Contents

Formaliz. Math. 29 (**1**)

Continued on inside back cover

FORMALIZED MATHEMATICS
Vol. 29, No. 1, Pages 1–8, 2021
DOI: 10.2478/forma-2021-0001

sciendo
https://sciendo.com/journal/forma

Derivation of Commutative Rings and the Leibniz Formula for Power of Derivation

Yasushige Watase
Suginami-ku Matsunoki
3-21-6 Tokyo, Japan

Summary. In this article we formalize in Mizar [1], [2] a derivation of commutative rings, its definition and some properties. The details are to be referred to [5], [7]. A derivation of a ring, say D, is defined generally as a map from a commutative ring A to A-Module M with specific conditions. However we start with simpler case, namely dom $D =$ rng D. This allows to define a derivation in other rings such as a polynomial ring.

A derivation is a map $D : A \longrightarrow A$ satisfying the following conditions:

(i) $D(x + y) = Dx + Dy$,

(ii) $D(xy) = xDy + yDx$, $\forall x, y \in A$.

Typical properties are formalized such as:

$$D(\sum_{i=1}^{n} x_i) = \sum_{i=1}^{n} Dx_i$$

and

$$D(\prod_{i=1}^{n} x_i) = \sum_{i=1}^{n} x_1 x_2 \cdots Dx_i \cdots x_n \ (\forall x_i \in A).$$

We also formalized the Leibniz Formula for power of derivation D :

$$D^n(xy) = \sum_{i=0}^{n} \binom{n}{i} D^i x D^{n-i} y.$$

Lastly applying the definition to the polynomial ring of A and a derivation of polynomial ring was formalized. We mentioned a justification about compatibility of the derivation in this article to the same object that has treated as differentiations of polynomial functions [3].

MSC: 13B25 13N15 68V20

Keywords: derivation; Leibniz Formula; derivation of polynomial ring

MML identifier: RINGDER1, version: 8.1.11 5.65.1394

1. Preliminaries

From now on L denotes an Abelian, left zeroed, add-associative, associative, right zeroed, right complementable, distributive, non empty double loop structure, a, b, c denote elements of L, R denotes a non degenerated commutative ring, and n, m, i, j, k denote natural numbers.

Now we state the propositions:

(1) $n \cdot a + n \cdot b = n \cdot (a + b)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \$_1 \cdot a + \$_1 \cdot b = \$_1 \cdot (a + b)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(2) $(n \cdot a) \cdot b = a \cdot (n \cdot b)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv (\$_1 \cdot a) \cdot b = a \cdot (\$_1 \cdot b)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(3) $n \cdot (0_L) = 0_L$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \$_1 \cdot (0_L) = 0_L$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$. For every natural number n, $\mathcal{P}[n]$. □

(4) $0_L \cdot n = 0_L$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv 0_L \cdot \$_1 = 0_L$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$. For every natural number n, $\mathcal{P}[n]$. □

2. Definition of Derivation of Rings and its Properties

From now on D denotes a function from R into R and x, y, z denote elements of R.

Definition of derivation of rings.

Let us consider R. Let Δ be a function from R into R. We say that Δ is derivation if and only if

(Def. 1) for every elements x, y of R, $\Delta(x + y) = \Delta(x) + \Delta(y)$ and $\Delta(x \cdot y) = x \cdot \Delta(y) + y \cdot \Delta(x)$.

Observe that every function from R into R which is derivation is also additive and there exists a function from R into R which is derivation.

A derivation of R is derivation function from R into R. The functor $\mathrm{Der}\, R$ yielding a subset of $(\Omega_R)^{\Omega_R}$ is defined by the term

(Def. 2) $\{f$, where f is a function from R into $R : f$ is derivation$\}$.

Let us observe that $\mathrm{Der}\,R$ is non empty.

From now on D denotes a derivation of R.

Now we state the propositions:

(5) (i) $D(1_R) = 0_R$, and

(ii) $D(0_R) = 0_R$.

(6) $D(n \cdot x) = n \cdot D(x)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv D(\$_1 \cdot x) = \$_1 \cdot D(x)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(7) $D(x^{m+1}) = (m+1) \cdot (x^m \cdot D(x))$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv D(x^{\$_1+1}) = (\$_1+1) \cdot (x^{\$_1} \cdot D(x))$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(8) (i) $D^{n+1} = D \cdot (D^n)$, and

(ii) $\mathrm{dom}\,D =$ the carrier of R, and

(iii) $\mathrm{dom}(D^n) =$ the carrier of R, and

(iv) D^n is a (the carrier of R)-valued function.

(9) $(D^{n+1})(x) = D((D^n)(x))$. The theorem is a consequence of (8).

(10) If $z \cdot y = 1_R$, then $y^2 \cdot D(x \cdot z) = y \cdot D(x) - x \cdot D(y)$.

In the sequel s denotes a finite sequence of elements of the carrier of R and h denotes a function from R into R.

Let us consider R, s, and h. One can check that the functor $h \cdot s$ yields a finite sequence of elements of the carrier of R. Now we state the proposition:

(11) If h is additive, then $h(\sum s) = \sum (h \cdot s)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every h and s such that $\mathrm{len}\,s = \$_1$ and h is additive holds $h(\sum s) = \sum (h \cdot s)$. $\mathcal{P}[0]$ by [4, (6)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(12) Formula $(f_1 + f_2 + \cdots + f_n)' = f_1' + f_2' + \cdots + f_n'$:
$D(\sum s) = \sum (D \cdot s)$.

Let us consider R, D, and s. The functor $\mathrm{DProd}(D, s)$ yielding a finite sequence of elements of the carrier of R is defined by

(Def. 3) $\mathrm{len}\,it = \mathrm{len}\,s$ and for every i such that $i \in \mathrm{dom}\,it$ holds $it(i) = \prod \mathrm{Replace}(s, i, D(s_{/i}))$.

Now we state the propositions:

(13) If $\mathrm{len}\,s = 1$, then $\sum \mathrm{DProd}(D, s) = D(\prod s)$.

(14) Let us consider a finite sequence t of elements of the carrier of R. If $\operatorname{len} t \geqslant 1$, then $\sum \operatorname{DProd}(D, t) = D(\prod t)$.
PROOF: Define $\mathcal{P}$[non zero natural number] $\equiv$ for every s such that $\operatorname{len} s = \$_1$ holds $\sum \operatorname{DProd}(D, s) = D(\prod s)$. $\mathcal{P}[1]$. For every non zero natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every non zero natural number k, $\mathcal{P}[k]$. □

3. Proof of the Leibniz Formula for Power of Derivations

The Leibniz formula for power of a derivation of a commutative ring.

Let us consider R, D, and n. Let x, y be elements of R. The functor $\operatorname{LBZ}(D, n, x, y)$ yielding a finite sequence of elements of the carrier of R is defined by

(Def. 4) $\operatorname{len} it = n + 1$ and for every i such that $i \in \operatorname{dom} it$ holds $it(i) = \binom{n}{i -' 1} \cdot (D^{n+1-'i})(x) \cdot (D^{i-'1})(y)$.

Now we state the propositions:

(15) $\operatorname{LBZ}(D, 0, x, y) = \langle x \cdot y \rangle$.

(16) $\operatorname{LBZ}(D, 1, x, y) = \langle y \cdot D(x), x \cdot D(y) \rangle$.

Let us consider R, D, and m. Let x, y be elements of R. The functor $\operatorname{LBZ0}(D, m, x, y)$ yielding a finite sequence of elements of the carrier of R is defined by

(Def. 5) $\operatorname{len} it = m$ and for every i such that $i \in \operatorname{dom} it$ holds $it(i) = (\binom{m}{i -' 1} + \binom{m}{i}) \cdot (D^{m+1-'i})(x) \cdot (D^{i})(y)$.

The functor $\operatorname{LBZ1}(D, m, x, y)$ yielding a finite sequence of elements of the carrier of R is defined by

(Def. 6) $\operatorname{len} it = m$ and for every i such that $i \in \operatorname{dom} it$ holds $it(i) = \binom{m}{i -' 1} \cdot (D^{m+1-'i})(x) \cdot (D^{i})(y)$.

The functor $\operatorname{LBZ2}(D, m, x, y)$ yielding a finite sequence of elements of the carrier of R is defined by

(Def. 7) $\operatorname{len} it = m$ and for every i such that $i \in \operatorname{dom} it$ holds $it(i) = \binom{m}{i} \cdot (D^{m+1-'i})(x) \cdot (D^{i})(y)$.

Now we state the propositions:

(17) $D(\sum \operatorname{LBZ0}(D, n, x, y)) = \sum D \cdot (\operatorname{LBZ0}(D, n, x, y))$.

(18) $\operatorname{LBZ0}(D, m, x, y) = \operatorname{LBZ1}(D, m, x, y) + \operatorname{LBZ2}(D, m, x, y)$.
PROOF: Set $p = \operatorname{LBZ1}(D, m, x, y)$. Set $q = \operatorname{LBZ2}(D, m, x, y)$. Set $r = \operatorname{LBZ0}(D, m, x, y)$. For every k such that $1 \leqslant k \leqslant \operatorname{len}(p + q)$ holds $(p + q)(k) = r(k)$. □

(19) $\sum \mathrm{LBZ0}(D,n,x,y) = \sum \mathrm{LBZ1}(D,n,x,y) + \sum \mathrm{LBZ2}(D,n,x,y)$. The theorem is a consequence of (18).

(20) $D\cdot(\mathrm{LBZ0}(D,n,x,y)) = (\mathrm{LBZ2}(D,n+1,x,y))_{\restriction n+1} + (\mathrm{LBZ1}(D,n+1,x,y))_{\restriction 1}$.
Proof: Set $p = \mathrm{LBZ2}(D,n+1,x,y)$. Set $q = \mathrm{LBZ1}(D,n+1,x,y)$. Set $r = \mathrm{LBZ0}(D,n,x,y)$. Reconsider $p_1 = p_{\restriction n+1}$ as a finite sequence of elements of the carrier of R. Reconsider $q_1 = q_{\restriction 1}$ as a finite sequence of elements of the carrier of R. For every i such that $1 \leqslant i \leqslant \operatorname{len} D \cdot r$ holds $(D \cdot r)(i) = (p_1 + q_1)(i)$. □

(21) $\sum D \cdot (\mathrm{LBZ0}(D,n,x,y)) = -(\mathrm{LBZ1}(D,n+1,x,y))_{/1} + \sum \mathrm{LBZ0}(D,n+1,x,y) - (\mathrm{LBZ2}(D,n+1,x,y))_{/n+1}$. The theorem is a consequence of (20) and (19).

(22) $\mathrm{LBZ}(D,n+1,x,y) = (\langle (D^{n+1})(x)\cdot y\rangle ^\frown \mathrm{LBZ0}(D,n,x,y)) ^\frown \langle x\cdot (D^{n+1})(y)\rangle$.
Proof: Set $p = \mathrm{LBZ}(D,n+1,x,y)$. Set $q = \mathrm{LBZ0}(D,n,x,y)$. Set $r = (\langle (D^{n+1})(x)\cdot y\rangle ^\frown q) ^\frown \langle x \cdot (D^{n+1})(y)\rangle$. For every k such that $1 \leqslant k \leqslant \operatorname{len} p$ holds $p(k) = r(k)$. □

(23) $\sum((\langle (D^{n+1})(x)\cdot y\rangle ^\frown \mathrm{LBZ0}(D,n,x,y)) ^\frown \langle x \cdot (D^{n+1})(y)\rangle) = (D^{n+1})(x) \cdot y + \sum \mathrm{LBZ0}(D,n,x,y) + x \cdot (D^{n+1})(y)$.

(24) $D(\sum \mathrm{LBZ}(D,n+1,x,y)) = \sum \mathrm{LBZ}(D,n+2,x,y)$. The theorem is a consequence of (9), (21), (11), (22), and (23).

(25) The Leibniz formula for power of derivation:
$(D^n)(x\cdot y) = \sum \mathrm{LBZ}(D,n,x,y)$. The theorem is a consequence of (16), (9), (24), and (15).

4. Example of Derivation of Polynomial Ring over a Commutative Ring

Let us consider R. Let f be a function from PolyRing(R) into PolyRing(R) and p be an element of the carrier of PolyRing(R). Observe that the functor $f(p)$ yields an element of the carrier of PolyRing(R). Let R be a ring. The functor Der1(R) yielding a function from PolyRing(R) into PolyRing(R) is defined by

(Def. 8) for every element f of the carrier of PolyRing(R) and for every natural number i, $\mathit{it}(f)(i) = (i+1)\cdot f(i+1)$.

Let us consider R. One can verify that Der1(R) is additive.

In the sequel R denotes an integral domain and f, g denote elements of the carrier of PolyRing(R).

Now we state the proposition:

(26) Let us consider an element f of the carrier of PolyRing(R), and a polynomial f_1 over R. Suppose $f = f_1$ and f_1 is constant. Then $(\mathrm{Der1}(R))(f) = \mathbf{0}.R$.

Proof: For every element i of $\mathbb{N}$, $(\mathrm{Der1}(R))(f)(i) = (\mathbf{0}.R)(i)$. □

In the sequel a denotes an element of R. Now we state the propositions:

(27) Let us consider a natural number i, and an element p of the carrier of $\mathrm{PolyRing}(R)$. Then $((a\restriction R) * p)(i) = a \cdot p(i)$.

(28) Let us consider elements f, g of the carrier of $\mathrm{PolyRing}(R)$, and an element a of R. Suppose $f = a\restriction R$. Then $(\mathrm{Der1}(R))(f\cdot g) = (a\restriction R)*(\mathrm{Der1}(R))(g)$.
Proof: For every natural number n, $(\mathrm{Der1}(R))(f \cdot g)(n) = ((a\restriction R) * (\mathrm{Der1}(R))(g))(n)$. □

Let us consider an element f of the carrier of $\mathrm{PolyRing}(R)$ and an element a of R. Now we state the propositions:

(29) If $f = \mathrm{anpoly}(a, 0)$, then $(\mathrm{Der1}(R))(f) = \mathbf{0}.R$.
Proof: For every element n of $\mathbb{N}$, $(\mathrm{Der1}(R))(f)(n) = (\mathbf{0}.R)(n)$. □

(30) If $f = \mathrm{anpoly}(a, 1)$, then $(\mathrm{Der1}(R))(f) = \mathrm{anpoly}(a, 0)$.
Proof: For every element n of $\mathbb{N}$, $(\mathrm{Der1}(R))(f)(n) = (\mathrm{anpoly}(a, 0))(n)$. □

(31) Let us consider polynomials p, q over R. Suppose $p = \mathrm{anpoly}(1_R, 1)$. Let us consider an element i of $\mathbb{N}$. Then

(i) $(p * q)(i + 1) = q(i)$, and

(ii) $(p * q)(0) = 0_R$.

Proof: For every element i of $\mathbb{N}$, $(p * q)(i + 1) = q(i)$. Consider F_1 being a finite sequence of elements of the carrier of R such that $\mathrm{len}\, F_1 = 0 + 1$ and $(p * q)(0) = \sum F_1$ and for every element k of $\mathbb{N}$ such that $k \in \mathrm{dom}\, F_1$ holds $F_1(k) = p(k -' 1) \cdot q(0 + 1 -' k)$. □

(32) Let us consider elements f, g of the carrier of $\mathrm{PolyRing}(R)$. Suppose $f = \mathrm{anpoly}(1_R, 1)$. Then $(\mathrm{Der1}(R))(f \cdot g) = (\mathrm{Der1}(R))(f) \cdot g + f \cdot (\mathrm{Der1}(R))(g)$.
Proof: Reconsider $d_1 = (\mathrm{Der1}(R))(f)$, $d_2 = (\mathrm{Der1}(R))(g)$ as a polynomial over R. Reconsider $f_1 = f$, $g_1 = g$ as a polynomial over R. For every element i of $\mathbb{N}$, $(\mathrm{Der1}(R))(f \cdot g)(i) = (d_1 * g_1 + f_1 * d_2)(i)$. □

(33) Let us consider constant elements f, g of the carrier of $\mathrm{PolyRing}(R)$. Then $(\mathrm{Der1}(R))(f \cdot g) = (\mathrm{Der1}(R))(f) \cdot g + f \cdot (\mathrm{Der1}(R))(g)$. The theorem is a consequence of (29).

(34) Let us consider elements f, g of the carrier of $\mathrm{PolyRing}(R)$. Suppose f is constant. Then $(\mathrm{Der1}(R))(f \cdot g) = (\mathrm{Der1}(R))(f) \cdot g + f \cdot (\mathrm{Der1}(R))(g)$. The theorem is a consequence of (29) and (28).

(35) Let us consider elements x, y of the carrier of $\mathrm{PolyRing}(R)$. Suppose x is not constant. Then $(\mathrm{Der1}(R))(x \cdot y) = (\mathrm{Der1}(R))(x) \cdot y + x \cdot (\mathrm{Der1}(R))(y)$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every elements f, g of the carrier of $\mathrm{PolyRing}(R)$ for every elements f_0, g_0 of the carrier of $\mathrm{PolyRing}(R)$ such

that $f_0 = f$ and $g_0 = g$ and $\deg f_0 - 1 = \$_1$ holds $(\mathrm{Der1}(R))(f_0 \cdot g_0) = (\mathrm{Der1}(R))(f_0) \cdot g_0 + f_0 \cdot (\mathrm{Der1}(R))(g_0)$. For every natural number k such that for every natural number n such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$ by [8, (4)]. For every natural number n, $\mathcal{P}[n]$. □

(36) $(\mathrm{Der1}(R))(f \cdot g) = (\mathrm{Der1}(R))(f) \cdot g + f \cdot (\mathrm{Der1}(R))(g)$. The theorem is a consequence of (35) and (34).

Let us consider R. Let us observe that $\mathrm{Der1}(R)$ is derivation.

Now we state the propositions:

(37) Let us consider an element x of $\mathrm{PolyRing}(R)$, and a polynomial f over R. If $x = f$, then for every natural number n, $x^n = f^n$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv x^{\$_1} = f^{\$_1}$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [6, (19)]. For every natural number n, $\mathcal{P}[n]$. □

(38) Let us consider an element x of $\mathrm{PolyRing}(R)$. Suppose $x = \mathrm{anpoly}(1_R, 1)$. Then there exists an element y of $\mathrm{PolyRing}(R)$ such that

(i) $y = \mathrm{anpoly}(1_R, n)$, and

(ii) $(\mathrm{Der1}(R))(x^{n+1}) = (n+1) \cdot y$.

The theorem is a consequence of (30), (37), and (7).

From now on p denotes a polynomial over $\mathbb{R}_{\mathrm{F}}$.

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

(Def. 9) for every natural number n, $it(n) = p(n+1) \cdot (n+1)$.

Now we state the proposition:

(39) Let us consider an element p_0 of $\mathrm{PolyRing}(\mathbb{R}_{\mathrm{F}})$, and a polynomial p over $\mathbb{R}_{\mathrm{F}}$. If $p_0 = p$, then $p' = (\mathrm{Der1}(\mathbb{R}_{\mathrm{F}}))(p_0)$.

Proof: For every n, $(p')(n) = (\mathrm{Der1}(\mathbb{R}_{\mathrm{F}}))(p_0)(n)$. □

References

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

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Artur Korniłowicz. Differentiability of polynomials over reals. *Formalized Mathematics*, 25(**1**):31–37, 2017. doi:10.1515/forma-2017-0002.

[4] Artur Korniłowicz and Christoph Schwarzweller. The first isomorphism theorem and other properties of rings. *Formalized Mathematics*, 22(**4**):291–301, 2014. doi:10.2478/forma-2014-0029.

[5] Hideyuki Matsumura. *Commutative Ring Theory.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2nd edition, 1989.

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

[7] Masayoshi Nagata. *Theory of Commutative Fields*, volume 125 of *Translations of Mathematical Monographs.* American Mathematical Society, 1985.

[8] Christoph Schwarzweller. On roots of polynomials and algebraically closed fields. *Formalized Mathematics*, 25(**3**):185–195, 2017. doi:10.1515/forma-2017-0018.

Accepted March 30, 2021

FORMALIZED MATHEMATICS
Vol. **29**, No. **1**, Pages 9–19, **2021**
DOI: 10.2478/forma-2021-0002

sciendo
https://sciendo.com/journal/forma

Inverse Function Theorem. Part I[1]

Kazuhisa Nakasho
Yamaguchi University
Yamaguchi, Japan

Yuichi Futa
Tokyo University of Technology
Tokyo, Japan

Summary. In this article we formalize in Mizar [1], [2] the inverse function theorem for the class of C^1 functions between Banach spaces. In the first section, we prove several theorems about open sets in real norm space, which are needed in the proof of the inverse function theorem. In the next section, we define a function to exchange the order of a product of two normed spaces, namely $\mathbb{E}\curvearrowleft\frown\eqsim(x, y) \in X \times Y \mapsto (y, x) \in Y \times X$, and formalized its bijective isometric property and several differentiation properties. This map is necessary to change the order of the arguments of a function when deriving the inverse function theorem from the implicit function theorem proved in [6].

In the third section, using the implicit function theorem, we prove a theorem that is a necessary component of the proof of the inverse function theorem. In the last section, we finally formalized an inverse function theorem for class of C^1 functions between Banach spaces. We referred to [9], [10], and [3] in the formalization.

