Contents

Formaliz. Math. 31 (**1**)

On Bag of 1. Part I
By Yasushige Watase **1**

Differentiation on Interval
By Noboru Endou **9**

Elementary Number Theory Problems. Part VII
By Artur Korniłowicz **23**

Introduction to Graph Enumerations
By Sebastian Koch **31**

On the Formalization of Gram-Schmidt Process for Orthonormalizing a Set of Vectors
By Hiroyuki Okazaki **53**

Isosceles Triangular and Isosceles Trapezoidal Membership Functions Using Centroid Method
By Takashi Mitsuishi **59**

Introduction to Algebraic Geometry
By Yasushige Watase **67**

About Regular Graphs
By Sebastian Koch **75**

Elementary Number Theory Problems. Part VIII
By Artur Korniłowicz **87**

Internal Direct Products and the Universal Property of Direct Product Groups
By Alexander M. Nelson **101**

Normal Extensions
By Christoph Schwarzweller **121**

Antiderivatives and Integration
By Noboru Endou **131**

Embedding Principle for Rings and Abelian Groups
By Yasushige Watase **143**

On Fuzzy Negations and Laws of Contraposition. Lattice of Fuzzy Negations
By Adam Grabowski **151**

Elementary Number Theory Problems. Part IX
By Artur Korniłowicz **161**

Elementary Number Theory Problems. Part X – Diophantine Equations
By Artur Korniłowicz **171**

Multidimensional Measure Space and Integration
By Noboru Endou and Yasunari Shidama **181**

Conway Numbers – Formal Introduction
By Karol Pąk **193**

Integration of Game Theoretic and Tree Theoretic Approaches to Conway Numbers
By Karol Pąk **205**

The Ring of Conway Numbers in Mizar
By Karol Pąk **215**

Elementary Number Theory Problems. Part XI
By Adam Naumowicz **229**

Elementary Number Theory Problems. Part XII – Primes in Arithmetic Progression
By Adam Grabowski **277**

Simple Extensions
By Christoph Schwarzweller *et al.* **287**

Symmetrical Piecewise Linear Functions Composed by Absolute Value Function
By Takashi Mitsuishi **299**

Integral of Continuous Functions of Two Variables
By Noboru Endou and Yasunari Shidama **309**

Tarski Geometry Axioms. Part V – Half-planes and Planes
By Roland Coghetto and Adam Grabowski **325**

Extensions of Orderings
By Christoph Schwarzweller **341**

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 1–8, 2023
DOI: 10.2478/forma-2023-0001
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

On Bag of 1. Part I

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

Summary. The article concerns about formalizing multivariable formal power series and polynomials [3] in one variable in terms of "bag" (as described in detail in [9]), the same notion as multiset over a finite set, in the Mizar system [1], [2]. Polynomial rings and ring of formal power series, both in one variable, have been formalized in [6], [5] respectively, and elements of these rings are represented by infinite sequences of scalars. On the other hand, formalization of a multivariate polynomial requires extra techniques of using "bag" to represent monomials of variables, and polynomials are formalized as a function from bags of variables to the scalar ring. This means the way of construction of the rings are different between single variable and multi variables case (which implies some tedious constructions, e.g. in the case of ten variables in [8], or generally in the problem of prime representing polynomial [7]). Introducing bag-based construction to one variable polynomial ring provides straight way to apply mathematical induction to polynomial rings with respect to the number of variables. Another consequence from the article, a polynomial ring is a subring of an algebra [4] over the same scalar ring, namely a corresponding formal power series. A sketch of actual formalization of the article is consists of the following four steps:

1. translation between **Bags 1** (the set of all bags of a singleton) and $\mathbb{N}$;
2. formalization of a bag-based formal power series in multivariable case over a commutative ring denoted by **Formal-Series**(n, R);
3. formalization of a polynomial ring in one variable by restricting one variable case denoted by **Polynom-Ring**$(1, R)$. A formal proof of the fact that polynomial rings are a subring of **Formal-Series**(n, R), that is R-Algebra, is included as well;
4. formalization of a ring isomorphism to the existing polynomial ring in one variable given by sequence: **Polynom-Ring**$(1, R) \xrightarrow{\sim}$ **Polynom-Ring** R.

MSC: 13F25 13B25 68V20

Keywords: bag; formal power series; polynomial ring

MML identifier: `POLYALGX`, version: `8.1.12 5.74.1441`

1. Preliminaries

From now on o, o_1, o_2 denote objects, n denotes an ordinal number, R, L denote non degenerated commutative rings, and b denotes a bag of 1.

Let us consider a sequence f of R. Now we state the propositions:

(1) Support $f = \emptyset$ if and only if $f = \mathbf{0}.R$.

(2) If Support f is finite, then f is a finite-Support sequence of R. The theorem is a consequence of (1).

(3) If f is a finite-Support sequence of R, then Support f is finite.

Let us consider a bag b of 1. Now we state the propositions:

(4) Translation Bags 1 notation to NAT:

(i) $\operatorname{dom} b = \{0\}$, and

(ii) $\operatorname{rng} b = \{b(0)\}$.

(5) $b = 1 \longmapsto b(0)$.

Proof: For every o such that $o \in \operatorname{dom} b$ holds $b(o) = (1 \longmapsto b(0))(o)$. □

Let us consider bags b_1, b_2 of 1. Now we state the propositions:

(6) $b_1 + b_2 = 1 \longmapsto b_1(0) + b_2(0)$.

Proof: $\operatorname{dom}(b_1 + b_2) = \{0\}$. For every object x such that $x \in \operatorname{dom}(b_1 + b_2)$ holds $(b_1 + b_2)(x) = (1 \longmapsto b_1(0) + b_2(0))(x)$. □

(7) $b_1 -' b_2 = 1 \longmapsto b_1(0) -' b_2(0)$.

Proof: $\operatorname{dom}(b_1 -' b_2) = \{0\}$. For every object x such that $x \in \operatorname{dom}(b_1 -' b_2)$ holds $(b_1 -' b_2)(x) = (1 \longmapsto b_1(0) -' b_2(0))(x)$. □

(8) $b_1(0) \leqslant b_2(0)$ if and only if $b_1 \mid b_2$.

Proof: If $b_1(0) \leqslant b_2(0)$, then $b_1 \mid b_2$. □

(9) Let us consider an ordinal number n. Then BagOrder n linearly orders Bags n.

The functor NBag1 yielding a function from $\mathbb{N}$ into Bags 1 is defined by

(Def. 1) for every element m of $\mathbb{N}$, $it(m) = 1 \longmapsto m$.

