as an element of $\mathbb{R}$. $\square^0 = \mathbb{R} \longmapsto s$ by [8, (34)], [10, (7)]. $\square$

2. Differentiability of Real Functions

One can check that every function from $\mathbb{R}$ into $\mathbb{R}$ which is differentiable is also continuous.

Let f be a differentiable function from $\mathbb{R}$ into $\mathbb{R}$. The functor f' yielding a function from $\mathbb{R}$ into $\mathbb{R}$ is defined by the term

(Def. 1) $f'_{\restriction \mathbb{R}}$.

Now we state the propositions:

(9) Let us consider a function f from $\mathbb{R}$ into $\mathbb{R}$. Then f is differentiable if and only if for every r, f is differentiable in r.

(10) Let us consider a differentiable function f from $\mathbb{R}$ into $\mathbb{R}$. Then $f'(r) = f'(r)$[1].

Let f be a function from $\mathbb{R}$ into $\mathbb{R}$. Observe that f is differentiable if and only if the condition (Def. 2) is satisfied.

(Def. 2) for every r, f is differentiable in r.

Let us note that every function from $\mathbb{R}$ into $\mathbb{R}$ which is constant is also differentiable.

Now we state the proposition:

(11) Let us consider a constant function f from $\mathbb{R}$ into $\mathbb{R}$. Then $f' = \mathbb{R} \longmapsto 0$.
PROOF: Reconsider $z = 0$ as an element of $\mathbb{R}$. $f' = \mathbb{R} \longmapsto z$ by [9, (22)], [10, (7)]. $\square$

One can verify that $\mathrm{id}_{\mathbb{R}}$ is differentiable as a function from $\mathbb{R}$ into $\mathbb{R}$.

Now we state the proposition:

(12) $\mathrm{id}'_{\mathbb{R}} = \mathbb{R} \longmapsto 1$.
PROOF: Set $f = \mathrm{id}_{\mathbb{R}}$. Reconsider $z = 1$ as an element of $\mathbb{R}$. $f' = \mathbb{R} \longmapsto z$ by [9, (17)], [10, (7)]. $\square$

Let us consider n. One can verify that $\square^n$ is differentiable.

Now we state the proposition:

(13) $(\square^n)' = n \cdot (\square^{n-1})$.

From now on f, g denote differentiable functions from $\mathbb{R}$ into $\mathbb{R}$.

[1] Left-side $f'(r)$ is the value of the derivative defined in this article for differentiable functions $f : \mathbb{R} \mapsto \mathbb{R}$, and right-side $f'(r)$ is the value of the derivative defined for partial functions in [9].

Let us consider f and g. Let us observe that $f+g$ is differentiable as a function from $\mathbb{R}$ into $\mathbb{R}$ and $f-g$ is differentiable as a function from $\mathbb{R}$ into $\mathbb{R}$ and $f \cdot g$ is differentiable as a function from $\mathbb{R}$ into $\mathbb{R}$.

Let us consider r. One can verify that $r+f$ is differentiable as a function from $\mathbb{R}$ into $\mathbb{R}$ and $r \cdot f$ is differentiable as a function from $\mathbb{R}$ into $\mathbb{R}$ and $f-r$ is differentiable as a function from $\mathbb{R}$ into $\mathbb{R}$ and $-f$ is differentiable as a function from $\mathbb{R}$ into $\mathbb{R}$ and $f^{\mathbf{2}}$ is differentiable as a function from $\mathbb{R}$ into $\mathbb{R}$.

Now we state the propositions:

(14) $(f+g)' = f' + g'$. The theorem is a consequence of (9) and (10).

(15) $(f-g)' = f' - g'$. The theorem is a consequence of (9) and (10).

(16) $(f \cdot g)' = g \cdot f' + f \cdot g'$. The theorem is a consequence of (9) and (10).

(17) $(r+f)' = f'$. The theorem is a consequence of (11), (3), (14), and (6).

(18) $(f-r)' = f'$. The theorem is a consequence of (11), (4), (15), and (7).

(19) $(r \cdot f)' = r \cdot f'$. The theorem is a consequence of (9) and (10).

(20) $(-f)' = -f'$.

3. Polynomials

In the sequel L denotes a non empty zero structure and x denotes an element of L.

Now we state the proposition:

(21) Let us consider a (the carrier of L)-valued function f, and an object a. Then $\operatorname{Support}(f +\cdot (a, x)) \subseteq \operatorname{Support} f \cup \{a\}$.

Proof: $a = z$ or $z \in \operatorname{Support} f$ by [2, (32), (30)]. $\square$

Let us consider L and x. Let f be a finite-Support sequence of L and a be an object. Observe that $f +\cdot (a, x)$ is finite-Support as a sequence of L.

Now we state the proposition:

(22) Let us consider a polynomial p over L. If $p \neq \mathbf{0}.\,L$, then $\operatorname{len} p -' 1 = \operatorname{len} p - 1$.

Let L be a non empty zero structure and x be an element of L. Let us note that $\langle x \rangle$ is constant and $\langle x, 0_L \rangle$ is constant.

Now we state the proposition:

(23) Let us consider a non empty zero structure L, and a constant polynomial p over L. Then

(i) $p = \mathbf{0}.\,L$, or

(ii) $p = \langle p(0) \rangle$.

Let us consider L, x, and n. The functor $\operatorname{seq}(n, x)$ yielding a sequence of L is defined by the term

(Def. 3) $\mathbf{0}.\,L +\cdot\, (n, x)$.

Observe that $\operatorname{seq}(n, x)$ is finite-Support.

Now we state the propositions:

(24) $(\operatorname{seq}(n, x))(n) = x$.

(25) If $m \neq n$, then $(\operatorname{seq}(n, x))(m) = 0_L$.

(26) the length of $\operatorname{seq}(n, x)$ is at most $n + 1$.

(27) If $x \neq 0_L$, then $\operatorname{len} \operatorname{seq}(n, x) = n + 1$.

PROOF: Set $p = \operatorname{seq}(n, x)$. For every m such that the length of p is at most m holds $n + 1 \leqslant m$ by (24), [1, (13)]. □

(28) $\operatorname{seq}(n, 0_L) = \mathbf{0}.\,L$. The theorem is a consequence of (24).

(29) Let us consider a right zeroed, non empty additive loop structure L, and elements x, y of L. Then $\operatorname{seq}(n, x) + \operatorname{seq}(n, y) = \operatorname{seq}(n, x + y)$. The theorem is a consequence of (24) and (25).

(30) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, and an element x of L. Then $-\operatorname{seq}(n, x) = \operatorname{seq}(n, -x)$. The theorem is a consequence of (24) and (25).

(31) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, and elements x, y of L. Then $\operatorname{seq}(n, x) - \operatorname{seq}(n, y) = \operatorname{seq}(n, x - y)$. The theorem is a consequence of (30) and (29).

Let L be a non empty zero structure and p be a sequence of L. Let us consider n. The functor $p \upharpoonright n$ yielding a sequence of L is defined by the term

(Def. 4) $p +\cdot\, (n, 0_L)$.

Let p be a polynomial over L. Let us note that $p \upharpoonright n$ is finite-Support.

Let us consider a non empty zero structure L and a sequence p of L. Now we state the propositions:

(32) $(p \upharpoonright n)(n) = 0_L$.

(33) If $m \neq n$, then $(p \upharpoonright n)(m) = p(m)$.

Now we state the proposition:

(34) Let us consider a non empty zero structure L. Then $\mathbf{0}.\,L \upharpoonright n = \mathbf{0}.\,L$. The theorem is a consequence of (32).

Let L be a non empty zero structure. Let us consider n. One can verify that $\mathbf{0}.\,L \upharpoonright n$ reduces to $\mathbf{0}.\,L$.

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

(35) If $n > \operatorname{len} p -' 1$, then $p \restriction n = p$. The theorem is a consequence of (32).

(36) If $p \neq \mathbf{0}. L$, then $\operatorname{len}(p \restriction (\operatorname{len} p -' 1)) < \operatorname{len} p$.

Proof: Set $m = \operatorname{len} p -' 1$. $m = \operatorname{len} p - 1$. the length of $p \restriction m$ is at most $\operatorname{len} p$ by [2, (32)], [7, (8)]. $\square$

Now we state the proposition:

(37) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, and a polynomial p over L. Then $p \restriction (\operatorname{len} p -' 1) + \text{Leading-Monomial}\, p = p$. The theorem is a consequence of (32).

Let L be a non empty zero structure and p be a constant polynomial over L. Observe that Leading-Monomial p is constant.

Now we state the proposition:

(38) Let us consider an add-associative, right zeroed, right complementable, distributive, unital, non empty double loop structure L, and elements x, y of L. Then $\operatorname{eval}(\operatorname{seq}(n, x), y) = (\operatorname{seq}(n, x))(n) \cdot \operatorname{power}(y, n)$. The theorem is a consequence of (28), (27), and (25).

4. Differentiability of Polynomials over Reals

In the sequel p, q denote polynomials over $\mathbb{R}_{\mathrm{F}}$.

Now we state the propositions:

(39) Let us consider an element r of $\mathbb{R}_{\mathrm{F}}$. Then $\operatorname{power}(r, n) = r^n$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \operatorname{power}(r, \$_1) = r^{\$_1}$. For every natural number n, $\mathcal{P}[n]$ from [1, Sch. 2]. $\square$

(40) $\square^n = \operatorname{FPower}(1_{\mathbb{R}_{\mathrm{F}}}, n)$.

Proof: Reconsider $f = \operatorname{FPower}(1_{\mathbb{R}_{\mathrm{F}}}, n)$ as a function from $\mathbb{R}$ into $\mathbb{R}$. $\square^n = f$ by [8, (36)], (39). $\square$

Let us consider an element r of $\mathbb{R}_{\mathrm{F}}$. Now we state the propositions:

(41) $\operatorname{FPower}(r, n+1) = \operatorname{FPower}(r, n) \cdot \mathrm{id}_{\mathbb{R}}$.

(42) $\operatorname{FPower}(r, n)$ is a differentiable function from $\mathbb{R}$ into $\mathbb{R}$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \operatorname{FPower}(r, \$_1)$ is a differentiable function from $\mathbb{R}$ into $\mathbb{R}$. $\mathcal{P}[0]$ by [6, (66)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$ from [1, Sch. 2]. $\square$

(43) $\operatorname{power}(r, n) = (\square^n)(r)$. The theorem is a consequence of (40).

Let us consider p. The functor p' yielding a sequence of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 5) for every natural number n, $it(n) = p(n+1) \cdot (n+1)$.

Note that p' is finite-Support.

Now we state the propositions:

(44) If $p \neq \mathbf{0}.\mathbb{R}_{\mathrm{F}}$, then $\mathrm{len}\, p' = \mathrm{len}\, p - 1$.
PROOF: Set $x = \mathrm{len}\, p - 1$. Set $d = p'$. the length of d is at most x by [7, (8)]. For every n such that the length of d is at most n holds $x \leqslant n$ by [11, (7)], [7, (10)], [1, (21)]. □

(45) If $p \neq \mathbf{0}.\mathbb{R}_{\mathrm{F}}$, then $\mathrm{len}\, p = \mathrm{len}\, p' + 1$. The theorem is a consequence of (44).

(46) Let us consider a constant polynomial p over $\mathbb{R}_{\mathrm{F}}$. Then $p' = \mathbf{0}.\mathbb{R}_{\mathrm{F}}$. The theorem is a consequence of (45).

(47) $(p+q)' = p' + q'$.

(48) $(-p)' = -p'$.

(49) $(p-q)' = p' - q'$. The theorem is a consequence of (47) and (48).

(50) $\text{Leading-Monomial}\, p' = \mathbf{0}.\mathbb{R}_{\mathrm{F}} +\cdot (\mathrm{len}\, p -' 2, p(\mathrm{len}\, p -' 1) \cdot (\mathrm{len}\, p -' 1))$.
PROOF: Set $l = \text{Leading-Monomial}\, p$. Set $m = \mathrm{len}\, p -' 1$. Set $k = \mathrm{len}\, p -' 2$. Reconsider $a = p(m) \cdot m$ as an element of $\mathbb{R}_{\mathrm{F}}$. Set $f = z +\cdot (k, a)$. $l' = f$ by [1, (53)], [2, (31), (32)], [10, (7)]. □

(51) Let us consider elements r, s of $\mathbb{R}_{\mathrm{F}}$. Then $\langle r, s\rangle' = \langle s\rangle$.

Let us consider p. The functor $\mathrm{Eval}(p)$ yielding a function from $\mathbb{R}$ into $\mathbb{R}$ is defined by the term

(Def. 6) $\text{Polynomial-Function}(\mathbb{R}_{\mathrm{F}}, p)$.

Let us note that $\mathrm{Eval}(p)$ is differentiable.

Now we state the propositions:

(52) $\mathrm{Eval}(\mathbf{0}.\mathbb{R}_{\mathrm{F}}) = \mathbb{R} \longmapsto 0$.
PROOF: $\mathrm{Eval}(z) = \mathbb{R} \longmapsto 0 (\in \mathbb{R})$ by [5, (17)], [10, (7)]. □

(53) Let us consider an element r of $\mathbb{R}_{\mathrm{F}}$. Then $\mathrm{Eval}(\langle r\rangle) = \mathbb{R} \longmapsto r$.
PROOF: $\mathrm{Eval}(\langle r\rangle) = \mathbb{R} \longmapsto r (\in \mathbb{R})$ by [6, (37)], [10, (7)]. □

(54) If p is constant, then $\mathrm{Eval}(p)' = \mathbb{R} \longmapsto 0$. The theorem is a consequence of (23), (52), and (11).

(55) $\mathrm{Eval}(p+q) = \mathrm{Eval}(p) + \mathrm{Eval}(q)$.

(56) $\mathrm{Eval}(-p) = -\mathrm{Eval}(p)$.

(57) $\mathrm{Eval}(p-q) = \mathrm{Eval}(p) - \mathrm{Eval}(q)$. The theorem is a consequence of (55) and (56).

(58) $\mathrm{Eval}(\text{Leading-Monomial}\, p) = \mathrm{FPower}(p(\mathrm{len}\, p -' 1), \mathrm{len}\, p -' 1)$.
PROOF: Set $l = \text{Leading-Monomial}\, p$. Set $m = \mathrm{len}\, p -' 1$. Reconsider $f = \mathrm{FPower}(p(m), m)$ as a function from $\mathbb{R}$ into $\mathbb{R}$. $\mathrm{Eval}(l) = f$ by [5, (22)]. □

(59) $\mathrm{Eval}(\text{Leading-Monomial}\, p) = p(\mathrm{len}\, p -' 1) \cdot (\square^{\mathrm{len}\, p -' 1})$.
PROOF: Set $l = \text{Leading-Monomial}\, p$. Set $m = \mathrm{len}\, p -' 1$. Set $f = p(m) \cdot (\square^{m})$. $\mathrm{Eval}(l) = f$ by (39), [8, (36)], [5, (22)]. □

(60) Let us consider an element r of $\mathbb{R}_{\mathrm{F}}$. Then $\mathrm{Eval}(\mathrm{seq}(n, r)) = r \cdot (\square^n)$. The theorem is a consequence of (24), (43), and (38).

(61) $\mathrm{Eval}(p)' = \mathrm{Eval}(p')$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every p such that $\mathrm{len}\, p \leqslant \$_1$ holds $\mathrm{Eval}(p)' = \mathrm{Eval}(p')$. $\mathcal{P}[0]$ by [5, (5)], (46), (52), (54). If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$ by (36), [5, (3)], [1, (13)], (37). $\mathcal{P}[n]$ from [1, Sch. 2]. $\square$

Let us consider p. Let us observe that $\mathrm{Eval}(p)'$ is differentiable.

References

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

[2] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

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

[4] Kazimierz Kuratowski. *Rachunek różniczkowy i całkowy – funkcje jednej zmiennej*. Biblioteka Matematyczna. PWN – Warszawa (in polish), 1964.

[5] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.

[6] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.

[7] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.

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

[9] Konrad Raczkowski and Paweł Sadowski. Real function differentiability. *Formalized Mathematics*, 1(**4**):797–801, 1990.

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

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

Received February 23, 2017

FORMALIZED MATHEMATICS
Vol. 25, No. 1, Pages 39–48, 2017
DOI: 10.1515/forma-2017-0003

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

Introduction to Liouville Numbers

Adam Grabowski
Institute of Informatics
University of Białystok
Poland

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Summary. The article defines Liouville numbers, the object introduced by Joseph Liouville in 1844 [17] as an example of an object which can be approximated "quite closely" by a sequence of rational numbers. x is a Liouville number iff for every positive integer n, there exist integers p and q such that $q > 1$ and

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}.$$

It is easy to show that all Liouville numbers are irrational. Liouville constant, which is also defined formally, is the first transcendental (not algebraic) number. It is defined in Section 6 quite generally as the sum

$$\Sigma_{k=1}^{\infty} \frac{a_k}{b^{k!}}$$

for a finite sequence $\{a_k\}_{k \in \mathbb{N}}$ and $b \in \mathbb{N}$. Based on this definition, we also introduced the so-called Liouville number as

$$L = \Sigma_{k=1}^{\infty} 10^{-k!} = 0.110001000000000000000001\ldots,$$

substituting in the definition of $L(a, b)$ the constant sequence of 1's and $b = 10$. At the end, we show that the construction of an arbitrary Liouville number leads to Liouville numbers [12], [1]. We show additionally, that the set of all Liouville numbers is infinite, opening the next item from Abad and Abad's list of "Top 100 Theorems". We show also some preliminary constructions linking real sequences and finite sequences, where summing formulas are involved. In the Mizar [14] proof, we follow closely `https://en.wikipedia.org/wiki/Liouville_number`. The aim is to show that all Liouville numbers are transcendental (and to continue the series of proving specific numbers as e or π to be transcendental [7], [13], [6]).

MSC: 11J81 11K60 03B35

Keywords: Liouville number; Diophantine approximation; transcendental number; Liouville constant

MML identifier: LIOUVIL1, version: 8.1.05 5.40.1286

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

1. Preliminaries

Now we state the proposition:

(1) Let us consider natural numbers x, y. If $x > 1$ and $y > 1$, then $x \cdot y \geqslant x + y$.

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

(2) $n \leqslant n!$.

(3) $n \cdot n! = (n + 1)! - n!$.

(4) If $n \geqslant 1$, then $2 \leqslant (n + 1)!$.

Let us consider natural numbers n, i. Now we state the propositions:

(5) If $n \geqslant 1$ and $i \geqslant 1$, then $(n + i)! \geqslant n! + i$.

(6) If $n \geqslant 2$ and $i \geqslant 1$, then $(n + i)! > n! + i$. The theorem is a consequence of (1).

Now we state the propositions:

(7) Let us consider a natural number b. If $b > 1$, then $|\frac{1}{b}| < 1$.