MSC: 26B10 47A05 47J07 68V20

Keywords: inverse function theorem; Lipschitz continuity; differentiability; implicit function; inverse function

MML identifier: `NDIFF10`, version: `8.1.11 5.65.1394`

1. Preliminaries

From now on S, T, W, Y denote real normed spaces, f, f_1, f_2 denote partial functions from S to T, Z denotes a subset of S, and i, n denote natural numbers.

Now we state the propositions:

[1] This study has been supported in part by JSPS KAKENHI Grant Numbers JP20K19863 and JP17K00182.

(1) Let us consider real normed spaces X, Y, a partial function f from X to Y, a subset A of X, and a subset B of Y. Suppose $\operatorname{dom} f = A$ and f is continuous on A and A is open and B is open. Then $f^{-1}(B)$ is open.
PROOF: For every point a of X such that $a \in f^{-1}(B)$ there exists a real number s such that $s > 0$ and $\operatorname{Ball}(a, s) \subseteq f^{-1}(B)$. □

(2) Let us consider real normed spaces X, Y, a point x of X, a point y of Y, a point z of $X \times Y$, and real numbers r_1, r_2. Suppose $0 < r_1$ and $0 < r_2$ and $z = \langle x, y \rangle$. Then there exists a real number s such that

(i) $s = \min(r_1, r_2)$, and

(ii) $s > 0$, and

(iii) $\operatorname{Ball}(z, s) \subseteq \operatorname{Ball}(x, r_1) \times \operatorname{Ball}(y, r_2)$.

(3) Let us consider real normed spaces X, Y, and a subset V of $X \times Y$. Then V is open if and only if for every point x of X and for every point y of Y such that $\langle x, y \rangle \in V$ there exist real numbers r_1, r_2 such that $0 < r_1$ and $0 < r_2$ and $\operatorname{Ball}(x, r_1) \times \operatorname{Ball}(y, r_2) \subseteq V$.
PROOF: For every point z of $X \times Y$ such that $z \in V$ there exists a real number s such that $s > 0$ and $\operatorname{Ball}(z, s) \subseteq V$. □

(4) Let us consider real normed spaces X, Y, a subset V of $X \times Y$, and a subset D of X. Suppose D is open and $V = D \times$ (the carrier of Y). Then V is open.
PROOF: For every point x of X and for every point y of Y such that $\langle x, y \rangle \in V$ there exist real numbers r_1, r_2 such that $0 < r_1$ and $0 < r_2$ and $\operatorname{Ball}(x, r_1) \times \operatorname{Ball}(y, r_2) \subseteq V$. □

(5) Let us consider real normed spaces X, Y, a subset V of $X \times Y$, and a subset D of Y. Suppose D is open and $V =$ (the carrier of X) $\times D$. Then V is open.
PROOF: For every point x of X and for every point y of Y such that $\langle x, y \rangle \in V$ there exist real numbers r_1, r_2 such that $0 < r_1$ and $0 < r_2$ and $\operatorname{Ball}(x, r_1) \times \operatorname{Ball}(y, r_2) \subseteq V$. □

2. A Map Reversing the Order of Product of Two Norm Spaces

Now we state the proposition:

(6) Let us consider real numbers x, y, and elements u, v of $\mathcal{R}^2$. Suppose $u = \langle x, y \rangle$ and $v = \langle y, x \rangle$. Then $|u| = |v|$.

Let X, Y be real normed spaces. The functor $\operatorname{Exch}(X, Y)$ yielding a linear operator from $X \times Y$ into $Y \times X$ is defined by

(Def. 1) *it* is one-to-one, onto, and isometric and for every point x of X and for every point y of Y, $it(x,y) = \langle y,\, x\rangle$.

Now we state the propositions:

(7) Let us consider real normed spaces X, Y, a subset Z of $X \times Y$, and objects x, y. Then $\langle x,\, y\rangle \in Z$ if and only if $\langle y,\, x\rangle \in (\mathrm{Exch}(Y,X))^{-1}(Z)$.

(8) Let us consider real normed spaces X, Y, a non empty set Z, a partial function f from $X \times Y$ to Z, and a function I from $Y \times X$ into $X \times Y$. Suppose for every point y of Y for every point x of X, $I(y,x) = \langle x,\, y\rangle$. Then

(i) $\mathrm{dom}(f \cdot I) = I^{-1}(\mathrm{dom}\, f)$, and

(ii) for every point x of X and for every point y of Y, $f \cdot I(y,x) = f(x,y)$.

Proof: For every object w, $w \in \mathrm{dom}(f \cdot I)$ iff $w \in I^{-1}(\mathrm{dom}\, f)$. □

(9) Let us consider real normed spaces X, Y, Z, a partial function f from Y to Z, a linear operator I from X into Y, and a subset V of Y. Suppose f is differentiable on V and I is one-to-one, onto, and isometric. Let us consider a point y of Y. Suppose $y \in V$. Then $(f'_{\restriction V})(y) = (f \cdot I'_{\restriction I^{-1}(V)})_{/(I^{-1})(y)} \cdot (I^{-1})$.
Proof: Consider J being a linear operator from Y into X such that $J = I^{-1}$ and J is one-to-one, onto, and isometric. Set $g = f \cdot I$. Set $U = I^{-1}(V)$. For every point y of Y such that $y \in \mathrm{dom}(f'_{\restriction V})$ holds $(f'_{\restriction V})(y) = (g'_{\restriction U})_{/J(y)} \cdot (I^{-1})$ by [4, (31)]. □

(10) Let us consider real normed spaces X, Y, Z, a subset V of Y, a partial function g from Y to Z, and a linear operator I from X into Y. Suppose I is one-to-one, onto, and isometric and g is differentiable on V. Then $g'_{\restriction V}$ is continuous on V if and only if $g \cdot I'_{\restriction I^{-1}(V)}$ is continuous on $I^{-1}(V)$.
Proof: Consider J being a linear operator from Y into X such that $J = I^{-1}$ and J is one-to-one, onto, and isometric. Set $f = g \cdot I$. Set $U = I^{-1}(V)$. Set $F = f'_{\restriction U}$. Set $G = g'_{\restriction V}$. If G is continuous on V, then F is continuous on U. If F is continuous on U, then G is continuous on V. □

(11) Let us consider real normed spaces X, Y, Z, a partial function f from $X \times Y$ to Z, a subset U of $X \times Y$, and a function I from $Y \times X$ into $X \times Y$. Suppose for every point y of Y for every point x of X, $I(y,x) = \langle x,\, y\rangle$. Let us consider a point a of X, a point b of Y, a point u of $X \times Y$, and a point v of $Y \times X$. Suppose $u \in U$ and $u = \langle a,\, b\rangle$ and $v = \langle b,\, a\rangle$. Then

(i) $f \cdot (\mathrm{reproj1}(u)) = f \cdot I \cdot (\mathrm{reproj2}(v))$, and

(ii) $f \cdot (\mathrm{reproj2}(u)) = f \cdot I \cdot (\mathrm{reproj1}(v))$.

Proof: For every object x, $x \in \mathrm{dom}(f \cdot (\mathrm{reproj1}(u)))$ iff $x \in \mathrm{dom}(f \cdot I \cdot (\mathrm{reproj2}(v)))$. For every object y, $y \in \mathrm{dom}(f \cdot (\mathrm{reproj2}(u)))$ iff $y \in \mathrm{dom}(f \cdot$

$I \cdot (\mathrm{reproj1}(v)))$. For every object x such that $x \in \mathrm{dom}(f \cdot (\mathrm{reproj1}(u)))$ holds $(f \cdot (\mathrm{reproj1}(u)))(x) = (f \cdot I \cdot (\mathrm{reproj2}(v)))(x)$. For every object y such that $y \in \mathrm{dom}(f \cdot (\mathrm{reproj2}(u)))$ holds $(f \cdot (\mathrm{reproj2}(u)))(y) = (f \cdot I \cdot (\mathrm{reproj1}(v)))(y)$. □

Let us consider real normed spaces X, Y, Z, a partial function f from $X \times Y$ to Z, a subset U of $X \times Y$, a linear operator I from $Y \times X$ into $X \times Y$, a point a of X, a point b of Y, a point u of $X \times Y$, and a point v of $Y \times X$. Now we state the propositions:

(12) Suppose $U = \mathrm{dom}\, f$ and f is differentiable on U and I is one-to-one, onto, and isometric and for every point y of Y and for every point x of X, $I(y, x) = \langle x, y \rangle$. Then suppose $u \in U$ and $u = \langle a, b \rangle$ and $v = \langle b, a \rangle$. Then

(i) f is partially differentiable in u w.r.t. 1 iff $f \cdot I$ is partially differentiable in v w.r.t. 2, and

(ii) f is partially differentiable in u w.r.t. 2 iff $f \cdot I$ is partially differentiable in v w.r.t. 1.

(13) Suppose $U = \mathrm{dom}\, f$ and f is differentiable on U and I is one-to-one, onto, and isometric and for every point y of Y and for every point x of X, $I(y, x) = \langle x, y \rangle$. Then suppose $u \in U$ and $u = \langle a, b \rangle$ and $v = \langle b, a \rangle$. Then

(i) $\mathrm{partdiff}(f, u)\,\mathrm{w.r.t.}\,1 = \mathrm{partdiff}(f \cdot I, v)\,\mathrm{w.r.t.}\,2$, and

(ii) $\mathrm{partdiff}(f, u)\,\mathrm{w.r.t.}\,2 = \mathrm{partdiff}(f \cdot I, v)\,\mathrm{w.r.t.}\,1$.

3. Properties of the Differentiation of the Inverse Mapping

Now we state the propositions:

(14) Let us consider a real normed space F, non trivial real Banach spaces G, E, a subset Z of $E \times F$, a partial function f from $E \times F$ to G, a point a of E, a point b of F, a point c of G, and a point z of $E \times F$. Suppose Z is open and $\mathrm{dom}\, f = Z$ and f is differentiable on Z and $f'_{\restriction Z}$ is continuous on Z and $\langle a, b \rangle \in Z$ and $f(a, b) = c$ and $z = \langle a, b \rangle$ and $\mathrm{partdiff}(f, z)\,\mathrm{w.r.t.}\,1$ is invertible. Then there exist real numbers r_1, r_2 such that

(i) $0 < r_1$, and

(ii) $0 < r_2$, and

(iii) $\overline{\mathrm{Ball}}(a, r_1) \times \mathrm{Ball}(b, r_2) \subseteq Z$, and

(iv) for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ there exists a point x of E such that $x \in \mathrm{Ball}(a, r_1)$ and $f(x, y) = c$, and

(v) for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ for every points x_1, x_2 of E such that x_1, $x_2 \in \mathrm{Ball}(a, r_1)$ and $f(x_1, y) = c$ and $f(x_2, y) = c$ holds $x_1 = x_2$, and

(vi) there exists a partial function g from F to E such that $\mathrm{dom}\, g = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g \subseteq \mathrm{Ball}(a, r_1)$ and g is continuous on $\mathrm{Ball}(b, r_2)$ and $g(b) = a$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f(g(y), y) = c$ and g is differentiable on $\mathrm{Ball}(b, r_2)$ and $g'_{\restriction \mathrm{Ball}(b, r_2)}$ is continuous on $\mathrm{Ball}(b, r_2)$ and for every point y of F and for every point z of $E \times F$ such that $y \in \mathrm{Ball}(b, r_2)$ and $z = \langle g(y),\, y\rangle$ holds $g'(y) = -(\mathrm{Inv}\,\mathrm{partdiff}(f, z)\ \mathrm{w.r.t.}\ 1) \cdot (\mathrm{partdiff}(f, z)\ \mathrm{w.r.t.}\ 2)$ and for every point y of F and for every point z of $E \times F$ such that $y \in \mathrm{Ball}(b, r_2)$ and $z = \langle g(y),\, y\rangle$ holds $\mathrm{partdiff}(f, z)$ w.r.t. 1 is invertible, and

(vii) for every partial functions g_1, g_2 from F to E such that $\mathrm{dom}\, g_1 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_1 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f(g_1(y), y) = c$ and $\mathrm{dom}\, g_2 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_2 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f(g_2(y), y) = c$ holds $g_1 = g_2$.

Proof: Set $I = \mathrm{Exch}(F, E)$. Consider J being a linear operator from $E \times F$ into $F \times E$ such that $J = I^{-1}$ and J is one-to-one, onto, and isometric. Set $Z_1 = J^{\circ}Z$. Set $f_1 = f \cdot I$. $\mathrm{dom}\, f_1 = I^{-1}(\mathrm{dom}\, f)$. Reconsider $z_1 = \langle b,\, a\rangle$ as a point of $F \times E$. ${f_1}'_{\restriction Z_1}$ is continuous on Z_1. $f_1(b, a) = c$. $\mathrm{partdiff}(f, z)$ w.r.t. $1 = \mathrm{partdiff}(f_1, z_1)$ w.r.t. 2. Consider r_2, r_1 being real numbers such that $0 < r_2$ and $0 < r_1$ and $\mathrm{Ball}(b, r_2) \times \overline{\mathrm{Ball}}(a, r_1) \subseteq Z_1$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ there exists a point x of E such that $x \in \mathrm{Ball}(a, r_1)$ and $f_1(y, x) = c$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ for every points x_1, x_2 of E such that x_1, $x_2 \in \mathrm{Ball}(a, r_1)$ and $f_1(y, x_1) = c$ and $f_1(y, x_2) = c$ holds $x_1 = x_2$ and there exists a partial function g from F to E such that $\mathrm{dom}\, g = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g \subseteq \mathrm{Ball}(a, r_1)$ and g is continuous on $\mathrm{Ball}(b, r_2)$ and $g(b) = a$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_1(y, g(y)) = c$.

g is differentiable on $\mathrm{Ball}(b, r_2)$ and $g'_{\restriction \mathrm{Ball}(b, r_2)}$ is continuous on $\mathrm{Ball}(b, r_2)$ and for every point y of F and for every point z of $F \times E$ such that $y \in \mathrm{Ball}(b, r_2)$ and $z = \langle y,\, g(y)\rangle$ holds $g'(y) = -(\mathrm{Inv}\,\mathrm{partdiff}(f_1, z)\ \mathrm{w.r.t.}\ 2) \cdot (\mathrm{partdiff}(f_1, z)\ \mathrm{w.r.t.}\ 1)$ and for every point y of F and for every point z of $F \times E$ such that $y \in \mathrm{Ball}(b, r_2)$ and $z = \langle y,\, g(y)\rangle$ holds $\mathrm{partdiff}(f_1, z)$ w.r.t. 2 is invertible.

For every partial functions g_1, g_2 from F to E such that $\mathrm{dom}\, g_1 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_1 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that

$y \in \mathrm{Ball}(b, r_2)$ holds $f_1(y, g_1(y)) = c$ and $\mathrm{dom}\, g_2 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_2 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_1(y, g_2(y)) = c$ holds $g_1 = g_2$. For every object s such that $s \in \overline{\mathrm{Ball}}(a, r_1) \times \mathrm{Ball}(b, r_2)$ holds $s \in Z$. For every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ there exists a point x of E such that $x \in \mathrm{Ball}(a, r_1)$ and $f(x, y) = c$.

For every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ for every points x_1, x_2 of E such that x_1, $x_2 \in \mathrm{Ball}(a, r_1)$ and $f(x_1, y) = c$ and $f(x_2, y) = c$ holds $x_1 = x_2$. There exists a partial function g from F to E such that $\mathrm{dom}\, g = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g \subseteq \mathrm{Ball}(a, r_1)$ and g is continuous on $\mathrm{Ball}(b, r_2)$ and $g(b) = a$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f(g(y), y) = c$.

g is differentiable on $\mathrm{Ball}(b, r_2)$ and $g'_{\restriction \mathrm{Ball}(b, r_2)}$ is continuous on $\mathrm{Ball}(b, r_2)$ and for every point y of F and for every point z of $E \times F$ such that $y \in \mathrm{Ball}(b, r_2)$ and $z = \langle g(y), y \rangle$ holds $g'(y) = -(\mathrm{Inv}\, \mathrm{partdiff}(f, z)\, \text{w.r.t.}\, 1) \cdot (\mathrm{partdiff}(f, z)\, \text{w.r.t.}\, 2)$ and for every point y of F and for every point z of $E \times F$ such that $y \in \mathrm{Ball}(b, r_2)$ and $z = \langle g(y), y \rangle$ holds $\mathrm{partdiff}(f, z)\, \text{w.r.t.}\, 1$ is invertible.

For every partial functions g_1, g_2 from F to E such that $\mathrm{dom}\, g_1 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_1 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f(g_1(y), y) = c$ and $\mathrm{dom}\, g_2 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_2 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f(g_2(y), y) = c$ holds $g_1 = g_2$. □

(15) Let us consider non trivial real Banach spaces E, F, a subset D of E, a partial function f from E to F, a partial function f_1 from $E \times F$ to F, and a subset Z of $E \times F$. Suppose D is open and $\mathrm{dom}\, f = D$ and $D \neq \emptyset$ and f is differentiable on D and $f'_{\restriction D}$ is continuous on D and $Z = D \times$ (the carrier of F) and $\mathrm{dom}\, f_1 = Z$ and for every point s of E and for every point t of F such that $s \in D$ holds $f_1(s, t) = f_{/s} - t$. Then

(i) f_1 is differentiable on Z, and

(ii) ${f_1}'_{\restriction Z}$ is continuous on Z, and

(iii) for every point x of E and for every point y of F and for every point z of $E \times F$ such that $x \in D$ and $z = \langle x, y \rangle$ there exists a point I of the real norm space of bounded linear operators from F into F such that $I = \mathrm{id}_\alpha$ and $\mathrm{partdiff}(f_1, z)\, \text{w.r.t.}\, 1 = f'(x)$ and $\mathrm{partdiff}(f_1, z)\, \text{w.r.t.}\, 2 = -I$,

where α is the carrier of F.

Proof: Z is open. For every point z of $E \times F$ such that $z \in Z$ holds f_1 is partially differentiable in z w.r.t. 1 and $\mathrm{partdiff}(f_1, z)\, \text{w.r.t.}\, 1 = f'((z)_{\mathbf{1}})$. For every point x_0 of $E \times F$ and for every real number r such that $x_0 \in Z$

and $0 < r$ there exists a real number s such that $0 < s$ and for every point x_1 of $E \times F$ such that $x_1 \in Z$ and $\|x_1 - x_0\| < s$ holds $\|(f_1 \restriction^1 Z)_{/x_1} - (f_1 \restriction^1 Z)_{/x_0}\| < r$ by [8, (15)]. Reconsider $J = \mathrm{FuncUnit}(F)$ as a point of the real norm space of bounded linear operators from F into F.

For every point z of $E \times F$ such that $z \in Z$ holds f_1 is partially differentiable in z w.r.t. 2 and $\mathrm{partdiff}(f_1, z)$ w.r.t. $2 = -J$. For every point x_0 of $E \times F$ and for every real number r such that $x_0 \in Z$ and $0 < r$ there exists a real number s such that $0 < s$ and for every point x_1 of $E \times F$ such that $x_1 \in Z$ and $\|x_1 - x_0\| < s$ holds $\|(f_1 \restriction^2 Z)_{/x_1} - (f_1 \restriction^2 Z)_{/x_0}\| < r$. For every point x of E and for every point y of F and for every point z of $E \times F$ such that $x \in D$ and $z = \langle x, y \rangle$ there exists a point I of the real norm space of bounded linear operators from F into F such that $I = \mathrm{id}_\alpha$ and $\mathrm{partdiff}(f_1, z)$ w.r.t. $1 = f'(x)$ and $\mathrm{partdiff}(f_1, z)$ w.r.t. $2 = -I$, where α is the carrier of F. $\square$

(16) Let us consider non trivial real Banach spaces E, F, a subset Z of E, a partial function f from E to F, a point a of E, and a point b of F. Suppose Z is open and $\mathrm{dom}\, f = Z$ and f is differentiable on Z and $f'_{\restriction Z}$ is continuous on Z and $a \in Z$ and $f(a) = b$ and $f'(a)$ is invertible. Then there exist real numbers r_1, r_2 such that

(i) $0 < r_1$, and

(ii) $0 < r_2$, and

(iii) $\overline{\mathrm{Ball}}(a, r_1) \subseteq Z$, and

(iv) for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ there exists a point x of E such that $x \in \mathrm{Ball}(a, r_1)$ and $f_{/x} = y$, and

(v) for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ for every points x_1, x_2 of E such that x_1, $x_2 \in \mathrm{Ball}(a, r_1)$ and $f_{/x_1} = y$ and $f_{/x_2} = y$ holds $x_1 = x_2$, and

(vi) there exists a partial function g from F to E such that $\mathrm{dom}\, g = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g \subseteq \mathrm{Ball}(a, r_1)$ and g is continuous on $\mathrm{Ball}(b, r_2)$ and $g(b) = a$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_{/g_{/y}} = y$ and g is differentiable on $\mathrm{Ball}(b, r_2)$ and $g'_{\restriction \mathrm{Ball}(b, r_2)}$ is continuous on $\mathrm{Ball}(b, r_2)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $g'(y) = \mathrm{Inv}\, f'(g_{/y})$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f'(g_{/y})$ is invertible, and

(vii) for every partial functions g_1, g_2 from F to E such that $\mathrm{dom}\, g_1 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_1 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_{/g_1(y)} = y$ and $\mathrm{dom}\, g_2 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_2 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_{/g_2(y)} = y$ holds $g_1 = g_2$.