The functor BagN1 yielding a function from Bags 1 into $\mathbb{N}$ is defined by

(Def. 2) for every element b of Bags 1, $it(b) = b(0)$.

Now we state the propositions:

(10) $(\text{BagN1}) \cdot (\text{NBag1}) = \mathrm{id}_{\mathbb{N}}$.

Proof: For every o such that $o \in \operatorname{dom}((\text{BagN1}) \cdot (\text{NBag1}))$ holds $((\text{BagN1}) \cdot (\text{NBag1}))(o) = (\mathrm{id}_{\mathbb{N}})(o)$. □

(11) $(\text{NBag1}) \cdot (\text{BagN1}) = \mathrm{id}_{\text{Bags } 1}$.

Proof: For every o such that $o \in \operatorname{dom}((\text{NBag1}) \cdot (\text{BagN1}))$ holds $((\text{NBag1}) \cdot (\text{BagN1}))(o) = (\mathrm{id}_{\text{Bags } 1})(o)$. □

One can check that NBag1 is one-to-one and onto and BagN1 is one-to-one and onto. Now we state the proposition:

(12) Let us consider bags b_1, b_2 of 1. Then

(i) $b_2 \in \operatorname{rng} \operatorname{divisors} b_1$ iff $b_2(0) \leqslant b_1(0)$, and

(ii) $b_2 \in \operatorname{rng} \operatorname{divisors} b_1$ iff $b_2 \mid b_1$.

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

Let us consider a bag b of 1. Now we state the propositions:

(13) $\operatorname{rng} \operatorname{divisors} b = \{x$, where x is a bag of $1 : x(0) \leqslant b(0)\}$. The theorem is a consequence of (12).

(14) $\operatorname{rng}(\text{NBag1} \restriction \mathbb{Z}_{b(0)+1}) = \{x$, where x is a bag of $1 : x(0) \leqslant b(0)\}$.
PROOF: For every o such that $o \in \operatorname{rng}(\text{NBag1} \restriction \mathbb{Z}_{b(0)+1})$ holds $o \in \{x$, where x is a bag of $1 : x(0) \leqslant b(0)\}$. For every o such that $o \in \{x$, where x is a bag of $1 : x(0) \leqslant b(0)\}$ holds $o \in \operatorname{rng}(\text{NBag1} \restriction \mathbb{Z}_{b(0)+1})$. □

(15) $\operatorname{len} \operatorname{divisors} b = b(0) + 1$. The theorem is a consequence of (14) and (13).

2. Natural Number vs. Bag of Singleton

Let n be an ordinal number. Let us consider L. The functor Formal-Series(n, L) yielding a strict, non empty algebra structure over L is defined by

(Def. 3) for every set x, $x \in$ the carrier of it iff x is a series of n, L and for every elements x, y of it and for every series p, q of n, L such that $x = p$ and $y = q$ holds $x + y = p + q$ and for every elements x, y of it and for every series p, q of n, L such that $x = p$ and $y = q$ holds $x \cdot y = p * q$ and for every element a of L and for every element x of it and for every series p of n, L such that $x = p$ holds $a \cdot x = a \cdot p$ and $0_{it} = 0_n L$ and $1_{it} = 1\_(n, L)$.

Let us observe that Formal-Series(n, L) is Abelian, add-associative, right zeroed, right complementable, commutative, and associative and Formal-Series(n, L) is well unital and right distributive.

Now we state the proposition:

(16) Let us consider an ordinal number n, L, an element a of L, and series p, q of n, L. Then $a \cdot (p + q) = a \cdot p + a \cdot q$.
PROOF: For every element i of Bags n, $(a \cdot (p + q))(i) = (a \cdot p + a \cdot q)(i)$. □

Let us consider an ordinal number n, L, elements a, b of L, and a series p of n, L. Now we state the propositions:

(17) $(a + b) \cdot p = a \cdot p + b \cdot p$.
PROOF: For every element i of Bags n, $((a + b) \cdot p)(i) = (a \cdot p + b \cdot p)(i)$. □

(18) $(a \cdot b) \cdot p = a \cdot (b \cdot p)$.

(19) Let us consider an ordinal number n, L, and a series p of n, L. Then $1_L \cdot p = p$.

Let n be an ordinal number. Let us consider L. One can verify that Formal-Series(n, L) is vector distributive, scalar distributive, scalar associative, and scalar unital. Now we state the proposition:

(20) Let us consider an ordinal number n, and L. Then Formal-Series(n, L) is mix-associative.

PROOF: For every element a of L and for every elements x, y of Formal-Series(n, L), $a \cdot (x \cdot y) = (a \cdot x) \cdot y$. □

Let n be an ordinal number. Let us consider L. Let us observe that Formal-Series(n, L) is mix-associative.

3. Constructing R-Algebra of Multivariate Formal Power Series

Now we state the proposition:

(21) Polynom-Ring(n, R) is a subring of Formal-Series(n, R).

PROOF: Set P_2 = Polynom-Ring(n, R). Set F_2 = Formal-Series(n, R). If $o \in$ the carrier of P_2, then $o \in$ the carrier of F_2. The addition of P_2 = (the addition of F_2) $\restriction$ (the carrier of P_2). The multiplication of P_2 = (the multiplication of F_2) $\restriction$ (the carrier of P_2). □

Let us consider R. Now we state the propositions:

(22) $(0_1 R) \cdot (\mathrm{NBag1}) = \mathbf{0}.R$.

PROOF: For every o such that $o \in \mathrm{dom}((0_1 R) \cdot (\mathrm{NBag1}))$ holds $((0_1 R) \cdot (\mathrm{NBag1}))(o) = (\mathbf{0}.R)(o)$. □

(23) $(0_1 R +\cdot (\mathrm{EmptyBag}\, 1, 1_R)) \cdot (\mathrm{NBag1}) = \mathbf{0}.R +\cdot (0, 1_R)$.

PROOF: For every o such that $o \in \mathrm{dom}(\mathbf{0}.R +\cdot (0, 1_R))$ holds $((0_1 R +\cdot (\mathrm{EmptyBag}\, 1, 1_R)) \cdot (\mathrm{NBag1}))(o) = (\mathbf{0}.R +\cdot (0, 1_R))(o)$. □

(24) $(0_1 R +\cdot (1 \longmapsto 1, 1_R)) \cdot (\mathrm{NBag1}) = \mathbf{0}.R +\cdot (1, 1_R)$.