(8) Let us consider an integer d. Then there exists a non zero natural number n such that $2^{n-1} > d$.

Let a be an integer and b be a natural number. Note that a^b is integer.

2. Sequences

Now we state the propositions:

(9) Let us consider sequences s_1, s_2 of real numbers. Suppose for every natural number n, $0 \leqslant s_1(n) \leqslant s_2(n)$ and there exists a natural number n such that $1 \leqslant n$ and $s_1(n) < s_2(n)$ and s_2 is summable. Then

   (i) s_1 is summable, and

   (ii) $\sum s_1 < \sum s_2$.

(10) Let us consider a sequence f of real numbers. Suppose there exists a natural number n such that for every natural number k such that $k \geqslant n$ holds $f(k) = 0$. Then f is summable.

Proof: Set $p = (\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}$. Reconsider $p_2 = p(n)$ as a real number. Set $r = \{p_2\}_{n \in \mathbb{N}}$. For every natural number k such that $k \geqslant n$ holds $p(k) = r(k)$ by [15, (57)], [3, (12)]. □

(11) Let us consider a natural number b. If $b > 1$, then $\sum((\frac{1}{b})^{\kappa})_{\kappa \in \mathbb{N}} = \frac{b}{b-1}$. The theorem is a consequence of (7).

Let n be a natural number. Let us observe that $\{n\}_{n \in \mathbb{N}}$ is $\mathbb{N}$-valued.

Let r be a positive natural number. Note that $\{r\}_{n \in \mathbb{N}}$ is positive yielding and there exists a sequence of real numbers which is $\mathbb{N}$-valued and $\mathbb{Z}$-valued.

Now we state the propositions:

(12) Let us consider a sequence F of real numbers, a natural number n, and a real number a. Suppose for every natural number k, $F(k) = a$. Then $(\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(n) = a \cdot (n+1)$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (\sum_{\alpha=0}^{\kappa} F(\alpha))_{\kappa \in \mathbb{N}}(\$_1) = a \cdot (\$_1 + 1)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i, $\mathcal{P}[i]$ from [3, Sch. 2]. $\square$

(13) Let us consider a natural number n, and a real number a. Then $(\sum_{\alpha=0}^{\kappa}(\{a\}_{n \in \mathbb{N}})(\alpha))_{\kappa}$ $a \cdot (n+1)$. The theorem is a consequence of (12).

Let f be a $\mathbb{Z}$-valued sequence of real numbers. Note that $(\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}$ is $\mathbb{Z}$-valued.

Let f be a $\mathbb{N}$-valued sequence of real numbers. Observe that $(\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}$ is $\mathbb{N}$-valued.

Now we state the propositions:

(14) Let us consider a sequence f of real numbers. Suppose there exists a natural number n such that for every natural number k such that $k \geqslant n$ holds $f(k) = 0$. Then there exists a natural number n such that for every natural number k such that $k \geqslant n$ holds $(\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}(k) = (\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}(n)$.
PROOF: Set $p = (\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}$. Reconsider $p_2 = p(n)$ as a real number. Set $r = \{p_2\}_{n \in \mathbb{N}}$. For every natural number k such that $k \geqslant n$ holds $p(k) = r(k)$ by [15, (57)], [3, (12)]. $\square$

(15) Let us consider a $\mathbb{Z}$-valued sequence f of real numbers. Suppose there exists a natural number n such that for every natural number k such that $k \geqslant n$ holds $f(k) = 0$. Then $\sum f$ is an integer.
PROOF: Set $p = (\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}$. Reconsider $p_2 = p(n)$ as a real number. Set $r = \{p_2\}_{n \in \mathbb{N}}$. For every natural number k such that $k \geqslant n$ holds $p(k) = r(k)$ by [15, (57)], [3, (12)]. $\square$

Let f be a non-negative yielding sequence of real numbers and n be a natural number. One can verify that $f \uparrow n$ is non-negative yielding.

3. Transformations between Real Functions and Finite Sequences

Let f be a sequence of real numbers and X be a subset of $\mathbb{N}$. The functor $f|X$ yielding a sequence of real numbers is defined by the term

(Def. 1) $(\mathbb{N} \longmapsto 0) + \cdot f \restriction X$.

Note that $f \restriction X$ is $\mathbb{N}$-defined.

Let n be a natural number. Let us note that $f \mid \mathrm{Seg\,n}$ is summable.

Let f be a $\mathbb{Z}$-valued sequence of real numbers. One can verify that $f \mid \mathrm{Seg\,n}$ is $\mathbb{Z}$-valued.

Now we state the proposition:

(16) Let us consider a sequence f of real numbers. Then $f \mid \mathrm{Seg}\,0 = \{0\}_{\mathrm{n}\in\mathbb{N}}$.
PROOF: Set $f_3 = f \mid \mathrm{Seg}\,0$. Set $g = \{0\}_{n\in\mathbb{N}}$. For every element x of $\mathbb{N}$, $f_3(x) = g(x)$ by [10, (11)]. $\square$

Let f be a sequence of real numbers and n be a natural number. The functor $\boxed{\mathrm{FinSeq}(f, n)}$ yielding a finite sequence of elements of $\mathbb{R}$ is defined by the term

(Def. 2) $f \restriction \mathrm{Seg}\,n$.

Now we state the proposition:

(17) Let us consider a sequence f of real numbers, and natural numbers k, n. If $k \in \mathrm{Seg}\,n$, then $(f \mid \mathrm{Seg\,n})(\mathrm{k}) = \mathrm{f}(\mathrm{k})$.

Let us consider a sequence f of real numbers and a natural number n. Now we state the propositions:

(18) If $f(0) = 0$, then $\sum \mathrm{FinSeq}(f, n) = \sum(f \mid \mathrm{Seg\,n})$.
PROOF: Set $f_1 = f \mid \mathrm{Seg\,n}$. Set $g = \mathrm{FinSeq}(f, n)$. Reconsider $f_0 = f(0)$ as an element of $\mathbb{R}$. Set $h = \langle f_0 \rangle \frown g$. For every natural number k such that $k < n+1$ holds $f_1(k) = h(k+1)$ by [3, (13), (14)], [22, (25)], [8, (49)]. For every natural number k such that $k \geqslant n+1$ holds $f_1(k) = 0$ by [3, (16)], [4, (1)], [24, (57)], [10, (11)]. $\square$

(19) $\mathrm{dom}\,\mathrm{FinSeq}(f, n) = \mathrm{Seg}\,n$.

Now we state the proposition:

(20) Let us consider a sequence f of real numbers, and a natural number i. Then $\mathrm{FinSeq}(f, i) \frown \langle f(i+1) \rangle = \mathrm{FinSeq}(f, i+1)$.
PROOF: Set $f_1 = \mathrm{FinSeq}(f, i)$. Set $g = \langle f(i+1) \rangle$. Set $h = \mathrm{FinSeq}(f, i+1)$. $\mathrm{dom}\, f_1 = \mathrm{Seg}\,i$. For every natural number k such that $k \in \mathrm{dom}(f_1 \frown g)$ holds $(f_1 \frown g)(k) = h(k)$ by [3, (13)], [4, (5), (25)], (19). $\square$

Let us consider a sequence f of real numbers and a natural number n. Now we state the propositions:

(21) If $f(0) = 0$, then $\sum \mathrm{FinSeq}(f, n) = (\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa\in\mathbb{N}}(n)$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \sum \mathrm{FinSeq}(f, \$_1) = (\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa\in\mathbb{N}}(\$_1)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by (20), [23, (4)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(22) If $f(0) = 0$, then $\sum(f \mid \mathrm{Seg\,n}) = (\sum_{\alpha=0}^{\kappa} \mathrm{f}(\alpha))_{\kappa\in\mathbb{N}}(\mathrm{n})$. The theorem is a consequence of (21) and (18).

Now we state the propositions:

(23) Let us consider a $\mathbb{Z}$-valued sequence f of real numbers, and a natural number n. If $f(0) = 0$, then $\sum(f \mid \mathrm{Seg}\, \mathrm{n})$ is an integer. The theorem is a consequence of (22).

(24) Let us consider a sequence f of real numbers, and a natural number n. Suppose f is summable and $f(0) = 0$. Then $\sum f = \sum \mathrm{FinSeq}(f, n) + \sum(f \uparrow (n+1))$. The theorem is a consequence of (21).

One can check that there exists a sequence of real numbers which is positive yielding and $\mathbb{N}$-valued.

4. Sequences not Vanishing at Infinity

Let f be a sequence of real numbers. We say that f is eventually non-zero if and only if

(Def. 3) for every natural number n, there exists a natural number N such that $n \leqslant N$ and $f(N) \neq 0$.

Observe that every sequence of real numbers which is eventually nonzero is also eventually non-zero and $\mathrm{id}_{\mathrm{seq}}(\mathrm{id}_{\mathbb{N}})$ is eventually nonzero and there exists a sequence of real numbers which is eventually non-zero.

Now we state the proposition:

(25) Let us consider an eventually non-zero sequence f of real numbers, and a natural number n. Then $f \uparrow n$ is eventually non-zero.

Let f be an eventually non-zero sequence of real numbers and n be a natural number. Note that $f \uparrow n$ is eventually non-zero as a sequence of real numbers and every sequence of real numbers which is non-zero and constant is also eventually non-zero.

Let b be a natural number. The functor $\mathrm{pfact}(b)$ yielding a sequence of real numbers is defined by

(Def. 4) for every natural number i, $it(i) = \frac{1}{b^{i!}}$.

Now we state the propositions:

(26) Let us consider natural numbers b, i. Suppose $b \geqslant 1$. Then $(\mathrm{pfact}(b))(i) \leqslant ((\frac{1}{b})^{\kappa})_{\kappa \in \mathbb{N}}(i)$.

(27) Let us consider a natural number b. Suppose $b > 1$. Then

(i) $\mathrm{pfact}(b)$ is summable, and

(ii) $\sum \mathrm{pfact}(b) \leqslant \frac{b}{b-1}$.

The theorem is a consequence of (26) and (11).

Let b be a non trivial natural number. Observe that $\mathrm{pfact}(b)$ is summable and there exists a sequence of real numbers which is non-negative yielding.

Now we state the proposition:

(28) Let us consider natural numbers n, b. Suppose $b > 1$ and $n \geqslant 1$. Then $\sum((b-1) \cdot (\mathrm{pfact}(b) \uparrow (n+1))) < \frac{1}{(b^{n!})^n}$.

PROOF: $\mathrm{pfact}(b) \uparrow (n+1)$ is summable. Set $s_1 = \mathrm{pfact}(b) \uparrow (n+1)$. Set $s_2 = ((\frac{1}{b})^\kappa)_{\kappa \in \mathbb{N}} \uparrow (n+1)!$. For every natural number k, $0 \leqslant s_1(k) \leqslant s_2(k)$ by [3, (13)], [19, (7)], [3, (16)], [5, (8)]. There exists a natural number k such that $1 \leqslant k$ and $s_1(k) < s_2(k)$ by [19, (7)], [20, (39)]. $\sum s_1 < \sum s_2$. Reconsider $b_3 = b^{(n+1)!}$ as a natural number. $((\frac{1}{b})^\kappa)_{\kappa \in \mathbb{N}} \uparrow (n+1)! = (\frac{1}{b_3}) \cdot ((\frac{1}{b})^\kappa)_{\kappa \in \mathbb{N}}$ by [16, (8)], [19, (7)], [9, (63)]. □

5. Liouville Numbers

Let x be a real number. We say that x is Liouville if and only if

(Def. 5) for every natural number n, there exists an integer p and there exists a natural number q such that $q > 1$ and $0 < |x - \frac{p}{q}| < \frac{1}{q^n}$.

Now we state the proposition:

(29) Let us consider a real number r. Then r is Liouville if and only if for every non zero natural number n, there exists an integer p and there exists a natural number q such that $1 < q$ and $0 < |r - \frac{p}{q}| < \frac{1}{q^n}$.

Let a be a sequence of real numbers and b be a natural number. The functor $\mathrm{LiouvilleSeq}(a, b)$ yielding a sequence of real numbers is defined by

(Def. 6) $it(0) = 0$ and for every non zero natural number k, $it(k) = \frac{a(k)}{b^{k!}}$.

One can check that every real number which is Liouville is also irrational.

6. Liouville Constant

Let a be a sequence of real numbers and b be a natural number. The functor $\mathrm{LiouvilleConst}(a, b)$ yielding a real number is defined by the term

(Def. 7) $\sum \mathrm{LiouvilleSeq}(a, b)$.

The functor $\mathrm{BLiouvilleSeq}(b)$ yielding a sequence of real numbers is defined by

(Def. 8) for every natural number n, $it(n) = b^{n!}$.

Let us note that $\mathrm{BLiouvilleSeq}(b)$ is $\mathbb{N}$-valued.

Let a be a sequence of real numbers. The functor $\mathrm{ALiouvilleSeq}(a, b)$ yielding a sequence of real numbers is defined by

(Def. 9) for every natural number n, $it(n) = (\mathrm{BLiouvilleSeq}(b))(n) \cdot \sum(\mathrm{LiouvilleSeq}(a, b) \mid \mathrm{Se}$

Now we state the propositions:

(30) Let us consider a $\mathbb{N}$-valued sequence a of real numbers, and natural numbers b, n, k. Suppose $b > 0$ and $k \leqslant n$. Then $(\mathrm{LiouvilleSeq}(a, b))(k) \cdot (\mathrm{BLiouvilleSeq}(b))(n)$ is an integer.

(31) Let us consider a $\mathbb{N}$-valued sequence a of real numbers, and natural numbers b, n. If $b > 0$, then $(\mathrm{ALiouvilleSeq}(a, b))(n)$ is an integer.

Proof: Set $L = \mathrm{LiouvilleSeq}(a, b)$. Set $B = \mathrm{BLiouvilleSeq}(b)$. Set $f_3 = B(n) \cdot (L \mid \mathrm{Seg}\,\mathrm{n})$. $\mathrm{rng}\, f_3 \subseteq \mathbb{Z}$ by [4, (1)], [24, (62)], [10, (13)], [8, (49)]. Set $m = n + 1$. For every natural number k such that $k \geqslant m$ holds $f_3(k) = 0$ by [3, (13)], [4, (1)], [24, (57)], [10, (11)]. □

Let a be a $\mathbb{N}$-valued sequence of real numbers and b be a non zero natural number. Let us observe that $\mathrm{ALiouvilleSeq}(a, b)$ is $\mathbb{Z}$-valued.

Now we state the propositions:

(32) Let us consider non zero natural numbers n, b. If $b > 1$, then $(\mathrm{BLiouvilleSeq}(b))(n) \geqslant 1$.

(33) Let us consider a $\mathbb{N}$-valued sequence a of real numbers, and a non zero natural number b. Suppose $b \geqslant 2$ and $\mathrm{rng}\, a \subseteq b$. Then $\mathrm{LiouvilleSeq}(a, b)$ is summable.

Proof: Set $f = \mathrm{LiouvilleSeq}(a, b)$. For every natural number i, $\frac{b-1}{b^{i!}} = ((b - 1) \cdot \mathrm{pfact}(b))(i)$. For every natural number i, $f(i) \geqslant 0$ and $f(i) \leqslant ((b-1) \cdot \mathrm{pfact}(b))(i)$ by [21, (3)], [16, (12)], [3, (51), (44), (13)]. $\mathrm{pfact}(b)$ is summable. □

(34) Let us consider a sequence a of real numbers, a non zero natural number n, and a non zero natural number b. Suppose $b > 1$. Then $\frac{(\mathrm{ALiouvilleSeq}(a,b))(n)}{(\mathrm{BLiouvilleSeq}(b))(n)} = \sum \mathrm{FinSeq}(\mathrm{LiouvilleSeq}(a, b), n)$. The theorem is a consequence of (32) and (18).

(35) Let us consider a $\mathbb{N}$-valued sequence a of real numbers, a non trivial natural number b, and a natural number n. Then $(\mathrm{LiouvilleSeq}(a, b))(n) \geqslant 0$.

(36) Let us consider a positive yielding, $\mathbb{N}$-valued sequence a of real numbers, a non trivial natural number b, and a non zero natural number n. Then $(\mathrm{LiouvilleSeq}(a, b))(n) > 0$.

Let a be a $\mathbb{N}$-valued sequence of real numbers and b be a non trivial natural number. One can check that $\mathrm{LiouvilleSeq}(a, b)$ is non-negative yielding.

Now we state the propositions:

(37) Let us consider a $\mathbb{N}$-valued sequence a of real numbers, and natural numbers b, c. Suppose $b \geqslant 2$ and $c \geqslant 1$ and $\mathrm{rng}\, a \subseteq c$ and $c \leqslant b$. Let us consider a natural number i. Then $(\mathrm{LiouvilleSeq}(a, b))(i) \leqslant ((c - 1) \cdot \mathrm{pfact}(b))(i)$.

(38) Let us consider a $\mathbb{N}$-valued sequence a of real numbers, and natural numbers b, c. Suppose $b \geqslant 2$ and $c \geqslant 1$ and $\operatorname{rng} a \subseteq c$ and $c \leqslant b$. Then $\sum \mathrm{LiouvilleSeq}(a,b) \leqslant \sum((c-1)\cdot \mathrm{pfact}(b))$. The theorem is a consequence of (27), (35), and (37).

(39) Let us consider a $\mathbb{N}$-valued sequence a of real numbers, and natural numbers b, c, n. Suppose $b \geqslant 2$ and $c \geqslant 1$ and $\operatorname{rng} a \subseteq c$ and $c \leqslant b$. Then $\sum(\mathrm{LiouvilleSeq}(a,b) \upharpoonright (n+1)) \leqslant \sum((c-1)\cdot(\mathrm{pfact}(b)\upharpoonright(n+1)))$.
Proof: Set $g = (c-1)\cdot(\mathrm{pfact}(b)\upharpoonright(n+1))$. $\mathrm{pfact}(b)\upharpoonright(n+1)$ is summable. Set $f = \mathrm{LiouvilleSeq}(a,b)\upharpoonright(n+1)$. For every natural number i, $0 \leqslant f(i)$ by [8, (3)]. For every natural number i, $f(i) \leqslant g(i)$ by [15, (9)], (37). $\square$

(40) Let us consider a $\mathbb{N}$-valued sequence a of real numbers, a non trivial natural number b, and a natural number n. Suppose a is eventually non-zero and $\operatorname{rng} a \subseteq b$. Then $\sum(\mathrm{LiouvilleSeq}(a,b)\upharpoonright(n+1)) > 0$.
Proof: Set $L = \mathrm{LiouvilleSeq}(a,b)\upharpoonright(n+1)$. For every natural number i, $0 \leqslant L(i)$. There exists a natural number i such that $i \in \operatorname{dom} L$ and $0 < L(i)$ by [21, (5)]. Consider k being a natural number such that $k \in \operatorname{dom} L$ and $L(k) > 0$. $\mathrm{LiouvilleSeq}(a,b)$ is summable. $\square$

(41) Let us consider a $\mathbb{N}$-valued sequence a of real numbers, and a non trivial natural number b. Suppose $\operatorname{rng} a \subseteq b$ and a is eventually non-zero. Let us consider a non zero natural number n. Then there exists an integer p and there exists a natural number q such that $q > 1$ and $0 < |\,\mathrm{LiouvilleConst}(a,b) - \frac{p}{q}| < \frac{1}{q^n}$. The theorem is a consequence of (32), (33), (40), (24), (34), (39), and (28).