Proof: Reconsider $Z = D \times$ (the carrier of F) as a subset of $E \times F$. Z is open. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a point x of E and there exists a point y of F such that $\$_1 = \langle x,\, y\rangle$ and $\$_2 = f_{/x} - y$. For every object z such that $z \in Z$ there exists an object y such that $y \in$ the carrier of F and $\mathcal{P}[z, y]$.

Consider f_1 being a function from Z into the carrier of F such that for every object x such that $x \in Z$ holds $\mathcal{P}[x, f_1(x)]$. For every point s of E and for every point t of F such that $s \in D$ holds $f_1(s, t) = f_{/s} - t$. Reconsider $z = \langle a,\, b\rangle$ as a point of $E \times F$. f_1 is differentiable on Z. ${f_1}'_{\restriction Z}$ is continuous on Z. There exists a point J of the real norm space of bounded linear operators from F into F such that $J = \mathrm{id}_\alpha$ and $\mathrm{partdiff}(f_1, z)$ w.r.t. $1 = f'(a)$ and $\mathrm{partdiff}(f_1, z)$ w.r.t. $2 = -J$, where α is the carrier of F.

Consider r_1, r_2 being real numbers such that $0 < r_1$ and $0 < r_2$ and $\overline{\mathrm{Ball}}(a, r_1) \times \mathrm{Ball}(b, r_2) \subseteq Z$ and for every point x of F such that $x \in \mathrm{Ball}(b, r_2)$ there exists a point y of E such that $y \in \mathrm{Ball}(a, r_1)$ and $f_1(y, x) = 0_F$ and for every point x of F such that $x \in \mathrm{Ball}(b, r_2)$ for every points y_1, y_2 of E such that y_1, $y_2 \in \mathrm{Ball}(a, r_1)$ and $f_1(y_1, x) = 0_F$ and $f_1(y_2, x) = 0_F$ holds $y_1 = y_2$ and there exists a partial function g from F to E such that $\mathrm{dom}\, g = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g \subseteq \mathrm{Ball}(a, r_1)$ and g is continuous on $\mathrm{Ball}(b, r_2)$ and $g(b) = a$ and for every point x of F such that $x \in \mathrm{Ball}(b, r_2)$ holds $f_1(g(x), x) = 0_F$ and g is differentiable on $\mathrm{Ball}(b, r_2)$.

$g'_{\restriction \mathrm{Ball}(b, r_2)}$ is continuous on $\mathrm{Ball}(b, r_2)$ and for every point y of F and for every point z of $E \times F$ such that $y \in \mathrm{Ball}(b, r_2)$ and $z = \langle g(y),\, y\rangle$ holds $g'(y) = -(\mathrm{Inv}\, \mathrm{partdiff}(f_1, z)$ w.r.t. $1) \cdot (\mathrm{partdiff}(f_1, z)$ w.r.t. $2)$ and for every point y of F and for every point z of $E \times F$ such that $y \in \mathrm{Ball}(b, r_2)$ and $z = \langle g(y),\, y\rangle$ holds $\mathrm{partdiff}(f_1, z)$ w.r.t. 1 is invertible and for every partial functions g_1, g_2 from F to E such that $\mathrm{dom}\, g_1 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_1 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_1(g_1(y), y) = 0_F$ and $\mathrm{dom}\, g_2 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_2 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_1(g_2(y), y) = 0_F$ holds $g_1 = g_2$. For every object s such that $s \in \overline{\mathrm{Ball}}(a, r_1)$ holds $s \in D$. For every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ there exists a point x of E such that $x \in \mathrm{Ball}(a, r_1)$ and $f_{/x} = y$. For every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ for every points x_1, x_2 of E such that x_1, $x_2 \in \mathrm{Ball}(a, r_1)$ and $f_{/x_1} = y$ and $f_{/x_2} = y$ holds $x_1 = x_2$.

There exists a partial function g from F to E such that $\mathrm{dom}\, g = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g \subseteq \mathrm{Ball}(a, r_1)$ and g is continuous on $\mathrm{Ball}(b, r_2)$ and $g(b) = a$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_{/g_{/y}} = y$ and g is differentiable on $\mathrm{Ball}(b, r_2)$ and $g'_{\restriction \mathrm{Ball}(b, r_2)}$ is continuous on $\mathrm{Ball}(b, r_2)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds

$g'(y) = \mathrm{Inv}\, f'(g_{/y})$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f'(g_{/y})$ is invertible by (15), [5, (26),(27)]. For every partial functions g_1, g_2 from F to E such that $\mathrm{dom}\, g_1 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_1 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_{/g_1(y)} = y$ and $\mathrm{dom}\, g_2 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_2 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_{/g_2(y)} = y$ holds $g_1 = g_2$. □

4. Inverse Function Theorem for Class of C^1 Functions

Now we state the propositions:

(17) Let us consider non trivial real Banach spaces E, F, a subset Z of E, a partial function f from E to F, a point a of E, and a point b of F. Suppose Z is open and $\mathrm{dom}\, f = Z$ and f is differentiable on Z and $f'_{\restriction Z}$ is continuous on Z and $a \in Z$ and $f(a) = b$ and $f'(a)$ is invertible.

Then there exists a subset A of E and there exists a subset B of F and there exists a partial function g from F to E such that A is open and B is open and $A \subseteq \mathrm{dom}\, f$ and $a \in A$ and $b \in B$ and $f^\circ A = B$ and $\mathrm{dom}\, g = B$ and $\mathrm{rng}\, g = A$ and $\mathrm{dom}(f\restriction A) = A$ and $\mathrm{rng}(f\restriction A) = B$ and $f\restriction A$ is one-to-one and g is one-to-one and $g = (f\restriction A)^{-1}$ and $f\restriction A = g^{-1}$ and $g(b) = a$ and g is continuous on B and differentiable on B and $g'_{\restriction B}$ is continuous on B and for every point y of F such that $y \in B$ holds $f'(g_{/y})$ is invertible and for every point y of F such that $y \in B$ holds $g'(y) = \mathrm{Inv}\, f'(g_{/y})$.

Proof: Consider r_1, r_2 being real numbers such that $0 < r_1$ and $0 < r_2$ and $\overline{\mathrm{Ball}}(a, r_1) \subseteq Z$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ there exists a point x of E such that $x \in \mathrm{Ball}(a, r_1)$ and $f_{/x} = y$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ for every points x_1, x_2 of E such that $x_1, x_2 \in \mathrm{Ball}(a, r_1)$ and $f_{/x_1} = y$ and $f_{/x_2} = y$ holds $x_1 = x_2$ and there exists a partial function g from F to E such that $\mathrm{dom}\, g = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g \subseteq \mathrm{Ball}(a, r_1)$ and g is continuous on $\mathrm{Ball}(b, r_2)$ and $g(b) = a$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_{/g_{/y}} = y$.

g is differentiable on $\mathrm{Ball}(b, r_2)$ and $g'_{\restriction \mathrm{Ball}(b, r_2)}$ is continuous on $\mathrm{Ball}(b, r_2)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $g'(y) = \mathrm{Inv}\, f'(g_{/y})$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f'(g_{/y})$ is invertible and for every partial functions g_1, g_2 from F to E such that $\mathrm{dom}\, g_1 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_1 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_{/g_1(y)} = y$ and $\mathrm{dom}\, g_2 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, g_2 \subseteq \mathrm{Ball}(a, r_1)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_{/g_2(y)} = y$ holds $g_1 = g_2$.

Consider I_1 being a partial function from F to E such that $\mathrm{dom}\, I_1 = \mathrm{Ball}(b, r_2)$ and $\mathrm{rng}\, I_1 \subseteq \mathrm{Ball}(a, r_1)$ and I_1 is continuous on $\mathrm{Ball}(b, r_2)$

and $I_1(b) = a$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f_{/{I_1}_{/y}} = y$ and I_1 is differentiable on $\mathrm{Ball}(b, r_2)$ and ${I_1}'_{\restriction \mathrm{Ball}(b,r_2)}$ is continuous on $\mathrm{Ball}(b, r_2)$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds ${I_1}'(y) = \mathrm{Inv}\, f'({I_1}_{/y})$ and for every point y of F such that $y \in \mathrm{Ball}(b, r_2)$ holds $f'({I_1}_{/y})$ is invertible. Set $B = \mathrm{Ball}(b, r_2)$. Set $A = \mathrm{Ball}(a, r_1) \cap f^{-1}(B)$. For every object s such that $s \in B$ holds $s \in f^\circ \mathrm{Ball}(a, r_1)$. $f^{-1}(B)$ is open. For every object s, $s \in f^\circ A$ iff $s \in B$.

For every objects y_1, y_2 such that y_1, $y_2 \in \mathrm{dom}\, I_1$ and $I_1(y_1) = I_1(y_2)$ holds $y_1 = y_2$. For every objects x_1, x_2 such that x_1, $x_2 \in \mathrm{dom}(f\restriction A)$ and $(f\restriction A)(x_1) = (f\restriction A)(x_2)$ holds $x_1 = x_2$. For every object x such that $x \in \mathrm{dom}((f\restriction A)^{-1})$ holds $((f\restriction A)^{-1})(x) = I_1(x)$. □

(18) Let us consider non trivial real Banach spaces E, F, a subset Z of E, a partial function f from E to F, a point a of E, and a point b of F. Suppose Z is open and $\mathrm{dom}\, f = Z$ and f is differentiable on Z and $f'_{\restriction Z}$ is continuous on Z and $a \in Z$ and $f(a) = b$ and $f'(a)$ is invertible. Let us consider a real number r_1. Suppose $0 < r_1$. Then there exists a real number r_2 such that

(i) $0 < r_2$, and

(ii) $\mathrm{Ball}(b, r_2) \subseteq f^\circ \mathrm{Ball}(a, r_1)$.

The theorem is a consequence of (17) and (1).

(19) Let us consider non trivial real Banach spaces E, F, a subset Z of E, and a partial function f from E to F. Suppose Z is open and $\mathrm{dom}\, f = Z$ and f is differentiable on Z and $f'_{\restriction Z}$ is continuous on Z and for every point x of E such that $x \in Z$ holds $f'(x)$ is invertible. Then

(i) for every point x of E and for every real number r_1 such that $x \in Z$ and $0 < r_1$ there exists a point y of F and there exists a real number r_2 such that $y = f(x)$ and $0 < r_2$ and $\mathrm{Ball}(y, r_2) \subseteq f^\circ \mathrm{Ball}(x, r_1)$, and

(ii) $f^\circ Z$ is open.

Proof: For every point x of E and for every real number r_1 such that $x \in Z$ and $0 < r_1$ there exists a point y of F and there exists a real number r_2 such that $y = f(x)$ and $0 < r_2$ and $\mathrm{Ball}(y, r_2) \subseteq f^\circ \mathrm{Ball}(x, r_1)$. For every point y of F such that $y \in f^\circ Z$ there exists a real number r such that $0 < r$ and $\mathrm{Ball}(y, r) \subseteq f^\circ Z$ by [7, (20)]. □

Acknowledgement: The authors would like to express their gratitude to Prof. Yasunari Shidama for his support and encouragement.

References

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

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Bruce K. Driver. *Analysis Tools with Applications.* Springer, Berlin, 2003.

[4] Hiroshi Imura, Morishige Kimura, and Yasunari Shidama. The differentiable functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):321–327, 2004.

[5] Kazuhisa Nakasho. Invertible operators on Banach spaces. *Formalized Mathematics*, 27 (**2**):107–115, 2019. doi:10.2478/forma-2019-0012.

[6] Kazuhisa Nakasho and Yasunari Shidama. Implicit function theorem. Part II. *Formalized Mathematics*, 27(**2**):117–131, 2019. doi:10.2478/forma-2019-0013.

[7] Kazuhisa Nakasho, Yuichi Futa, and Yasunari Shidama. Implicit function theorem. Part I. *Formalized Mathematics*, 25(**4**):269–281, 2017. doi:10.1515/forma-2017-0026.

[8] Hideki Sakurai, Hiroyuki Okazaki, and Yasunari Shidama. Banach's continuous inverse theorem and closed graph theorem. *Formalized Mathematics*, 20(**4**):271–274, 2012. doi:10.2478/v10037-012-0032-y.

[9] Laurent Schwartz. *Théorie des ensembles et topologie, tome 1. Analyse.* Hermann, 1997.

[10] Laurent Schwartz. *Calcul différentiel, tome 2. Analyse.* Hermann, 1997.

Accepted March 30, 2021

FORMALIZED MATHEMATICS
Vol. 29, No. 1, Pages 21–38, 2021
DOI: 10.2478/forma-2021-0003

sciendo
https://sciendo.com/journal/forma

Miscellaneous Graph Preliminaries. Part I

Sebastian Koch
Johannes Gutenberg University
Mainz, Germany[1]

Summary. This article contains many auxiliary theorems which were missing in the Mizar Mathematical Library to the best of the author's knowledge. Most of them regard graph theory as formalized in the GLIB series and are needed in upcoming articles.

MSC: 05C99 68V20

Keywords: graph

MML identifier: GLIBPRE1, version: 8.1.11 5.65.1394

0. Introduction

A generalized approach to graph theory as it was done in [2, 4] in contrast to [9, 3] is rather uncommon. To avoid duplication of the same theorems in different formalization frameworks in the Mizar Mathematical Library [1], a generalized approach to formalization is preferable (cf. [8, 7]). However, due to the sheer amount of "obvious facts" such an approach brings with it, it is only natural some of them not immediately needed slip the initial formalization process. This article, like its precedessor [5], aims to fill some of the gaps that emerged.

Many theorems in this article regard the property of a walk in a graph to be the shortest one, which have been rather neglected in the author's work on graphs in Mizar until now. Another good portion is concered with theorems about graph mappings which are missing from [7]. Further worthy of note is the theorem that combines adding an edge or adjacent vertex with the reversal of

[1] The author is enrolled in the Johannes Gutenberg University in Mayence, Germany, mailto: skoch02@students.uni-mainz.de

the edge to be added and the two theorems noting that a connected graph is unicyclic if and only if the connected subgraph it can be constructed from by adding an edge is a tree.

1. Preliminaries not Directly Related to Graphs

Now we state the propositions:

(1) Let us consider sets X_1, X_2, X_3, X_4, X_5, X_6, X_7. Then it is not true that $X_1 \in X_2$ and $X_2 \in X_3$ and $X_3 \in X_4$ and $X_4 \in X_5$ and $X_5 \in X_6$ and $X_6 \in X_7$ and $X_7 \in X_1$.

(2) Let us consider sets X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8. Then it is not true that $X_1 \in X_2$ and $X_2 \in X_3$ and $X_3 \in X_4$ and $X_4 \in X_5$ and $X_5 \in X_6$ and $X_6 \in X_7$ and $X_7 \in X_8$ and $X_8 \in X_1$.

One can verify that every function which is one-to-one and constant is also trivial. Now we state the proposition:

(3) Let us consider a function f. Then f is non empty and constant if and only if there exists an object y such that $\operatorname{rng} f = \{y\}$.

Let X be a set. Observe that there exists a many sorted set indexed by X which is one-to-one and there exists an X-defined function which is total and one-to-one.

Let X be a non empty set. One can check that there exists an X-defined function which is total, one-to-one, and non empty.

The scheme *LambdaDf* deals with non empty sets $\mathcal{C}$, $\mathcal{D}$ and a unary functor $\mathcal{F}$ yielding an object and states that

(Sch. 1) There exists a function f from $\mathcal{C}$ into $\mathcal{D}$ such that for every element x of $\mathcal{C}$, $f(x) = \mathcal{F}(x)$

provided

- for every element x of $\mathcal{C}$, $\mathcal{F}(x) \in \mathcal{D}$.

Now we state the proposition:

(4) Let us consider a one-to-one function f, and an object y. Suppose $\operatorname{rng} f = \{y\}$. Then there exists an object x such that $f = x \dot{\longmapsto} y$.

Let f be a one-to-one function. Note that $f^{\smile}$ is one-to-one. Let f be a function and g be a one-to-one function. Let us observe that $\langle f, g \rangle$ is one-to-one and $\langle g, f \rangle$ is one-to-one. Now we state the propositions:

(5) Let us consider an empty function f. Then ${}^{\circ}f = \emptyset \dot{\longmapsto} \emptyset$.

Let f be a one-to-one function. One can check that ${}^{\circ}f$ is one-to-one.

(6) Let us consider a non empty, one-to-one function f, and a non empty subset X of $2^{\operatorname{dom} f}$. Then $\operatorname{rng}({}^\circ f{\restriction}X) =$ the set of all $f^\circ x$ where x is an element of X.

(7) Let us consider a function f, and one-to-one functions g, h. Suppose $h = f{+\cdot}g$. Then $h^{-1}{\restriction}\operatorname{rng} g = g^{-1}$.

(8) Let us consider functions f, g, h. If $\operatorname{rng} f \subseteq \operatorname{dom} h$, then $(g{+\cdot}h)\cdot f = h\cdot f$.

(9) Let us consider a function f, and a one-to-one function g. Then $(f{+\cdot}g)\cdot(g^{-1}) = \mathrm{id}_{\operatorname{rng} g}$. The theorem is a consequence of (8).

Observe that every binary relation which is reflexive and connected is also strongly connected. Now we state the propositions:

(10) Let us consider a set X, and a binary relation R on X. Then R is antisymmetric if and only if $R \setminus (\mathrm{id}_X)$ is asymmetric.

(11) Let us consider a set X. Suppose X is mutually-disjoint. Then $X \setminus \{\emptyset\}$ is a partition of $\bigcup X$.

Let X be a set. Let us note that every partition of X is mutually-disjoint.

(12) Let us consider cardinal numbers M, N, and a function f. Suppose $M \subseteq \overline{\overline{\operatorname{dom} f}}$ and for every object x such that $x \in \operatorname{dom} f$ holds $N \subseteq \overline{\overline{f(x)}}$. Then $M \cdot N \subseteq \sum \operatorname{Card} f$.

(13) Let us consider sets X, x. Suppose $x \in X$. Then $(\text{disjoint} \operatorname{Card} \mathrm{id}_X)(x) = \overline{\overline{x}} \times \{x\}$.

(14) Let us consider a set X. Suppose X is mutually-disjoint. Then $\sum \operatorname{Card} \mathrm{id}_X = \overline{\overline{\bigcup X}}$. The theorem is a consequence of (11) and (13).

(15) Let us consider a set X, and cardinal numbers M, N. Suppose X is mutually-disjoint and $M \subseteq \overline{\overline{X}}$ and for every set Y such that $Y \in X$ holds $N \subseteq \overline{\overline{Y}}$. Then $M \cdot N \subseteq \overline{\overline{\bigcup X}}$. The theorem is a consequence of (12) and (14).

(16) Let us consider a compatible, functional set F. Suppose for every function f_1 such that $f_1 \in F$ holds f_1 is one-to-one and for every function f_2 such that $f_2 \in F$ and $f_1 \neq f_2$ holds $\operatorname{rng} f_1$ misses $\operatorname{rng} f_2$. Then $\bigcup F$ is one-to-one.

2. Into GLIB_000

Let G be a non trivial graph. Observe that there exists a subset of the vertices of G which is non empty and proper. Now we state the propositions:

(17) Let us consider a graph G, and a set X. Then $G.\mathrm{edgesBetween}(X, X) = G.\mathrm{edgesBetween}(X)$.

(18) Let us consider a graph G. Then G is trivial if and only if the vertices of G is trivial.

(19) Let us consider a graph G_1. Then every subgraph of G_1 is a subgraph of G_1 induced by the vertices of G_2 and the edges of G_2.

(20) Let us consider graphs G_1, G_2, and a spanning subgraph G_3 of G_1. If $G_2 \approx G_3$, then G_2 is a spanning subgraph of G_1.

(21) Let us consider a graph G, and an object e. Suppose $e \in$ the edges of G. Then $e \in G.\mathrm{edgesBetween}(\{(\text{the source of } G)(e), (\text{the target of } G)(e)\})$.

(22) Let us consider a graph G. Then $G \approx \mathrm{createGraph}(\text{the vertices of } G, \text{the edges of } G, \text{the source of } G, \text{the target of } G)$.

(23) Let us consider a graph G, and a vertex v of G. Then v is endvertex if and only if $v.\mathrm{degree}() = 1$.
Proof: $v.\mathrm{inDegree}() = 1$ and $v.\mathrm{outDegree}() = 0$ or $v.\mathrm{inDegree}() = 0$ and $v.\mathrm{outDegree}() = 1$. □

(24) Let us consider a loopless graph G, and a vertex v of G. Then

(i) $v.\mathrm{inNeighbors}() \subseteq (\text{the vertices of } G) \setminus \{v\}$, and

(ii) $v.\mathrm{outNeighbors}() \subseteq (\text{the vertices of } G) \setminus \{v\}$, and

(iii) $v.\mathrm{allNeighbors}() \subseteq (\text{the vertices of } G) \setminus \{v\}$.

(25) Let us consider a graph G. Suppose for every vertex v of G, $v.\mathrm{inNeighbors}() \subseteq (\text{the vertices of } G) \setminus \{v\}$ or $v.\mathrm{outNeighbors}() \subseteq (\text{the vertices of } G) \setminus \{v\}$ or $v.\mathrm{allNeighbors}() \subseteq (\text{the vertices of } G) \setminus \{v\}$. Then G is loopless.

Let X be a set and G be a graph. Let us note that $X \longmapsto G$ is graph-yielding.

Let x be an object. Let us note that $x \stackrel{\cdot}{\longmapsto} G$ is graph-yielding.