PROOF: For every o such that $o \in \mathrm{dom}(\mathbf{0}.R +\cdot (1, 1_R))$ holds $((0_1 R +\cdot (1 \longmapsto 1, 1_R)) \cdot (\mathrm{NBag1}))(o) = (\mathbf{0}.R +\cdot (1, 1_R))(o)$. □

(25) Let us consider a bag b of 1. Then

(i) $\mathrm{SgmX}(\mathrm{BagOrder}\, 1, \mathrm{rng\ divisors}\, b) = \mathrm{XFS2FS}(\mathrm{NBag1} \restriction \mathbb{Z}_{b(0)+1})$, and

(ii) $\mathrm{divisors}\, b = \mathrm{XFS2FS}(\mathrm{NBag1} \restriction \mathbb{Z}_{b(0)+1})$.

PROOF: Set $F = \mathrm{NBag1} \restriction \mathbb{Z}_{b(0)+1}$. For every natural numbers n, m such that n, $m \in \mathrm{dom}(\mathrm{XFS2FS}(F))$ and $n < m$ holds $(\mathrm{XFS2FS}(F))_{/n} \neq (\mathrm{XFS2FS}(F))_{/m}$ and $\langle (\mathrm{XFS2FS}(F))_{/n}, (\mathrm{XFS2FS}(F))_{/m} \rangle \in \mathrm{BagOrder}\, 1$. Reconsider $S = \mathrm{rng\ divisors}\, b$ as a non empty, finite subset of Bags 1. For every bag p of 1, $p \in S$ iff $p \mid b$. □

4. Constructing Isomorphism from Formal-Series$(1, R)$ to Formal-Series R

Let us consider R. The functor BSFSeries(R) yielding a function from Formal-Series$(1, R)$ into Formal-Series R is defined by

(Def. 4) for every object x such that $x \in$ the carrier of Formal-Series$(1, R)$ there exists a series x_1 of 1, R such that $x_1 = x$ and $it(x) = x_1 \cdot$ (NBag1).

Let us observe that BSFSeries(R) is one-to-one and onto. Now we state the propositions:

(26) Let us consider a ring R, and series f, g of 1, R. Then $(f+g)\cdot$(NBag1) $= f \cdot$ (NBag1) $+ g \cdot$ (NBag1).

Proof: For every o such that $o \in \mathbb{N}$ holds $((f + g) \cdot (\text{NBag1}))(o) = (f \cdot (\text{NBag1}) + g \cdot (\text{NBag1}))(o)$. □

(27) Let us consider elements f, g of Formal-Series$(1, R)$. Then (BSFSeries(R)) $(f + g) =$ (BSFSeries(R))$(f) +$ (BSFSeries(R))(g). The theorem is a consequence of (26).

(28) Let us consider series f, g of 1, R. Then $(f * g) \cdot$ (NBag1) $= f \cdot$ (NBag1) $*$ $g \cdot$ (NBag1).

Proof: For every o such that $o \in \mathbb{N}$ holds $((f * g) \cdot (\text{NBag1}))(o) = (f \cdot (\text{NBag1}) * g \cdot (\text{NBag1}))(o)$. □

(29) Let us consider elements f, g of Formal-Series$(1, R)$. Then (BSFSeries(R)) $(f \cdot g) =$ (BSFSeries(R))$(f) \cdot$ (BSFSeries(R))(g). The theorem is a consequence of (28).

(30) (BSFSeries(R))$(1_{\text{Formal-Series}(1,R)}) = 1_{\text{Formal-Series } R}$. The theorem is a consequence of (23).

Let us consider R. Let us note that BSFSeries(R) is additive, multiplicative, and unity-preserving. Now we state the proposition:

(31) (i) BSFSeries(R) inherits ring isomorphism, and

(ii) Formal-Series R is (Formal-Series$(1, R)$)-isomorphic.

Let us consider R. One can verify that Formal-Series R is (Formal-Series$(1, R)$)-homomorphic, (Formal-Series$(1, R)$)-monomorphic, and (Formal-Series$(1, R)$)-isomorphic.

The functor SBFSeries(R) yielding a function from Formal-Series R into Formal-Series$(1, R)$ is defined by

(Def. 5) for every object x such that $x \in$ the carrier of Formal-Series R there exists a sequence x_1 of R such that $x_1 = x$ and $it(x) = x_1 \cdot$ (BagN1).

Now we state the proposition:

(32) $(\mathrm{BSFSeries}(R))^{-1} = \mathrm{SBFSeries}(R)$.

PROOF: For every o such that $o \in \mathrm{dom}((\mathrm{SBFSeries}(R)) \cdot (\mathrm{BSFSeries}(R)))$ holds $((\mathrm{SBFSeries}(R)) \cdot (\mathrm{BSFSeries}(R)))(o) = (\mathrm{id}_{\mathrm{dom}(\mathrm{BSFSeries}(R))})(o)$. □

Let us consider R. One can check that $\mathrm{SBFSeries}(R)$ is one-to-one and onto.

Now we state the proposition:

(33) $\mathrm{SBFSeries}(R)$ inherits ring homomorphism.

PROOF: Set $P = \mathrm{BSFSeries}(R)$. Set $F_1 = \text{Formal-Series}(1, R)$. Set $F_2 = \text{Formal-Series}\, R$. For every elements x, y of F_2, $(P^{-1})(x+y) = (P^{-1})(x) + (P^{-1})(y)$ and $(P^{-1})(x \cdot y) = (P^{-1})(x) \cdot (P^{-1})(y)$ and $(P^{-1})(\mathbf{1}_{F_2}) = \mathbf{1}_{F_1}$. □

Let us consider R. One can check that $\mathrm{SBFSeries}(R)$ is additive, multiplicative, and unity-preserving. Now we state the proposition:

(34) (i) $\mathrm{SBFSeries}(R)$ inherits ring isomorphism, and

(ii) $\text{Formal-Series}(1, R)$ is $(\text{Formal-Series}\, R)$-isomorphic.

Let us consider R. Let us observe that $\text{Formal-Series}(1, R)$ is $(\text{Formal-Series}\, R)$-homomorphic, $(\text{Formal-Series}\, R)$-monomorphic, and $(\text{Formal-Series}\, R)$-isomorphic.

5. Constructing Isomorphism from Polynom-Ring$(1, R)$ to Polynom-Ring R

Now we state the propositions:

(35) Polynom-Ring R is a subring of Formal-Series R.