The functor LiouvilleConst yielding a real number is defined by the term

(Def. 10) $\mathrm{LiouvilleConst}(\{1\}_{n\in\mathbb{N}}, 10)$.

Now we state the proposition:

(42) Let us consider a $\mathbb{N}$-valued sequence a of real numbers, and a non trivial natural number b. Suppose $\operatorname{rng} a \subseteq b$ and a is eventually non-zero. Then $\mathrm{LiouvilleConst}(a,b)$ is Liouville. The theorem is a consequence of (41) and (29).

One can check that LiouvilleConst is Liouville and there exists a real number which is Liouville.

A Liouville number is a Liouville real number. Now we state the propositions:

(43) Let us consider non zero natural numbers m, n. Then $(\mathrm{LiouvilleSeq}(\{1\}_{n\in\mathbb{N}}, m))(n)$ $m^{-n!}$.

(44) Let us consider a natural number m. If $1 < m$, then $\mathrm{LiouvilleSeq}(\{1\}_{n\in\mathbb{N}}, m)$ is negligible.

PROOF: There exists a function f from $\mathbb{N}$ into $\mathbb{R}$ such that for every natural number x, $f(x) = \frac{1}{2^x}$. Consider f being a function from $\mathbb{N}$ into $\mathbb{R}$ such that for every natural number x, $f(x) = \frac{1}{2^x}$. Set $g = \text{LiouvilleSeq}(\{1\}_{n\in\mathbb{N}}, m)$. For every natural number x, $|g(x)| \leqslant |f(x)|$ by [18, (5), (4)]. $\square$

(45) $\frac{1}{10} < \text{LiouvilleConst} \leqslant \frac{10}{9} - \frac{1}{10}$.

PROOF: Set $a = \{1\}_{n\in\mathbb{N}}$. Set $b = 10$. Reconsider $n = 1$ as a non zero natural number. Set $f = \text{LiouvilleSeq}(a, b)$. Set $p_1 = \text{pfact}(b)$. f is summable. For every natural number n, $0 \leqslant f(n)$. $f(1) = 10^{-1}$. Set $s_1 = f \uparrow 2$. Set $s_2 = p_1 \uparrow 2$. $\sum p_1 = (\sum_{\alpha=0}^{\kappa} p_1(\alpha))_{\kappa\in\mathbb{N}}(1) + \sum(p_1 \uparrow (1+1))$. $\sum p_1 \leqslant \frac{b}{b-1}$. s_2 is summable. For every natural number n, $0 \leqslant s_1(n) \leqslant s_2(n)$ by (37), [11, (7)], [2, (50)], (35). $\square$

(46) Let us consider a Liouville number n_1, and an integer z. Then $z + n_1$ is Liouville. The theorem is a consequence of (29).

Let n_1 be a Liouville number and z be an integer. One can verify that $n_1 + z$ is Liouville.

The set of all Liouville numbers yielding a subset of $\mathbb{R}$ is defined by the term

(Def. 11) the set of all n_1 where n_1 is a Liouville number.

Note that the set of all Liouville numbers is infinite.

References

[1] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. 2nd edition, 1997.

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

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

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

[5] Grzegorz Bancerek and Piotr Rudnicki. Two programs for **SCM**. Part I – preliminaries. *Formalized Mathematics*, 4(**1**):69–72, 1993.

[6] Sophie Bernard, Yves Bertot, Laurence Rideau, and Pierre-Yves Strub. Formal proofs of transcendence for e and π as an application of multivariate and symmetric polynomials. In Jeremy Avigad and Adam Chlipala, editors, *Proceedings of the 5th ACM SIGPLAN Conference on Certified Programs and Proofs*, pages 76–87. ACM, 2016. doi:10.1145/2854065.2854072.

[7] Jesse Bingham. Formalizing a proof that e is transcendental. *Journal of Formalized Reasoning*, 4:71–84, 2011.

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

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

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

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

[12] J.H. Conway and R.K. Guy. *The Book of Numbers*. 1996.

[13] Manuel Eberl. Liouville numbers. *Archive of Formal Proofs*, December 2015. `http://isa-afp.org/entries/Liouville_Numbers.shtml`, Formal proof development.

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

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

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

[17] Joseph Liouville. Nouvelle démonstration d'un théorème sur les irrationnelles algébriques, inséré dans le Compte Rendu de la dernière séance. *Compte Rendu Acad. Sci. Paris*, Sér.A (18):910–911, 1844.

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

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

[20] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.

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

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

[23] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1 (**5**):979–981, 1990.

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

Received February 23, 2017

FORMALIZED MATHEMATICS
Vol. 25, No. 1, Pages 49–54, 2017
DOI: 10.1515/forma-2017-0004

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

All Liouville Numbers are Transcendental

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Adam Naumowicz
Institute of Informatics
University of Białystok
Poland

Adam Grabowski
Institute of Informatics
University of Białystok
Poland

Summary. In this Mizar article, we complete the formalization of one of the items from Abad and Abad's challenge list of "Top 100 Theorems" about Liouville numbers and the existence of transcendental numbers. It is item #18 from the "Formalizing 100 Theorems" list maintained by Freek Wiedijk at http://www.cs.ru.nl/F.Wiedijk/100/. Liouville numbers were introduced by Joseph Liouville in 1844 [15] as an example of an object which can be approximated "quite closely" by a sequence of rational numbers. x is a Liouville number iff for every positive integer n, there exist integers p and q such that $q > 1$ and

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}.$$

It is easy to show that all Liouville numbers are irrational. The definition and basic notions are contained in [12]. Liouville's constant, which is also defined formally, is the first explicit transcendental (not algebraic) number. Algebraic numbers were formalized with the help of the Mizar system [13] very recently, by Yasushige Watase in [23] and now we expand these techniques into the area of not only pure algebraic domains (as field, rings and formal polynomials), but also for more set-theoretic fields. Finally we show that all Liouville numbers are transcendental, based on Liouville's theorem on Diophantine approximation. Liouville's constant, which is also defined formally, is the first explicit transcendental (not algebraic) number [10], [1]. We plan to develop the theory of transcendental numbers in the Mizar Mathematical Library, following HOL Light [5], Isabelle [11], and Coq [4].

MSC: 11J81 11K60 03B35

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

Keywords: Liouville numbers; Diophantine approximation; transcendental numbers; Liouville's constant

MML identifier: `LIOUVIL2`, version: `8.1.05 5.40.1286`

From now on m, n denote natural numbers, r denotes a real number, and c denotes an element of $\mathbb{C}_{\mathrm{F}}$.

Let f be a non empty, complex-valued function. One can check that $|f|$ is non empty.

Now we state the propositions:

(1) If $2 \leqslant m$, then for every real number A, there exists a positive natural number n such that $A \leqslant m^n$.

(2) Let us consider a positive real number A. Then there exists a positive natural number n such that $\frac{1}{2^n} \leqslant A$. The theorem is a consequence of (1).

Let us consider r and n. Observe that $[r-n, r+n]$ is right-ended.

Let a, b be real numbers. One can verify that $[a, b]$ is closed interval as a subset of $\mathbb{R}$ and there exists an element of $\mathbb{R}_{\mathrm{F}}$ which is irrational.

Now we state the propositions:

(3) $\mathbb{R}_{\mathrm{F}}$ is a subring of $\mathbb{C}_{\mathrm{F}}$.

(4) $\mathbb{F}_{\mathbb{Q}}$ is a subring of $\mathbb{R}_{\mathrm{F}}$.

(5) $\mathbb{Z}^{\mathrm{R}}$ is a subring of $\mathbb{R}_{\mathrm{F}}$.

Let us consider a ring R and a subring S of R. Now we state the propositions:

(6) Every element of S is an element of R.

(7) Every polynomial over S is a polynomial over R.

Let us consider a ring R, a subring S of R, a polynomial f over S, and a polynomial g over R. Now we state the propositions:

(8) If $f = g$, then $\operatorname{len} f = \operatorname{len} g$.

PROOF: the length of f is at most $\operatorname{len} g$ by [20, (8)]. For every natural number m such that the length of f is at most m holds $\operatorname{len} g \leqslant m$. $\square$

(9) If $f = g$, then $\operatorname{LC} f = \operatorname{LC} g$.

Now we state the proposition:

(10) Let us consider a non degenerated ring R, a subring S of R, a polynomial f over S, and a monic polynomial g over R. If $f = g$, then f is monic. The theorem is a consequence of (8).

Let R be a non degenerated ring. Let us note that every subring of R is non degenerated and there exists a subring of R which is non degenerated.

Now we state the propositions:

(11) Let us consider a non degenerated ring R, a non degenerated subring S of R, a monic polynomial f over S, and a polynomial g over R. If $f = g$, then g is monic. The theorem is a consequence of (8).

(12) Let us consider a non degenerated ring R, a subring S of R, a polynomial f over S, and a non-zero polynomial g over R. If $f = g$, then f is non-zero. The theorem is a consequence of (8).

(13) Let us consider a non degenerated ring R, a subring S of R, a non-zero polynomial f over S, and a polynomial g over R. If $f = g$, then g is non-zero. The theorem is a consequence of (8).

(14) Let us consider rings R, T, a subring S of R, a polynomial f over S, and a polynomial g over R. Suppose $f = g$. Let us consider an element a of R. Then $\mathrm{ExtEval}(f, a(\in T)) = \mathrm{ExtEval}(g, a(\in T))$. The theorem is a consequence of (8).

(15) Let us consider a ring R, a subring S of R, a polynomial f over S, an element r of R, and an element s of S. If $r = s$, then $\mathrm{ExtEval}(f, r) = \mathrm{ExtEval}(f, s)$. The theorem is a consequence of (6).

(16) Let us consider a ring R, a subring S of R, an element r of R, and an element s of S. If $r = s$ and s is integral over S, then r is integral over R. The theorem is a consequence of (7), (8), (14), and (15).

(17) Let us consider a ring R, a subring S of R, an element r of R, an element s of S, a polynomial f over R, and a polynomial g over S. If $r = s$ and $f = g$ and r is a root of f, then s is a root of g.

Proof: Consider F being a finite sequence of elements of R such that $\mathrm{eval}(f, r) = \sum F$ and $\mathrm{len}\, F = \mathrm{len}\, f$ and for every element n of $\mathbb{N}$ such that $n \in \mathrm{dom}\, F$ holds $F(n) = f(n -' 1) \cdot \mathrm{power}_R(r, n -' 1)$. For every element n of $\mathbb{N}$ such that $n \in \mathrm{dom}\, F$ holds $F(n) = g(n -' 1) \cdot \mathrm{power}_S(s, n -' 1)$ by (6), [23, (11)]. $\mathrm{rng}\, F \subseteq$ the carrier of S. Reconsider $G = F$ as a finite sequence of elements of S. $\mathrm{len}\, G = \mathrm{len}\, g$. $\sum G$ is an element of R. $\square$

(18) Every ring is a subring of R.

One can check that $\mathbf{0}.\mathbb{C}_{\mathrm{F}}$ is $\mathbb{Z}$-valued and $\mathbf{1}.\mathbb{C}_{\mathrm{F}}$ is $\mathbb{Z}$-valued.

Let L be a non degenerated, non empty double loop structure. One can check that every polynomial over L which is monic is also non-zero and there exists a polynomial over $\mathbb{C}_{\mathrm{F}}$ which is monic and $\mathbb{Z}$-valued and there exists a polynomial over $\mathbb{C}_{\mathrm{F}}$ which is monic and $\mathbb{Q}$-valued and there exists a polynomial over $\mathbb{C}_{\mathrm{F}}$ which is monic and $\mathbb{R}$-valued.

Now we state the propositions:

(19) Every $\mathbb{Z}$-valued polynomial over $\mathbb{C}_{\mathrm{F}}$ is a polynomial over $\mathbb{Z}^{\mathrm{R}}$.

(20) Every $\mathbb{Q}$-valued polynomial over $\mathbb{C}_{\mathrm{F}}$ is a polynomial over $\mathbb{F}_{\mathbb{Q}}$.

(21) Every $\mathbb{R}$-valued polynomial over $\mathbb{C}_{\mathrm{F}}$ is a polynomial over $\mathbb{R}_{\mathrm{F}}$.

Let L be a non empty zero structure. Let us note that every polynomial over L which is non-zero is also non zero and every polynomial over L which is zero is also non non-zero.

Now we state the propositions:

(22) Let us consider an integer i, and a $\mathbb{Z}$-valued finite sequence f. If $i \in \operatorname{rng} f$, then $i \mid \prod f$.

PROOF: Define $\mathcal{P}$[finite sequence of elements of $\mathbb{Z}$] $\equiv$ for every integer a such that $a \in \operatorname{rng} \$_1$ holds $a \mid \prod \$_1$. For every finite sequence p of elements of $\mathbb{Z}$ and for every element n of $\mathbb{Z}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle n \rangle]$ by [3, (31)], [8, (96)], [14, (2)], [3, (39)]. For every finite sequence p of elements of $\mathbb{Z}$, $\mathcal{P}[p]$ from [6, Sch. 2]. $\square$

(23) there exists a non-zero, $\mathbb{Z}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f if and only if there exists a monic, $\mathbb{Q}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f.

PROOF: If there exists a non-zero, $\mathbb{Z}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f, then there exists a monic, $\mathbb{Q}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f by [18, (5)], [16, (6)], [19, (59)]. Reconsider $l = \operatorname{len} f$ as an element of $\mathbb{N}$. Define $\mathcal{F}$(element of $\mathbb{N}$) $= (\operatorname{den}(f(\$_1)))(\in \mathbb{C}_{\mathrm{F}})$. Consider d being a polynomial over $\mathbb{C}_{\mathrm{F}}$ such that $\operatorname{len} d \leqslant l$ and for every element n of $\mathbb{N}$ such that $n < l$ holds $d(n) = \mathcal{F}(n)$ from [17, Sch. 2]. Define $\mathcal{G}$(natural number) $= d(\$_1 -' 1)$. Consider d_2 being a finite sequence such that $\operatorname{len} d_2 = \operatorname{len} d$ and for every natural number k such that $k \in \operatorname{dom} d_2$ holds $d_2(k) = \mathcal{G}(k)$ from [3, Sch. 2]. $\operatorname{rng} d_2 \subseteq \mathbb{Z}$ by [22, (25)]. Reconsider $d_3 = d_2$ as a finite sequence of elements of $\mathbb{C}_{\mathrm{F}}$. Reconsider $d_1 = \prod d_2$ as an element of $\mathbb{C}_{\mathrm{F}}$. For every natural number i such that $i \in \operatorname{dom} d_3$ holds $d_3(i) \neq 0_{\mathbb{C}_{\mathrm{F}}}$ by [22, (25)]. Consider d_4 being a finite sequence of elements of $\mathbb{C}$ such that $d_4 = d_2$ and $\prod d_2 = \cdot_{\mathbb{C}} \circledast d_4$. $\operatorname{rng}(d_1 \cdot f) \subseteq \mathbb{Z}$ by [20, (8)], [2, (12), (13)], [22, (25)]. $\square$

(24) c is algebraic if and only if there exists a monic, $\mathbb{Q}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f. The theorem is a consequence of (7), (8), (14), and (20).

(25) c is algebraic if and only if there exists a non-zero, $\mathbb{Z}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f. The theorem is a consequence of (24) and (23).

(26) c is algebraic integer if and only if there exists a monic, $\mathbb{Z}$-valued polynomial f over $\mathbb{C}_{\mathrm{F}}$ such that c is a root of f. The theorem is a consequence of (7), (8), (14), and (19).

Let us observe that every complex which is algebraic integer is also algebraic and every complex which is transcendental is also non algebraic integer.

Now we state the proposition:

(27) Liouville's theorem on diophantine approximation:
Let us consider a non-zero, $\mathbb{Z}$-valued polynomial f over $\mathbb{R}_{\mathrm{F}}$, and an irrational element a of $\mathbb{R}_{\mathrm{F}}$. Suppose a is a root of f. Then there exists a positive real number A such that for every integer p for every positive natural number q, $|a - \frac{p}{q}| > \frac{A}{q^{\operatorname{len} f}}$.

Proof: Set $n = \operatorname{len} f$. Set $X = [a-1, a+1]$. Set $E = \operatorname{Eval}(f)$. Set $F = E`| \upharpoonright X$. Set $M_1 = \sup \operatorname{rng} |F|$. Set $M = M_1 + 1$. Consider Y being an object such that $Y \in \operatorname{rng} |F|$. Consider A being an object such that $A \in \operatorname{dom} |F|$ and $|F|(A) = Y$. Set $R_1 = \operatorname{Roots} f \setminus \{a\}$. Define $\mathcal{F}(\text{real number}) = |a - \$_1|$. Set $D = \{\mathcal{F}(b)$, where b is an element of $\mathbb{R}_{\mathrm{F}} : b \in R_1\}$. D is finite from [21, Sch. 21]. $D \subseteq \mathbb{R}$. Set $M_2 = \{1, \frac{1}{M}\} \cup D$. For every real number x such that $x \in M_2$ holds $x > 0$ by [9, (56)]. Consider A being a real number such that $0 < A$ and $A < \inf M_2$. Set $q_1 = q^n$. Reconsider $q_2 = q_1$ as an element of $\mathbb{R}_{\mathrm{F}}$. Reconsider $p_1 = \frac{p}{q}$ as an element of $\mathbb{R}_{\mathrm{F}}$. Consider E_1 being a finite sequence of elements of the carrier of $\mathbb{R}_{\mathrm{F}}$ such that $E(\frac{p}{q}) = \sum E_1$ and $\operatorname{len} E_1 = \operatorname{len} f$ and for every element n of $\mathbb{N}$ such that $n \in \operatorname{dom} E_1$ holds $E_1(n) = f(n -' 1) \cdot \operatorname{power}_{\mathbb{R}_{\mathrm{F}}}(p_1, n -' 1)$. Set $G = q_2 \cdot E_1$. $\operatorname{rng} G \subseteq \mathbb{Z}$ by [3, (1)], [2, (10)], [7, (3)], [24, (50)]. $\square$

Main Result: All Liouville numbers are transcendental.