Let X be a set. Let us note that there exists a many sorted set indexed by X which is graph-yielding.

Let X be a non empty set. One can verify that there exists a many sorted set indexed by X which is non empty and graph-yielding.

Let f be a graph-yielding many sorted set indexed by X and x be an element of X. One can verify that the functor $f(x)$ yields a graph.

3. Into GLIB_001

Let G be a graph and P be a path of G. One can verify that $P.\mathrm{vertexSeq}() \restriction P.\mathrm{length}()$ is one-to-one. Now we state the propositions:

(26) Let us consider a graph G, and a path P of G. Then $P.\mathrm{length}() \subseteq G.\mathrm{order}()$.

(27) Let us consider a graph G, and a trail T of G. Then $T.\mathrm{length}() \subseteq G.\mathrm{size}()$.

(28) Let us consider a graph G, and a walk W of G. Suppose $\operatorname{len} W = 3$ or W.length() $= 1$. Then there exists an object e such that

(i) e joins W.first() and W.last() in G, and

(ii) $W = G$.walkOf(W.first(), e, W.last()).

(29) Let us consider a graph G, a walk W of G, and an object e. Suppose $e \in W$.edges() and $e \notin G$.loops() and W is circuit-like. Then there exists an object e_0 such that

(i) $e_0 \in W$.edges(), and

(ii) $e_0 \neq e$.

Proof: Consider n being an odd element of $\mathbb{N}$ such that $n < \operatorname{len} W$ and $W(n+1) = e$. $\operatorname{len} W > 3$. □

(30) Let us consider a graph G, a path P of G, and odd elements n, m of $\mathbb{N}$. Suppose $n < m \leqslant \operatorname{len} P$ and ($n \neq 1$ or $m \neq \operatorname{len} P$). Then P.cut(n, m) is open.

(31) Let us consider a graph G, a closed walk W of G, and an odd element n of $\mathbb{N}$. Suppose $n < \operatorname{len} W$. Then

(i) (W.cut($n+2, \operatorname{len} W$)).append(($W$.cut($1, n$))) is a walk from $W(n+2)$ to $W(n)$, and

(ii) if W is trail-like, then (W.cut($n+2, \operatorname{len} W$)).edges() misses ($W$.cut($1$, n)).edges() and ((W.cut($n+2, \operatorname{len} W$)).append(($W$.cut($1, n$)))).edges () $= W$.edges() $\setminus \{W(n+1)\}$, and

(iii) if W is path-like, then (W.cut($n+2, \operatorname{len} W$)).vertices()$\cap$($W$.cut($1, n$)) .vertices() $= \{W$.first()$\}$ and if $W(n+1) \notin G$.loops(), then (W.cut($n+ 2, \operatorname{len} W$)).append(($W$.cut($1, n$))) is open and ($W$.cut($n+2, \operatorname{len} W$)) .append(($W$.cut($1, n$))) is path-like.

Proof: Set $W_7 = W$.cut($n+2, \operatorname{len} W$). Set $W_8 = W$.cut($1, n$). Set $W' = W_7$.append(W_8). If W is trail-like, then W_7.edges() misses W_8.edges() and W'.edges() $= W$.edges() $\setminus \{W(n+1)\}$. If $W(n+1) \notin G$.loops(), then W' is open. □

(32) Let us consider a graph G, a walk W_1 of G, and objects e, x, y. Suppose e joins x and y in G and $e \in W_1$.edges() and W_1 is cycle-like. Then there exists a path W_2 of G such that

(i) W_2 is a walk from x to y, and

(ii) W_2.edges() $= W_1$.edges() $\setminus \{e\}$, and

(iii) if $e \notin G$.loops(), then W_2 is open.

The theorem is a consequence of (31).

(33) Let us consider graphs G_1, G_2, a walk W_1 of G_1, and a walk W_2 of G_2. Then $\operatorname{len} W_1 \leqslant \operatorname{len} W_2$ if and only if W_1.length() $\leqslant$ W_2.length().

(34) Let us consider a graph G, and a walk W of G. Then W.length() $=$ W.reverse().length().

(35) Let us consider a graph G, a walk W of G, and an object e. If $e \notin$ W.last().edgesInOut(), then W.addEdge(e) $= W$.

(36) Let us consider a graph G, a walk W of G, and objects e, x. Suppose e joins W.last() and x in G. Then (W.addEdge(e)).length() $=$ W.length()$+$ 1.

(37) Let us consider a graph G_1, a set E, a subgraph G_2 of G_1 with edges E removed, and a walk W_1 of G_1. If W_1.edges() misses E, then W_1 is a walk of G_2.

4. Into GLIB_002

Let us consider graphs G_1, G_2 and a component G_3 of G_1. Now we state the propositions:

(38) If $G_2 \approx G_3$, then G_2 is a component of G_1.

(39) If $G_1 \approx G_2$, then G_3 is a component of G_2.

Now we state the proposition:

(40) Let us consider a tree-like graph G, and a spanning subgraph H of G. If H is connected, then $G \approx H$.

Proof: The edges of $G \subseteq$ the edges of H. □

Let G be a graph. Note that every element of G.componentSet() is non empty and G.componentSet() is mutually-disjoint.

5. Into CHORD

Now we state the propositions:

(41) Let us consider a graph G, and vertices v, w of G. Then v and w are adjacent if and only if $w \in v$.allNeighbors().

(42) Let us consider a graph G, a set S, and a vertex v of G. Suppose $v \notin S$ and S meets G.reachableFrom(v). Then G.adjacentSet(S) $\neq \emptyset$.

Proof: Consider w being an object such that $w \in S$ and $w \in G$.reachable From(v). Consider W being a walk of G such that W is a walk from v to w. There exists an odd natural number n such that $n < \operatorname{len} W$ and $W(n) \notin S$ and $W(n+2) \in S$. Consider n being an odd natural number such that $n < \operatorname{len} W$ and $W(n) \notin S$ and $W(n+2) \in S$. □

Let G be a non trivial, connected graph and S be a non empty, proper subset of the vertices of G. One can check that G.adjacentSet(S) is non empty.

Now we state the propositions:

(43) Let us consider a complete graph G, and a vertex v of G. Then (the vertices of $G) \setminus \{v\} \subseteq v$.allNeighbors().

(44) Let us consider a loopless, complete graph G, and a vertex v of G. Then v.allNeighbors() = (the vertices of $G) \setminus \{v\}$. The theorem is a consequence of (43).

(45) Let us consider a simple, complete graph G, and a vertex v of G. Then v.degree() $+ 1 = G$.order(). The theorem is a consequence of (44).

Let G be a graph. Observe that every walk of G which is trivial is also minimum length and there exists a walk of G which is minimum length and path-like.

Let W be a minimum length walk of G. One can check that W.reverse() is minimum length.

Now we state the propositions:

(46) Let us consider a graph G_1, a subgraph G_2 of G_1, a walk W_1 of G_1, and a walk W_2 of G_2. If $W_1 = W_2$ and W_1 is minimum length, then W_2 is minimum length.

(47) Let us consider a graph G, a vertex v of G, and a walk W of G. Suppose W is a walk from v to v. Then W is minimum length if and only if $W = G$.walkOf(v).

(48) Let us consider graphs G_1, G_2, a walk W_1 of G_1, and a walk W_2 of G_2. Suppose $G_1 \approx G_2$ and $W_1 = W_2$ and W_1 is minimum length. Then W_2 is minimum length.

6. Into GLIB_006

Now we state the propositions:

(49) Let us consider graphs G_1, G_2. Suppose the vertices of $G_2 \subseteq$ the vertices of G_1 and for every objects e, x, y such that e joins x to y in G_2 holds e joins x to y in G_1. Then

(i) G_2 is a subgraph of G_1, and

(ii) G_1 is a supergraph of G_2.

(50) Let us consider a graph G_1, a subgraph G_3 of G_1, objects v, e, w, and a supergraph G_2 of G_3 extended by e between vertices v and w. If e joins v to w in G_1, then G_2 is a subgraph of G_1.

(51) Let us consider a tree-like graph G, vertices v_1, v_2 of G, an object e, and a supergraph H of G extended by e between vertices v_1 and v_2. Suppose $e \notin$ the edges of G. Then

  (i) H is not acyclic, and

  (ii) for every walks W_1, W_2 of H such that W_1 is cycle-like and W_2 is cycle-like holds W_1.edges() $=$ W_2.edges().

PROOF: $e \in W_1$.edges(). $e \in W_2$.edges(). Consider W_3 being a path of H such that W_3 is a walk from v_1 to v_2 and W_3.edges() $=$ W_1.edges() $\setminus \{e\}$ and if $e \notin H$.loops(), then W_3 is open. Consider W_4 being a path of H such that W_4 is a walk from v_1 to v_2 and W_4.edges() $=$ W_2.edges() $\setminus \{e\}$ and if $e \notin H$.loops(), then W_4 is open. □

(52) Let us consider a connected graph G. Suppose there exist vertices v_1, v_2 of G and there exists an object e and there exists a supergraph H of G extended by e between vertices v_1 and v_2 such that $e \notin$ the edges of G and for every walks W_1, W_2 of H such that W_1 is cycle-like and W_2 is cycle-like holds W_1.edges() $=$ W_2.edges(). Then G is tree-like.
PROOF: G is acyclic by [6, (75),(24),(105)], [8, (16)]. □

(53) Let us consider a graph G_2, objects v, e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Then

  (i) the vertices of $G_1 \subseteq$ (the vertices of G_2) $\cup \{v, w\}$, and

  (ii) the edges of $G_1 \subseteq$ (the edges of G_2) $\cup \{e\}$.

(54) Let us consider a graph G_2, vertices v, v_2 of G_2, objects e, w, a supergraph G_1 of G_2 extended by v, w and e between them, and a vertex v_1 of G_1. Suppose $v_1 = v_2$ and $v \notin G_2$.reachableFrom(v_2) and $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2. Then G_1.reachableFrom(v_1) $=$ G_2.reachableFrom(v_2).

(55) Let us consider a graph G_2, vertices w, v_2 of G_2, objects v, e, a supergraph G_1 of G_2 extended by v, w and e between them, and a vertex v_1 of G_1. Suppose $v_1 = v_2$ and $w \notin G_2$.reachableFrom(v_2) and $e \notin$ the edges of G_2 and $v \notin$ the vertices of G_2. Then G_1.reachableFrom(v_1) $=$ G_2.reachableFrom(v_2).

(56) Let us consider a graph G_2, a vertex v of G_2, objects e, w, a supergraph G_1 of G_2 extended by v, w and e between them, and a vertex v_1 of G_1. Suppose $v_1 = v$ and $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2. Then G_1.reachableFrom(v_1) $=$ (G_2.reachableFrom(v)) $\cup \{w\}$.

(57) Let us consider a graph G_2, objects v, e, a vertex w of G_2, a supergraph G_1 of G_2 extended by v, w and e between them, and a vertex v_1 of G_1.

Suppose $v_1 = w$ and $e \notin$ the edges of G_2 and $v \notin$ the vertices of G_2. Then G_1.reachableFrom(v_1) $=$ (G_2.reachableFrom(w)) $\cup \{v\}$.

(58) Let us consider a graph G_2, a vertex v of G_2, objects e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Suppose $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2. Then G_1.componentSet() $=$ G_2.componentSet() $\setminus \{G_2$.reachableFrom(v)$\} \cup \{(G_2$.reachableFrom(v)) $\cup$ $\{w\}\}$. The theorem is a consequence of (54) and (56).

(59) Let us consider a graph G_2, objects v, e, a vertex w of G_2, and a supergraph G_1 of G_2 extended by v, w and e between them. Suppose $e \notin$ the edges of G_2 and $v \notin$ the vertices of G_2. Then G_1.componentSet() $=$ G_2.componentSet() $\setminus \{G_2$.reachableFrom(w)$\} \cup \{(G_2$.reachableFrom(w)) $\cup$ $\{v\}\}$. The theorem is a consequence of (55) and (57).

(60) Let us consider a graph G_2, objects v, e, w, a supergraph G_1 of G_2 extended by v, w and e between them, a walk W_1 of G_1, and a walk W_2 of G_2. If $W_1 = W_2$ and W_2 is minimum length, then W_1 is minimum length. The theorem is a consequence of (48).

(61) Let us consider a non trivial, connected graph G_1, and a non spanning subgraph G_2 of G_1. Then there exist objects v, e, w such that

(i) $v \neq w$, and

(ii) e joins v to w in G_1, and

(iii) $e \notin$ the edges of G_2, and

(iv) every supergraph of G_2 extended by v, w and e between them is a subgraph of G_1, and

(v) $v \in$ the vertices of G_2 and $w \notin$ the vertices of G_2 or $v \notin$ the vertices of G_2 and $w \in$ the vertices of G_2.

Proof: Set $S =$ the vertices of G_2. Set $v_0 =$ the element of G_1.adjacentSet (S). Consider w_0 being a vertex of G_1 such that $w_0 \in S$ and v_0 and w_0 are adjacent. Consider e being an object such that e joins v_0 and w_0 in G_1. $e \notin$ the edges of G_2. □

(62) Let us consider a graph G_2, a vertex v of G_2, objects e, w, x, a supergraph G_1 of G_2 extended by v, w and e between them, a walk W_1 of G_1, and a walk W_2 of G_2. Suppose $W_1 = W_2$ and W_2 is minimum length and a walk from x to v and $e \notin$ the edges of G_2. Then W_1.addEdge(e) is minimum length. The theorem is a consequence of (60) and (35).

(63) Let us consider a graph G_2, objects v, e, x, a vertex w of G_2, a supergraph G_1 of G_2 extended by v, w and e between them, a walk W_1 of G_1, and a walk W_2 of G_2. Suppose $W_1 = W_2$ and W_2 is minimum length and a walk

from x to w and $e \notin$ the edges of G_2. Then W_1.addEdge(e) is minimum length. The theorem is a consequence of (60) and (35).

Observe that there exists a graph-yielding function which is non empty, non non-directed-multi, and non non-multi and there exists a graph-yielding function which is non empty, non acyclic, and non connected and there exists a graph-yielding function which is non empty and non edgeless and there exists a graph-yielding function which is non empty and non loopfull.

7. Into GLIB_007

Now we state the propositions:

(64) Let us consider graphs G_2, G_3, sets V, E, a supergraph G_1 of G_3 extended by the vertices from V, and a graph G_4 given by reversing directions of the edges E of G_3. Then G_2 is a graph given by reversing directions of the edges E of G_1 if and only if G_2 is a supergraph of G_4 extended by the vertices from V. The theorem is a consequence of (49).

(65) Let us consider graphs G_2, G_3, objects v, e, w, and a supergraph G_1 of G_3 extended by e between vertices v and w. Suppose $e \notin$ the edges of G_3. Then G_2 is a graph given by reversing directions of the edges $\{e\}$ of G_1 if and only if G_2 is a supergraph of G_3 extended by e between vertices w and v. The theorem is a consequence of (49).

(66) Let us consider graphs G_2, G_3, objects v, e, w, and a supergraph G_1 of G_3 extended by v, w and e between them. Suppose $e \notin$ the edges of G_3. Then G_2 is a graph given by reversing directions of the edges $\{e\}$ of G_1 if and only if G_2 is a supergraph of G_3 extended by w, v and e between them. The theorem is a consequence of (65).

(67) Let us consider a graph G_1, a set E, a graph G_2 given by reversing directions of the edges E of G_1, a walk W_1 of G_1, and a walk W_2 of G_2. If $W_1 = W_2$, then W_1 is minimum length iff W_2 is minimum length.

8. Into GLIB_008

Now we state the proposition:

(68) Let us consider an edgeless graph G_1, and a graph G_2. Then G_1 is a subgraph of G_2 if and only if the vertices of $G_1 \subseteq$ the vertices of G_2.

One can check that there exists a graph which is loopless and non edgeless.

9. Into GLIB_009

Let G be a graph. Note that there exists a subgraph of G which is plain, spanning, and acyclic and there exists a subgraph of G which is plain and tree-like and there exists a component of G which is plain.

Now we state the proposition:

(69) Let us consider a plain graph G. Then $G = \text{createGraph}(\text{the vertices of } G, \text{the edges of } G, \text{the source of } G, \text{the target of } G)$.

Let us consider a graph G and a subgraph H of G with loops removed. Now we state the propositions:

(70) the edges of $G = G.\text{loops}()$ if and only if H is edgeless.

(71) Every loopless subgraph of G is a subgraph of H.
Proof: (The edges of H') $\cap\, G.\text{loops}() = \emptyset$. □

(72) Let us consider a graph G_1, and a subgraph G_2 of G_1 with loops removed. Then every minimum length walk of G_1 is a walk of G_2. The theorem is a consequence of (37).

(73) Let us consider a graph G_1, a subgraph G_2 of G_1 with loops removed, a walk W_1 of G_1, and a walk W_2 of G_2. If $W_1 = W_2$, then W_1 is minimum length iff W_2 is minimum length. The theorem is a consequence of (46), (37), and (47).

(74) Let us consider a graph G_1, a subgraph G_2 of G_1 with loops removed, vertices v_1, w_1 of G_1, and vertices v_2, w_2 of G_2. Suppose $v_1 = v_2$ and $w_1 = w_2$ and $v_1 \neq w_1$. Then v_1 and w_1 are adjacent if and only if v_2 and w_2 are adjacent. The theorem is a consequence of (41).

(75) Let us consider a graph G_1, a subgraph G_2 of G_1 with parallel edges removed, vertices v_1, w_1 of G_1, and vertices v_2, w_2 of G_2. Suppose $v_1 = v_2$ and $w_1 = w_2$. Then v_1 and w_1 are adjacent if and only if v_2 and w_2 are adjacent. The theorem is a consequence of (41).

(76) Let us consider a graph G_1, a subgraph G_2 of G_1 with directed-parallel edges removed, vertices v_1, w_1 of G_1, and vertices v_2, w_2 of G_2. Suppose $v_1 = v_2$ and $w_1 = w_2$. Then v_1 and w_1 are adjacent if and only if v_2 and w_2 are adjacent. The theorem is a consequence of (41).

(77) Let us consider a graph G_1, a simple graph G_2 of G_1, vertices v_1, w_1 of G_1, and vertices v_2, w_2 of G_2. Suppose $v_1 = v_2$ and $w_1 = w_2$ and $v_1 \neq w_1$. Then v_1 and w_1 are adjacent if and only if v_2 and w_2 are adjacent. The theorem is a consequence of (75) and (74).

(78) Let us consider a graph G_1, a directed-simple graph G_2 of G_1, vertices v_1, w_1 of G_1, and vertices v_2, w_2 of G_2. Suppose $v_1 = v_2$ and $w_1 = w_2$

and $v_1 \neq w_1$. Then v_1 and w_1 are adjacent if and only if v_2 and w_2 are adjacent. The theorem is a consequence of (76) and (74).

10. Into GLIB_010

Let us consider graphs G_1, G_2, a partial graph mapping F from G_1 to G_2, a vertex v_1 of G_1, and a vertex v_2 of G_2. Now we state the propositions:

(79) If $v_2 = (F_{\mathbb{V}})(v_1)$ and F is total, then $(F_{\mathbb{V}})^{\circ}(G_1.\text{reachableFrom}(v_1)) \subseteq G_2.\text{reachableFrom}(v_2)$.

(80) Suppose $v_1 \in \text{dom}(F_{\mathbb{V}})$ and $v_2 = (F_{\mathbb{V}})(v_1)$ and F is one-to-one and onto. Then $G_2.\text{reachableFrom}(v_2) \subseteq (F_{\mathbb{V}})^{\circ}(G_1.\text{reachableFrom}(v_1))$.

(81) If $v_2 = (F_{\mathbb{V}})(v_1)$ and F is isomorphism, then $(F_{\mathbb{V}})^{\circ}(G_1.\text{reachableFrom}(v_1)) = G_2.\text{reachableFrom}(v_2)$. The theorem is a consequence of (79) and (80).

Let us consider graphs G_1, G_2 and a partial graph mapping F from G_1 to G_2. Now we state the propositions:

(82) Suppose F is isomorphism. Then $G_2.\text{componentSet}() =$ the set of all $(F_{\mathbb{V}})^{\circ}C$ where C is an element of $G_1.\text{componentSet}()$. The theorem is a consequence of (81).

(83) If F is isomorphism, then $G_1.\text{numComponents}() = G_2.\text{numComponents}()$. The theorem is a consequence of (6) and (82).

Let G be a loopless graph. Let us note that every graph which is G-isomorphic is also loopless. Now we state the proposition:

(84) Let us consider graphs G_1, G_2, G_3, G_4, an empty partial graph mapping F_1 from G_1 to G_2, and an empty partial graph mapping F_2 from G_3 to G_4. Then $F_1 = F_2$.

Let us consider graphs G_1, G_2 and a partial graph mapping F from G_1 to G_2. Now we state the propositions:

(85) (i) $F \restriction \operatorname{dom} F = F$, and

(ii) $\operatorname{rng} F \upharpoonleft F = F$.

The theorem is a consequence of (84).

(86) If F is total, then $\operatorname{rng} F \upharpoonleft F$ is total. The theorem is a consequence of (85).

(87) If F is onto, then $F \restriction \operatorname{dom} F$ is onto. The theorem is a consequence of (85).

Let us consider graphs G_1, G_2. Now we state the propositions:

(88) Every partial graph mapping from G_1 to G_2 is a partial graph mapping from G_1 to $\operatorname{rng} F$. The theorem is a consequence of (85).