(36) Let us consider sequences f_1, g_1 of R. Then $(f_1 + g_1) \cdot (\mathrm{BagN1}) = f_1 \cdot (\mathrm{BagN1}) + g_1 \cdot (\mathrm{BagN1})$.

PROOF: For every o such that $o \in \mathrm{dom}((f_1 + g_1) \cdot (\mathrm{BagN1}))$ holds $((f_1 + g_1) \cdot (\mathrm{BagN1}))(o) = (f_1 \cdot (\mathrm{BagN1}) + g_1 \cdot (\mathrm{BagN1}))(o)$. □

(37) Let us consider a sequence f of the carrier of R. Then $f = f \cdot (\mathrm{BagN1}) \cdot (\mathrm{NBag1})$. The theorem is a consequence of (10).

(38) Let us consider a series f of 1, R. Then $f = f \cdot (\mathrm{NBag1}) \cdot (\mathrm{BagN1})$. The theorem is a consequence of (11).

(39) Let us consider a sequence f of R.

Then $(\mathrm{NBag1})^\circ(\mathrm{Support}\, f) = \mathrm{Support}\, f \cdot (\mathrm{BagN1})$.

PROOF: For every o, $o \in (\mathrm{NBag1})^\circ(\mathrm{Support}\, f)$ iff $o \in \mathrm{Support}\, f \cdot (\mathrm{BagN1})$. □

(40) Let us consider a subset B of $\mathbb{N}$. Then $\overline{\overline{B}} = \overline{\overline{(\mathrm{NBag1})^\circ B}}$.

(41) Let us consider a sequence f of R. Then $\overline{\overline{\mathrm{Support}\, f}} = \overline{\overline{\mathrm{Support}\, f \cdot (\mathrm{BagN1})}}$. The theorem is a consequence of (40) and (39).

(42) Let us consider a series f of 1, R. Then (BagN1)°(Support f) = Support f· (NBag1).

Proof: For every o, $o \in$ (BagN1)°(Support f) iff $o \in$ Support $f \cdot$ (NBag1). □

(43) Let us consider a subset B of Bags 1. Then $\overline{\overline{B}} = \overline{\overline{\text{(BagN1)°}B}}$.

(44) Let us consider a series f of 1, R. Then $\overline{\overline{\text{Support } f}} = \overline{\overline{\text{Support } f \cdot \text{(NBag1)}}}$. The theorem is a consequence of (43) and (42).

Let us consider R. The functor BSPoly(R) yielding a function from Polynom-Ring(1, R) into Polynom-Ring R is defined by the term

(Def. 6) BSFSeries(R)$\restriction\Omega_{\text{Polynom-Ring}(1,R)}$.

Now we state the proposition:

(45) BSPoly(R) is one-to-one and onto.

Proof: BSPoly(R) is onto. □

Let us consider R. Let us observe that BSPoly(R) is one-to-one and onto.

Let us consider elements p, q of Polynom-Ring(1, R) and elements f, g of Formal-Series(1, R). Now we state the propositions:

(46) If $p = f$ and $q = g$, then $p + q = f + g$.

(47) If $p = f$ and $q = g$, then $p \cdot q = f \cdot g$.

Let us consider elements f, g of Polynom-Ring(1, R). Now we state the propositions:

(48) (BSPoly(R))($f + g$) = (BSPoly(R))(f) + (BSPoly(R))(g). The theorem is a consequence of (35), (27), and (46).

(49) (BSPoly(R))($f \cdot g$) = (BSPoly(R))(f) · (BSPoly(R))(g). The theorem is a consequence of (35), (29), and (47).

(50) (BSPoly(R))($1_{\text{Polynom-Ring}(1,R)}$) = $1_{\text{Polynom-Ring } R}$. The theorem is a consequence of (35) and (30).

Let us consider R. Note that BSPoly(R) is additive, multiplicative, and unity-preserving. Now we state the proposition:

(51) (i) BSPoly(R) inherits ring isomorphism, and

(ii) Polynom-Ring R is (Polynom-Ring(1, R))-isomorphic.

Let us consider R. Let us observe that Polynom-Ring R is (Polynom-Ring(1, R))-homomorphic, (Polynom-Ring(1, R))-monomorphic, and (Polynom-Ring(1, R))-isomorphic.

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] Edward J. Barbeau. *Polynomials*. Springer, 2003.

[4] 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.

[5] Ewa Grądzka. The algebra of polynomials. *Formalized Mathematics*, 9(**3**):637–643, 2001.

[6] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.

[7] Karol Pąk. Prime representing polynomial. *Formalized Mathematics*, 29(**4**):221–228, 2021. doi:10.2478/forma-2021-0020.

[8] Karol Pąk. Prime representing polynomial with 10 unknowns. *Formalized Mathematics*, 30(**4**):255–279, 2022. doi:10.2478/forma-2022-0021.

[9] Piotr Rudnicki, Christoph Schwarzweller, and Andrzej Trybulec. Commutative algebra in the Mizar system. *Journal of Symbolic Computation*, 32(1/2):143–169, 2001. doi:10.1006/jsco.2001.0456.

Accepted March 31, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 9–21, 2023
DOI: 10.2478/forma-2023-0002
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Differentiation on Interval

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

Summary. This article generalizes the differential method on intervals, using the Mizar system [2], [3], [12]. Differentiation of real one-variable functions is introduced in Mizar [13], along standard lines (for interesting survey of formalizations of real analysis in various proof-assistants like ACL2 [11], Isabelle/HOL [10], Coq [4], see [5]), but the differentiable interval is restricted to open intervals. However, when considering the relationship with integration [9], since integration is an operation on a closed interval, it would be convenient for differentiation to be able to handle derivates on a closed interval as well. Regarding differentiability on a closed interval, the right and left differentiability have already been formalized [6], but they are the derivatives at the endpoints of an interval and not demonstrated as a differentiation over intervals.

Therefore, in this paper, based on these results, although it is limited to real one-variable functions, we formalize the differentiation on arbitrary intervals and summarize them as various basic propositions. In particular, the chain rule [1] is an important formula in relation to differentiation and integration, extending recent formalized results [7], [8] in the latter field of research.

MSC: 26A06 68V20

Keywords: differentiation on closed interval; chain rule

MML identifier: FDIFF_12, version: 8.1.12 5.74.1441

1. Preliminaries

Now we state the propositions:

(1) Let us consider open subsets A, B of $\mathbb{R}$, and partial functions f, g from $\mathbb{R}$ to $\mathbb{R}$. Suppose f is differentiable on A and $\operatorname{rng}(f\restriction A) \subseteq B$ and g is differentiable on B. Then

(i) $g \cdot f$ is differentiable on A, and

(ii) $(g \cdot f)'_{\restriction A} = g'_{\restriction B} \cdot f \cdot f'_{\restriction A}$.