Observe that every Liouville number is transcendental.

References

[1] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. 2nd edition, 1997.

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

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

[4] Sophie Bernard, Yves Bertot, Laurence Rideau, and Pierre-Yves Strub. Formal proofs of transcendence for e and π as an application of multivariate and symmetric polynomials. In Jeremy Avigad and Adam Chlipala, editors, *Proceedings of the 5th ACM SIGPLAN Conference on Certified Programs and Proofs*, pages 76–87. ACM, 2016. doi:10.1145/2854065.2854072.

[5] Jesse Bingham. Formalizing a proof that e is transcendental. *Journal of Formalized Reasoning*, 4:71–84, 2011.

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

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

[10] J.H. Conway and R.K. Guy. *The Book of Numbers*. 1996.
[11] Manuel Eberl. Liouville numbers. *Archive of Formal Proofs*, December 2015. `http://isa-afp.org/entries/Liouville_Numbers.shtml`, Formal proof development.
[12] Adam Grabowski and Artur Korniłowicz. Introduction to Liouville numbers. *Formalized Mathematics*, 25(**1**):39–48, 2017. doi:10.1515/forma-2017-0003.
[13] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.
[14] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[15] Joseph Liouville. Nouvelle démonstration d'un théorème sur les irrationnelles algébriques, inséré dans le Compte Rendu de la dernière séance. *Compte Rendu Acad. Sci. Paris*, Sér.A (18):910–911, 1844.
[16] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**): 265–269, 2001.
[17] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.
[18] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.
[19] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.
[20] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):97–104, 1991.
[21] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1 (**3**):495–500, 1990.
[22] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
[23] Yasushige Watase. Algebraic numbers. *Formalized Mathematics*, 24(**4**):291–299, 2016. doi:10.1515/forma-2016-0025.
[24] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.

Received February 23, 2017

FORMALIZED MATHEMATICS
Vol. 25, No. 1, Pages 55–62, 2017
DOI: 10.1515/forma-2017-0005

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

Group of Homography in Real Projective Plane

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

Summary. Using the Mizar system [2], we formalized that homographies of the projective real plane (as defined in [5]), form a group.

Then, we prove that, using the notations of Borsuk and Szmielew in [3]

> "Consider in space $\mathbb{RP}^2$ points P_1, P_2, P_3, P_4 of which three points are not collinear and points Q_1, Q_2, Q_3, Q_4 each three points of which are also not collinear. There exists one homography h of space $\mathbb{RP}^2$ such that $h(P_i) = Q_i$ for $i = 1, 2, 3, 4$."

(Existence Statement 52 and Existence Statement 53) [3]. Or, using notations of Richter [11]

> "Let $[a]$, $[b]$, $[c]$, $[d]$ in $\mathbb{RP}^2$ be four points of which no three are collinear and let $[a']$,$[b']$,$[c']$,$[d']$ in $\mathbb{RP}^2$ be another four points of which no three are collinear, then there exists a 3×3 matrix M such that $[Ma] = [a']$, $[Mb] = [b']$, $[Mc] = [c']$, and $[Md] = [d']$"

Makarios has formalized the same results in Isabelle/Isar (the collineations form a group, lemma statement52-existence and lemma statement 53-existence) and published it in Archive of Formal Proofs[1] [10], [9].

MSC: 51N15 03B35

Keywords: projectivity; projective transformation; real projective plane; group of homography

MML identifier: ANPROJ_9, version: 8.1.05 5.40.1289

[1]http://isa-afp.org/entries/Tarskis_Geometry.shtml

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

1. Preliminaries

From now on i, n denote natural numbers, r denotes a real number, r_1 denotes an element of $\mathbb{R}_{\rm F}$, a, b, c denote non zero elements of $\mathbb{R}_{\rm F}$, u, v denote elements of $\mathcal{E}^3_{\rm T}$, p_1 denotes a finite sequence of elements of $\mathbb{R}^1$, p_3, u_4 denote finite sequences of elements of $\mathbb{R}_{\rm F}$, N denotes a square matrix over $\mathbb{R}_{\rm F}$ of dimension 3, K denotes a field, and k denotes an element of K.

Now we state the propositions:

(1) $I^{3\times 3}_{\mathbb{R}_{\rm F}} = \langle\langle 1,0,0\rangle, \langle 0,1,0\rangle, \langle 0,0,1\rangle\rangle$.

(2) $r_1 \cdot N = r_1 \cdot I^{3\times 3}_{\mathbb{R}_{\rm F}} \cdot N$.

(3) If $r \neq 0$ and u is not zero, then $r \cdot u$ is not zero.

Proof: $r \cdot u \neq 0_{\mathcal{E}^3_{\rm T}}$ by [4, (52), (49)]. $\square$

Let us consider elements a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33} of $\mathbb{R}_{\rm F}$ and a square matrix A over $\mathbb{R}_{\rm F}$ of dimension 3. Now we state the propositions:

(4) Suppose $A = \langle\langle a_{11}, a_{12}, a_{13}\rangle, \langle a_{21}, a_{22}, a_{23}\rangle, \langle a_{31}, a_{32}, a_{33}\rangle\rangle$. Then

(i) $\mathrm{Line}(A, 1) = \langle a_{11}, a_{12}, a_{13}\rangle$, and

(ii) $\mathrm{Line}(A, 2) = \langle a_{21}, a_{22}, a_{23}\rangle$, and

(iii) $\mathrm{Line}(A, 3) = \langle a_{31}, a_{32}, a_{33}\rangle$.

(5) Suppose $A = \langle\langle a_{11}, a_{12}, a_{13}\rangle, \langle a_{21}, a_{22}, a_{23}\rangle, \langle a_{31}, a_{32}, a_{33}\rangle\rangle$. Then

(i) $A_{\square,1} = \langle a_{11}, a_{21}, a_{31}\rangle$, and

(ii) $A_{\square,2} = \langle a_{12}, a_{22}, a_{32}\rangle$, and

(iii) $A_{\square,3} = \langle a_{13}, a_{23}, a_{33}\rangle$.

The theorem is a consequence of (4).

Now we state the propositions:

(6) Let us consider elements a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33}, b_{11}, b_{12}, b_{13}, b_{21}, b_{22}, b_{23}, b_{31}, b_{32}, b_{33} of $\mathbb{R}_{\rm F}$, and square matrices A, B over $\mathbb{R}_{\rm F}$ of dimension 3. Suppose $A = \langle\langle a_{11}, a_{12}, a_{13}\rangle, \langle a_{21}, a_{22}, a_{23}\rangle, \langle a_{31}, a_{32}, a_{33}\rangle\rangle$ and $B = \langle\langle b_{11}, b_{12}, b_{13}\rangle, \langle b_{21}, b_{22}, b_{23}\rangle, \langle b_{31}, b_{32}, b_{33}\rangle\rangle$. Then $A \cdot B = \langle\langle a_{11} \cdot b_{11} + a_{12} \cdot b_{21} + a_{13} \cdot b_{31}, a_{11} \cdot b_{12} + a_{12} \cdot b_{22} + a_{13} \cdot b_{32}, a_{11} \cdot b_{13} + a_{12} \cdot b_{23} + a_{13} \cdot b_{33}\rangle, \langle a_{21} \cdot b_{11} + a_{22} \cdot b_{21} + a_{23} \cdot b_{31}, a_{21} \cdot b_{12} + a_{22} \cdot b_{22} + a_{23} \cdot b_{32}, a_{21} \cdot b_{13} + a_{22} \cdot b_{23} + a_{23} \cdot b_{33}\rangle, \langle a_{31} \cdot b_{11} + a_{32} \cdot b_{21} + a_{33} \cdot b_{31}, a_{31} \cdot b_{12} + a_{32} \cdot b_{22} + a_{33} \cdot b_{32}, a_{31} \cdot b_{13} + a_{32} \cdot b_{23} + a_{33} \cdot b_{33}\rangle\rangle$. The theorem is a consequence of (4) and (5).

(7) Let us consider elements a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33}, b_1, b_2, b_3 of $\mathbb{R}_{\rm F}$, a matrix A over $\mathbb{R}_{\rm F}$ of dimension 3×3, and a matrix B over $\mathbb{R}_{\rm F}$ of dimension 3×1. Suppose $A = \langle\langle a_{11}, a_{12}, a_{13}\rangle, \langle a_{21}, a_{22}, a_{23}\rangle, \langle a_{31}, a_{32}, a_{33}\rangle\rangle$ and $B = \langle\langle b_1\rangle, \langle b_2\rangle, \langle b_3\rangle\rangle$. Then $A \cdot B = \langle\langle a_{11} \cdot b_1 + a_{12} \cdot b_2 + a_{13} \cdot b_3\rangle,$

$\langle a_{21} \cdot b_1 + a_{22} \cdot b_2 + a_{23} \cdot b_3 \rangle, \langle a_{31} \cdot b_1 + a_{32} \cdot b_2 + a_{33} \cdot b_3 \rangle \rangle$. The theorem is a consequence of (4).

(8) Let us consider non zero elements a, b, c of $\mathbb{R}_{\rm F}$, and square matrices M_1, M_2 over $\mathbb{R}_{\rm F}$ of dimension 3. Suppose $M_1 = \langle \langle a, 0, 0 \rangle, \langle 0, b, 0 \rangle, \langle 0, 0, c \rangle \rangle$ and $M_2 = \langle \langle \frac{1}{a}, 0, 0 \rangle, \langle 0, \frac{1}{b}, 0 \rangle, \langle 0, 0, \frac{1}{c} \rangle \rangle$. Then

(i) $M_1 \cdot M_2 = I^{3 \times 3}_{\mathbb{R}_{\rm F}}$, and

(ii) $M_2 \cdot M_1 = I^{3 \times 3}_{\mathbb{R}_{\rm F}}$.

The theorem is a consequence of (1).

(9) Let us consider non zero elements a, b, c of $\mathbb{R}_{\rm F}$. Then $\langle \langle a, 0, 0 \rangle, \langle 0, b, 0 \rangle, \langle 0, 0, c \rangle \rangle$ is an invertible square matrix over $\mathbb{R}_{\rm F}$ of dimension 3. The theorem is a consequence of (8).

(10) (i) $[1, 0, 0]$ is not zero, and

(ii) $[0, 1, 0]$ is not zero, and

(iii) $[0, 0, 1]$ is not zero, and

(iv) $[1, 1, 1]$ is not zero.

(11) (i) $[1, 0, 0] \neq 0_{\mathcal{E}^3_{\rm T}}$, and

(ii) $[0, 1, 0] \neq 0_{\mathcal{E}^3_{\rm T}}$, and

(iii) $[0, 0, 1] \neq 0_{\mathcal{E}^3_{\rm T}}$, and

(iv) $[1, 1, 1] \neq 0_{\mathcal{E}^3_{\rm T}}$.

PROOF: $[1, 0, 0] \neq [0, 0, 0]$ by [7, (2)]. $[0, 1, 0] \neq [0, 0, 0]$ by [7, (2)]. $[0, 0, 1] \neq [0, 0, 0]$ by [7, (2)]. $[1, 1, 1] \neq [0, 0, 0]$ by [7, (2)]. □

(12) (i) $e_1 \neq 0_{\mathcal{E}^3_{\rm T}}$, and

(ii) $e_2 \neq 0_{\mathcal{E}^3_{\rm T}}$, and

(iii) $e_3 \neq 0_{\mathcal{E}^3_{\rm T}}$.

PROOF: $[1, 0, 0] \neq [0, 0, 0]$ by [7, (2)]. $[0, 1, 0] \neq [0, 0, 0]$ by [7, (2)]. $[0, 0, 1] \neq [0, 0, 0]$ by [7, (2)]. □

Let n be a natural number. Note that $I^{n \times n}_{\mathbb{R}_{\rm F}}$ is invertible.

Let M be an invertible square matrix over $\mathbb{R}_{\rm F}$ of dimension n. One can verify that $M^{\smile}$ is invertible.

Let K be a field and N_1, N_2 be invertible square matrices over K of dimension n. One can check that $N_1 \cdot N_2$ is invertible.

2. Group of Homography

From now on N, N_1, N_2 denote invertible square matrices over $\mathbb{R}_{\rm F}$ of dimension 3 and P, P_1, P_2, P_3 denote points of the projective space over $\mathcal{E}^3_{\rm T}$.

(13) (The homography of N_1)((the homography of N_2)(P)) = (the homography of $N_1 \cdot N_2$)(P).

Proof: Consider u_{12}, v_{12} being elements of $\mathcal{E}^3_{\rm T}$, u_8 being a finite sequence of elements of $\mathbb{R}_{\rm F}$, p_{12} being a finite sequence of elements of $\mathbb{R}^1$ such that $P =$ the direction of u_{12} and u_{12} is not zero and $u_{12} = u_8$ and $p_{12} = N_1 \cdot N_2 \cdot u_8$ and $v_{12} = \mathrm{M2F}(p_{12})$ and v_{12} is not zero and (the homography of $N_1 \cdot N_2$)(P) = the direction of v_{12}. Consider u_2, v_2 being elements of $\mathcal{E}^3_{\rm T}$, u_6 being a finite sequence of elements of $\mathbb{R}_{\rm F}$, p_2 being a finite sequence of elements of $\mathbb{R}^1$ such that $P =$ the direction of u_2 and u_2 is not zero and $u_2 = u_6$ and $p_2 = N_2 \cdot u_6$ and $v_2 = \mathrm{M2F}(p_2)$ and v_2 is not zero and (the homography of N_2)(P) = the direction of v_2. Consider u_1, v_1 being elements of $\mathcal{E}^3_{\rm T}$, u_7 being a finite sequence of elements of $\mathbb{R}_{\rm F}$, p_1 being a finite sequence of elements of $\mathbb{R}^1$ such that (the homography of N_2)(P) = the direction of u_1 and u_1 is not zero and $u_1 = u_7$ and $p_1 = N_1 \cdot u_7$ and $v_1 = \mathrm{M2F}(p_1)$ and v_1 is not zero and (the homography of N_1)((the homography of N_2)(P)) = the direction of v_1. Consider a being a real number such that $a \neq 0$ and $u_2 = a \cdot u_{12}$. Consider b being a real number such that $b \neq 0$ and $u_1 = b \cdot v_2$. $v_1 = \langle (N_1 \cdot \langle u_7 \rangle^{\rm T})_{1,1}, (N_1 \cdot \langle u_7 \rangle^{\rm T})_{2,1}, (N_1 \cdot \langle u_7 \rangle^{\rm T})_{3,1} \rangle$ by [1, (1), (40)]. $v_2 = \langle (N_2 \cdot \langle u_6 \rangle^{\rm T})_{1,1}, (N_2 \cdot \langle u_6 \rangle^{\rm T})_{2,1}, (N_2 \cdot \langle u_6 \rangle^{\rm T})_{3,1} \rangle$ by [1, (1), (40)]. $v_{12} = \langle (N_1 \cdot N_2 \cdot \langle u_8 \rangle^{\rm T})_{1,1}, (N_1 \cdot N_2 \cdot \langle u_8 \rangle^{\rm T})_{2,1}, (N_1 \cdot N_2 \cdot \langle u_8 \rangle^{\rm T})_{3,1} \rangle$ by [1, (1), (40)]. Reconsider $v_6 = v_2$ as a finite sequence of elements of $\mathbb{R}_{\rm F}$. Reconsider $i_4 = \frac{1}{b}$ as a real number. $v_6 = i_4 \cdot u_1$ by [4, (49), (52)]. Reconsider $l_{11} = \mathrm{Line}(N_2, 1)(1)$, $l_{12} = \mathrm{Line}(N_2, 1)(2)$, $l_{13} = \mathrm{Line}(N_2, 1)(3)$, $l_{21} = \mathrm{Line}(N_2, 2)(1)$, $l_{22} = \mathrm{Line}(N_2, 2)(2)$, $l_{23} = \mathrm{Line}(N_2, 2)(3)$, $l_{31} = \mathrm{Line}(N_2, 3)(1)$, $l_{32} = \mathrm{Line}(N_2, 3)(2)$, $l_{33} = \mathrm{Line}(N_2, 3)(3)$ as an element of $\mathbb{R}_{\rm F}$. $N_{2\square,1} = \langle l_{11}, l_{21}, l_{31} \rangle$ and $N_{2\square,2} = \langle l_{12}, l_{22}, l_{32} \rangle$ and $N_{2\square,3} = \langle l_{13}, l_{23}, l_{33} \rangle$ by [1, (1), (45)]. The direction of $v_1 =$ the direction of v_{12} by [5, (7)], [1, (45)], [5, (93)], [7, (8)]. $\square$

(14) (The homography of $I^{3 \times 3}_{\mathbb{R}_{\rm F}}$)($P$) = P.

(15) (i) (the homography of N)((the homography of $N^{\smile}$)(P)) = P, and

(ii) (the homography of $N^{\smile}$)((the homography of N)(P)) = P.

The theorem is a consequence of (13) and (14).

(16) If (the homography of N)(P_1) = (the homography of N)(P_2), then $P_1 = P_2$. The theorem is a consequence of (15).

(17) Let us consider a non zero element a of $\mathbb{R}_{\mathrm{F}}$. Suppose $a \cdot I^{3\times 3}_{\mathbb{R}_{\mathrm{F}}} = N$. Then (the homography of N)$(P) = P$.

The functor EnsHomography3 yielding a set is defined by the term

(Def. 1) the set of all the homography of N where N is an invertible square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3.

One can check that EnsHomography3 is non empty.

Let h_1, h_2 be elements of EnsHomography3. The functor $h_1 \circ h_2$ yielding an element of EnsHomography3 is defined by

(Def. 2) there exist invertible square matrices N_1, N_2 over $\mathbb{R}_{\mathrm{F}}$ of dimension 3 such that $h_1 =$ the homography of N_1 and $h_2 =$ the homography of N_2 and $it =$ the homography of $N_1 \cdot N_2$.

(18) Let us consider elements h_1, h_2 of EnsHomography3. Suppose $h_1 =$ the homography of N_1 and $h_2 =$ the homography of N_2. Then the homography of $N_1 \cdot N_2 = h_1 \circ h_2$. The theorem is a consequence of (13).

(19) Let us consider elements x, y, z of EnsHomography3. Then $(x \circ y) \circ z = x \circ (y \circ z)$. The theorem is a consequence of (18).

The functor BinOpHomography3 yielding a binary operation on EnsHomography3 is defined by

(Def. 3) for every elements h_1, h_2 of EnsHomography3, $it(h_1, h_2) = h_1 \circ h_2$.

The functor GroupHomography3 yielding a strict multiplicative magma is defined by the term

(Def. 4) $\langle$EnsHomography3, BinOpHomography3$\rangle$.

Note that GroupHomography3 is non empty, associative, and group-like.