(89) Every partial graph mapping from G_1 to G_2 is a partial graph mapping from $\operatorname{dom} F$ to G_2. The theorem is a consequence of (85).

(90) Let us consider graphs G_1, G_2, a partial graph mapping F from G_1 to G_2, and subsets X, Y of the vertices of G_1. Suppose F is total. Then $(F_{\mathbb{E}})^{\circ}(G_1.\text{edgesBetween}(X,Y)) \subseteq G_2.\text{edgesBetween}((F_{\mathbb{V}})^{\circ}X,(F_{\mathbb{V}})^{\circ}Y)$.

Proof: Set $f = F_{\mathbb{E}}{\restriction}G_1.\text{edgesBetween}(X,Y)$. For every object y such that $y \in \operatorname{rng} f$ holds $y \in G_2.\text{edgesBetween}((F_{\mathbb{V}})^{\circ}X,(F_{\mathbb{V}})^{\circ}Y)$. □

(91) Let us consider graphs G_1, G_2, a partial graph mapping F from G_1 to G_2, and a set V. Then $(F_{\mathbb{E}})^{\circ}(G_1.\text{edgesBetween}(V)) \subseteq G_2.\text{edgesBetween}((F_{\mathbb{V}})^{\circ}V)$.

(92) Let us consider graphs G_1, G_2, a partial graph mapping F from G_1 to G_2, and subsets X, Y of the vertices of G_1. Suppose F is weak subgraph embedding and onto.

Then $(F_{\mathbb{E}})^{\circ}(G_1.\text{edgesBetween}(X,Y)) = G_2.\text{edgesBetween}((F_{\mathbb{V}})^{\circ}X,(F_{\mathbb{V}})^{\circ}Y)$. The theorem is a consequence of (90).

(93) Let us consider graphs G_1, G_2, a partial graph mapping F from G_1 to G_2, and a set V. Suppose F is continuous. Then $(F_{\mathbb{E}})^{\circ}(G_1.\text{edgesBetween}(V)) = G_2.\text{edgesBetween}((F_{\mathbb{V}})^{\circ}V)$. The theorem is a consequence of (91).

Let us consider graphs G_1, G_2, a non empty, one-to-one partial graph mapping F from G_1 to G_2, and an F-valued walk W_2 of G_2. Now we state the propositions:

(94) $(F^{-1}(W_2)).\text{vertices}() = (F_{\mathbb{V}})^{-1}(W_2.\text{vertices}())$.

(95) $(F^{-1}(W_2)).\text{edges}() = (F_{\mathbb{E}})^{-1}(W_2.\text{edges}())$.

(96) Let us consider graphs G_1, G_2, a non empty, one-to-one partial graph mapping F from G_1 to G_2, an F-valued walk W_2 of G_2, and objects v, w. Suppose W_2 is a walk from v to w. Then $F^{-1}(W_2)$ is a walk from $(F^{-1}{}_{\mathbb{V}})(v)$ to $(F^{-1}{}_{\mathbb{V}})(w)$.

(97) Let us consider graphs G_1, G_2, a one-to-one partial graph mapping F from G_1 to G_2, a vertex v_1 of G_1, and a vertex v_2 of G_2. Suppose $v_2 = (F_{\mathbb{V}})(v_1)$ and F is isomorphism. Then $(F_{\mathbb{V}})^{-1}(G_2.\text{reachableFrom}(v_2)) = G_1.\text{reachableFrom}(v_1)$. The theorem is a consequence of (81).

(98) Let us consider graphs G_1, G_2, a partial graph mapping F from G_1 to G_2, and a subgraph H of G_2. Then $(F_{\mathbb{E}})^{-1}(\text{the edges of } H) \subseteq G_1.\text{edgesBetween}$ $((F_{\mathbb{V}})^{-1}(\text{the vertices of } H))$.

(99) Let us consider graphs G_1, G_2, a non empty partial graph mapping F from G_1 to G_2, a subgraph H_2 of $\operatorname{rng} F$, and a subgraph H_1 of G_1 induced by $(F_{\mathbb{V}})^{-1}(\text{the vertices of } H_2)$ and $(F_{\mathbb{E}})^{-1}(\text{the edges of } H_2)$. Then $\operatorname{rng}(F{\restriction}H_1) \approx H_2$. The theorem is a consequence of (98).

(100) Let us consider graphs G_1, G_2, a non empty partial graph mapping F

from G_1 to G_2, a non empty subset V_2 of the vertices of $\operatorname{rng} F$, and a subgraph H of $\operatorname{rng} F$ induced by V_2. Suppose G_1.edgesBetween($(F_{\mathbb{V}})^{-1}$(the vertices of H)) $\subseteq \operatorname{dom}(F_{\mathbb{E}})$. Then $(F_{\mathbb{E}})^{-1}$(the edges of H) $= G_1$.edges Between($(F_{\mathbb{V}})^{-1}$(the vertices of H)). The theorem is a consequence of (98).

(101) Let us consider graphs G_1, G_2, a non empty partial graph mapping F from G_1 to G_2, a non empty subset V_2 of the vertices of $\operatorname{rng} F$, a subgraph H_2 of $\operatorname{rng} F$ induced by V_2, and a subgraph H_1 of G_1 induced by $(F_{\mathbb{V}})^{-1}$(the vertices of H_2). Suppose G_1.edgesBetween($(F_{\mathbb{V}})^{-1}$(the vertices of H_2)) $\subseteq \operatorname{dom}(F_{\mathbb{E}})$. Then $\operatorname{rng}(F \restriction H_1) \approx H_2$. The theorem is a consequence of (100).

(102) Let us consider graphs G_1, G_2, a non empty partial graph mapping F from G_1 to G_2, a non empty subset V of the vertices of $\operatorname{dom} F$, and a subgraph H of G_1 induced by V. Suppose F is continuous. Then $\operatorname{rng}(F \restriction H)$ is a subgraph of G_2 induced by $(F_{\mathbb{V}})^{\circ}V$. The theorem is a consequence of (93).

(103) Let us consider graphs G_1, G_2, a non empty partial graph mapping F from G_1 to G_2, a subgraph H_2 of $\operatorname{rng} F$, and a subgraph H_1 of G_1 induced by $(F_{\mathbb{V}})^{-1}$(the vertices of H_2) and $(F_{\mathbb{E}})^{-1}$(the edges of H_2). Then every walk of H_1 is an F-defined walk of G_1.

Proof: the vertices of $H_1 = (F_{\mathbb{V}})^{-1}$(the vertices of H_2) and the edges of $H_1 = (F_{\mathbb{E}})^{-1}$(the edges of H_2). □

(104) Let us consider graphs G_1, G_2, a non empty partial graph mapping F from G_1 to G_2, a subgraph H_2 of $\operatorname{rng} F$, a subgraph H_1 of G_1 induced by $(F_{\mathbb{V}})^{-1}$(the vertices of H_2) and $(F_{\mathbb{E}})^{-1}$(the edges of H_2), and an F-defined walk W_1 of G_1. If W_1 is a walk of H_1, then $F^{\circ}W_1$ is a walk of H_2.

Proof: the vertices of $H_1 = (F_{\mathbb{V}})^{-1}$(the vertices of H_2) and the edges of $H_1 = (F_{\mathbb{E}})^{-1}$(the edges of H_2). $(F^{\circ}W_1)$.vertices() $\subseteq$ the vertices of H_2. $(F^{\circ}W_1)$.edges() $\subseteq$ the edges of H_2. □

(105) Let us consider graphs G_1, G_2, a non empty partial graph mapping F from G_1 to G_2, and a subgraph H of $\operatorname{rng} F$. Then every walk of H is an F-valued walk of G_2.

(106) Let us consider graphs G_1, G_2, a non empty, one-to-one partial graph mapping F from G_1 to G_2, a subgraph H_2 of $\operatorname{rng} F$, a subgraph H_1 of G_1 induced by $(F_{\mathbb{V}})^{-1}$(the vertices of H_2) and $(F_{\mathbb{E}})^{-1}$(the edges of H_2), and an F-valued walk W_2 of G_2. If W_2 is a walk of H_2, then $F^{-1}(W_2)$ is a walk of H_1.

Proof: the vertices of $H_1 = (F_{\mathbb{V}})^{-1}$(the vertices of H_2) and the edges of $H_1 = (F_{\mathbb{E}})^{-1}$(the edges of H_2). $(F^{-1}(W_2))$.vertices() $\subseteq$ the vertices of H_1. $(F^{-1}(W_2))$.edges() $\subseteq$ the edges of H_1. □

(107) Let us consider graphs G_1, G_2, a non empty, one-to-one partial graph mapping F from G_1 to G_2, and an acyclic subgraph H_2 of $\operatorname{rng} F$. Then every subgraph of G_1 induced by $(F_{\mathbb{V}})^{-1}$(the vertices of H_2) and $(F_{\mathbb{E}})^{-1}$(the edges of H_2) is acyclic. The theorem is a consequence of (103) and (104).

(108) Let us consider graphs G_1, G_2, a non empty, one-to-one partial graph mapping F from G_1 to G_2, and a connected subgraph H_2 of $\operatorname{rng} F$. Then every subgraph of G_1 induced by $(F_{\mathbb{V}})^{-1}$(the vertices of H_2) and $(F_{\mathbb{E}})^{-1}$(the edges of H_2) is connected. The theorem is a consequence of (98), (105), (106), and (96).

Let us consider graphs G_1, G_2, a partial graph mapping F from G_1 to G_2, a subgraph H of G_1, and a partial graph mapping F' from H to $\operatorname{rng}(F{\restriction}H)$. Now we state the propositions:

(109) Suppose $F' = F{\restriction}H$. Then

(i) if F' is not empty, then F' is onto, and

(ii) if F is total, then F' is total, and

(iii) if F is one-to-one, then F' is one-to-one, and

(iv) if F is directed, then F' is directed, and

(v) if F is semi-continuous, then F' is semi-continuous, and

(vi) if F is continuous and $F_{\mathbb{E}}$ is one-to-one, then F' is continuous, and

(vii) if F is semi-directed-continuous, then F' is semi-directed-continuous, and

(viii) if F is directed-continuous and $F_{\mathbb{E}}$ is one-to-one, then F' is directed-continuous.

The theorem is a consequence of (85) and (86).

(110) Suppose $F' = F{\restriction}H$. Then

(i) if F is weak subgraph embedding, then F' is weak subgraph embedding, and

(ii) if F is strong subgraph embedding, then F' is isomorphism, and

(iii) if F is directed and strong subgraph embedding, then F' is directed-isomorphism.

The theorem is a consequence of (109).

11. Into GLIB_013

Now we state the propositions:

(111) Let us consider a vertex-finite, directed-simple graph G_1, a directed graph complement G_2 of G_1, a vertex v_1 of G_1, and a vertex v_2 of G_2. Suppose $v_1 = v_2$. Then

(i) v_2.inDegree() $= G_1$.order() $-$ (v_1.inDegree() $+ 1$), and

(ii) v_2.outDegree() $= G_1$.order() $-$ (v_1.outDegree() $+ 1$), and

(iii) v_2.degree() $= 2 \cdot (G_1$.order()) $-$ (v_1.degree() $+ 2$).

(112) Let us consider a vertex-finite, simple graph G_1, a graph complement G_2 of G_1, a vertex v_1 of G_1, and a vertex v_2 of G_2. If $v_1 = v_2$, then v_2.degree() $= G_1$.order() $-$ (v_1.degree() $+ 1$).

(113) Let us consider a vertex-finite, directed-simple graph G, and a vertex v of G. Then

(i) v.inDegree() $<$ G.order(), and

(ii) v.outDegree() $<$ G.order().

(114) Let us consider a vertex-finite, simple graph G, and a vertex v of G. Then v.degree() $<$ G.order().

One can check that every graph which is 1-edge is also non-multi.

12. Into GLIB_014

Let S be a $\cup$-tolerating, graph-membered set. Observe that every subset of S is $\cup$-tolerating.

Now we state the proposition:

(115) Let us consider graph-membered sets S_1, S_2. Suppose $S_1 \subseteq S_2$. Then

(i) the vertices of $S_1 \subseteq$ the vertices of S_2, and

(ii) the edges of $S_1 \subseteq$ the edges of S_2, and

(iii) the source of $S_1 \subseteq$ the source of S_2, and

(iv) the target of $S_1 \subseteq$ the target of S_2.

Let us consider a graph union set S, a graph union G of S, and objects e, v, w. Now we state the propositions:

(116) If e joins v to w in G, then there exists an element H of S such that e joins v to w in H.

(117) If e joins v and w in G, then there exists an element H of S such that e joins v and w in H. The theorem is a consequence of (116).

Let us consider graph union sets S_1, S_2, a graph union G_1 of S_1, and a graph union G_2 of S_2. Now we state the propositions:

(118) If for every element H_2 of S_2, there exists an element H_1 of S_1 such that H_2 is a subgraph of H_1, then G_2 is a subgraph of G_1. The theorem is a consequence of (116).

(119) If $S_2 \subseteq S_1$, then G_2 is a subgraph of G_1. The theorem is a consequence of (118).

Let us consider graphs G_1, G_2 and a graph union G of G_1 and G_2. Now we state the propositions:

(120) If G_1 tolerates G_2 and the vertices of G_1 misses the vertices of G_2, then $G.\mathrm{order}() = G_1.\mathrm{order}() + G_2.\mathrm{order}()$.

(121) If G_1 tolerates G_2 and the edges of G_1 misses the edges of G_2, then $G.\mathrm{size}() = G_1.\mathrm{size}() + G_2.\mathrm{size}()$.

(122) Let us consider connected graphs G_1, G_2, and a graph union G of G_1 and G_2. If the vertices of G_1 meets the vertices of G_2, then G is connected.

(123) Let us consider graphs G_1, G_2, a graph union G of G_1 and G_2, and a walk W of G. Suppose G_1 tolerates G_2 and the vertices of G_1 misses the vertices of G_2. Then W is a walk of G_1 or a walk of G_2.

(124) Let us consider graphs G_1, G_2, a graph union G of G_1 and G_2, a vertex v_1 of G_1, and a vertex v of G. Suppose the vertices of G_1 misses the vertices of G_2. If $v = v_1$, then $G.\mathrm{reachableFrom}(v) = G_1.\mathrm{reachableFrom}(v_1)$. The theorem is a consequence of (123).

(125) Let us consider graphs G_1, G_2, a graph union G of G_1 and G_2, a vertex v_2 of G_2, and a vertex v of G. Suppose G_1 tolerates G_2 and the vertices of G_1 misses the vertices of G_2. If $v = v_2$, then $G.\mathrm{reachableFrom}(v) = G_2.\mathrm{reachableFrom}(v_2)$. The theorem is a consequence of (123).

(126) Let us consider graphs G_1, G_2, and a graph union G of G_1 and G_2. Suppose G_1 tolerates G_2 and the vertices of G_1 misses the vertices of G_2. Then

(i) $G.\mathrm{componentSet}() = G_1.\mathrm{componentSet}() \cup G_2.\mathrm{componentSet}()$, and

(ii) $G.\mathrm{numComponents}() = G_1.\mathrm{numComponents}() + G_2.\mathrm{numComponents}()$.

The theorem is a consequence of (124) and (125).

13. Into GLUNIR00

Let us consider a non empty set V and a binary relation E on V. Now we state the propositions:

(127) createGraph(V, E).loops$() = E \cap \mathrm{id}_V$.

(128) createGraph$(V, E \setminus (\mathrm{id}_V))$ is a subgraph of createGraph(V, E) with loops removed. The theorem is a consequence of (127).

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] John Adrian Bondy and U. S. R. Murty. *Graph Theory.* Graduate Texts in Mathematics, 244. Springer, New York, 2008. ISBN 978-1-84628-969-9.

[3] Pavol Hell and Jaroslav Nesetril. *Graphs and homomorphisms.* Oxford Lecture Series in Mathematics and Its Applications; 28. Oxford University Press, Oxford, 2004. ISBN 0-19-852817-5.

[4] Ulrich Knauer. *Algebraic graph theory: morphisms, monoids and matrices*, volume 41 of *De Gruyter Studies in Mathematics.* Walter de Gruyter, 2011.

[5] Sebastian Koch. Miscellaneous graph preliminaries. *Formalized Mathematics*, 28(**1**):23–39, 2020. doi:10.2478/forma-2020-0003.

[6] Sebastian Koch. About supergraphs. Part I. *Formalized Mathematics*, 26(**2**):101–124, 2018. doi:10.2478/forma-2018-0009.

[7] Sebastian Koch. About graph mappings. *Formalized Mathematics*, 27(**3**):261–301, 2019. doi:10.2478/forma-2019-0024.

[8] Gilbert Lee and Piotr Rudnicki. Alternative graph structures. *Formalized Mathematics*, 13(**2**):235–252, 2005.

[9] Robin James Wilson. *Introduction to Graph Theory.* Oliver & Boyd, Edinburgh, 1972. ISBN 0-05-002534-1.

Accepted March 30, 2021

FORMALIZED MATHEMATICS
Vol. 29, No. 1, Pages 39–47, 2021
DOI: 10.2478/forma-2021-0004

sciendo
https://sciendo.com/journal/forma

Algebraic Extensions

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Agnieszka Rowińska-Schwarzweller
Sopot, Poland

Summary. In this article we further develop field theory in Mizar [1], [2], [3] towards splitting fields. We deal with algebraic extensions [4], [5]: a field extension E of a field F is algebraic, if every element of E is algebraic over F. We prove amongst others that finite extensions are algebraic and that field extensions generated by a finite set of algebraic elements are finite. From this immediately follows that field extensions generated by roots of a polynomial over F are both finite and algebraic. We also define the field of algebraic elements of E over F and show that this field is an intermediate field of $E|F$.

MSC: 12F05 68V20

Keywords: algebraic extensions; finite extensions; field of algebraic numbers

MML identifier: FIELD_7, version: 8.1.11 5.65.1394

1. Preliminaries

Let L_1, L_2 be double loop structures. We say that $L_1 \approx L_2$ if and only if

(Def. 1) the double loop structure of $L_1 =$ the double loop structure of L_2.

One can verify that the predicate is reflexive and symmetric.

Now we state the propositions:

(1) Let us consider rings R, S. Then $R \approx S$ if and only if there exists a function f from R into S such that $f = \mathrm{id}_R$ and f is isomorphism.

(2) Let us consider strict rings R, S. Then $R \approx S$ if and only if $R = S$.

Let F_1, F_2 be fields. Let us note that $F_1 \approx F_2$ if and only if the condition (Def. 2) is satisfied.

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

(Def. 2) F_1 is a subfield of F_2 and F_2 is a subfield of F_1.

Now we state the proposition:

(3) Let us consider a field F, an extension E of F, and a subset T of E. Then $\mathrm{FAdj}(F,T) \approx F$ if and only if T is a subset of F.

Let us consider a field F and extensions E_1, E_2 of F. Now we state the propositions:

(4) If $E_1 \approx E_2$, then $\mathrm{VecSp}(E_1,F) = \mathrm{VecSp}(E_2,F)$.

(5) If $E_1 \approx E_2$, then $\deg(E_1,F) = \deg(E_2,F)$. The theorem is a consequence of (4).

Let F be a field and E be an extension of F. Note that there exists an extension of F which is E-homomorphic and there exists an extension of F which is E-monomorphic and there exists an extension of F which is E-isomorphic.

Let R be a ring and a, b be elements of R. One can check that the functor $\{a,b\}$ yields a subset of R. Let F be a field, V be a vector space over F, and a be an element of V. Note that the functor $\{a\}$ yields a subset of V. Let a, b be elements of V. Let us observe that the functor $\{a,b\}$ yields a subset of V. Let us note that every basis of V is linearly independent.

Now we state the proposition:

(6) Let us consider a field F, a vector space V over F, and a subset X of V. Then X is linearly independent if and only if for every linear combinations l_1, l_2 of X such that $\sum l_1 = \sum l_2$ holds $l_1 = l_2$.

Let F be a field and E be an extension of F. Observe that every basis of $\mathrm{VecSp}(E,F)$ is non empty and $\deg(E,F)$ is non zero.

Let E be an F-finite extension of F. Observe that every basis of $\mathrm{VecSp}(E,F)$ is finite. Let us consider a field F and an extension E of F. Now we state the propositions:

(7) $\deg(E,F) = 1$ if and only if the carrier of $E =$ the carrier of F.

(8) $\deg(E,F) = 1$ if and only if $E \approx F$. The theorem is a consequence of (7).

(9) $\deg(E,F) = 1$ if and only if $\{1_E\}$ is a basis of $\mathrm{VecSp}(E,F)$. The theorem is a consequence of (7).

Let F be a field and E be an extension of F. One can check that there exists a subset of $\mathrm{VecSp}(E,F)$ which is non empty, finite, and linearly independent.

Now we state the proposition:

(10) Let us consider a field F, an extension E of F, and subsets T_1, T_2 of E. Suppose $T_1 \subseteq T_2$. Then $\mathrm{FAdj}(F,T_1)$ is a subfield of $\mathrm{FAdj}(F,T_2)$.

Let F be a field and p be a polynomial over F. The functor $\mathrm{Coeff}(p)$ yielding a subset of F is defined by the term

(Def. 3) $\{p(i)$, where i is an element of $\mathbb{N} : p(i) \neq 0_F\}$.