(2) Let us consider an interval I. Then

(i) $]\inf I, \sup I[$ is an open subset of $\mathbb{R}$, and

(ii) $]\inf I, \sup I[\subseteq I$.

(3) Let us consider an interval I, and a real number x. Suppose $x \in I$ and $x \neq \inf I$ and $x \neq \sup I$. Then $x \in]\inf I, \sup I[$.

Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, an interval I, and a real number x. Now we state the propositions:

(4) If f is right differentiable in x and $x \in I$ and $x \neq \sup I$, then $f \restriction I$ is right differentiable in x.

PROOF: Consider r being a real number such that $r > 0$ and $[x, x + r] \subseteq \operatorname{dom} f$. For every 0-convergent, non-zero sequence h of real numbers and for every constant sequence c of real numbers such that $\operatorname{rng} c = \{x\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom}(f \restriction I)$ and for every natural number n, $h(n) > 0$ holds $h^{-1} \cdot ((f \restriction I_*(h + c)) - (f \restriction I_* c))$ is convergent. □

(5) If f is left differentiable in x and $x \in I$ and $x \neq \inf I$, then $f \restriction I$ is left differentiable in x.

PROOF: Consider r being a real number such that $r > 0$ and $[x - r, x] \subseteq \operatorname{dom} f$. For every 0-convergent, non-zero sequence h of real numbers and for every constant sequence c of real numbers such that $\operatorname{rng} c = \{x\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom}(f \restriction I)$ and for every natural number n, $h(n) < 0$ holds $h^{-1} \cdot ((f \restriction I_*(h + c)) - (f \restriction I_* c))$ is convergent. □

(6) Let us consider a set X, and partial functions f_1, f_2 from X to $\mathbb{R}$. Suppose $\operatorname{dom} f_1 = \operatorname{dom} f_2$. Then

(i) $f_1 + f_2 - f_2 = f_1$, and

(ii) $f_1 - f_2 + f_2 = f_1$.

2. Differentiation on Intervals

Let f be a partial function from $\mathbb{R}$ to $\mathbb{R}$ and I be a non empty interval. We say that f is differentiable on interval I if and only if

(Def. 1) $I \subseteq \operatorname{dom} f$ and $\inf I < \sup I$ and if $\inf I \in I$, then f is right differentiable in $\inf I$ and if $\sup I \in I$, then f is left differentiable in $\sup I$ and f is differentiable on $]\inf I, \sup I[$.

Let I be an interval, non empty subset of $\mathbb{R}$. Assume f is differentiable on interval I. The functor f'_I yielding a partial function from $\mathbb{R}$ to $\mathbb{R}$ is defined by

(Def. 2) $\operatorname{dom} it = I$ and for every real number x such that $x \in I$ holds if $x = \inf I$, then $it(x) = f'_+(x)$ and if $x = \sup I$, then $it(x) = f'_-(x)$ and if $x \neq \inf I$ and $x \neq \sup I$, then $it(x) = f'(x)$.

Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$ and real numbers a, b. Now we state the propositions:

(7) If $a < b$ and f is differentiable on interval $[a, b]$, then f is differentiable on $]a, b[$.

(8) Suppose $a \leqslant b$ and f is differentiable on interval $[a, b]$. Then

(i) $f'_{[a,b]}(a) = f'_+(a)$, and

(ii) $f'_{[a,b]}(b) = f'_-(b)$, and

(iii) for every real number x such that $x \in]a, b[$ holds $f'_{[a,b]}(x) = f'(x)$.

Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, an interval I, and a real number x. Now we state the propositions:

(9) If $f\restriction I$ is right differentiable in x, then f is right differentiable in x and $(f\restriction I)'_+(x) = f'_+(x)$.

PROOF: Consider r being a real number such that $r > 0$ and $[x, x + r] \subseteq \operatorname{dom}(f\restriction I)$. For every 0-convergent, non-zero sequence h of real numbers and for every constant sequence c of real numbers such that $\operatorname{rng} c = \{x\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom} f$ and for every natural number n, $h(n) > 0$ holds $h^{-1} \cdot ((f_*(h+c)) - (f_*c))$ is convergent and $\lim(h^{-1} \cdot ((f_*(h+c)) - (f_*c))) = (f\restriction I)'_+(x)$. □

(10) If $f\restriction I$ is left differentiable in x, then f is left differentiable in x and $(f\restriction I)'_-(x) = f'_-(x)$.

PROOF: Consider r being a real number such that $r > 0$ and $[x - r, x] \subseteq \operatorname{dom}(f\restriction I)$. For every 0-convergent, non-zero sequence h of real numbers and for every constant sequence c of real numbers such that $\operatorname{rng} c = \{x\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom} f$ and for every natural number n, $h(n) < 0$ holds $h^{-1} \cdot ((f_*(h+c)) - (f_*c))$ is convergent and $\lim(h^{-1} \cdot ((f_*(h+c)) - (f_*c))) = (f\restriction I)'_-(x)$. □

Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$ and a non empty interval I. Now we state the propositions:

(11) f is differentiable on interval I if and only if $I \subseteq \operatorname{dom} f$ and for every real number x such that $x \in I$ holds if $x = \inf I$, then $f\restriction I$ is right differentiable in x and if $x = \sup I$, then $f\restriction I$ is left differentiable in x and if $x \in]\inf I, \sup I[$, then f is differentiable in x.

PROOF: If $\inf I \in I$, then f is right differentiable in $\inf I$. If $\sup I \in I$, then f is left differentiable in $\sup I$. $]\inf I, \sup I[\subseteq I$. For every real number x such that $x \in]\inf I, \sup I[$ holds $f\restriction]\inf I, \sup I[$ is differentiable in x. □

(12) If I is open interval, then f is differentiable on I iff f is differentiable on interval I.

Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$ and real numbers x_0, r. Now we state the propositions:

(13) If f is right differentiable in x_0 and $\operatorname{rng} f = \{r\}$, then $f'_+(x_0) = 0$.
PROOF: For every non-zero, 0-convergent sequence h of real numbers and for every constant sequence c of real numbers such that $\operatorname{rng} c = \{x_0\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom} f$ and for every natural number n, $h(n) > 0$ holds $h^{-1} \cdot ((f_*(h+c)) - (f_*c))$ is convergent and $\lim(h^{-1} \cdot ((f_*(h+c)) - (f_*c))) = 0$. □

(14) If f is left differentiable in x_0 and $\operatorname{rng} f = \{r\}$, then $f'_-(x_0) = 0$.
PROOF: For every non-zero, 0-convergent sequence h of real numbers and for every constant sequence c of real numbers such that $\operatorname{rng} c = \{x_0\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom} f$ and for every natural number n, $h(n) < 0$ holds $h^{-1} \cdot ((f_*(h+c)) - (f_*c))$ is convergent and $\lim(h^{-1} \cdot ((f_*(h+c)) - (f_*c))) = 0$. □

(15) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and a non empty interval I. Suppose $I \subseteq \operatorname{dom} f$ and $\inf I < \sup I$ and there exists a real number r such that $\operatorname{rng} f = \{r\}$. Then

(i) f is differentiable on interval I, and

(ii) for every real number x such that $x \in I$ holds $f'_I(x) = 0$.

PROOF: Consider r being a real number such that $\operatorname{rng} f = \{r\}$. Set $J =]\inf I, \sup I[$. For every real number x such that $x \in J$ holds $f \upharpoonright J$ is differentiable in x. For every real number x such that $x \in I$ holds $f'_I(x) = 0$. □

Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$ and a real number x_0. Now we state the propositions:

(16) If $\operatorname{dom} f \subseteq]-\infty, x_0[$ and f is left continuous in x_0, then f is continuous in x_0.

(17) If $\operatorname{dom} f \subseteq]x_0, +\infty[$ and f is right continuous in x_0, then f is continuous in x_0.

3. Fundamental Properties

Now we state the proposition:

(18) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and a non empty interval I. Suppose $I \subseteq \operatorname{dom} f$ and $\inf I < \sup I$ and $f \upharpoonright I = \mathrm{id}_I$. Then

(i) f is differentiable on interval I, and

(ii) for every real number x such that $x \in I$ holds $f'_I(x) = 1$.

PROOF: For every set x such that $x \in I$ holds $f(x) = x$. Set $J =]\inf I, \sup I[$. For every set x such that $x \in J$ holds $(f\restriction J)(x) = x$. For every real number x such that $x \in J$ holds $f\restriction J$ is differentiable in x. For every real number x such that $x \in I$ holds $f'_I(x) = 1$. □

Let us consider partial functions f, g from $\mathbb{R}$ to $\mathbb{R}$ and a non empty interval I. Now we state the propositions:

(19) Suppose $I \subseteq \operatorname{dom}(f + g)$ and f is differentiable on interval I and g is differentiable on interval I. Then

(i) $f + g$ is differentiable on interval I, and

(ii) $(f + g)'_I = f'_I + g'_I$, and

(iii) for every real number x such that $x \in I$ holds $(f + g)'_I(x) = f'_I(x) + g'_I(x)$.

PROOF: Set $J =]\inf I, \sup I[$. For every real number x such that $x \in J$ holds $(f + g)\restriction J$ is differentiable in x. For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom}(f + g)'_I$ holds $(f + g)'_I(x) = (f'_I + g'_I)(x)$. □

(20) Suppose $I \subseteq \operatorname{dom}(f - g)$ and f is differentiable on interval I and g is differentiable on interval I. Then

(i) $f - g$ is differentiable on interval I, and

(ii) $(f - g)'_I = f'_I - g'_I$, and

(iii) for every real number x such that $x \in I$ holds $(f - g)'_I(x) = f'_I(x) - g'_I(x)$.

PROOF: Reconsider $J =]\inf I, \sup I[$ as an open subset of $\mathbb{R}$. $J \subseteq I$. For every real number x such that $x \in J$ holds $(f - g)\restriction J$ is differentiable in x. For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom}(f - g)'_I$ holds $(f - g)'_I(x) = (f'_I - g'_I)(x)$. □

Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$ and real numbers x_0, r. Now we state the propositions:

(21) If f is right differentiable in x_0, then $r \cdot f$ is right differentiable in x_0 and $(r \cdot f)'_+(x_0) = r \cdot f'_+(x_0)$.

(22) If f is left differentiable in x_0, then $r \cdot f$ is left differentiable in x_0 and $(r \cdot f)'_-(x_0) = r \cdot f'_-(x_0)$.

(23) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, a non empty interval I, and a real number r. Suppose f is differentiable on interval I. Then

(i) $r \cdot f$ is differentiable on interval I, and

(ii) $(r \cdot f)'_I = r \cdot f'_I$, and

(iii) for every real number x such that $x \in I$ holds $(r \cdot f)'_I(x) = r \cdot f'_I(x)$.

PROOF: For every real number x such that $x \in]\inf I, \sup I[$ holds $(r \cdot f) \upharpoonright]\inf I, \sup I[$ is differentiable in x. For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom}(r \cdot f)'_I$ holds $(r \cdot f)'_I(x) = (r \cdot f'_I)(x)$. □

Let us consider partial functions f, g from $\mathbb{R}$ to $\mathbb{R}$ and a non empty interval I. Now we state the propositions:

(24) Suppose f is differentiable on interval I and g is differentiable on interval I. Then

(i) $f \cdot g$ is differentiable on interval I, and

(ii) $(f \cdot g)'_I = g \cdot f'_I + f \cdot g'_I$, and

(iii) for every real number x such that $x \in I$ holds $(f \cdot g)'_I(x) = g(x) \cdot f'_I(x) + f(x) \cdot g'_I(x)$.

PROOF: Reconsider $J =]\inf I, \sup I[$ as an open subset of $\mathbb{R}$. $J \subseteq I$. For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom}(f \cdot g)'_I$ holds $(f \cdot g)'_I(x) = (g \cdot f'_I + f \cdot g'_I)(x)$. □

(25) Suppose $I \subseteq \operatorname{dom}(\frac{f}{g})$ and f is differentiable on interval I and g is differentiable on interval I. Then

(i) $\frac{f}{g}$ is differentiable on interval I, and

(ii) $(\frac{f}{g})'_I = \frac{f'_I \cdot g - g'_I \cdot f}{g^2}$, and

(iii) for every real number x such that $x \in I$ holds $(\frac{f}{g})'_I(x) = \frac{f'_I(x) \cdot g(x) - g'_I(x) \cdot f(x)}{g(x)^2}$.