(20) $\mathbf{1}_{\mathrm{GroupHomography3}} =$ the homography of $I^{3\times 3}_{\mathbb{R}_{\mathrm{F}}}$.

(21) Let us consider elements h, g of GroupHomography3, and invertible square matrices N, N_{10} over $\mathbb{R}_{\mathrm{F}}$ of dimension 3. Suppose $h =$ the homography of N and $g =$ the homography of N_{10} and $N_{10} = N^{\smile}$. Then $g = h^{-1}$. The theorem is a consequence of (20).

3. Main Results

The functors: Dir100, Dir010, Dir001, and Dir111 yielding points of the projective space over $\mathcal{E}^3_{\mathrm{T}}$ are defined by terms

(Def. 5) the direction of $[1, 0, 0]$,

(Def. 6) the direction of $[0, 1, 0]$,

(Def. 7) the direction of $[0, 0, 1]$,

(Def. 8) the direction of $[1, 1, 1]$,

respectively. Now we state the proposition:

(22) (i) Dir100 $\neq$ Dir010, and

(ii) Dir100 $\neq$ Dir001, and

(iii) Dir100 $\neq$ Dir111, and

(iv) Dir010 $\neq$ Dir001, and

(v) Dir010 $\neq$ Dir111, and

(vi) Dir001 $\neq$ Dir111.

Let a be a non zero element of $\mathbb{R}_{\mathrm{F}}$. Let us consider N. Note that $a \cdot N$ is invertible as a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3.

(23) Let us consider a non zero element a of $\mathbb{R}_{\mathrm{F}}$. Then (the homography of $a \cdot N_1)(P) =$ (the homography of $N_1)(P)$. The theorem is a consequence of (2), (13), and (17).

(24) Suppose P_1, P_2 and P_3 are not collinear. Then there exists an invertible square matrix N over $\mathbb{R}_{\mathrm{F}}$ of dimension 3 such that

(i) (the homography of $N)(P_1) =$ Dir100, and

(ii) (the homography of $N)(P_2) =$ Dir010, and

(iii) (the homography of $N)(P_3) =$ Dir001.

Proof: Consider u_1 being an element of $\mathcal{E}^3_{\mathrm{T}}$ such that u_1 is not zero and $P_1 =$ the direction of u_1. Consider u_2 being an element of $\mathcal{E}^3_{\mathrm{T}}$ such that u_2 is not zero and $P_2 =$ the direction of u_2. Consider u_3 being an element of $\mathcal{E}^3_{\mathrm{T}}$ such that u_3 is not zero and $P_3 =$ the direction of u_3. Reconsider $p_3 = u_1$, $q_1 = u_2$, $r_2 = u_3$ as a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$. Consider N being a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3 such that N is invertible and $N \cdot p_3 = \mathrm{F2M}(e_1)$ and $N \cdot q_1 = \mathrm{F2M}(e_2)$ and $N \cdot r_2 = \mathrm{F2M}(e_3)$. (The homography of $N)(P_1) =$ Dir100 by [8, (22), (1)], [6, (22)], [5, (75)]. (The homography of $N)(P_2) =$ Dir010 by [8, (22), (1)], [6, (22)], [5, (75)]. (The homography of $N)(P_3) =$ Dir001 by [8, (22), (1)], [6, (22)], [5, (75)]. $\square$

(25) Let us consider non zero elements a, b, c of $\mathbb{R}_{\mathrm{F}}$. Suppose $N = \langle\langle a, 0, 0\rangle, \langle 0, b, 0\rangle, \langle 0, 0, c\rangle\rangle$. Then

(i) (the homography of $N)(\mathrm{Dir100}) =$ Dir100, and

(ii) (the homography of $N)(\mathrm{Dir010}) =$ Dir010, and

(iii) (the homography of $N)(\mathrm{Dir001}) =$ Dir001.

Proof: (The homography of $N)(\mathrm{Dir100}) =$ Dir100 by (12), [8, (22), (1)], [7, (8), (2)]. (The homography of $N)(\mathrm{Dir010}) =$ Dir010 by (12), [8, (22), (1)], [7, (8), (2)]. (The homography of $N)(\mathrm{Dir001}) =$ Dir001 by (12), [8, (22), (1)], [7, (8), (2)]. $\square$

Let us consider a point P of the projective space over $\mathcal{E}^3_{\mathrm{T}}$. Now we state the propositions:

(26) There exist elements a, b, c of $\mathbb{R}_{\mathrm{F}}$ such that

(i) $P =$ the direction of $[a, b, c]$, and

(ii) $a \neq 0$ or $b \neq 0$ or $c \neq 0$.

(27) Suppose Dir100, Dir010 and P are not collinear and Dir100, Dir001 and P are not collinear and Dir010, Dir001 and P are not collinear. Then there exist non zero elements a, b, c of $\mathbb{R}_{\mathrm{F}}$ such that $P =$ the direction of $[a, b, c]$. The theorem is a consequence of (26).

(28) Let us consider non zero elements a, b, c, i_1, i_2, i_3 of $\mathbb{R}_{\mathrm{F}}$, a point P of the projective space over $\mathcal{E}^3_{\mathrm{T}}$, and an invertible square matrix N over $\mathbb{R}_{\mathrm{F}}$ of dimension 3. Suppose $P =$ the direction of $[a, b, c]$ and $i_1 = \frac{1}{a}$ and $i_2 = \frac{1}{b}$ and $i_3 = \frac{1}{c}$ and $N = \langle\langle i_1, 0, 0\rangle, \langle 0, i_2, 0\rangle, \langle 0, 0, i_3\rangle\rangle$. Then (the homography of $N)(P) =$ the direction of $[1, 1, 1]$.

PROOF: Consider u, v being elements of $\mathcal{E}^3_{\mathrm{T}}$, u_4 being a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$, p being a finite sequence of elements of $\mathbb{R}^1$ such that $P =$ the direction of u and u is not zero and $u = u_4$ and $p = N \cdot u_4$ and $v =$ M2F(p) and v is not zero and (the homography of $N)(P) =$ the direction of v. $[a, b, c]$ is not zero by [7, (4)], [1, (78)]. Consider d being a real number such that $d \neq 0$ and $u = d \cdot [a, b, c]$. Reconsider $z = 0$, $d_1 = d \cdot a$, $d_2 = d \cdot b$, $d_3 = d \cdot c$ as an element of $\mathbb{R}_{\mathrm{F}}$. $v = [i_1 \cdot d_1, i_2 \cdot d_2, i_3 \cdot d_3]$ by [1, (45)]. $\square$

(29) Let us consider a point P of the projective space over $\mathcal{E}^3_{\mathrm{T}}$. Suppose Dir100, Dir010 and P are not collinear and Dir100, Dir001 and P are not collinear and Dir010, Dir001 and P are not collinear. Then there exist non zero elements a, b, c of $\mathbb{R}_{\mathrm{F}}$ such that for every invertible square matrix N over $\mathbb{R}_{\mathrm{F}}$ of dimension 3 such that $N = \langle\langle a, 0, 0\rangle, \langle 0, b, 0\rangle, \langle 0, 0, c\rangle\rangle$ holds (the homography of $N)(P) =$ Dir111. The theorem is a consequence of (27) and (28).

(30) Let us consider points P_1, P_2, P_3, P_4 of the projective space over $\mathcal{E}^3_{\mathrm{T}}$. Suppose P_1, P_2 and P_3 are not collinear and P_1, P_2 and P_4 are not collinear and P_1, P_3 and P_4 are not collinear and P_2, P_3 and P_4 are not collinear. Then there exists an invertible square matrix N over $\mathbb{R}_{\mathrm{F}}$ of dimension 3 such that

(i) (the homography of $N)(P_1) =$ Dir100, and

(ii) (the homography of $N)(P_2) =$ Dir010, and

(iii) (the homography of $N)(P_3) =$ Dir001, and

(iv) (the homography of $N)(P_4) =$ Dir111.

The theorem is a consequence of (24), (29), (9), (25), and (13).

(31) Let us consider points P_1, P_2, P_3, P_4, Q_1, Q_2, Q_3, Q_4 of the projective space over $\mathcal{E}^3_{\mathrm{T}}$. Suppose P_1, P_2 and P_3 are not collinear and P_1, P_2 and P_4 are not collinear and P_1, P_3 and P_4 are not collinear and P_2, P_3 and P_4 are not collinear and Q_1, Q_2 and Q_3 are not collinear and Q_1, Q_2 and Q_4 are not collinear and Q_1, Q_3 and Q_4 are not collinear and Q_2, Q_3 and Q_4 are not collinear. Then there exists an invertible square matrix N over $\mathbb{R}_{\mathrm{F}}$ of dimension 3 such that

(i) (the homography of N)(P_1) $= Q_1$, and

(ii) (the homography of N)(P_2) $= Q_2$, and

(iii) (the homography of N)(P_3) $= Q_3$, and

(iv) (the homography of N)(P_4) $= Q_4$.

The theorem is a consequence of (30), (15), and (13).

References

[1] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 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] Karol Borsuk and Wanda Szmielew. *Foundations of Geometry.* North Holland, 1960.

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

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

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

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

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

[9] Timothy James McKenzie Makarios. The independence of Tarski's Euclidean Axiom. *Archive of Formal Proofs*, October 2012.

[10] Timothy James McKenzie Makarios. A mechanical verification of the independence of Tarski's Euclidean Axiom. Victoria University of Wellington, New Zealand, 2012. Master's thesis.

[11] Jürgen Richter-Gebert. *Perspectives on projective geometry: a guided tour through real and complex geometry.* Springer Science & Business Media, 2011.

Received March 17, 2017

FORMALIZED MATHEMATICS
Vol. 25, No. 1, Pages 63–72, 2017
DOI: 10.1515/forma-2017-0006

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

Ordered Rings and Fields

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. We introduce ordered rings and fields following Artin-Schreier's approach using positive cones. We show that such orderings coincide with total order relations and give examples of ordered (and non ordered) rings and fields. In particular we show that polynomial rings can be ordered in (at least) two different ways [8, 5, 4, 9]. This is the continuation of the development of algebraic hierarchy in Mizar [2, 3].

MSC: 12J15 03B35

Keywords: commutative algebra; ordered fields; positive cones

MML identifier: REALALG1, version: 8.1.05 5.40.1289

1. On Order Relations

Let X be a set and R be a binary relation on X. We say that R is strongly reflexive if and only if

(Def. 1) R is reflexive in X.

We say that R is totally connected if and only if

(Def. 2) R is strongly connected in X.

One can check that there exists a binary relation on X which is strongly reflexive and there exists a binary relation on X which is totally connected and every binary relation on X which is strongly reflexive is also reflexive and every binary relation on X which is totally connected is also strongly connected.

Let X be a non empty set. One can check that every binary relation on X which is strongly reflexive is also non empty and every binary relation on X which is totally connected is also non empty.

Now we state the propositions:

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

(1) Let us consider a non empty set X, a strongly reflexive binary relation R on X, and an element x of X. Then $x \leqslant_R x$.

(2) Let us consider a non empty set X, an antisymmetric binary relation R on X, and elements x, y of X. If $x \leqslant_R y$ and $y \leqslant_R x$, then $x = y$.

(3) Let us consider a non empty set X, a transitive binary relation R on X, and elements x, y, z of X. If $x \leqslant_R y$ and $y \leqslant_R z$, then $x \leqslant_R z$.

(4) Let us consider a non empty set X, a totally connected binary relation R on X, and elements x, y of X. Then

(i) $x \leqslant_R y$, or

(ii) $y \leqslant_R x$.

Let L be an additive loop structure and R be a binary relation on L. We say that R is respecting addition if and only if

(Def. 3) for every elements a, b, c of L such that $a \leqslant_R b$ holds $a + c \leqslant_R b + c$.

Let L be a multiplicative loop with zero structure. We say that R is respecting multipli
if and only if

(Def. 4) for every elements a, b, c of L such that $a \leqslant_R b$ and $0_L \leqslant_R c$ holds $a \cdot c \leqslant_R b \cdot c$.

2. On Minimal Non Zero Indices of Polynomials

Now we state the proposition:

(5) Let us consider a degenerated ring R, and a polynomial p over R. Then $\{i$, where i is a natural number : $p(i) \neq 0_R\} = \emptyset$.

Let us consider a ring R and a polynomial p over R. Now we state the propositions:

(6) $p = \mathbf{0}.\, R$ if and only if $\{i$, where i is a natural number : $p(i) \neq 0_R\} = \emptyset$.

(7) $\min^*\{i$, where i is a natural number : $(p+\mathbf{0}.\, R)(i) \neq 0_R\} = \min^*\{i$, where i is a natural number : $p(i) \neq 0_R\}$. The theorem is a consequence of (6).

Now we state the proposition:

(8) Let us consider a non degenerated ring R, and a polynomial p over R. Then $\min^*\{i$, where i is a natural number : $(-p)(i) \neq 0_R\} = \min^*\{i$, where i is a natural number : $p(i) \neq 0_R\}$.

Let us consider a non degenerated ring R and non zero polynomials p, q over R. Now we state the propositions:

(9) Suppose $\min^*\{i$, where i is a natural number : $p(i) \neq 0_R\} > \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}$. Then $\min^*\{i$, where i is a natural

number : $(p+q)(i) \neq 0_R\} = \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}$.

(10) Suppose $p+q \neq \mathbf{0}.\,R$ and $\min^*\{i$, where i is a natural number : $p(i) \neq 0_R\} = \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}$. Then $\min^*\{i$, where i is a natural number : $(p+q)(i) \neq 0_R\} \geqslant \min^*\{i$, where i is a natural number : $p(i) \neq 0_R\}$. The theorem is a consequence of (6).

(11) Suppose $p(\min^*\{i$, where i is a natural number : $p(i) \neq 0_R\})+q(\min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}) \neq 0_R$. Then $\min^*\{i$, where i is a natural number : $(p+q)(i) \neq 0_R\} = \min(\min^*\{i$, where i is a natural number : $p(i) \neq 0_R\}, \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\})$. The theorem is a consequence of (9), (6), and (10).

(12) Suppose $p * q \neq \mathbf{0}.\,R$. Then $\min^*\{i$, where i is a natural number : $(p * q)(i) \neq 0_R\} \geqslant \min^*\{i$, where i is a natural number : $p(i) \neq 0_R\}+\min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}$.

Now we state the proposition:

(13) Let us consider an integral domain R, and non zero polynomials p, q over R. Then $\min^*\{i$, where i is a natural number : $(p * q)(i) \neq 0_R\} = \min^*\{i$, where i is a natural number : $p(i) \neq 0_R\} + \min^*\{i$, where i is a natural number : $q(i) \neq 0_R\}$. The theorem is a consequence of (12).

3. Preliminaries

Let L be a non empty multiplicative loop structure and S be a subset of L. We say that S is closed under multiplication if and only if

(Def. 5) for every elements s_1, s_2 of L such that $s_1, s_2 \in S$ holds $s_1 \cdot s_2 \in S$.

Let L be a non empty additive loop structure. The functor $-S$ yielding a subset of L is defined by the term

(Def. 6) $\{-s$, where s is an element of $L : s \in S\}$.

Let L be an add-associative, right zeroed, right complementable, non empty additive loop structure. One can check that $--S$ reduces to S.

Now we state the proposition:

(14) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L, a subset S of L, and an element a of L. Then $a \in S$ if and only if $-a \in -S$.

Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L and subsets S_1, S_2 of L. Now we state the propositions:

(15) $-S_1 \cap S_2 = (-S_1) \cap (-S_2)$.

(16) $-(S_1 \cup S_2) = -S_1 \cup -S_2$.

Let L be a non empty additive loop structure and S be a subset of L. We say that S is negative-disjoint if and only if

(Def. 7) $S \cap (-S) = \{0_L\}$.

We say that S is spanning if and only if

(Def. 8) $S \cup -S =$ the carrier of L.

4. Squares and Sums of Squares

Let R be a ring and a be an element of R. We introduce the notation a is a square as a synonym of a is a square.

Let us note that 0_R is a square and 1_R is a square and there exists an element of R which is a square.

Let a be an element of R. We say that a is a sum of squares if and only if

(Def. 9) there exists a finite sequence f of elements of R such that $\sum f = a$ and for every natural number i such that $i \in \operatorname{dom} f$ there exists an element a of R such that $f(i) = a^{\mathbf{2}}$.

Let us note that every element of R which is a square is also a sum of squares.

Let R be a commutative ring and a, b be square elements of R. Observe that $a \cdot b$ is a square.

Let R be a ring and a, b be sum of squares elements of R. One can verify that $a + b$ is a sum of squares.

Let R be a commutative ring. Let us observe that $a \cdot b$ is a sum of squares.

Let R be a ring. The functors: $\mathrm{Squares}(R)$ and $\mathrm{QuadraticSums}(R)$ yielding subsets of R are defined by terms

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

(Def. 11) $\{a$, where a is an element of $R : a$ is a sum of squares$\}$,

respectively. We introduce the notation $\mathrm{SQ}(R)$ as a synonym of $\mathrm{Squares}(R)$ and $\mathrm{QS}(R)$ as a synonym of $\mathrm{QuadraticSums}(R)$.

One can check that $\mathrm{SQ}(R)$ is non empty and $\mathrm{QS}(R)$ is non empty.

Let S be a subset of R. We say that S has all squares if and only if

(Def. 12) $\mathrm{SQ}(R) \subseteq S$.

We say that S has all sums of squares if and only if

(Def. 13) $\mathrm{QS}(R) \subseteq S$.

One can check that there exists a subset of R which has all squares and there exists a subset of R which has all sums of squares and every subset of R which has all squares is also non empty and every subset of R which has all sums of squares is also non empty and every subset of R which has all sums of squares has also all squares and every subset of R which is closed under addition and has all squares has also all sums of squares and $\mathrm{SQ}(R)$ has all squares and $\mathrm{QS}(R)$ has all sums of squares.

Let us consider a ring R. Now we state the propositions:

(17) 0_R, $1_R \in \mathrm{SQ}(R)$.

(18) $\mathrm{SQ}(R) \subseteq \mathrm{QS}(R)$.

Let R be a ring. Note that $\mathrm{QS}(R)$ is closed under addition.

Let R be a commutative ring. Note that $\mathrm{QS}(R)$ is closed under multiplication.

Let us consider a ring R and a subring S of R. Now we state the propositions:

(19) $\mathrm{SQ}(S) \subseteq \mathrm{SQ}(R)$.

(20) $\mathrm{QS}(S) \subseteq \mathrm{QS}(R)$.

5. Positive Cones and Orderings

Let R be a ring and S be a subset of R. We say that S is a prepositive cone if and only if

(Def. 14) $S + S \subseteq S$ and $S \cdot S \subseteq S$ and $S \cap (-S) = \{0_R\}$ and $\mathrm{SQ}(R) \subseteq S$.