Let us note that $\mathrm{Coeff}(p)$ is finite. Now we state the propositions:

(11) Let us consider a field F, an extension E of F, and a polynomial p over E. Suppose $\mathrm{Coeff}(p) \subseteq$ the carrier of F. Then p is a polynomial over F.

(12) Let us consider a field F, an extension E of F, and a non zero polynomial p over E. Suppose $\mathrm{Coeff}(p) \subseteq$ the carrier of F. Then p is a non zero polynomial over F. The theorem is a consequence of (11).

(13) Let us consider a ring R, a ring extension S of R, an element p of the carrier of $\mathrm{PolyRing}(R)$, and an element q of the carrier of $\mathrm{PolyRing}(S)$. If $p = q$, then $\mathrm{Roots}(S, p) = \mathrm{Roots}(q)$.

Let R be an integral domain and p be a non zero element of the carrier of $\mathrm{PolyRing}(R)$. Note that $\mathrm{Roots}(p)$ is finite. Let S be a domain ring extension of R. One can check that $\mathrm{Roots}(S, p)$ is finite. Let F be a field and E be an extension of F. Let us observe that there exists an extension of E which is F-extending. Let E be an F-finite extension of F. Note that there exists an F-extending extension of E which is F-finite and there exists an F-extending extension of E which is E-finite. Now we state the propositions:

(14) Let us consider a field F, an element p of the carrier of $\mathrm{PolyRing}(F)$, an extension E of F, an E-extending extension U of F, an element a of E, and an element b of U. If $a = b$, then $\mathrm{ExtEval}(p, a) = \mathrm{ExtEval}(p, b)$.

(15) Let us consider a field F, an element p of the carrier of $\mathrm{PolyRing}(F)$, an extension E of F, and an element q of the carrier of $\mathrm{PolyRing}(E)$. Suppose $q = p$. Let us consider an E-extending extension U of F, and an element a of U. Then $\mathrm{ExtEval}(q, a) = \mathrm{ExtEval}(p, a)$.

Let R be a ring, S be a ring extension of R, and a be an element of R. The functor $^{@}(a, S)$ yielding an element of S is defined by the term

(Def. 4) a.

Let a be an element of S. We say that a is R-membered if and only if

(Def. 5) $a \in$ the carrier of R.

One can verify that there exists an element of S which is R-membered.

Let a be an element of S. Assume a is R-membered. The functor $^{@}(R, a)$ yielding an element of R is defined by the term

(Def. 6) a.

Let a be an R-membered element of S. Let us observe that $^{@}(R, a)$ reduces to a. Let F be a field and E be an extension of F. One can check that there exists an element of E which is non zero and F-algebraic.

Let a be an element of F. One can check that $^{@}(a, E)$ is F-algebraic.

Let K be an E-extending extension of F and a be an F-algebraic element of E. Note that ${}^{@}(a, K)$ is F-algebraic.

2. More on Finite Extensions

Now we state the propositions:

(16) Let us consider a field F, an extension E of F, and an E-extending extension K of F. Then every linear combination of $\mathrm{VecSp}(K, F)$ is a linear combination of $\mathrm{VecSp}(K, E)$.

(17) Let us consider a field F, an extension E of F, an E-extending extension K of F, a subset B_E of $\mathrm{VecSp}(K, E)$, and a subset B_F of $\mathrm{VecSp}(K, F)$. Suppose $B_F \subseteq B_E$. Then every linear combination of B_F is a linear combination of B_E. The theorem is a consequence of (16).

(18) Let us consider a field F, an extension E of F, an E-extending extension K of F, a finite subset B_E of $\mathrm{VecSp}(K, E)$, a finite subset B_F of $\mathrm{VecSp}(K, F)$, a linear combination l_1 of B_F, and a linear combination l_2 of B_E. If $l_1 = l_2$ and $B_F \subseteq B_E$, then $\sum l_1 = \sum l_2$.

Proof: by induction on card(the support of l_1).

Let F be a field, E be an extension of F, K be an F-extending extension of E, B_E be a subset of $\mathrm{VecSp}(E, F)$, and B_K be a subset of $\mathrm{VecSp}(K, E)$. The functor $\mathrm{Base}(B_E, B_K)$ yielding a subset of $\mathrm{VecSp}((K$ **qua** extension of $F), F)$ is defined by the term

(Def. 7) $\{a \cdot b$, where a, b are elements of $K : a \in B_E$ and $b \in B_K\}$.

Let B_E be a non empty subset of $\mathrm{VecSp}(E, F)$ and B_K be a non empty subset of $\mathrm{VecSp}(K, E)$. One can verify that $\mathrm{Base}(B_E, B_K)$ is non empty.

Now we state the propositions:

(19) Let us consider a field F, an extension E of F, an F-extending extension K of E, a linearly independent subset B_E of $\mathrm{VecSp}(E, F)$, a linearly independent subset B_K of $\mathrm{VecSp}(K, E)$, and elements a_1, a_2, b_1, b_2 of K. Suppose $a_1, a_2 \in B_E$ and $b_1, b_2 \in B_K$. If $a_1 \cdot b_1 = a_2 \cdot b_2$, then $a_1 = a_2$ and $b_1 = b_2$.

(20) Let us consider a field F, an extension E of F, an F-extending extension K of E, a non empty, linearly independent subset B_E of $\mathrm{VecSp}(E, F)$, and a non empty, linearly independent subset B_K of $\mathrm{VecSp}(K, E)$. Then $\overline{\overline{\mathrm{Base}(B_E, B_K)}} = \overline{\overline{B_E \times B_K}}$.

Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exist elements a, b of K such that $a \in B_E$ and $b \in B_K$ and $\$_1 = a \cdot b$ and $\$_2 = \langle a, b \rangle$. Consider f being a function from $\mathrm{Base}(B_E, B_K)$ into $B_E \times B_K$ such that for every object

x such that $x \in \mathrm{Base}(B_E, B_K)$ holds $\mathcal{P}[x, f(x)]$. $\mathrm{rng}\, f = B_E \times B_K$. f is one-to-one. □

(21) Let us consider a field F, an extension E of F, an F-extending extension K of E, a non empty, finite, linearly independent subset B_E of $\mathrm{VecSp}(E, F)$, and a non empty, finite, linearly independent subset B_K of $\mathrm{VecSp}(K, E)$. Then $\overline{\overline{\mathrm{Base}(B_E, B_K)}} = \overline{\overline{B_E}} \cdot \overline{\overline{B_K}}$. The theorem is a consequence of (20).

Let F be a field, E be an extension of F, K be an F-extending extension of E, B_E be a non empty, finite, linearly independent subset of $\mathrm{VecSp}(E, F)$, and B_K be a non empty, finite, linearly independent subset of $\mathrm{VecSp}(K, E)$. Observe that $\mathrm{Base}(B_E, B_K)$ is finite.

Let B_K be a non empty, linearly independent subset of $\mathrm{VecSp}(K, E)$, l be a linear combination of $\mathrm{Base}(B_E, B_K)$, and b be an element of K. The functor $\mathrm{down}(l, b)$ yielding a linear combination of B_E is defined by

(Def. 8) for every element a of K such that $a \in B_E$ and $b \in B_K$ holds $\mathit{it}(a) = l(a \cdot b)$ and for every element a of E such that $a \notin B_E$ or $b \notin B_K$ holds $\mathit{it}(a) = 0_F$.

Let B_K be a non empty, finite, linearly independent subset of $\mathrm{VecSp}(K, E)$. The functor $\mathrm{down}\, l$ yielding a linear combination of B_K is defined by

(Def. 9) for every element b of K such that $b \in B_K$ holds $\mathit{it}(b) = \sum \mathrm{down}(l, b)$.

Let E be an F-finite extension of F, B_E be a basis of $\mathrm{VecSp}(E, F)$, and l_1 be a linear combination of B_K. The functor $\mathrm{lift}(l_1, B_E)$ yielding a linear combination of $\mathrm{Base}(B_E, B_K)$ is defined by

(Def. 10) for every element b of K such that $b \in B_K$ there exists a linear combination l_2 of B_E such that $\sum l_2 = l_1(b)$ and for every element a of K such that $a \in B_E$ and $a \cdot b \in \mathrm{Base}(B_E, B_K)$ holds $\mathit{it}(a \cdot b) = l_2(a)$.

Now we state the propositions:

(22) Let us consider a field F, an F-finite extension E of F, an E-finite, F-extending extension K of E, a basis B_E of $\mathrm{VecSp}(E, F)$, a basis B_K of $\mathrm{VecSp}(K, E)$, and a linear combination l of $\mathrm{Base}(B_E, B_K)$. Then $\mathrm{lift}(\mathrm{down}\, l, B_E) = l$. The theorem is a consequence of (6).

(23) Let us consider a field F, an F-finite extension E of F, an E-finite, F-extending extension K of E, a basis B_E of $\mathrm{VecSp}(E, F)$, a basis B_K of $\mathrm{VecSp}(K, E)$, and a linear combination l of B_K. Then $\mathrm{down}\, \mathrm{lift}(l, B_E) = l$.

(24) Let us consider a field F, an extension E of F, an F-extending extension K of E, a non empty, finite, linearly independent subset B_E of $\mathrm{VecSp}(E, F)$, a non empty, finite, linearly independent subset B_K of $\mathrm{VecSp}(K, E)$, and linear combinations l, l_1, l_2 of $\mathrm{Base}(B_E, B_K)$. Suppo-

se $l = l_1 + l_2$. Let us consider an element b of K. Then $\mathrm{down}(l, b) = \mathrm{down}(l_1, b) + \mathrm{down}(l_2, b)$.

(25) Let us consider a field F, an extension E of F, an F-extending extension K of E, a non empty, finite, linearly independent subset B_E of $\mathrm{VecSp}(E, F)$, a non empty, finite, linearly independent subset B_K of $\mathrm{VecSp}(K, E)$, and linear combinations l, l_1, l_2 of $\mathrm{Base}(B_E, B_K)$. If $l = l_1 + l_2$, then $\mathrm{down}\, l = \mathrm{down}\, l_1 + \mathrm{down}\, l_2$. The theorem is a consequence of (24).

Let us consider a field F, an F-finite extension E of F, an E-finite, F-extending extension K of E, a basis B_E of $\mathrm{VecSp}(E, F)$, a basis B_K of $\mathrm{VecSp}(K, E)$, and a linear combination l of $\mathrm{Base}(B_E, B_K)$. Now we state the propositions:

(26) $\sum l = \sum \mathrm{down}\, l$.

PROOF: by induction on card(the support of l).

(27) If $\sum l = 0_{\mathrm{VecSp}((K \textbf{ qua } \text{extension of } F), F)}$, then the support of $l = \emptyset$. The theorem is a consequence of (26).

Let us consider a field F, an F-finite extension E of F, an E-finite, F-extending extension K of E, a basis B_E of $\mathrm{VecSp}(E, F)$, and a basis B_K of $\mathrm{VecSp}(K, E)$. Now we state the propositions:

(28) $\mathrm{Lin}(\mathrm{Base}(B_E, B_K))$ = the vector space structure of $\mathrm{VecSp}((K$ **qua** extension of $F), F)$. The theorem is a consequence of (23) and (26).

(29) $\mathrm{Base}(B_E, B_K)$ is a basis of $\mathrm{VecSp}((K$ **qua** extension of $F), F)$. The theorem is a consequence of (27) and (28).

(30) Let us consider a field F, an F-finite extension E of F, and an E-finite, F-extending extension K of E. Then $\deg(K, F) = (\deg(K, E)) \cdot (\deg(E, F))$. The theorem is a consequence of (29) and (21).

(31) Let us consider a field F, an extension E of F, and an E-extending extension K of F. Suppose K is F-finite. Then

(i) E is F-finite, and

(ii) $\deg(E, F) \leqslant \deg(K, F)$, and

(iii) K is E-finite, and

(iv) $\deg(K, E) \leqslant \deg(K, F)$.

PROOF: Set B_F = the basis of $\mathrm{VecSp}(K, F)$. Reconsider $B_E = B_F$ as a finite subset of $\mathrm{VecSp}(K, E)$. $\mathrm{Lin}(B_E) = \mathrm{VecSp}(K, E)$. Consider I being a subset of $\mathrm{VecSp}(K, E)$ such that $I \subseteq B_E$ and I is linearly independent and $\mathrm{Lin}(I) = \mathrm{VecSp}(K, E)$. □

Let F be a field and E be an F-finite extension of F. One can check that every E-finite, F-extending extension of E is F-finite.

3. Algebraic Extensions

Let F be a field and E be an extension of F. We say that E is F-algebraic if and only if

(Def. 11) every element of E is F-algebraic.

One can verify that every extension of F which is F-finite is also F-algebraic.

Let E be an F-algebraic extension of F. Note that every element of E is F-algebraic. Now we state the propositions:

(32) Let us consider a field F, and an extension E of F. Then E is F-algebraic if and only if for every element a of E, $\mathrm{FAdj}(F, \{a\})$ is F-finite.

(33) Let us consider a field F, an extension E of F, and an element a of E. Then a is F-algebraic if and only if there exists an F-finite extension B of F such that E is B-extending and $a \in B$.

Let F be a field, E be an extension of F, and T be a subset of E. We say that T is F-algebraic if and only if

(Def. 12) for every element a of E such that $a \in T$ holds a is F-algebraic.

One can verify that there exists a subset of E which is finite and F-algebraic.

Now we state the propositions:

(34) Let us consider a field F, an extension E of F, an element b of E, a subset T of E, an extension E_1 of $\mathrm{FAdj}(F, T)$, and an element b_1 of E_1. Suppose $E_1 = E$ and $b_1 = b$. Then $\mathrm{FAdj}(F, \{b\} \cup T) = \mathrm{FAdj}(\mathrm{FAdj}(F, T), \{b_1\})$.
Proof: $\{b\} \cup T \subseteq$ the carrier of $\mathrm{FAdj}(\mathrm{FAdj}(F, T), \{b_1\})$ by [6, (35),(36)]. $\mathrm{FAdj}(F, T)$ is a subfield of $\mathrm{FAdj}(F, \{b\} \cup T)$. □

(35) Let us consider a field F, an extension E of F, an element b of E, a subset T of E, an extension E_1 of $\mathrm{FAdj}(F, \{b\})$, and a subset T_1 of E_1. Suppose $E_1 = E$ and $T_1 = T$. Then $\mathrm{FAdj}(F, \{b\} \cup T) = \mathrm{FAdj}(\mathrm{FAdj}(F, \{b\}), T_1)$.
Proof: $\{b\} \cup T \subseteq$ the carrier of $\mathrm{FAdj}(\mathrm{FAdj}(F, \{b\}), T_1)$ by [6, (35),(36)]. $\mathrm{FAdj}(F, \{b\})$ is a subfield of $\mathrm{FAdj}(F, \{b\} \cup T)$. □

Let F be a field, E be an extension of F, and T be a finite, F-algebraic subset of E. One can verify that $\mathrm{FAdj}(F, T)$ is F-finite.

Now we state the propositions:

(36) Let us consider a field F, an extension E of F, and an F-algebraic element a of E. Then $E \approx \mathrm{FAdj}(F, \{a\})$ if and only if $\deg \mathrm{MinPoly}(a, F) = \deg(E, F)$. The theorem is a consequence of (5), (31), (30), and (8).

(37) Let us consider a field F, and an extension E of F. Then E is F-finite if and only if there exists a finite, F-algebraic subset T of E such that $E \approx \mathrm{FAdj}(F, T)$.
Proof: by induction on $\deg(E, F)$.

Let F be a field, E be an extension of F, and p be a non zero element of the carrier of PolyRing(F). Note that Roots(E, p) is F-algebraic.

Now we state the proposition:

(38) Let us consider a field F, an extension E of F, and a non zero element p of the carrier of PolyRing(F). Then FAdj(F, Roots(E, p)) is F-algebraic.

Let us consider a field F, an extension E of F, and an E-extending extension K of F. Now we state the propositions:

(39) If K is E-algebraic and E is F-algebraic, then K is F-algebraic. The theorem is a consequence of (12), (15), and (33).

(40) If K is F-algebraic, then K is E-algebraic and E is F-algebraic. The theorem is a consequence of (15).

4. The Field of Algebraic Elements

Let F be a field, E be an extension of F, and a, b be F-algebraic elements of E. Observe that FAdj($F, \{a, b\}$) is F-finite and 0_E is F-algebraic and 1_E is F-algebraic.

Let a, b be F-algebraic elements of E. One can verify that $a+b$ is F-algebraic and $a-b$ is F-algebraic and $a \cdot b$ is F-algebraic.

Let a be an F-algebraic element of E. Let us note that $-a$ is F-algebraic.

Let a be a non zero, F-algebraic element of E. Let us observe that a^{-1} is F-algebraic.

The functor Alg-Elem(E) yielding a subset of E is defined by the term

(Def. 13) the set of all a where a is an F-algebraic element of E.

The functor Field-Alg-Elem(E) yielding a strict double loop structure is defined by

(Def. 14) the carrier of *it* = Alg-Elem(E) and the addition of *it* = (the addition of E) $\restriction$ (the carrier of *it*) and the multiplication of *it* = (the multiplication of E) $\restriction$ (the carrier of *it*) and the one of *it* = 1_E and the zero of *it* = 0_E.

We introduce the notation F-Alg(E) as a synonym of Field-Alg-Elem(E).

Observe that F-Alg(E) is non degenerated and F-Alg(E) is Abelian, add-associative, right zeroed, and right complementable and F-Alg(E) is commutative, associative, well unital, distributive, and almost left invertible and F-Alg(E) is F-extending and F-Alg(E) is F-algebraic. Now we state the propositions:

(41) Let us consider a field F, and an extension E of F. Then F-Alg(E) is an extension of F.

(42) Let us consider a field F, and an extension E of F. Then E is an extension of F-Alg(E).

(43) Let us consider a field F, an extension E of F, and an extension K of E. Then F-Alg(K) is an extension of F-Alg(E).

(44) Let us consider a field F, and an F-algebraic extension E of F. Then F-Alg$(E) \approx E$.

References

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

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[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. *Basic Algebra I.* Dover Books on Mathematics, 1985.

[5] Serge Lang. *Algebra.* Springer, 3rd edition, 2005.

[6] Christoph Schwarzweller. Ring and field adjunctions, algebraic elements and minimal polynomials. *Formalized Mathematics*, 28(**3**):251–261, 2020. doi:10.2478/forma-2020-0022.

Accepted March 30, 2021

FORMALIZED MATHEMATICS
Vol. 29, No. 1, Pages 49–62, 2021
DOI: 10.2478/forma-2021-0005

sciendo
https://sciendo.com/journal/forma

Functional Space Consisted by Continuous Functions on Topological Space

Hiroshi Yamazaki
Nagano Prefectural Institute of Technology
Nagano, Japan

Keiichi Miyajima
Ibaraki University
Ibaraki, Japan

Yasunari Shidama
Karuizawa Hotch 244-1
Nagano, Japan

Summary. In this article, using the Mizar system [1], [2], first we give a definition of a functional space which is constructed from all continuous functions defined on a compact topological space [5]. We prove that this functional space is a Banach space [3]. Next, we give a definition of a function space which is constructed from all continuous functions with bounded support. We also prove that this function space is a normed space.

MSC: 46E10 68V20

Keywords: continuous function space; compact topological space; Banach space

MML identifier: `COSP3`, version: `8.1.11 5.65.1394`

1. Real Vector Space of Continuous Functions

From now on S denotes a non empty topological space, T denotes a linear topological space, and X denotes a non empty subset of the carrier of S.

Now we state the propositions:

(1) Let us consider a non empty topological space X, a non empty linear topological space S, functions f, g from X into S, and a point x of X. Suppose f is continuous at x and g is continuous at x. Then $f+g$ is continuous at x.
Proof: For every neighbourhood G of $(f+g)(x)$, there exists a neighbourhood H of x such that $(f+g)^\circ H \subseteq G$. □

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

(2) Let us consider a non empty topological space X, a non empty linear topological space S, a function f from X into S, a point x of X, and a real number a. If f is continuous at x, then $a \cdot f$ is continuous at x.
PROOF: For every neighbourhood G of $(a \cdot f)(x)$, there exists a neighbourhood H of x such that $(a \cdot f)^{\circ}H \subseteq G$. □

(3) Let us consider a non empty topological space X, a non empty linear topological space S, and functions f, g from X into S. If f is continuous and g is continuous, then $f + g$ is continuous.
PROOF: For every point x of X, $f + g$ is continuous at x. □

(4) Let us consider a non empty topological space X, a non empty linear topological space S, a function f from X into S, and a real number a. If f is continuous, then $a \cdot f$ is continuous. The theorem is a consequence of (2).

Let S be a non empty topological space and T be a non empty linear topological space. The continuous functions of S and T yielding a subset of RealVectSpace((the carrier of S), T) is defined by the term

(Def. 1) $\{f$, where f is a function from the carrier of S into the carrier of T : f is continuous$\}$.

Let us observe that the continuous functions of S and T is non empty and functional.

Let us consider a non empty topological space S and a non empty linear topological space T. Now we state the propositions:

(5) The continuous functions of S and T is linearly closed.
PROOF: Set $W =$ the continuous functions of S and T. For every vectors v, u of RealVectSpace((the carrier of S), T) such that v, $u \in$ the continuous functions of S and T holds $v{+}u \in$ the continuous functions of S and T. For every real number a and for every vector v of RealVectSpace((the carrier of S), T) such that $v \in W$ holds $a \cdot v \in W$. □

(6) ⟨the continuous functions of S and T, Zero(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Add(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Mult(the continuous functions of S and T, RealVectSpace((the carrier of S), T))⟩ is a subspace of RealVectSpace((the carrier of S), T).