PROOF: Reconsider $J =]\inf I, \sup I[$ as an open subset of $\mathbb{R}$. $J \subseteq I$. For every set x such that $x \in I$ holds $g(x) \neq 0$. For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom}(\frac{f}{g})'_I$ holds $(\frac{f}{g})'_I(x) = (\frac{f'_I \cdot g - g'_I \cdot f}{g^2})(x)$. □

4. One-Sided Continuity

Now we state the proposition:

(26) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and a real number x_0. Suppose $x_0 \in \operatorname{dom} f$ and f is continuous in x_0. Then f is left continuous in x_0 and right continuous in x_0.

Let us consider a real number x_0 and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(27) f is left continuous in x_0 if and only if $x_0 \in \operatorname{dom} f$ and for every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every real number x such that $x \in \operatorname{dom} f$ and $x_0 - d < x < x_0$ holds $|f(x) - f(x_0)| < e$.

(28) f is right continuous in x_0 if and only if $x_0 \in \operatorname{dom} f$ and for every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every real number x such that $x \in \operatorname{dom} f$ and $x_0 < x < x_0 + d$ holds $|f(x) - f(x_0)| < e$.

(29) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and a real number x_0. Suppose f is left continuous in x_0 and right continuous in x_0. Then f is continuous in x_0.

PROOF: For every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every real number x such that $x \in \operatorname{dom} f$ and $|x - x_0| < d$ holds $|f(x) - f(x_0)| < e$. □

Let us consider a real number x_0 and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(30) Suppose f is left continuous in x_0 and for every real number r such that $r < x_0$ there exists a real number g such that $r < g < x_0$ and $g \in \operatorname{dom} f$. Then

(i) f is left convergent in x_0, and

(ii) $\lim_{x_0-} f = f(x_0)$.

(31) Suppose f is right continuous in x_0 and for every real number r such that $x_0 < r$ there exists a real number g such that $g < r$ and $x_0 < g$ and $g \in \operatorname{dom} f$. Then

(i) f is right convergent in x_0, and

(ii) $\lim_{x_0+} f = f(x_0)$.

(32) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and a real number x_0. Suppose $x_0 \in \operatorname{dom} f$ and f is right convergent in x_0 and $\lim_{x_0+} f = f(x_0)$. Then f is right continuous in x_0.

(33) Let us consider a real number x_0, and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Suppose $x_0 \in \operatorname{dom} f$ and f is left convergent in x_0 and $\lim_{x_0-} f = f(x_0)$. Then f is left continuous in x_0.

(34) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and a real number x_0. Suppose f is convergent in x_0 and $\lim_{x_0} f = f(x_0)$. Then f is continuous in x_0.

PROOF: For every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every real number x such that $x \in \operatorname{dom} f$ and $|x - x_0| < d$ holds $|f(x) - f(x_0)| < e$. □

From now on h denotes a non-zero, 0-convergent sequence of real numbers and c denotes a constant sequence of real numbers.

Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$ and a real number x_0. Now we state the propositions:

(35) If f is right continuous in x_0, then $f\restriction[x_0, +\infty[$ is continuous in x_0.

PROOF: $x_0 \in \operatorname{dom} f$ and for every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every real number x such that $x \in \operatorname{dom} f$ and $x_0 < x < x_0 + d$ holds $|f(x) - f(x_0)| < e$. Set $f_1 = f\restriction[x_0, +\infty[$. For every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every real number x such that $x \in \operatorname{dom} f_1$ and $|x - x_0| < d$ holds $|f_1(x) - f_1(x_0)| < e$. □

(36) If f is left continuous in x_0, then $f\restriction]-\infty, x_0]$ is continuous in x_0.

PROOF: $x_0 \in \operatorname{dom} f$ and for every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every real number x such that $x \in \operatorname{dom} f$ and $x_0 - d < x < x_0$ holds $|f(x) - f(x_0)| < e$. Set $f_1 = f\restriction]-\infty, x_0]$. For every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every real number x such that $x \in \operatorname{dom} f_1$ and $|x - x_0| < d$ holds $|f_1(x) - f_1(x_0)| < e$. □

(37) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and a non empty interval I. If f is differentiable on interval I, then $f\restriction I$ is continuous.

PROOF: For every real number x such that $x \in \operatorname{dom}(f\restriction I)$ holds $f\restriction I$ is continuous in x. □

(38) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and non empty intervals I, J. Suppose f is differentiable on interval I and $J \subseteq I$ and $\inf J < \sup J$. Then

(i) f is differentiable on interval J, and

(ii) for every real number x such that $x \in J$ holds $f'_I(x) = f'_J(x)$.

PROOF: For every real number x such that $x \in J$ holds if $x = \inf J$, then $f\restriction J$ is right differentiable in x and if $x = \sup J$, then $f\restriction J$ is left differentiable in x and if $x \in]\inf J, \sup J[$, then f is differentiable in x. For every real number x such that $x \in J$ holds $f'_I(x) = f'_J(x)$. □

(39) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, an open subset Z of $\mathbb{R}$, and a non empty interval I. Suppose $I \subseteq Z$ and $\inf I < \sup I$ and f is differentiable on Z. Then f is differentiable on interval I.

PROOF: For every real number x such that $x \in I$ holds if $x = \inf I$, then $f\restriction I$ is right differentiable in x and if $x = \sup I$, then $f\restriction I$ is left differentiable in x and if $x \in]\inf I, \sup I[$, then f is differentiable in x. □

5. CHAIN RULE

From now on R, R_1, R_2 denote rests and L, L_1, L_2 denote linear functions.

Let us consider a real number x_0 and partial functions f, g from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(40) Suppose f is right differentiable in x_0 and g is differentiable in $f(x_0)$. Then

(i) $g \cdot f$ is right differentiable in x_0, and

(ii) $(g \cdot f)'_+(x_0) = g'(f(x_0)) \cdot f'_+(x_0)$.

PROOF: Consider r being a real number such that $r > 0$ and $[x_0, x_0 + r] \subseteq \operatorname{dom}(g \cdot f)$. For every h and c such that $\operatorname{rng} c = \{x_0\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom}(g \cdot f)$ and for every natural number n, $h(n) > 0$ holds $h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))$ is convergent and $\lim(h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))) = g'(f(x_0)) \cdot f'_+(x_0)$. □

(41) Suppose f is left differentiable in x_0 and g is differentiable in $f(x_0)$. Then

(i) $g \cdot f$ is left differentiable in x_0, and

(ii) $(g \cdot f)'_-(x_0) = g'(f(x_0)) \cdot f'_-(x_0)$.