We say that S is a positive cone if and only if

(Def. 15) $S + S \subseteq S$ and $S \cdot S \subseteq S$ and $S \cap (-S) = \{0_R\}$ and $S \cup -S =$ the carrier of R.

One can check that every subset of R which is a prepositive cone is also non empty and every subset of R which is a positive cone is also non empty and every subset of R which is a prepositive cone is also closed under addition, closed under multiplication, and negative-disjoint and has also all squares and every subset of R which is closed under addition, closed under multiplication, and negative-disjoint and has all squares is also a prepositive cone and every subset of R which is a positive cone is also closed under addition, closed under multiplication, negative-disjoint, and spanning and every subset of R which is closed under addition, closed under multiplication, negative-disjoint, and spanning is also a positive cone and every subset of R which is a positive cone is also a prepositive cone.

Let us consider a field F and a subset S of F. Now we state the propositions:

(21) If $S \cdot S \subseteq S$ and $\mathrm{SQ}(F) \subseteq S$, then $S \cap (-S) = \{0_F\}$ iff $-1_F \notin S$.

(22) Suppose $S \cdot S \subseteq S$ and $S \cup -S =$ the carrier of F. Then $S \cap (-S) = \{0_F\}$ if and only if $-1_F \notin S$.

Proof: $\mathrm{SQ}(F) \subseteq S$ by [7, (10)]. $\square$

Let R be a ring. We say that R is preordered if and only if

(Def. 16) there exists a subset P of R such that P is a prepositive cone.

We say that R is ordered if and only if

(Def. 17) there exists a subset P of R such that P is a positive cone.

Let us note that there exists a field which is preordered and there exists a field which is ordered and every ring which is ordered is also preordered.

Let R be a preordered ring. One can verify that there exists a subset of R which is a prepositive cone.

Let R be an ordered ring. Let us note that there exists a subset of R which is a positive cone.

Let R be a preordered ring.

A preordering of R is prepositive cone subset of R. Let R be an ordered ring.

An ordering of R is positive cone subset of R. Now we state the proposition:

(23) Let us consider a preordered ring R, a preordering P of R, and an element a of R. Then $a^{\mathbf{2}} \in P$.

Let us consider a preordered ring R and a preordering P of R. Now we state the propositions:

(24) $\mathrm{QS}(R) \subseteq P$.

(25) 0_R, $1_R \in P$. The theorem is a consequence of (24).

Now we state the propositions:

(26) Let us consider a preordered, non degenerated ring R, and a preordering P of R. Then $-1_R \notin P$. The theorem is a consequence of (25).

(27) Let us consider a preordered field F, a preordering P of F, and a non zero element a of F. If $a \in P$, then $a^{-1} \in P$. The theorem is a consequence of (23).

(28) Let us consider a preordered, non degenerated ring R. Then $\mathrm{char}(R) = 0$. The theorem is a consequence of (25) and (24).

(29) Let us consider an ordered ring R, and orderings O, P of R. If $O \subseteq P$, then $O = P$. The theorem is a consequence of (25).

6. Orderings vs. Order Relations

Let R be a preordered ring, P be a preordering of R, and a, b be elements of R. We say that $a \leqslant_b P$ if and only if

(Def. 18) $b - a \in P$.

The functor $\mathrm{OrdRel}\, P$ yielding a binary relation on R is defined by the term

(Def. 19) $\{\langle a, b\rangle$, where a, b are elements of $R : a \leqslant_b P\}$.

One can verify that OrdRel P is non empty and OrdRel P is strongly reflexive, antisymmetric, and transitive and OrdRel P is respecting addition and respecting multiplication.

Let R be an ordered ring and O be an ordering of R. One can verify that OrdRel O is totally connected.

Let R be a preordered ring. Note that there exists a binary relation on R which is strongly reflexive, antisymmetric, transitive, respecting addition, and respecting multiplication.

Let R be an ordered ring. Note that there exists a binary relation on R which is strongly reflexive, antisymmetric, transitive, respecting addition, respecting multiplication, and totally connected.

Let R be a preordered ring.

An order relation of R is a strongly reflexive, antisymmetric, transitive, respecting addition, respecting multiplication binary relation on R. Let R be an ordered ring.

A total order relation of R is a strongly reflexive, antisymmetric, transitive, respecting addition, respecting multiplication, totally connected binary relation on R. Let R be a ring and Q be a binary relation on R. The functor Positives(Q) yielding a subset of R is defined by the term

(Def. 20) $\{a$, where a is an element of $R : 0_R \leqslant_Q a\}$.

Let R be a preordered ring and Q be a strongly reflexive binary relation on R. One can verify that Positives(Q) is non empty.

Let Q be an order relation of R. Observe that Positives(Q) is closed under addition, closed under multiplication, and negative-disjoint.

Let R be an ordered ring and Q be a total order relation of R. One can verify that Positives(Q) is spanning.

Now we state the propositions:

(30) Let us consider a preordered ring R, and a preordering P of R. Then OrdRel P is an order relation of R.

(31) Let us consider an ordered ring R, and an ordering P of R. Then OrdRel P is a total order relation of R.

(32) Let us consider an ordered ring R, and a total order relation Q of R. Then Positives(Q) is an ordering of R.

7. Some Ordered (and Non-ordered) Rings

Let R be a preordered ring. Observe that every subring of R is preordered.

Let R be an ordered ring. One can check that every subring of R is ordered.

Now we state the propositions:

(33) Let us consider a preordered ring R, a preordering P of R, and a subring S of R. Then $P \cap$ (the carrier of S) is a preordering of S.

(34) Let us consider an ordered ring R, an ordering O of R, and a subring S of R. Then $O \cap$ (the carrier of S) is an ordering of S.

Let us observe that $\mathbb{C}_{\mathrm{F}}$ is non preordered.

Let n be a non trivial natural number. Let us observe that $\mathbb{Z}/n$ is non preordered.

The functor $\boxed{\text{Positives}(\mathbb{R}_{\mathrm{F}})}$ yielding a subset of $\mathbb{R}_{\mathrm{F}}$ is defined by the term

(Def. 21) $\{r$, where r is an element of $\mathbb{R} : 0 \leqslant r\}$.

One can verify that Positives($\mathbb{R}_{\mathrm{F}}$) is closed under addition, closed under multiplication, negative-disjoint, and spanning and $\mathbb{R}_{\mathrm{F}}$ is ordered.

Now we state the propositions:

(35) Positives($\mathbb{R}_{\mathrm{F}}$) is an ordering of $\mathbb{R}_{\mathrm{F}}$.

(36) Let us consider an ordering O of $\mathbb{R}_{\mathrm{F}}$. Then $O =$ Positives($\mathbb{R}_{\mathrm{F}}$). The theorem is a consequence of (24) and (29).

The functor $\boxed{\text{Positives}(\mathbb{F}_{\mathbb{Q}})}$ yielding a subset of $\mathbb{F}_{\mathbb{Q}}$ is defined by the term

(Def. 22) $\{r$, where r is an element of $\mathbb{Q} : 0 \leqslant r\}$.

Observe that Positives($\mathbb{F}_{\mathbb{Q}}$) is closed under addition, closed under multiplication, negative-disjoint, and spanning and $\mathbb{F}_{\mathbb{Q}}$ is ordered.

Now we state the propositions:

(37) Positives($\mathbb{F}_{\mathbb{Q}}$) is an ordering of $\mathbb{F}_{\mathbb{Q}}$.

(38) Let us consider an ordering O of $\mathbb{F}_{\mathbb{Q}}$. Then $O =$ Positives($\mathbb{F}_{\mathbb{Q}}$).
PROOF: Define $\mathcal{P}$[natural number] $\equiv \$_1 \in O$. $1_{\mathbb{F}_{\mathbb{Q}}}, 0_{\mathbb{F}_{\mathbb{Q}}} \in O$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 2]. Positives($\mathbb{F}_{\mathbb{Q}}$) $\subseteq O$ by [6, (1)], (25), [10, (3)], (27). $\square$

The functor $\boxed{\text{Positives}(\mathbb{Z}^{\mathrm{R}})}$ yielding a subset of $\mathbb{Z}^{\mathrm{R}}$ is defined by the term

(Def. 23) $\{i$, where i is an element of $\mathbb{Z} : 0 \leqslant i\}$.

Note that Positives($\mathbb{Z}^{\mathrm{R}}$) is closed under addition, closed under multiplication, negative-disjoint, and spanning and $\mathbb{Z}^{\mathrm{R}}$ is ordered.

Now we state the propositions:

(39) Positives($\mathbb{Z}^{\mathrm{R}}$) is an ordering of $\mathbb{Z}^{\mathrm{R}}$.

(40) Let us consider an ordering O of $\mathbb{Z}^{\mathrm{R}}$. Then $O =$ Positives($\mathbb{Z}^{\mathrm{R}}$).
PROOF: Define $\mathcal{P}$[natural number] $\equiv \$_1 \in O$. $1_{\mathbb{Z}^{\mathrm{R}}}, 0_{\mathbb{Z}^{\mathrm{R}}} \in O$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$ from [1, Sch. 2]. $\square$

8. Ordered Polynomial Rings

Let R be a preordered ring and P be a preordering of R. The functor PositPoly(P) yielding a subset of PolyRing(R) is defined by the term

(Def. 24) $\{p$, where p is a polynomial over $R : \mathrm{LC}\, p \in P\}$.

Let R be a preordered, non degenerated ring. Note that PositPoly(P) is closed under addition and negative-disjoint.

Let R be a preordered integral domain. Let us observe that PositPoly(P) is closed under multiplication and has all sums of squares.

Let R be an ordered ring and O be an ordering of R. Let us observe that PositPoly(O) is spanning.

Let R be a preordered integral domain. One can verify that PolyRing(R) is preordered.

Let R be an ordered integral domain. Note that PolyRing(R) is ordered.

Now we state the propositions:

(41) Let us consider a preordered integral domain R, and a preordering P of R. Then PositPoly(P) is a preordering of PolyRing(R).

(42) Let us consider an ordered integral domain R, and an ordering O of R. Then PositPoly(O) is an ordering of PolyRing(R).

Let R be a preordered ring and P be a preordering of R. The functor LowPositPoly(P) yielding a subset of PolyRing(R) is defined by the term

(Def. 25) $\{p$, where p is a polynomial over $R : p(\min^*\{i$, where i is a natural number $: p(i) \neq 0_R\}) \in P\}$.

Let R be a preordered, non degenerated ring. Observe that LowPositPoly(P) is closed under addition and negative-disjoint.

Let R be a preordered integral domain. One can verify that LowPositPoly(P) is closed under multiplication and has all sums of squares.

Let R be an ordered, non degenerated ring and O be an ordering of R. One can check that LowPositPoly(O) is spanning.

Now we state the propositions:

(43) Let us consider a preordered integral domain R, and a preordering P of R. Then LowPositPoly(P) is a preordering of PolyRing(R).

(44) Let us consider an ordered integral domain R, and an ordering O of R. Then LowPositPoly(O) is an ordering of PolyRing(R).

(45) Let us consider a preordered, non degenerated ring R, and a preordering P of R. Then PositPoly(P) $\neq$ LowPositPoly(P). The theorem is a consequence of (25) and (26).

References

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

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

[3] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. On algebraic hierarchies in mathematical repository of Mizar. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371, 2016. doi:10.15439/2016F520.

[4] Nathan Jacobson. *Lecture Notes in Abstract Algebra, III. Theory of Fields and Galois Theory*. Springer-Verlag, 1964.

[5] Manfred Knebusch and Claus Scheiderer. *Einführung in die reelle Algebra*. Vieweg-Verlag, 1989.

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

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

[8] Alexander Prestel. *Lectures on Formally Real Fields*. Springer-Verlag, 1984.

[9] Knut Radbruch. *Geordnete Körper*. Lecture Notes, University of Kaiserslautern, Germany, 1991.

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

Received March 17, 2017

FORMALIZED MATHEMATICS
Vol. 25, No. 1, Pages 73–86, 2017
DOI: 10.1515/forma-2017-0007

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

Embedded Lattice and Properties of Gram Matrix[1]

Yuichi Futa
Tokyo University of Technology
Tokyo, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize in Mizar [14] the definition of embedding of lattice and its properties. We formally define an inner product on an embedded module. We also formalize properties of Gram matrix. We formally prove that an inverse of Gram matrix for a rational lattice exists. Lattice of $\mathbb{Z}$-module is necessary for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm [16] and cryptographic systems with lattice [17].

MSC: 15A09 15A63 03B35

Keywords: $\mathbb{Z}$-lattice; Gram matrix; rational $\mathbb{Z}$-lattice

MML identifier: `ZMODLAT2`, version: `8.1.05 5.40.1289`

1. Inner Product of Embedded Module

Now we state the propositions:

(1) Let us consider a ring K, a left module V over K, a function L from the carrier of V into the carrier of K, a subset A of V, and finite sequences F, F_1 of elements of the carrier of V. Suppose F is one-to-one and $\operatorname{rng} F = A$ and F_1 is one-to-one and $\operatorname{rng} F_1 = A$. Then $\sum(L \cdot F) = \sum(L \cdot F_1)$.
Proof: Define $\mathcal{G}[\text{object}, \text{object}] \equiv \{\$_2\} = F^{-1}(\{F_1(\$_1)\})$. For every object x such that $x \in \operatorname{dom} F$ there exists an object y such that $y \in \operatorname{dom} F$ and $\mathcal{G}[x, y]$ by [6, (74)]. Consider f being a function from $\operatorname{dom} F$ into $\operatorname{dom} F$ such that for every object x such that $x \in \operatorname{dom} F$ holds $\mathcal{G}[x, f(x)]$ from [7, Sch. 1]. $\operatorname{rng} f = \operatorname{dom} F$ by [6, (59), (82)], [8, (18)]. f is one-to-one by [8, (31)], [6, (91)], [8, (3)]. $\square$

[1] This work was supported by JSPS KAKENHI Grant Number JP15K00183.

(2) Let us consider a ring K, a left module V over K, and a finite subset A of V. Then A is linearly independent if and only if for every linear combination L of A such that there exists a finite sequence F of elements of the carrier of V such that F is one-to-one and $\operatorname{rng} F = A$ and $\sum(L\cdot F) = 0_V$ holds the support of $L = \emptyset$.
PROOF: For every linear combination L of A such that $\sum L = 0_V$ holds the support of $L = \emptyset$ by [22, (13)], [26, (13)], [24, (41)]. □

(3) Let us consider a ring K, a left module V over K, and a finite sequence b of elements of V. Suppose b is one-to-one. Then $\operatorname{rng} b$ is linearly independent if and only if for every finite sequence r of elements of K and for every finite sequence r_1 of elements of V such that $\operatorname{len} r = \operatorname{len} b$ and $\operatorname{len} r_1 = \operatorname{len} b$ and for every natural number i such that $i \in \operatorname{dom} r_1$ holds $r_1(i) = r_i \cdot b_i$ and $\sum r_1 = 0_V$ holds $r = \operatorname{Seg} \operatorname{len} r \longmapsto 0_K$.
PROOF: For every linear combination L of $\operatorname{rng} b$ such that there exists a finite sequence F of elements of the carrier of V such that F is one-to-one and $\operatorname{rng} F = \operatorname{rng} b$ and $\sum(L \cdot F) = 0_V$ holds the support of $L = \emptyset$ by [29, (27)], [23, (29)], [6, (13)], (1). □

(4) Let us consider a ring K, a left module V over K, and a finite subset A of V. Then A is linearly independent if and only if there exists a finite sequence b of elements of V such that b is one-to-one and $\operatorname{rng} b = A$ and for every finite sequence r of elements of K and for every finite sequence r_1 of elements of V such that $\operatorname{len} r = \operatorname{len} b$ and $\operatorname{len} r_1 = \operatorname{len} b$ and for every natural number i such that $i \in \operatorname{dom} r_1$ holds $r_1(i) = r_i \cdot b_i$ and $\sum r_1 = 0_V$ holds $r = \operatorname{Seg} \operatorname{len} r \longmapsto 0_K$. The theorem is a consequence of (3).

Let V be a non trivial, free $\mathbb{Z}$-module. Let us note that every basis of V is non empty.

Let I_1 be a $\mathbb{Z}$-lattice. We say that I_1 is rational if and only if

(Def. 1) for every vectors v, u of I_1, $\langle v, u\rangle \in \mathbb{Q}$.

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

Let L be a rational $\mathbb{Z}$-lattice and v, u be vectors of L. Note that $\langle v,\ u\rangle$is rational and every integral $\mathbb{Z}$-lattice is rational.

Let L be a $\mathbb{Z}$-lattice. The functor ScProductEM(L) yielding a function from (the carrier of Embedding(L)) $\times$ (the carrier of Embedding(L)) into the carrier of $\mathbb{R}_\mathrm{F}$ is defined by

(Def. 2) for every vectors v, u of L and for every vectors v_1, u_1 of Embedding(L) such that $v_1 = (\mathrm{MorphsZQ}(L))(v)$ and $u_1 = (\mathrm{MorphsZQ}(L))(u)$ holds $it(v_1, u_1) = \langle v, u\rangle$.

Now we state the proposition:

(5) Let us consider a $\mathbb{Z}$-lattice L. Then

(i) for every vector x of Embedding(L) such that for every vector y of Embedding(L), (ScProductEM(L))(x, y) $= 0$ holds $x = 0_{\mathrm{Embedding}(L)}$, and

(ii) for every vectors x, y of Embedding(L), (ScProductEM(L))(x, y) $=$ (ScProductEM(L))(y, x), and

(iii) for every vectors x, y, z of Embedding(L) and for every element a of $\mathbb{Z}^{\mathrm{R}}$, (ScProductEM(L))($x + y, z$) $=$ (ScProductEM(L))(x, z) $+$ (ScProductEM(L))(y, z) and (ScProductEM(L))($a \cdot x, y$) $= a \cdot$(ScProductEM(L

PROOF: Set $Z =$ Embedding(L). Set $f =$ ScProductEM(L). For every vector x of Z such that for every vector y of Z, $f(x, y) = 0$ holds $x = 0_{\mathrm{Embedding}(L)}$ by [10, (22)], [7, (4)]. For every vectors x, y of Z, $f(x, y) = f(y, x)$ by [10, (22)]. For every vectors x, y, z of Z and for every element a of $\mathbb{Z}^{\mathrm{R}}$, $f(x + y, z) = f(x, z) + f(y, z)$ and $f(a \cdot x, y) = a \cdot f(x, y)$ by [10, (22), (19)]. $\square$

Let L be a $\mathbb{Z}$-lattice. The functor ScProductDM(L) yielding a function from (the carrier of DivisibleMod(L)) $\times$ (the carrier of DivisibleMod(L)) into the carrier of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 3) for every vectors v_1, u_1 of DivisibleMod(L) and for every vectors v, u of Embedding(L) and for every elements a, b of $\mathbb{Z}^{\mathrm{R}}$ and for every elements a_1, b_1 of $\mathbb{R}_{\mathrm{F}}$ such that $a = a_1$ and $b = b_1$ and $a_1 \neq 0$ and $b_1 \neq 0$ and $v = a \cdot v_1$ and $u = b \cdot u_1$ holds $it(v_1, u_1) = {a_1}^{-1} \cdot {b_1}^{-1} \cdot$ (ScProductEM(L))(v, u).