Let S be a non empty topological space and T be a non empty linear topological space.

One can verify that ⟨the continuous functions of S and T, Zero(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Add(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Mult(the continuous functions of S and T, RealVectSpace((the carrier of S), T))⟩ is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

The $\mathbb{R}$-vector space of continuous functions of S and T yielding a strict real linear space is defined by the term

(Def. 2) $\langle$the continuous functions of S and T, Zero(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Add(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Mult(the continuous functions of S and T, RealVectSpace((the carrier of S), T))$\rangle$.

Observe that the $\mathbb{R}$-vector space of continuous functions of S and T is constituted functions. Let f be a vector of the $\mathbb{R}$-vector space of continuous functions of S and T and v be an element of S. Let us note that the functor $f(v)$ yields a vector of T. Now we state the propositions:

(7) Let us consider a non empty topological space S, a non empty linear topological space T, and vectors f, g, h of the $\mathbb{R}$-vector space of continuous functions of S and T. Then $h = f + g$ if and only if for every element x of S, $h(x) = f(x) + g(x)$. The theorem is a consequence of (5).

(8) Let us consider a non empty topological space S, a non empty linear topological space T, vectors f, h of the $\mathbb{R}$-vector space of continuous functions of S and T, and a real number a. Then $h = a \cdot f$ if and only if for every element x of S, $h(x) = a \cdot f(x)$. The theorem is a consequence of (5).

(9) Let us consider a non empty topological space S, and a non empty linear topological space T. Then $0_{\alpha} =$ (the carrier of S) $\longmapsto 0_T$, where α is the $\mathbb{R}$-vector space of continuous functions of S and T. The theorem is a consequence of (5).

Let S be a non empty topological space and T be a non empty linear topological space. Let us note that the carrier of the $\mathbb{R}$-vector space of continuous functions of S and T is functional.

2. Real Vector Space of Continuous Functions (Norm Space Version)

In the sequel S, T denote real normed spaces and X denotes a non empty subset of the carrier of S.

Now we state the proposition:

(10) Let us consider a point x of T. Then (the carrier of S) $\longmapsto x$ is continuous on the carrier of S.

Let S, T be real normed spaces. The continuous functions of S and T yielding a subset of RealVectSpace((the carrier of S), T) is defined by the term

(Def. 3) $\{f$, where f is a function from the carrier of S into the carrier of T : f is continuous on the carrier of $S\}$.

One can check that the continuous functions of S and T is non empty and functional.

Let us consider real normed spaces S, T. Now we state the propositions:

(11) The continuous functions of S and T is linearly closed.
PROOF: Set $W =$ the continuous functions of S and T. For every vectors v, u of RealVectSpace((the carrier of S), T) such that v, $u \in$ the continuous functions of S and T holds $v+u \in$ the continuous functions of S and T. For every real number a and for every vector v of RealVectSpace((the carrier of S), T) such that $v \in W$ holds $a \cdot v \in W$ by [4, (27)]. □

(12) $\langle$the continuous functions of S and T, Zero(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Add(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Mult(the continuous functions of S and T, RealVectSpace((the carrier of S), T))$\rangle$ is a subspace of RealVectSpace((the carrier of S), T).

Let S, T be real normed spaces. Observe that $\langle$the continuous functions of S and T, Zero(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Add(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Mult(the continuous functions of S and T, RealVectSpace((the carrier of S), T))$\rangle$ is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

The $\mathbb{R}$-vector space of continuous functions of S and T yielding a strict real linear space is defined by the term

(Def. 4) $\langle$the continuous functions of S and T, Zero(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Add(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Mult(the continuous functions of S and T, RealVectSpace((the carrier of S), T))$\rangle$.

Note that the $\mathbb{R}$-vector space of continuous functions of S and T is constituted functions.

Let f be a vector of the $\mathbb{R}$-vector space of continuous functions of S and T and v be an element of S. One can check that the functor $f(v)$ yields a vector of T. Now we state the propositions:

(13) Let us consider real normed spaces S, T, and vectors f, g, h of the $\mathbb{R}$-vector space of continuous functions of S and T. Then $h = f + g$ if and only if for every element x of S, $h(x) = f(x) + g(x)$. The theorem is a consequence of (11).

(14) Let us consider real normed spaces S, T, vectors f, h of the $\mathbb{R}$-vector space of continuous functions of S and T, and a real number a. Then

$h = a \cdot f$ if and only if for every element x of S, $h(x) = a \cdot f(x)$. The theorem is a consequence of (11).

Let us consider real normed spaces S, T. Now we state the propositions:

(15) The $\mathbb{R}$-vector space of continuous functions of S and T is a subspace of RealVectSpace((the carrier of S), T).

(16) $0_{\alpha} =$ (the carrier of S) $\longmapsto 0_T$, where α is the $\mathbb{R}$-vector space of continuous functions of S and T. The theorem is a consequence of (11).

Let S, T be real normed spaces and f be an object. Assume $f \in$ the continuous functions of S and T. The functor PartFuncs(f, S, T) yielding a function from S into T is defined by

(Def. 5) *it* $= f$ and *it* is continuous on the carrier of S.

3. Normed Topological Linear Space

We consider normed real linear topological structures which extend real linear topological structures and normed structures and are systems

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

$$\text{a topology, a norm } \rangle$$

where the carrier is a set, the zero is an element of the carrier, the addition is a binary operation on the carrier, the external multiplication is a function from $\mathbb{R} \times$ (the carrier) into the carrier, the topology is a family of subsets of the carrier, the norm is a function from the carrier into $\mathbb{R}$.

Let X be a non empty set, O be an element of X, F be a binary operation on X, G be a function from $\mathbb{R} \times X$ into X, T be a family of subsets of X, and N be a function from X into $\mathbb{R}$. Observe that $\langle X, O, F, G, T, N \rangle$ is non empty and there exists a normed real linear topological structure which is strict and non empty.

Let X be a non empty normed real linear topological structure. We say that X is normed structure if and only if

(Def. 6) there exists a real normed space R such that $R =$ the normed structure of X and the topology of $X =$ the topology of TopSpaceNorm R.

One can verify that there exists a non empty normed real linear topological structure which is strict, add-continuous, mult-continuous, topological space-like, Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, discernible, reflexive, real normed space-like, normed structure, and T_2.

A normed linear topological space is a strict, add-continuous, mult-continuous, topological space-like, Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, discernible, reflexive, real normed space-like, normed structure, T_2, non empty normed real linear topological structure. Now we state the propositions:

(17) Every normed linear topological space is a linear topological space.

(18) Every normed linear topological space is a real normed space.

(19) Let us consider a normed linear topological space X, and a real normed space R. Suppose $R =$ the normed structure of X. Let us consider points x, y of X, points x_1, y_1 of R, and a real number a. Suppose $x_1 = x$ and $y_1 = y$. Then

(i) $x + y = x_1 + y_1$, and

(ii) $a \cdot x = a \cdot x_1$, and

(iii) $x - y = x_1 - y_1$, and

(iv) $\|x\| = \|x_1\|$.

Let us consider a normed linear topological space X, a sequence S of X, and a point x of X. Now we state the propositions:

(20) S is convergent to x if and only if for every real number r such that $0 < r$ there exists a natural number m such that for every natural number n such that $m \leqslant n$ holds $\|S(n) - x\| < r$. The theorem is a consequence of (19).

(21) S is convergent and $x = \lim S$ if and only if for every real number r such that $0 < r$ there exists a natural number m such that for every natural number n such that $m \leqslant n$ holds $\|S(n) - x\| < r$. The theorem is a consequence of (20).

(22) Let us consider a normed linear topological space X, and a sequence S of X. Suppose S is convergent. Let us consider a real number r. Suppose $0 < r$. Then there exists a natural number m such that for every natural number n such that $m \leqslant n$ holds $\|S(n) - \lim S\| < r$. The theorem is a consequence of (20).

(23) Let us consider a normed linear topological space X, and a subset V of X. Then V is open if and only if for every point x of X such that $x \in V$ there exists a real number r such that $r > 0$ and $\{y$, where y is a point of $X : \|x - y\| < r\} \subseteq V$. The theorem is a consequence of (19).

Let us consider a normed linear topological space X, a point x of X, a real number r, and a subset V of X. Now we state the propositions:

(24) If $V = \{y$, where y is a point of $X : \|x - y\| < r\}$, then V is open. The theorem is a consequence of (19).

(25) Suppose $V = \{y$, where y is a point of $X : \|x - y\| \leqslant r\}$. Then V is closed. The theorem is a consequence of (19).

Now we state the propositions:

(26) Let us consider a normed linear topological space X, a real normed space R, a sequence t of X, and a sequence s of R. Suppose $R =$ the normed structure of X and $t = s$ and t is convergent. Then

(i) s is convergent, and

(ii) $\lim s = \lim t$.

The theorem is a consequence of (22) and (19).

(27) Let us consider a normed linear topological space X, a real normed space R, a sequence s of X, and a sequence t of R. Suppose $R =$ the normed structure of X and $s = t$. Then s is convergent if and only if t is convergent. The theorem is a consequence of (26), (19), and (21).

(28) Let us consider a normed linear topological space X, and a subset V of X. Then V is closed if and only if for every sequence s_1 of X such that $\operatorname{rng} s_1 \subseteq V$ and s_1 is convergent holds $\lim s_1 \in V$. The theorem is a consequence of (26) and (27).

(29) Let us consider a normed linear topological space X, a real normed space R, a subset V of X, and a subset W of R. Suppose $R =$ the normed structure of X and the topology of $X =$ the topology of TopSpaceNorm R and $V = W$. Then V is closed if and only if W is closed. The theorem is a consequence of (27), (26), and (28).

(30) Let us consider a normed linear topological space X, a subset V of X, and a point x of X. Then V is a neighbourhood of x if and only if there exists a real number r such that $r > 0$ and $\{y$, where y is a point of $X : \|y - x\| < r\} \subseteq V$. The theorem is a consequence of (23) and (24).

(31) Let us consider a normed linear topological space X, and a subset V of X. Then V is compact if and only if for every sequence s_1 of X such that $\operatorname{rng} s_1 \subseteq V$ there exists a sequence s_2 of X such that s_2 is subsequence of s_1 and convergent and $\lim s_2 \in V$. The theorem is a consequence of (27) and (26).

(32) Let us consider a normed linear topological space X, a real normed space R, a subset V of X, and a subset W of R. Suppose $R =$ the normed structure of X and the topology of $X =$ the topology of TopSpaceNorm R and $V = W$. Then V is compact if and only if W is compact. The theorem is a consequence of (31), (26), and (27).

4. Real Norm Space of Continuous Functions

Now we state the propositions:

(33) Let us consider sets X, X_1, a real normed space S, and a partial function f from S to $\mathbb{R}$. Suppose f is continuous on X and $X_1 \subseteq X$. Then f is continuous on X_1.

Proof: $f{\restriction}X_1$ is continuous in r. □

(34) Let us consider a non empty, compact topological space S, a normed linear topological space T, and a set x. Suppose $x \in$ the continuous functions of S and T. Then $x \in \mathrm{BdFuncs}((\text{the carrier of } S), T)$.

(35) Let us consider a non empty, compact topological space S, and a normed linear topological space T. Then the $\mathbb{R}$-vector space of continuous functions of S and T is a subspace of the set of bounded real sequences from the carrier of S into T. The theorem is a consequence of (34) and (5).

Let S be a non empty, compact topological space and T be a normed linear topological space. The continuous functions norm of S and T yielding a function from the continuous functions of S and T into $\mathbb{R}$ is defined by the term

(Def. 7) $\mathrm{BdFuncsNorm}((\text{the carrier of } S), T){\restriction}(\text{the continuous functions of } S \text{ and } T)$.

The $\mathbb{R}$-norm space of continuous functions of S and T yielding a strict normed structure is defined by the term

(Def. 8) $\langle$the continuous functions of S and T, Zero(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Add(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), Mult(the continuous functions of S and T, RealVectSpace((the carrier of S), T)), the continuous functions norm of S and $T\rangle$.

One can check that the $\mathbb{R}$-norm space of continuous functions of S and T is non empty.

Now we state the propositions:

(36) Let us consider a non empty, compact topological space S, a normed linear topological space T, a point x of the $\mathbb{R}$-norm space of continuous functions of S and T, and a point y of the real normed space of bounded functions from the carrier of S into T. If $x = y$, then $\|x\| = \|y\|$.

(37) Let us consider a non empty, compact topological space S, a normed linear topological space T, a point f of the $\mathbb{R}$-norm space of continuous functions of S and T, and a function g from S into T. Suppose $f = g$. Let us consider a point t of S. Then $\|g(t)\| \leqslant \|f\|$. The theorem is a consequence of (34).

(38) Let us consider a non empty, compact topological space S, a normed linear topological space T, points x_1, x_2 of the $\mathbb{R}$-norm space of continuous functions of S and T, and points y_1, y_2 of the real normed space of bounded functions from the carrier of S into T. If $x_1 = y_1$ and $x_2 = y_2$, then $x_1 + x_2 = y_1 + y_2$. The theorem is a consequence of (5).

(39) Let us consider a non empty, compact topological space S, a normed linear topological space T, a real number a, a point x of the $\mathbb{R}$-norm space of continuous functions of S and T, and a point y of the real normed space of bounded functions from the carrier of S into T. If $x = y$, then $a \cdot x = a \cdot y$. The theorem is a consequence of (5).

Let S be a non empty, compact topological space and T be a normed linear topological space. One can verify that the $\mathbb{R}$-norm space of continuous functions of S and T is non empty, right complementable, Abelian, add-associative, right zeroed, vector distributive, scalar distributive, scalar associative, and scalar unital.

Let us consider a non empty, compact topological space S and a normed linear topological space T. Now we state the propositions:

(40) (The carrier of S) $\longmapsto 0_T = 0_\alpha$, where α is the $\mathbb{R}$-norm space of continuous functions of S and T. The theorem is a consequence of (9).

(41) $0_\alpha = 0_\beta$, where α is the $\mathbb{R}$-norm space of continuous functions of S and T and β is the real normed space of bounded functions from the carrier of S into T. The theorem is a consequence of (40).

Let us consider a non empty, compact topological space S, a normed linear topological space T, and a point F of the $\mathbb{R}$-norm space of continuous functions of S and T. Now we state the propositions:

(42) $0 \leqslant \|F\|$. The theorem is a consequence of (34).

(43) If $F = 0_\alpha$, then $0 = \|F\|$, where α is the $\mathbb{R}$-norm space of continuous functions of S and T. The theorem is a consequence of (34) and (40).

(44) Let us consider a non empty, compact topological space S, a normed linear topological space T, points F, G, H of the $\mathbb{R}$-norm space of continuous functions of S and T, and functions f, g, h from S into T. Suppose $f = F$ and $g = G$ and $h = H$. Then $H = F + G$ if and only if for every element x of S, $h(x) = f(x) + g(x)$. The theorem is a consequence of (7).

(45) Let us consider a real number a, a non empty, compact topological space S, a normed linear topological space T, points F, G of the $\mathbb{R}$-norm space of continuous functions of S and T, and functions f, g from S into T. Suppose $f = F$ and $g = G$. Then $G = a \cdot F$ if and only if for every element x of S, $g(x) = a \cdot f(x)$. The theorem is a consequence of (8).

(46) Let us consider a real number a, a non empty, compact topological space

S, a normed linear topological space T, and points F, G of the $\mathbb{R}$-norm space of continuous functions of S and T. Then

(i) $\|F\| = 0$ iff $F = 0_{\alpha}$, and

(ii) $\|a \cdot F\| = |a| \cdot \|F\|$, and

(iii) $\|F + G\| \leqslant \|F\| + \|G\|$,

where α is the $\mathbb{R}$-norm space of continuous functions of S and T. The theorem is a consequence of (34), (38), (36), (41), and (39).

Let S be a non empty, compact topological space and T be a normed linear topological space. Let us observe that the $\mathbb{R}$-norm space of continuous functions of S and T is reflexive, discernible, and real normed space-like.

Now we state the propositions:

(47) Let us consider a non empty, compact topological space S, a normed linear topological space T, points x_1, x_2 of the $\mathbb{R}$-norm space of continuous functions of S and T, and points y_1, y_2 of the real normed space of bounded functions from the carrier of S into T. If $x_1 = y_1$ and $x_2 = y_2$, then $x_1 - x_2 = y_1 - y_2$. The theorem is a consequence of (39) and (38).

(48) Let us consider a non empty, compact topological space S, a normed linear topological space T, points F, G, H of the $\mathbb{R}$-norm space of continuous functions of S and T, and functions f, g, h from S into T. Suppose $f = F$ and $g = G$ and $h = H$. Then $H = F - G$ if and only if for every element x of S, $h(x) = f(x) - g(x)$. The theorem is a consequence of (44).

(49) Let us consider a non empty topological space S, a normed linear topological space T, a sequence H of partial functions from the carrier of S into the carrier of T, and a function L_1 from S into T. Suppose H is uniform-convergent on the carrier of S and for every natural number n, there exists a function H_1 from S into T such that $H_1 = H(n)$ and H_1 is continuous and $L_1 = \lim_{\alpha} H$. Then L_1 is continuous, where α is the carrier of S.

PROOF: For every point x of S, L_1 is continuous at x by (30), [7, (33),(11)]. □

(50) Let us consider a non empty, compact topological space S, a normed linear topological space T, and a subset Y of the carrier of the real normed space of bounded functions from the carrier of S into T. Suppose $Y =$ the continuous functions of S and T. Then Y is closed. The theorem is a consequence of (49).

(51) Let us consider a non empty, compact topological space S, and a normed linear topological space T. Suppose T is complete. Let us consider a sequence s_3 of the $\mathbb{R}$-norm space of continuous functions of S and T.

If s_3 is Cauchy sequence by norm, then s_3 is convergent. The theorem is a consequence of (34), (47), (36), and (50).

(52) Let us consider a non empty, compact topological space S, and a normed linear topological space T. Suppose T is complete. Then the $\mathbb{R}$-norm space of continuous functions of S and T is complete. The theorem is a consequence of (51).

5. Some Properties of Support

Let X be a zero structure and f be a (the carrier of X)-valued function. The functor support f yielding a set is defined by

(Def. 9) for every object x, $x \in it$ iff $x \in \operatorname{dom} f$ and $f_{/x} \neq 0_X$.

Now we state the proposition:

(53) Let us consider a zero structure X, and a (the carrier of X)-valued function f. Then support $f \subseteq \operatorname{dom} f$.

Let X be a non empty topological space, T be a real linear space, and f be a function from X into T. One can verify that the functor support f yields a subset of X. Now we state the propositions:

(54) Let us consider a non empty topological space X, a real linear space T, and functions f, g from X into T. Then $\operatorname{support}(f+g) \subseteq \operatorname{support} f \cup \operatorname{support} g$.

(55) Let us consider a non empty topological space X, a real linear space T, a function f from X into T, and a real number a. Then $\operatorname{support}(a \cdot f) \subseteq \operatorname{support} f$.

6. Space of Real-valued Continuous Functionals with Bounded Support

Let X be a non empty topological space and T be a normed linear topological space. The functor $\mathrm{C_0Functions}(X, T)$ yielding a non empty subset of $\mathrm{RealVectSpace}((\text{the carrier of } X), T)$ is defined by the term

(Def. 10) $\{f$, where f is a function from the carrier of X into the carrier of T : f is continuous and there exists a non empty subset Y of X such that Y is compact and $\overline{\operatorname{support} f} \subseteq Y\}$.

Now we state the propositions:

(56) Let us consider a non empty topological space X, a normed linear topological space T, and elements v, u of $\mathrm{RealVectSpace}((\text{the carrier of } X), T)$.

Suppose v, $u \in \mathrm{C_0}$Functions(X, T). Then $v + u \in \mathrm{C_0}$Functions(X, T). The theorem is a consequence of (5) and (54).

(57) Let us consider a non empty topological space X, a normed linear topological space T, a real number a, and an element u of RealVectSpace((the carrier of X), T). Suppose $u \in \mathrm{C_0}$Functions(X, T). Then $a \cdot u \in \mathrm{C_0}$Functions$(X, T)$. The theorem is a consequence of (5) and (55).

(58) Let us consider a non empty topological space X, and a normed linear topological space T. Then $\mathrm{C_0}$Functions(X, T) is linearly closed.

Let X be a non empty topological space and T be a normed linear topological space. Let us note that $\mathrm{C_0}$Functions(X, T) is non empty and linearly closed.

The functor $\mathrm{RV_{SP}C_0}$Functions(X, T) yielding a real linear space is defined by the term

(Def. 11) $\langle \mathrm{C_0}$Functions(X, T), Zero($\mathrm{C_0}$Functions(X, T), RealVectSpace((the carrier of X), T)), Add($\mathrm{C_0}$Functions(X, T), RealVectSpace((the carrier of X), T)), Mult($\mathrm{C_0}$Functions(X, T), RealVectSpace((the carrier of X), T))$\rangle$.

Now we state the propositions:

(59) Let us consider a non empty topological space X, and a normed linear topological space T. Then $\mathrm{RV_{SP}C_0}$Functions(X, T) is a subspace of RealVectSpace((the carrier of X), T).

(60) Let us consider a non empty topological space X, a normed linear topological space T, and a set x. Suppose $x \in \mathrm{C_0}$Functions(X, T). Then $x \in$ BdFuncs((the carrier of X), T).

Proof: Consider f being a function from the carrier of X into the carrier of T such that $f = x$ and f is continuous and there exists a non empty subset Y of X such that Y is compact and $\overline{\mathrm{support}\, f} \subseteq Y$. Consider Y being a non empty subset of X such that Y is compact and $\overline{\mathrm{support}\, f} \subseteq Y$. Consider K being a real number such that $0 \leqslant K$ and for every point x of X such that $x \in Y$ holds $\|f(x)\| \leqslant K$. For every element x of X, $\|f(x)\| \leqslant K$. □

Let X be a non empty topological space and T be a normed linear topological space. The functor Norm$\mathrm{C_0}$Functions(X, T) yielding a function from $\mathrm{C_0}$Functions(X, T) into $\mathbb{R}$ is defined by the term

(Def. 12) BdFuncsNorm((the carrier of X), T)$\restriction \mathrm{C_0}$Functions$(X, T)$.

The functor $\mathrm{NormSp_{C_0}}$Functions(X, T) yielding a normed structure is defined by the term

(Def. 13) $\langle \mathrm{C_0}$Functions(X, T), Zero($\mathrm{C_0}$Functions(X, T), RealVectSpace((the carrier of X), T)), Add($\mathrm{C_0}$Functions(X, T), RealVectSpace((the carrier of X), T)), Mult($\mathrm{C_0}$Functions(X, T), RealVectSpace((the carrier of X), T)), NormC0Functions$(X, T)\rangle$.

Let us note that NormSp$_{\mathrm{C}_0}$Functions(X, T) is strict and non empty.

Now we state the proposition:

(61) Let us consider a non empty topological space X, a normed linear topological space T, and a set x. Suppose $x \in$ C$_0$Functions(X, T). Then $x \in$ the continuous functions of X and T.

Let us consider a non empty topological space X and a normed linear topological space T. Now we state the propositions:

(62) $0_{\mathrm{RV_{SP}C_0Functions}(X,T)} = X \longmapsto 0_T$.

(63) $0_{\mathrm{NormSp}_{\mathrm{C}_0}\mathrm{Functions}(X,T)} = X \longmapsto 0_T$. The theorem is a consequence of (62).

(64) Let us consider a non empty topological space X, a normed linear topological space T, points x_1, x_2 of NormSp$_{\mathrm{C}_0}$Functions(X, T), and points y_1, y_2 of the real normed space of bounded functions from the carrier of X into T. If $x_1 = y_1$ and $x_2 = y_2$, then $x_1 + x_2 = y_1 + y_2$.

(65) Let us consider a non empty topological space X, a normed linear topological space T, a real number a, a point x of NormSp$_{\mathrm{C}_0}$Functions(X, T), and a point y of the real normed space of bounded functions from the carrier of X into T. If $x = y$, then $a \cdot x = a \cdot y$.

(66) Let us consider a real number a, a non empty topological space X, a normed linear topological space T, and points F, G of NormSp$_{\mathrm{C}_0}$Functions(X, T). Then

(i) $\|F\| = 0$ iff $F = 0_{\mathrm{NormSp}_{\mathrm{C}_0}\mathrm{Functions}(X,T)}$, and

(ii) $\|a \cdot F\| = |a| \cdot \|F\|$, and

(iii) $\|F + G\| \leqslant \|F\| + \|G\|$.

Proof: $\|F\| = 0$ iff $F = 0_{\mathrm{NormSp}_{\mathrm{C}_0}\mathrm{Functions}(X,T)}$. $\|a \cdot F\| = |a| \cdot \|F\|$. $\|F + G\| \leqslant \|F\| + \|G\|$ by (60), (64) [6, (21)]. □

(67) Let us consider a non empty topological space X, and a normed linear topological space T. Then NormSp$_{\mathrm{C}_0}$Functions(X, T) is real normed space-like.

Let X be a non empty topological space and T be a normed linear topological space. Let us note that NormSp$_{\mathrm{C}_0}$Functions(X, T) is reflexive, discernible, real normed space-like, vector distributive.

And let us observe that NormSp$_{\mathrm{C}_0}$Functions(X, T) is scalar distributive, scalar associative, scalar unital, Abelian, add-associative, right zeroed, and right complementable.

Now we state the proposition:

(68) Let us consider a non empty topological space X, and a normed linear topological space T. Then $\mathrm{NormSp}_{\mathrm{C}_0}\mathrm{Functions}(X, T)$ is a real normed space.

References

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

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Bruce K. Driver. *Analysis Tools with Applications*. Springer, Berlin, 2003.

[4] Takaya Nishiyama, Keiji Ohkubo, and Yasunari Shidama. The continuous functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):269–275, 2004.

[5] Laurent Schwartz. *Théorie des ensembles et topologie, tome 1. Analyse*. Hermann, 1997.

[6] Yasumasa Suzuki. Banach space of bounded real sequences. *Formalized Mathematics*, 12 (**2**):77–83, 2004.

[7] Hiroshi Yamazaki. Functional sequence in norm space. *Formalized Mathematics*, 28(**4**): 263–268, 2020. doi:10.2478/forma-2020-0023.

Accepted March 30, 2021

FORMALIZED MATHEMATICS
Vol. 29, No. 1, Pages 63–68, 2021
DOI: 10.2478/forma-2021-0006

sciendo
https://sciendo.com/journal/forma

Elementary Number Theory Problems. Part II

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Dariusz Surowik
University of Białystok
Poland

Summary. In this paper problems 14, 15, 29, 30, 34, 78, 83, 97, and 116 from [6] are formalized, using the Mizar formalism [1], [2], [3]. Some properties related to the divisibility of prime numbers were proved. It has been shown that the equation of the form $p^2 + 1 = q^2 + r^2$, where p, q, r are prime numbers, has at least four solutions and it has been proved that at least five primes can be represented as the sum of two fourth powers of integers. We also proved that for at least one positive integer, the sum of the fourth powers of this number and its successor is a composite number. And finally, it has been shown that there are infinitely many odd numbers k greater than zero such that all numbers of the form $2^{2^n} + k$ ($n = 1, 2, \dots$) are composite.

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes

MML identifier: NUMBER02, version: 8.1.11 5.65.1394

1. Preliminaries

Let D be a non empty set, f be a D-valued finite sequence, and i be a natural number. One can verify that $f_{\restriction i}$ is D-valued.

From now on a, b, i, k, m, n denote natural numbers, s, z denote non zero natural numbers, and c denotes a complex number.

Now we state the propositions:

(1) $c^5 = c \cdot c \cdot c \cdot c \cdot c$.

(2) $c^6 = c \cdot c \cdot c \cdot c \cdot c \cdot c$. The theorem is a consequence of (1).

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

(3) $c^7 = c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c$. The theorem is a consequence of (2).

(4) $c^8 = c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c$. The theorem is a consequence of (3).

(5) $c^9 = c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c$. The theorem is a consequence of (4).

(6) $c^{10} = c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c \cdot c$. The theorem is a consequence of (5).

(7) If $a = n - 1$ and $k < n$, then $k = 0$ or ... or $k = a$.

(8) $-1 \operatorname{div} 3 = -1$.

(9) $-1 \bmod 3 = 2$. The theorem is a consequence of (8).

(10) 30 is not prime.

2. Divisibility of Natural Numbers

Now we state the propositions:

(11) If $n < 31$ and n is prime, then $n = 2$ or $n = 3$ or $n = 5$ or $n = 7$ or $n = 11$ or $n = 13$ or $n = 17$ or $n = 19$ or $n = 23$ or $n = 29$. The theorem is a consequence of (10).

(12) If $k < 961$ and $n \cdot n \leqslant k$ and n is prime, then $n = 2$ or $n = 3$ or $n = 5$ or $n = 7$ or $n = 11$ or $n = 13$ or $n = 17$ or $n = 19$ or $n = 23$ or $n = 29$. The theorem is a consequence of (11).

(13) 113 is prime.

Proof: For every element n of $\mathbb{N}$ such that $1 < n$ and $n \cdot n \leqslant 113$ and n is prime holds $n \nmid 113$. □

(14) 337 is prime.

Proof: For every element n of $\mathbb{N}$ such that $1 < n$ and $n \cdot n \leqslant 337$ and n is prime holds $n \nmid 337$. □

(15) 881 is prime.

Proof: For every element n of $\mathbb{N}$ such that $1 < n$ and $n \cdot n \leqslant 881$ and n is prime holds $n \nmid 881$ by [4, (9)], (12). □

(16) If $k < a$, then $a \cdot b + k \bmod a = k$.

(17) $a \mid a^s + a^z$.

(18) $a \mid a^s - a^z$.

(19) $a \mid a^s \cdot (a^z)$.

Let p, q be prime natural numbers. One can verify that $p \cdot q$ is non prime.

Now we state the propositions:

(20) $11 \mid 2^{341} - 2$. The theorem is a consequence of (6).

(21) $31 \mid 2^{341} - 2$. The theorem is a consequence of (1).

(22) There exists k such that $n = z \cdot k + 0$ or ... or $n = z \cdot k + (z - 1)$.

(23) There exists k such that $n = 3 \cdot k$ or $n = 3 \cdot k + 1$ or $n = 3 \cdot k + 2$. The theorem is a consequence of (22).

(24) There exists k such that $n = 4 \cdot k$ or $n = 4 \cdot k + 1$ or $n = 4 \cdot k + 2$ or $n = 4 \cdot k + 3$. The theorem is a consequence of (22).

(25) There exists k such that $n = 5 \cdot k$ or $n = 5 \cdot k + 1$ or $n = 5 \cdot k + 2$ or $n = 5 \cdot k + 3$ or $n = 5 \cdot k + 4$. The theorem is a consequence of (22).

(26) There exists k such that $n = 6 \cdot k$ or $n = 6 \cdot k + 1$ or $n = 6 \cdot k + 2$ or $n = 6 \cdot k + 3$ or $n = 6 \cdot k + 4$ or $n = 6 \cdot k + 5$. The theorem is a consequence of (22).

(27) There exists k such that $n = 7 \cdot k$ or $n = 7 \cdot k + 1$ or $n = 7 \cdot k + 2$ or $n = 7 \cdot k + 3$ or $n = 7 \cdot k + 4$ or $n = 7 \cdot k + 5$ or $n = 7 \cdot k + 6$. The theorem is a consequence of (22).

(28) There exists k such that $n = 8 \cdot k$ or $n = 8 \cdot k + 1$ or $n = 8 \cdot k + 2$ or $n = 8 \cdot k + 3$ or $n = 8 \cdot k + 4$ or $n = 8 \cdot k + 5$ or $n = 8 \cdot k + 6$ or $n = 8 \cdot k + 7$. The theorem is a consequence of (22).

(29) There exists k such that $n = 9 \cdot k$ or $n = 9 \cdot k + 1$ or $n = 9 \cdot k + 2$ or $n = 9 \cdot k + 3$ or $n = 9 \cdot k + 4$ or $n = 9 \cdot k + 5$ or $n = 9 \cdot k + 6$ or $n = 9 \cdot k + 7$ or $n = 9 \cdot k + 8$. The theorem is a consequence of (22).

(30) There exists k such that $n = 10 \cdot k$ or $n = 10 \cdot k + 1$ or $n = 10 \cdot k + 2$ or $n = 10 \cdot k + 3$ or $n = 10 \cdot k + 4$ or $n = 10 \cdot k + 5$ or $n = 10 \cdot k + 6$ or $n = 10 \cdot k + 7$ or $n = 10 \cdot k + 8$ or $n = 10 \cdot k + 9$. The theorem is a consequence of (22).

(31) $3 \nmid n$ if and only if there exists k such that $n = 3 \cdot k + 1$ or $n = 3 \cdot k + 2$. The theorem is a consequence of (23).

(32) $4 \nmid n$ if and only if there exists k such that $n = 4 \cdot k + 1$ or $n = 4 \cdot k + 2$ or $n = 4 \cdot k + 3$. The theorem is a consequence of (24).

(33) $5 \nmid n$ if and only if there exists k such that $n = 5 \cdot k + 1$ or $n = 5 \cdot k + 2$ or $n = 5 \cdot k + 3$ or $n = 5 \cdot k + 4$. The theorem is a consequence of (25).

(34) $6 \nmid n$ if and only if there exists k such that $n = 6 \cdot k + 1$ or $n = 6 \cdot k + 2$ or $n = 6 \cdot k + 3$ or $n = 6 \cdot k + 4$ or $n = 6 \cdot k + 5$. The theorem is a consequence of (26).

(35) $7 \nmid n$ if and only if there exists k such that $n = 7 \cdot k + 1$ or $n = 7 \cdot k + 2$ or $n = 7 \cdot k + 3$ or $n = 7 \cdot k + 4$ or $n = 7 \cdot k + 5$ or $n = 7 \cdot k + 6$. The theorem is a consequence of (27).

(36) $8 \nmid n$ if and only if there exists k such that $n = 8 \cdot k + 1$ or $n = 8 \cdot k + 2$ or $n = 8 \cdot k + 3$ or $n = 8 \cdot k + 4$ or $n = 8 \cdot k + 5$ or $n = 8 \cdot k + 6$ or $n = 8 \cdot k + 7$. The theorem is a consequence of (28).

(37) $9 \nmid n$ if and only if there exists k such that $n = 9 \cdot k + 1$ or $n = 9 \cdot k + 2$ or

$n = 9 \cdot k + 3$ or $n = 9 \cdot k + 4$ or $n = 9 \cdot k + 5$ or $n = 9 \cdot k + 6$ or $n = 9 \cdot k + 7$ or $n = 9 \cdot k + 8$. The theorem is a consequence of (29).

(38) $10 \nmid n$ if and only if there exists k such that $n = 10 \cdot k + 1$ or $n = 10 \cdot k + 2$ or $n = 10 \cdot k + 3$ or $n = 10 \cdot k + 4$ or $n = 10 \cdot k + 5$ or $n = 10 \cdot k + 6$ or $n = 10 \cdot k + 7$ or $n = 10 \cdot k + 8$ or $n = 10 \cdot k + 9$. The theorem is a consequence of (30).

(39) $2^{2^z} \bmod 3 = 1$.

Proof: Define $\mathcal{P}$[non zero natural number] $\equiv 2^{2^{\$_1}} \bmod 3 = 1$. $\mathcal{P}[1]$ by [5, (1)]. For every s such that $\mathcal{P}[s]$ holds $\mathcal{P}[s+1]$. For every s, $\mathcal{P}[s]$. □

Let n be an integer. We say that n is composite if and only if

(Def. 1) $2 \leqslant n$ and n is not prime.

One can check that there exists an integer which is composite and there exists a natural number which is composite and every integer which is composite is also positive and every integer which is prime is also non composite and every integer which is composite is also non prime.

Let m, n be composite natural numbers. Observe that $m \cdot n$ is composite.

Now we state the proposition:

(40) If n is composite, then $4 \leqslant n$.

3. Main Problems

Now we state the propositions:

(41) Suppose $1 \leqslant i \leqslant \operatorname{len}\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle - m$.
Then $a^m \mid \langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle(i)$.

(42) $n^{\mathbf{2}} \mid (n+1)^n - 1$.

Proof: Set $P = \langle \binom{n}{0} n^0 1^n, \ldots, \binom{n}{n} n^n 1^0 \rangle$. Set $c = \operatorname{len} P$. Set $F = P_{\restriction c}$. For every natural number b such that $b \in \operatorname{dom} F$ holds $n^{\mathbf{2}} \mid F(b)$. □

(43) $(2^n - 1)^{\mathbf{2}} \mid 2^{(2^n - 1) \cdot n} - 1$. The theorem is a consequence of (42).

(44) (i) $6 \nmid 2^6 - 2$, and

(ii) $6 \mid 3^6 - 3$, and

(iii) there exists no natural number n such that $n < 6$ and $n \nmid 2^n - 2$ and $n \mid 3^n - 3$.

The theorem is a consequence of (2), (34), (7), and (32).

(45) Let us consider a non zero natural number a. Then there exists a non prime natural number n such that $n \mid a^n - a$. The theorem is a consequence of (18), (20), and (21).

(46) If $7 \nmid a$, then there exists k such that $a^{\mathbf{2}} = 7 \cdot k + 1$ or $a^{\mathbf{2}} = 7 \cdot k + 2$ or $a^{\mathbf{2}} = 7 \cdot k + 4$. The theorem is a consequence of (35).

(47) There exists k such that $a^{\mathbf{2}} = 7 \cdot k$ or $a^{\mathbf{2}} = 7 \cdot k + 1$ or $a^{\mathbf{2}} = 7 \cdot k + 2$ or $a^{\mathbf{2}} = 7 \cdot k + 4$. The theorem is a consequence of (46).

(48) If $7 \nmid a$, then $a^{\mathbf{2}}$ mod $7 = 1$ or $a^{\mathbf{2}}$ mod $7 = 2$ or $a^{\mathbf{2}}$ mod $7 = 4$. The theorem is a consequence of (46) and (16).

(49) (i) $a^{\mathbf{2}}$ mod $7 = 0$, or

(ii) $a^{\mathbf{2}}$ mod $7 = 1$, or

(iii) $a^{\mathbf{2}}$ mod $7 = 2$, or

(iv) $a^{\mathbf{2}}$ mod $7 = 4$.

The theorem is a consequence of (46) and (16).

(50) Suppose there exists k such that $a = 7 \cdot k + 1$ or $a = 7 \cdot k + 2$ or $a = 7 \cdot k + 4$ and there exists k such that $b = 7 \cdot k + 1$ or $b = 7 \cdot k + 2$ or $b = 7 \cdot k + 4$. Then there exists k such that $a + b = 7 \cdot k + 1$ or ... or $a + b = 7 \cdot k + 6$.

(51) Suppose ($a \bmod 7 = 1$ or $a \bmod 7 = 2$ or $a \bmod 7 = 4$) and ($b \bmod 7 = 1$ or $b \bmod 7 = 2$ or $b \bmod 7 = 4$). Then $a+b \bmod 7 = 1$ or ... or $a+b \bmod 7 = 6$. The theorem is a consequence of (16).

(52) If $7 \mid a^{\mathbf{2}} + b^{\mathbf{2}}$, then $7 \mid a$ and $7 \mid b$. The theorem is a consequence of (48) and (49).

(53) (i) $13^{\mathbf{2}} + 1 = 7^{\mathbf{2}} + 11^{\mathbf{2}}$, and

(ii) $17^{\mathbf{2}} + 1 = 11^{\mathbf{2}} + 13^{\mathbf{2}}$, and

(iii) $23^{\mathbf{2}} + 1 = 13^{\mathbf{2}} + 19^{\mathbf{2}}$, and

(iv) $31^{\mathbf{2}} + 1 = 11^{\mathbf{2}} + 29^{\mathbf{2}}$.

(54) (i) $2 = 1^4 + 1^4$, and

(ii) $17 = 1^4 + 2^4$, and

(iii) $97 = 2^4 + 3^4$, and

(iv) $257 = 1^4 + 4^4$, and

(v) $641 = 2^4 + 5^4$.

(55) $0^4 + (0 + 1)^4$ is not composite.

(56) $1^4 + (1 + 1)^4$ is not composite.

(57) $2^4 + (2 + 1)^4$ is not composite.

(58) $3^4 + (3 + 1)^4$ is not composite.

(59) $4^4 + (4 + 1)^4$ is not composite.

(60) (i) $5^4 + (5 + 1)^4$ is composite, and

(ii) there exists no natural number n such that $n < 5$ and $n^4 + (n + 1)^4$ is composite.

The theorem is a consequence of (13), (56), (57), (58), and (59).

(61) If $1 \leqslant a$, then $2^{2^n} + (6 \cdot a - 1) > 6$.

(62) $3 \mid 2^{2^z} + (6 \cdot a - 1)$. The theorem is a consequence of (9) and (39).

(63) If $1 \leqslant a$, then $2^{2^z} + (6 \cdot a - 1)$ is not prime. The theorem is a consequence of (62) and (61).

(64) If $1 \leqslant a$, then $2^{2^z} + (6 \cdot a - 1)$ is composite. The theorem is a consequence of (61) and (63).

(65) Let us consider a non zero natural number z. Then $\{k$, where k is a natural number : k is odd and $2^{2^z} + k$ is composite$\}$ is infinite.
Proof: Set $S = \{k$, where k is a natural number : k is odd and $2^{2^z} + k$ is composite$\}$. Define $\mathcal{F}$(natural number) $= 6 \cdot \$_1 - 1$. Consider f being a many sorted set indexed by $\mathbb{N}_+$ such that for every element n of $\mathbb{N}_+$, $f(n) = \mathcal{F}(n)$. Set $R = \operatorname{rng} f$. $R \subseteq S$. For every element m of $\mathbb{N}$, there exists an element n of $\mathbb{N}$ such that $n \geqslant m$ and $n \in R$. □

References

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

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[4] Marco Riccardi. Pocklington's theorem and Bertrand's postulate. *Formalized Mathematics*, 14(**2**):47–52, 2006. doi:10.2478/v10037-006-0007-y.

[5] Marco Riccardi. Solution of cubic and quartic equations. *Formalized Mathematics*, 17(**2**): 117–122, 2009. doi:10.2478/v10037-009-0012-z.

[6] Wacław Sierpiński. *250 Problems in Elementary Number Theory.* Elsevier, 1970.

Accepted March 30, 2021