Let us consider a $\mathbb{Z}$-lattice L. Now we state the propositions:

(6) (i) for every vector x of DivisibleMod(L) such that for every vector y of DivisibleMod(L), (ScProductDM(L))(x, y) $= 0$ holds $x = 0_{\mathrm{DivisibleMod}(L)}$, and

(ii) for every vectors x, y of DivisibleMod(L), (ScProductDM(L))(x, y) $=$ (ScProductDM(L))(y, x), and

(iii) for every vectors x, y, z of DivisibleMod(L) and for every element a of $\mathbb{Z}^{\mathrm{R}}$, (ScProductDM(L))($x + y, z$) $=$ (ScProductDM(L))(x, z) $+$ (ScProductDM(L))(y, z) and (ScProductDM(L))($a \cdot x, y$) $= a \cdot$(ScProductDM(L

PROOF: Set $D =$ DivisibleMod(L). Set $f =$ ScProductDM(L). For every vector x of D such that for every vector y of D, $f(x, y) = 0$ holds $x = 0_D$ by [10, (29)], [11, (24)], [15, (25)], (5). For every vectors x, y of D, $f(x, y) = f(y, x)$ by [10, (29)], (5). For every vectors x, y, z of D and for every element i of $\mathbb{Z}^{\mathrm{R}}$, $f(x + y, z) = f(x, z) + f(y, z)$ and $f(i \cdot x, y) = i \cdot f(x, y)$ by [10, (29)], [11, (29), (28)], [18, (11)]. $\square$

(7) $\mathrm{ScProductEM}(L) = \mathrm{ScProductDM}(L) \restriction \mathrm{rng}\,\mathrm{MorphsZQ}(L)$.
PROOF: Reconsider $s = \mathrm{ScProductDM}(L) \restriction \mathrm{rng}\,\mathrm{MorphsZQ}(L)$ as a function from $\mathrm{rng}\,\mathrm{MorphsZQ}(L) \times \mathrm{rng}\,\mathrm{MorphsZQ}(L)$ into the carrier of $\mathbb{R}_{\mathrm{F}}$. For every object x such that $x \in \mathrm{rng}\,\mathrm{MorphsZQ}(L) \times \mathrm{rng}\,\mathrm{MorphsZQ}(L)$ holds $(\mathrm{ScProductEM}(L))(x) = s(x)$ by [11, (24)], [6, (49)], [8, (87)]. □

Now we state the propositions:

(8) Let us consider a $\mathbb{Z}$-lattice L, vectors v_1, v_2 of $\mathrm{DivisibleMod}(L)$, and vectors u_1, u_2 of $\mathrm{Embedding}(L)$. Suppose $v_1 = u_1$ and $v_2 = u_2$. Then $(\mathrm{ScProductEM}(L))(u_1, u_2) = (\mathrm{ScProductDM}(L))(v_1, v_2)$.

(9) Let us consider a $\mathbb{Z}$-lattice L, an element r of $\mathbb{F}_{\mathbb{Q}}$, and vectors v, u of $\mathrm{Embedding}(r, L)$. Then $(\mathrm{ScProductDM}(L) \restriction (\text{the carrier of } \mathrm{Embedding}(r, L)))(v, u)$ $(\mathrm{ScProductDM}(L))(v, u)$.

(10) Let us consider a $\mathbb{Z}$-lattice L, a non empty set A, an element z of A, a binary operation a_1 on A, a function m_1 from (the carrier of $\mathbb{Z}^{\mathrm{R}}$) $\times A$ into A, and a function s_1 from $A \times A$ into the carrier of $\mathbb{R}_{\mathrm{F}}$. Suppose A is a linearly closed subset of $\mathrm{DivisibleMod}(L)$ and $z = 0_{\mathrm{DivisibleMod}(L)}$ and $a_1 =$ (the addition of $\mathrm{DivisibleMod}(L)) \restriction A$ and $m_1 =$ (the left multiplication of $\mathrm{DivisibleMod}(L)) \restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}) \times A$). Then $\langle A, a_1, z, m_1, s_1 \rangle$ is a submodule of $\mathrm{DivisibleMod}(L)$.

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

(i) $(\mathrm{ScProductDM}(L))(-v, u) = -(\mathrm{ScProductDM}(L))(v, u)$, and

(ii) $(\mathrm{ScProductDM}(L))(u, -v) = -(\mathrm{ScProductDM}(L))(u, v)$.

The theorem is a consequence of (6).

(12) Let us consider a $\mathbb{Z}$-lattice L, and vectors v, u, w of $\mathrm{DivisibleMod}(L)$. Then $(\mathrm{ScProductDM}(L))(v, u+w) = (\mathrm{ScProductDM}(L))(v, u) + (\mathrm{ScProductDM}(L))($
The theorem is a consequence of (6).

(13) Let us consider a $\mathbb{Z}$-lattice L, vectors v, u of $\mathrm{DivisibleMod}(L)$, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Then $(\mathrm{ScProductDM}(L))(v, a \cdot u) = a \cdot (\mathrm{ScProductDM}(L))(v, u)$. The theorem is a consequence of (6).

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

(i) $(\mathrm{ScProductDM}(L))(0_{\mathrm{DivisibleMod}(L)}, v) = 0$, and

(ii) $(\mathrm{ScProductDM}(L))(v, 0_{\mathrm{DivisibleMod}(L)}) = 0$.

The theorem is a consequence of (6) and (11).

(15) Let us consider a $\mathbb{Z}$-lattice L, a vector v of $\mathrm{DivisibleMod}(L)$, and a basis I of $\mathrm{Embedding}(L)$. Suppose for every vector u of $\mathrm{DivisibleMod}(L)$ such that $u \in I$ holds $(\mathrm{ScProductDM}(L))(v, u) = 0$. Let us consider a vector u of $\mathrm{DivisibleMod}(L)$. Then $(\mathrm{ScProductDM}(L))(v, u) = 0$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset I of Embedding(L) such that $\overline{\overline{I}} = \$_1$ and I is linearly independent and for every vector u of DivisibleMod(L) such that $u \in I$ holds (ScProductDM(L))$(v, u) = 0$ for every vector w of DivisibleMod(L) such that $w \in \mathrm{Lin}(I)$ holds (ScProductDM(L))$(v, w) = 0$. $\mathcal{P}[0]$ by [12, (67), (66)], (14). For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [28, (41)], [2, (44)], [1, (30)], [8, (31)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. For every vector w of DivisibleMod(L), (ScProductDM(L))$(v, w) = 0$ by [10, (29)], (6). □

(16) Let us consider a $\mathbb{Z}$-lattice L, a vector v of DivisibleMod(L), and a basis I of Embedding(L). Suppose for every vector u of DivisibleMod(L) such that $u \in I$ holds (ScProductDM(L))$(v, u) = 0$. Then $v = 0_{\mathrm{DivisibleMod}(L)}$. The theorem is a consequence of (15) and (6).

(17) Let us consider a ring R, a left module V over R, a vector v of V, and an object u. Suppose $u \in \mathrm{Lin}(\{v\})$. Then there exists an element i of R such that $u = i \cdot v$.

(18) Let us consider a ring R, a left module V over R, and a vector v of V. Then $v \in \mathrm{Lin}(\{v\})$.

(19) Let us consider a ring R, a left module V over R, a vector v of V, and an element i of R. Then $i \cdot v \in \mathrm{Lin}(\{v\})$.

2. Embedding of Lattice

Let L be a $\mathbb{Z}$-lattice. The functor $\boxed{\mathrm{EMLat}(L)}$ yielding a strict $\mathbb{Z}$-lattice is defined by

(Def. 4) the carrier of *it* = rng MorphsZQ(L) and the zero of *it* = zeroCoset(L) and the addition of *it* = addCoset(L) $\restriction$ rng MorphsZQ(L) and the left multiplication of *it* = lmultCoset(L)$\restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}$)$\times$rng MorphsZQ(L)) and the scalar product of *it* = ScProductEM(L).

Let r be an element of $\mathbb{F}_{\mathbb{Q}}$. The functor $\boxed{\mathrm{EMLat}(r, L)}$ yielding a strict $\mathbb{Z}$-lattice is defined by

(Def. 5) the carrier of *it* = $r\cdot$rng MorphsZQ(L) and the zero of *it* = zeroCoset(L) and the addition of *it* = addCoset(L) $\restriction$ ($r\cdot$rng MorphsZQ(L)) and the left multiplication of *it* = lmultCoset(L)$\restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}$)$\times$($r\cdot$rng MorphsZQ(L))) and the scalar product of *it* = ScProductDM(L) $\restriction$ ($r \cdot$ rng MorphsZQ(L)).

Let L be a non trivial $\mathbb{Z}$-lattice. One can verify that EMLat(L) is non trivial.

Let r be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. One can verify that EMLat(r, L) is non trivial.

Let L be an integral $\mathbb{Z}$-lattice. Observe that $\mathrm{EMLat}(L)$ is integral.

Now we state the propositions:

(20) Let us consider a $\mathbb{Z}$-lattice L. Then $\mathrm{EMLat}(L)$ is a submodule of $\mathrm{DivisibleMod}(L)$.

(21) Let us consider a $\mathbb{Z}$-lattice L, and an element r of $\mathbb{F}_{\mathbb{Q}}$. Then $\mathrm{EMLat}(r, L)$ is a submodule of $\mathrm{DivisibleMod}(L)$.

(22) Let us consider a $\mathbb{Z}$-lattice L, a non zero element r of $\mathbb{F}_{\mathbb{Q}}$, elements m, n of $\mathbb{Z}^{\mathrm{R}}$, elements m, n_1 of $\mathbb{Z}$, and a vector v of $\mathrm{EMLat}(r, L)$. Suppose $m = m$ and $n = n_1$ and $r = \frac{m}{n_1}$ and $n_1 \neq 0$. Then there exists a vector x of $\mathrm{EMLat}(L)$ such that $n \cdot v = m \cdot x$. The theorem is a consequence of (20) and (21).

(23) Let us consider a $\mathbb{Z}$-lattice L, an element r of $\mathbb{F}_{\mathbb{Q}}$, vectors v, u of $\mathrm{EMLat}(r, L)$, and vectors x, y of $\mathrm{EMLat}(L)$. If $v = x$ and $u = y$, then $\langle v, u\rangle = \langle x, y\rangle$. The theorem is a consequence of (9) and (7).

(24) Let us consider an integral $\mathbb{Z}$-lattice L, a non zero element r of $\mathbb{F}_{\mathbb{Q}}$, a rational number a, and vectors v, u of $\mathrm{EMLat}(r, L)$. Suppose $r = a$. Then $a^{-1} \cdot a^{-1} \cdot \langle v, u\rangle \in \mathbb{Z}$. The theorem is a consequence of (22) and (23).

Let L be a positive definite $\mathbb{Z}$-lattice. One can verify that $\mathrm{EMLat}(L)$ is positive definite.

Let r be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. Let us observe that $\mathrm{EMLat}(r, L)$ is positive definite.

Now we state the proposition:

(25) Let us consider a positive definite $\mathbb{Z}$-lattice L, and a vector v of $\mathrm{DivisibleMod}(L)$. Then $(\mathrm{ScProductDM}(L))(v, v) = 0$ if and only if $v = 0_{\mathrm{DivisibleMod}(L)}$. The theorem is a consequence of (6) and (7).

Let us consider a positive definite $\mathbb{Z}$-lattice L and a non empty structure of $\mathbb{Z}$-lattice Z over $\mathbb{Z}^{\mathrm{R}}$. Now we state the propositions:

(26) Suppose Z is a submodule of $\mathrm{DivisibleMod}(L)$ and the scalar product of $Z = \mathrm{ScProductDM}(L) \restriction$ (the carrier of Z). Then Z is $\mathbb{Z}$-lattice-like.

PROOF: For every vectors x, y of Z, (the scalar product of $Z)(x, y) = (\mathrm{ScProductDM}(L))(x, y)$ by [6, (49)]. Z is $\mathbb{Z}$-lattice-like by [11, (25), (26)], (25), (6). $\square$

(27) Suppose Z is a finitely generated submodule of $\mathrm{DivisibleMod}(L)$ and the scalar product of $Z = \mathrm{ScProductDM}(L) \restriction$ (the carrier of Z). Then Z is a $\mathbb{Z}$-lattice.

Now we state the propositions:

(28) Let us consider a $\mathbb{Z}$-lattice L. Then the vector space structure of $\mathrm{EMLat}(L) = \mathrm{Embedding}(L)$.

(29) Let us consider $\mathbb{Z}$-modules L, E. Suppose the vector space structure of $L =$ the vector space structure of E. Then L is a submodule of E.

(30) Let us consider $\mathbb{Z}$-modules E, L, a subset I of L, a subset J of E, and a linear combination K of J. Suppose $I = J$ and the vector space structure of $L =$ the vector space structure of E. Then K is a linear combination of I.

Let us consider $\mathbb{Z}$-modules E, L, a linear combination K of E, and a linear combination H of L. Now we state the propositions:

(31) Suppose $K = H$ and the vector space structure of $L =$ the vector space structure of E. Then the support of $K =$ the support of H.

(32) Suppose $K = H$ and the vector space structure of $L =$ the vector space structure of E. Then $\sum K = \sum H$. The theorem is a consequence of (29).

Let us consider $\mathbb{Z}$-modules L, E, a subset I of L, and a subset J of E. Now we state the propositions:

(33) Suppose the vector space structure of $L =$ the vector space structure of E and $I = J$. Then I is linearly independent if and only if J is linearly independent. The theorem is a consequence of (30) and (32).

(34) Suppose the vector space structure of $L =$ the vector space structure of E and $I = J$. Then $\mathrm{Lin}(I) = \mathrm{Lin}(J)$. The theorem is a consequence of (29).

Now we state the propositions:

(35) Let us consider free $\mathbb{Z}$-modules L, E, a subset I of L, and a subset J of E. Suppose the vector space structure of $L =$ the vector space structure of E and $I = J$. Then I is a basis of L if and only if J is a basis of E. The theorem is a consequence of (33) and (34).

(36) Let us consider finite rank, free $\mathbb{Z}$-modules L, E. Suppose the vector space structure of $L =$ the vector space structure of E. Then $\operatorname{rank} L = \operatorname{rank} E$. The theorem is a consequence of (35).

Let us consider a $\mathbb{Z}$-lattice L and a subset I of L. Now we state the propositions:

(37) I is a basis of L if and only if $(\mathrm{MorphsZQ}(L))^{\circ}I$ is a basis of $\mathrm{Embedding}(L)$.

(38) I is a basis of L if and only if $(\mathrm{MorphsZQ}(L))^{\circ}I$ is a basis of $\mathrm{EMLat}(L)$. The theorem is a consequence of (37), (28), and (35).

Now we state the propositions:

(39) Let us consider a $\mathbb{Z}$-lattice L, and a finite sequence b of elements of L. Then b is an ordered basis of L if and only if $\mathrm{MorphsZQ}(L) \cdot b$ is an ordered basis of $\mathrm{Embedding}(L)$. The theorem is a consequence of (37).

(40) Let us consider a $\mathbb{Z}$-lattice L, a finite rank, free $\mathbb{Z}$-module E, a finite sequence I of elements of L, and a finite sequence J of elements of E. Suppose the vector space structure of $L =$ the vector space structure of E and $I = J$. Then I is an ordered basis of L if and only if J is an ordered basis of E. The theorem is a consequence of (35).

(41) Let us consider a $\mathbb{Z}$-lattice L, and a finite sequence b of elements of L. Then b is an ordered basis of L if and only if $\mathrm{MorphsZQ}(L) \cdot b$ is an ordered basis of $\mathrm{EMLat}(L)$. The theorem is a consequence of (39), (28), and (40).

(42) Let us consider a $\mathbb{Z}$-lattice L. Then $\mathrm{rank}\, L = \mathrm{rank}\, \mathrm{EMLat}(L)$. The theorem is a consequence of (28) and (36).

(43) Let us consider a $\mathbb{Z}$-lattice L, and an object x. Then x is a vector of $\mathrm{EMLat}(L)$ if and only if x is a vector of $\mathrm{Embedding}(L)$. The theorem is a consequence of (28).

Let L be a rational $\mathbb{Z}$-lattice and v, u be vectors of $\mathrm{EMLat}(L)$. One can check that $(\mathrm{ScProductEM}(L))(v, u)$ is rational.

Let v, u be vectors of $\mathrm{DivisibleMod}(L)$. One can verify that $(\mathrm{ScProductDM}(L))(v, u)$ is rational.

3. Properties of Gram Matrix

Let V be a vector space structure over $\mathbb{Z}^{\mathrm{R}}$ and f be an $\mathbb{R}$-form of V and V. We say that f is symmetric if and only if

(Def. 6) for every vectors v, w of V, $f(v, w) = f(w, v)$.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$. Let us observe that $\mathrm{NulFrForm}(V, V)$ is symmetric and there exists an $\mathbb{R}$-form of V and V which is symmetric and there exists an $\mathbb{R}$-bilinear form of V and V which is symmetric.

Let L be a $\mathbb{Z}$-lattice. Let us observe that $\mathrm{InnerProduct}\, L$ is symmetric.

Let V be a finite rank, free $\mathbb{Z}$-module, f be a symmetric $\mathbb{R}$-bilinear form of V and V, and b be an ordered basis of V. Let us note that $\mathrm{GramMatrix}(f, b)$ is symmetric.

Now we state the propositions:

(44) Let us consider a rational $\mathbb{Z}$-lattice L, and vectors v, u of $\mathrm{DivisibleMod}(L)$. Then $(\mathrm{ScProductDM}(L))(v, u) \in \mathbb{F}_{\mathbb{Q}}$.

(45) Let us consider a rational $\mathbb{Z}$-lattice L, and an ordered basis b of L. Then $\mathrm{GramMatrix}(b)$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\dim(L)$.
Proof: For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of $\mathrm{GramMatrix}(b)$ holds $(\mathrm{GramMatrix}(b))_{i,j} \in$ the carrier of $\mathbb{F}_{\mathbb{Q}}$ by [8, (87)]. $\square$

(46) Let us consider a finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$, and a finite sequence G of elements of $\mathbb{F}_{\mathbb{Q}}$. If $F = G$, then $\sum F = \sum G$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$ for every finite sequence G of elements of $\mathbb{F}_{\mathbb{Q}}$ such that $\operatorname{len} F = \$_1$ and $F = G$ holds $\sum F = \sum G$. $\mathcal{P}[0]$ by [24, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [4, (4)], [6, (3)], [4, (59)], [3, (11)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(47) Let us consider a natural number i, an element j of $\mathbb{R}_{\mathrm{F}}$, and an element k of $\mathbb{F}_{\mathbb{Q}}$. Suppose $j = k$. Then $\mathrm{power}_{\mathbb{R}_{\mathrm{F}}}(-\mathbf{1}_{\mathbb{R}_{\mathrm{F}}}, i) \cdot j = \mathrm{power}_{\mathbb{F}_{\mathbb{Q}}}(-\mathbf{1}_{\mathbb{F}_{\mathbb{Q}}}, i) \cdot k$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv \mathrm{power}_{\mathbb{R}_{\mathrm{F}}}(-\mathbf{1}_{\mathbb{R}_{\mathrm{F}}}, \$_1) \cdot j = \mathrm{power}_{\mathbb{F}_{\mathbb{Q}}}(-\mathbf{1}_{\mathbb{F}_{\mathbb{Q}}}, \$_1) \cdot k$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(48) Let us consider a finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$. Suppose for every natural number i such that $i \in \operatorname{dom} F$ holds $F(i) \in \mathbb{F}_{\mathbb{Q}}$. Then $\sum F \in \mathbb{F}_{\mathbb{Q}}$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$ such that $\operatorname{len} F = \$_1$ and for every natural number i such that $i \in \operatorname{dom} F$ holds $F(i) \in \mathbb{F}_{\mathbb{Q}}$ holds $\sum F \in \mathbb{F}_{\mathbb{Q}}$. $\mathcal{P}[0]$ by [24, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [4, (4)], [6, (3)], [4, (59)], [3, (11)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(49) Let us consider a natural number i. Then $\mathrm{power}_{\mathbb{R}_{\mathrm{F}}}(-\mathbf{1}_{\mathbb{R}_{\mathrm{F}}}, i) \in \mathbb{F}_{\mathbb{Q}}$. The theorem is a consequence of (47).

(50) Let us consider natural numbers n, i, j, k, m, a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$, and a square matrix L over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n+1$. Suppose $0 < n$ and $M = L$ and $\langle i, j \rangle \in$ the indices of M and $\langle k, m \rangle \in$ the indices of $\mathrm{Delete}(M, i, j)$. Then $(\mathrm{Delete}(M, i, j))_{k,m} = (\mathrm{Delete}(L, i, j))_{k,m}$.

(51) Let us consider natural numbers n, i, j, k, m, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$. Suppose $0 < n$ and M is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n+1$ and $\langle i, j \rangle \in$ the indices of M and $\langle k, m \rangle \in$ the indices of $\mathrm{Delete}(M, i, j)$. Then $(\mathrm{Delete}(M, i, j))_{k,m}$ is an element of $\mathbb{F}_{\mathbb{Q}}$. The theorem is a consequence of (50).

(52) Let us consider natural numbers n, i, j, a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$, and a square matrix L over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n+1$. Suppose $0 < n$ and $M = L$ and $\langle i, j \rangle \in$ the indices of M. Then $\mathrm{Delete}(M, i, j) = \mathrm{Delete}(L, i, j)$. The theorem is a consequence of (50).

(53) Let us consider natural numbers n, i, j, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$. Suppose $0 < n$ and M is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n+1$ and $\langle i, j \rangle \in$ the indices of M. Then $\mathrm{Delete}(M, i, j)$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension n. The theorem is a consequence of

(52).

(54) Let us consider a natural number n, a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension n, and a square matrix H over $\mathbb{F}_{\mathbb{Q}}$ of dimension n. If $M = H$, then $\mathrm{Det}\, M = \mathrm{Det}\, H$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $\$_1$ for every square matrix H over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\$_1$ such that $M = H$ holds $\mathrm{Det}\, M = \mathrm{Det}\, H$. $\mathcal{P}[0]$ by [21, (41)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [3, (14)], [20, (27)], [8, (87)], [13, (1)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(55) Let us consider a natural number n, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension n. Suppose M is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension n. Then $\mathrm{Det}\, M \in \mathbb{F}_{\mathbb{Q}}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $\$_1$ such that M is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\$_1$ holds $\mathrm{Det}\, M \in \mathbb{F}_{\mathbb{Q}}$. $\mathcal{P}[0]$ by [21, (41)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [3, (14)], [20, (27)], [8, (87)], [13, (41)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(56) Let us consider natural numbers n, i, j, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$. Suppose M is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n+1$ and $\langle i, j\rangle \in$ the indices of M. Then $\mathrm{Cofactor}(M, i, j) \in \mathbb{F}_{\mathbb{Q}}$.

PROOF: Reconsider $D_1 = \mathrm{Delete}(M, i, j)$ as a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension n. $\mathrm{Det}\, D_1 \in \mathbb{F}_{\mathbb{Q}}$ by (53), (55), [21, (41)]. $\mathrm{power}_{\mathbb{R}_{\mathrm{F}}}(-\mathbf{1}_{\mathbb{R}_{\mathrm{F}}}, i+j) \in \mathbb{F}_{\mathbb{Q}}$. $\square$

(57) Let us consider a rational $\mathbb{Z}$-lattice L, and an ordered basis b of L. Then $\mathrm{Det}\,\mathrm{GramMatrix}(b) \in \mathbb{F}_{\mathbb{Q}}$. The theorem is a consequence of (45) and (55).

(58) Let us consider a positive definite $\mathbb{Z}$-lattice L, a basis I of L, and vectors v, w of L. Suppose for every vector u of L such that $u \in I$ holds $\langle u, v\rangle = \langle u, w\rangle$. Let us consider a vector u of L. Then $\langle u, v\rangle = \langle u, w\rangle$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every vector u of L for every finite subset J of L such that $J \subseteq I$ and $\overline{\overline{J}} = \$_1$ and $u \in \mathrm{Lin}(J)$ holds $\langle u, v\rangle = \langle u, w\rangle$. $\mathcal{P}[0]$ by [27, (9)], [25, (35)], [9, (12)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [28, (41)], [2, (44)], [1, (30)], [27, (7)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(59) Let us consider a positive definite $\mathbb{Z}$-lattice L, an ordered basis b of L, and vectors v, w of L. Suppose for every natural number n such that $n \in \mathrm{dom}\, b$ holds $\langle b_n, v\rangle = \langle b_n, w\rangle$. Then $v = w$.

PROOF: Reconsider $I = \mathrm{rng}\, b$ as a basis of L. For every vector u of L such that $u \in I$ holds $\langle u, v\rangle = \langle u, w\rangle$ by [5, (10)]. $\langle v - w, v\rangle = \langle v - w, w\rangle$. $\square$

(60) Let us consider a natural number n, and a square matrix M over $\mathbb{F}_{\mathbb{Q}}$ of

dimension n. Suppose M is without repeated line. Then $\operatorname{Det} M \neq 0_{\mathbb{F}_{\mathbb{Q}}}$ if and only if lines(M) is linearly independent.

(61) Let us consider a positive definite $\mathbb{Z}$-lattice L, a basis I of L, and vectors v, w of L. Suppose for every vector u of L such that $u \in I$ holds $\langle v, u \rangle = \langle w, u \rangle$. Let us consider a vector u of L. Then $\langle v, u \rangle = \langle w, u \rangle$. The theorem is a consequence of (58).

(62) Let us consider a positive definite $\mathbb{Z}$-lattice L, an ordered basis b of L, and vectors v, w of L. Suppose for every natural number n such that $n \in \operatorname{dom} b$ holds $\langle v, b_n \rangle = \langle w, b_n \rangle$. Then $v = w$. The theorem is a consequence of (59).

Let us consider a positive definite $\mathbb{Z}$-lattice L, an ordered basis b of EMLat(L), and vectors v, w of DivisibleMod(L). Now we state the propositions:

(63) If for every natural number n such that $n \in \operatorname{dom} b$ holds $(\mathrm{ScProductDM}(L))(b_n, v) =$ $(\mathrm{ScProductDM}(L))(b_n, w)$, then $v = w$.
Proof: Consider i being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $i \neq 0$ and $i \cdot v \in$ Embedding(L). Consider j being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $j \neq 0$ and $j \cdot w \in$ Embedding(L). Reconsider $i_1 = i \cdot v$ as a vector of EMLat(L). Reconsider $j_1 = j \cdot w$ as a vector of EMLat(L). EMLat(L) is a submodule of DivisibleMod(L). For every natural number n such that $n \in \operatorname{dom} b$ holds $\langle b_n, j \cdot i_1 \rangle = \langle b_n, i \cdot j_1 \rangle$ by [11, (24)], (6), (8). $j \cdot i_1 = i \cdot j_1$. □

(64) If for every natural number n such that $n \in \operatorname{dom} b$ holds $(\mathrm{ScProductDM}(L))(v, b_n) =$ $(\mathrm{ScProductDM}(L))(w, b_n)$, then $v = w$.
Proof: For every natural number n such that $n \in \operatorname{dom} b$ holds $(\mathrm{ScProductDM}(L))(b_n$ $(\mathrm{ScProductDM}(L))(b_n, w)$ by (20), [11, (24)], (6). □

Now we state the propositions:

(65) Let us consider a non trivial, rational, positive definite $\mathbb{Z}$-lattice L, an element v of L, a finite sequence b of elements of L, and a finite sequence s of elements of $\mathbb{F}_{\mathbb{Q}}$. Suppose $\operatorname{len} b = \operatorname{len} s$ and for every natural number n such that $n \in \operatorname{dom} s$ holds $s(n) = \langle b_n, v \rangle$. Then $\langle \sum b, v \rangle = \sum s$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence F of elements of L for every finite sequence F_1 of elements of $\mathbb{F}_{\mathbb{Q}}$ such that $\operatorname{len} F = \$_1$ and $\operatorname{len} F = \operatorname{len} F_1$ and for every natural number i such that $i \in \operatorname{dom} F_1$ holds $F_1(i) = \langle F_i, v \rangle$ holds $\langle \sum F, v \rangle = \sum F_1$. $\mathcal{P}[0]$ by [24, (43)], [9, (12)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [4, (4)], [6, (3)], [4, (59)], [3, (11)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(66) Let us consider a natural number n, and a finite sequence r of elements of $\mathbb{F}_{\mathbb{Q}}$. Suppose $\operatorname{len} r = n$. Then there exists an integer K and there exists a finite sequence K_2 of elements of $\mathbb{Z}^{\mathrm{R}}$ such that $K \neq 0$ and $\operatorname{len} K_2 = n$ and for every natural number i such that $i \in \operatorname{dom} K_2$ holds $K_2(i) = K \cdot r_i$.

PROOF: Consider K being an integer such that $K \neq 0$ and for every natural number i such that $i \in \operatorname{Seg} n$ holds $K \cdot r_i \in \mathbb{Z}$. Define $\mathcal{Q}[\text{natural number}, \text{object}] \equiv \$_2 = K \cdot r_{\$_1}$. For every natural number i such that $i \in \operatorname{Seg} n$ there exists an element x of the carrier of $\mathbb{Z}^{\mathrm{R}}$ such that $\mathcal{Q}[i, x]$. Consider K_2 being a finite sequence of elements of the carrier of $\mathbb{Z}^{\mathrm{R}}$ such that $\operatorname{dom} K_2 = \operatorname{Seg} n$ and for every natural number k such that $k \in \operatorname{Seg} n$ holds $\mathcal{Q}[k, K_2(k)]$ from [4, Sch. 5]. □

(67) Let us consider natural numbers i, j, a field K, elements a, a_1 of K, and an element R of the i-dimension vector space over K. If $j \in \operatorname{Seg} i$ and $a_1 = R(j)$, then $(a \cdot R)(j) = a \cdot a_1$.

(68) Let us consider natural numbers i, j, a field K, elements a_1, b_2 of K, and elements A, B of the i-dimension vector space over K. Suppose $j \in \operatorname{Seg} i$ and $a_1 = A(j)$ and $b_2 = B(j)$. Then $(A + B)(j) = a_1 + b_2$.

(69) Let us consider a field K, and natural numbers n, i. Suppose $i \in \operatorname{Seg} n$. Let us consider a finite sequence s of elements of the n-dimension vector space over K. Then there exists a finite sequence s_1 of elements of K such that

(i) $\operatorname{len} s_1 = \operatorname{len} s$, and

(ii) $(\sum s)(i) = \sum s_1$, and

(iii) for every natural number k such that $k \in \operatorname{dom} s_1$ holds $s_1(k) = s_k(i)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence s of elements of the n-dimension vector space over K such that $\operatorname{len} s = \$_1$ there exists a finite sequence s_1 of elements of K such that $\operatorname{len} s_1 = \operatorname{len} s$ and $(\sum s)(i) = \sum s_1$ and for every natural number k such that $k \in \operatorname{dom} s_1$ holds $s_1(k) = s_k(i)$. $\mathcal{P}[0]$ by [22, (7)], [24, (43)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [4, (4)], [6, (3)], [4, (59)], [3, (11)]. For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 2]. □

(70) Let us consider a non trivial, rational, positive definite $\mathbb{Z}$-lattice L, and an ordered basis b of L. Then $\operatorname{Det} \operatorname{GramMatrix}(b) \neq 0_{\mathbb{R}_{\mathrm{F}}}$.

PROOF: Reconsider $M = \operatorname{GramMatrix}(b)$ as a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\operatorname{rank} L$. $\operatorname{Det} M = 0_{\mathbb{F}_{\mathbb{Q}}}$. M is one-to-one by [13, (49)], [8, (87)], (59). Reconsider $M_1 = M$ as a finite sequence of elements of the $\operatorname{rank} L$-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$. Consider r being a finite sequence of elements of $\mathbb{F}_{\mathbb{Q}}$, r_1 being a finite sequence of elements of the $\operatorname{rank} L$-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ such that $\operatorname{len} r = \operatorname{rank} L$ and $\operatorname{len} r_1 = \operatorname{rank} L$ and for every natural number i such that $i \in \operatorname{dom} r_1$ holds $r_1(i) = r_i \cdot M_{1i}$ and $\sum r_1 = 0_\alpha$ and $r \neq \operatorname{Seg} \operatorname{len} r \longmapsto 0_{\mathbb{F}_{\mathbb{Q}}}$, where α is the $\operatorname{rank} L$-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$. Consider K being an integer, K_2 being a finite sequence of elements of $\mathbb{Z}^{\mathrm{R}}$ such that $K \neq 0$ and $\operatorname{len} K_2 = \operatorname{rank} L$ and for every natural number i such that $i \in \operatorname{dom} K_2$ holds $K_2(i) = K \cdot r_i$. Reconsider $K_1 = K$ as an element of $\mathbb{F}_{\mathbb{Q}}$. Define $\mathcal{P}[\text{natural number}, \text{object}] \equiv$ there exists an element r_2 of the rank L-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ such that $r_2 = r_1(\$_1)$ and $\$_2 = K_1 \cdot r_2$. For every natural number k such that $k \in \operatorname{Seg} \operatorname{rank} L$ there exists an element x of the carrier of the rank L-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ such that $\mathcal{P}[k, x]$. Consider K_3 being a finite sequence of elements of the carrier of the rank L-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ such that $\operatorname{dom} K_3 = \operatorname{Seg} \operatorname{rank} L$ and for every natural number k such that $k \in \operatorname{Seg} \operatorname{rank} L$ holds $\mathcal{P}[k, K_3(k)]$ from [4, Sch. 5]. For every natural number i such that $i \in \operatorname{dom} K_3$ there exists an element M_2 of the rank L-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ and there exists an element K_5 of $\mathbb{F}_{\mathbb{Q}}$ such that $M_2 = M_1(i)$ and $K_5 = K_2(i)$ and $K_3(i) = K_5 \cdot M_2$. For every natural number k and for every element v of the rank L-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ such that $k \in \operatorname{dom} K_3$ and $v = r_1(k)$ holds $K_3(k) = K_1 \cdot v$. $K_2 \neq \operatorname{Seg} \operatorname{len} K_2 \longmapsto 0_{\mathbb{Z}^{\mathrm{R}}}$ by [22, (7)]. Set $S = \sum K_3$. For every natural number n such that $n \in \operatorname{dom} b$ holds $S(n) = 0_{\mathbb{Z}^{\mathrm{R}}}$ by [22, (7)]. Define $\mathcal{Q}[\text{natural number}, \text{object}] \equiv \$_2 = K_{2\$_1} \cdot b_{\$_1}$. Consider K_4 being a finite sequence of elements of the carrier of L such that $\operatorname{dom} K_4 = \operatorname{Seg} \operatorname{rank} L$ and for every natural number k such that $k \in \operatorname{Seg} \operatorname{rank} L$ holds $\mathcal{Q}[k, K_4(k)]$ from [4, Sch. 5]. For every natural number n such that $n \in \operatorname{dom} b$ holds $S(n) = \langle \sum K_4, b_n \rangle$ by (69), [19, (102)], [8, (87)], (67). For every natural number n such that $n \in \operatorname{dom} b$ holds $\langle 0_L, b_n \rangle = \langle \sum K_4, b_n \rangle$ by [9, (12)]. $\sum K_4 = 0_L$. $\operatorname{rng} b$ is linearly dependent. $\square$

Let L be a non trivial, rational, positive definite $\mathbb{Z}$-lattice and b be an ordered basis of L. Let us observe that $\operatorname{GramMatrix}(b)$ is invertible.

References

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

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

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

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

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

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

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

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

[9] Yuichi Futa and Yasunari Shidama. Lattice of $\mathbb{Z}$-module. *Formalized Mathematics*, 24(**1**):49–68, 2016. doi:10.1515/forma-2016-0005.

[10] Yuichi Futa and Yasunari Shidama. Divisible $\mathbb{Z}$-modules. *Formalized Mathematics*, 24

(**1**):37–47, 2016. doi:10.1515/forma-2016-0004.

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

[12] 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.

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

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

[16] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982. doi:10.1007/BF01457454.

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

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

[19] Karol Pąk. Basic properties of the rank of matrices over a field. *Formalized Mathematics*, 15(**4**):199–211, 2007. doi:10.2478/v10037-007-0024-5.

[20] Karol Pąk and Andrzej Trybulec. Laplace expansion. *Formalized Mathematics*, 15(**3**): 143–150, 2007. doi:10.2478/v10037-007-0016-5.

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

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

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

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

[25] Wojciech A. Trybulec. Subspaces and cosets of subspaces in vector space. *Formalized Mathematics*, 1(**5**):865–870, 1990.

[26] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1 (**5**):877–882, 1990.

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

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

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

Received March 17, 2017

Contents

Formaliz. Math. 25 (**1**)

Continued on inside back cover