PROOF: Consider r being a real number such that $r > 0$ and $[x_0 - r, x_0] \subseteq \operatorname{dom}(g \cdot f)$. For every h and c such that $\operatorname{rng} c = \{x_0\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom}(g \cdot f)$ and for every natural number n, $h(n) < 0$ holds $h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))$ is convergent and $\lim(h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))) = g'(f(x_0)) \cdot f'_-(x_0)$. □

(42) Suppose f is right differentiable in x_0 and g is right differentiable in $f(x_0)$ and for every real number r_1 such that $r_1 > 0$ there exists a real number r_0 such that $r_0 > 0$ and $[x_0, x_0 + r_0] \subseteq \operatorname{dom}([f(x_0), f(x_0) + r_1] \restriction f)$. Then

(i) $g \cdot f$ is right differentiable in x_0, and

(ii) $(g \cdot f)'_+(x_0) = g'_+(f(x_0)) \cdot f'_+(x_0)$.

PROOF: Consider r_1 being a real number such that $r_1 > 0$ and $[f(x_0), f(x_0) + r_1] \subseteq \operatorname{dom} g$. Consider r_0 being a real number such that $r_0 > 0$ and $[x_0, x_0 + r_0] \subseteq \operatorname{dom}([f(x_0), f(x_0) + r_1] \restriction f)$. For every h and c such that $\operatorname{rng} c = \{x_0\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom}(g \cdot f)$ and for every natural number n, $h(n) > 0$ holds $h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))$ is convergent and $\lim(h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))) = g'_+(f(x_0)) \cdot f'_+(x_0)$. □

(43) Suppose f is left differentiable in x_0 and g is right differentiable in $f(x_0)$ and for every real number r_1 such that $r_1 > 0$ there exists a real number r_0 such that $r_0 > 0$ and $[x_0 - r_0, x_0] \subseteq \operatorname{dom}([f(x_0), f(x_0) + r_1] \restriction f)$. Then

(i) $g \cdot f$ is left differentiable in x_0, and

(ii) $(g \cdot f)'_-(x_0) = g'_+(f(x_0)) \cdot f'_-(x_0)$.

PROOF: Consider r_1 being a real number such that $r_1 > 0$ and $[f(x_0), f(x_0) + r_1] \subseteq \operatorname{dom} g$. Consider r_0 being a real number such that $r_0 > 0$ and $[x_0 - r_0, x_0] \subseteq \operatorname{dom}([f(x_0), f(x_0) + r_1] \upharpoonright f)$. For every h and c such that $\operatorname{rng} c = \{x_0\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom}(g \cdot f)$ and for every natural number n, $h(n) < 0$ holds $h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))$ is convergent and $\lim(h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))) = g'_+(f(x_0)) \cdot f'_-(x_0)$. □

(44) Suppose f is differentiable in x_0 and g is right differentiable in $f(x_0)$ and for every real number r_1 such that $r_1 > 0$ there exists a real number r_0 such that $r_0 > 0$ and $[x_0 - r_0, x_0 + r_0] \subseteq \operatorname{dom}([f(x_0), f(x_0) + r_1] \upharpoonright f)$. Then

(i) $g \cdot f$ is differentiable in x_0, and

(ii) $(g \cdot f)'(x_0) = g'_+(f(x_0)) \cdot f'(x_0)$.

The theorem is a consequence of (42) and (43).

(45) Suppose f is right differentiable in x_0 and g is left differentiable in $f(x_0)$ and for every real number r_1 such that $r_1 > 0$ there exists a real number r_0 such that $r_0 > 0$ and $[x_0, x_0 + r_0] \subseteq \operatorname{dom}([f(x_0) - r_1, f(x_0)] \upharpoonright f)$. Then

(i) $g \cdot f$ is right differentiable in x_0, and

(ii) $(g \cdot f)'_+(x_0) = g'_-(f(x_0)) \cdot f'_+(x_0)$.

PROOF: Consider r_1 being a real number such that $r_1 > 0$ and $[f(x_0) - r_1, f(x_0)] \subseteq \operatorname{dom} g$. Consider r_0 being a real number such that $r_0 > 0$ and $[x_0, x_0 + r_0] \subseteq \operatorname{dom}([f(x_0) - r_1, f(x_0)] \upharpoonright f)$. For every h and c such that $\operatorname{rng} c = \{x_0\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom}(g \cdot f)$ and for every natural number n, $h(n) > 0$ holds $h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))$ is convergent and $\lim(h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))) = g'_-(f(x_0)) \cdot f'_+(x_0)$. □

(46) Suppose f is left differentiable in x_0 and g is left differentiable in $f(x_0)$ and for every real number r_1 such that $r_1 > 0$ there exists a real number r_0 such that $r_0 > 0$ and $[x_0 - r_0, x_0] \subseteq \operatorname{dom}([f(x_0) - r_1, f(x_0)] \upharpoonright f)$. Then

(i) $g \cdot f$ is left differentiable in x_0, and

(ii) $(g \cdot f)'_-(x_0) = g'_-(f(x_0)) \cdot f'_-(x_0)$.

PROOF: Consider r_1 being a real number such that $r_1 > 0$ and $[f(x_0) - r_1, f(x_0)] \subseteq \operatorname{dom} g$. Consider r_0 being a real number such that $r_0 > 0$ and $[x_0 - r_0, x_0] \subseteq \operatorname{dom}([f(x_0) - r_1, f(x_0)] \upharpoonright f)$. For every h and c such that $\operatorname{rng} c = \{x_0\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom}(g \cdot f)$ and for every natural number n, $h(n) < 0$ holds $h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))$ is convergent and $\lim(h^{-1} \cdot ((g \cdot f_*(h + c)) - (g \cdot f_* c))) = g'_-(f(x_0)) \cdot f'_-(x_0)$. □

(47) Suppose f is differentiable in x_0 and g is left differentiable in $f(x_0)$ and for every real number r_1 such that $r_1 > 0$ there exists a real number r_0 such that $r_0 > 0$ and $[x_0 - r_0, x_0 + r_0] \subseteq \mathrm{dom}([f(x_0) - r_1, f(x_0)]\restriction f)$. Then

(i) $g \cdot f$ is differentiable in x_0, and

(ii) $(g \cdot f)'(x_0) = g'_-(f(x_0)) \cdot f'(x_0)$.

The theorem is a consequence of (45) and (46).

(48) Suppose f is right differentiable in x_0 and g is right differentiable in $f(x_0)$ and there exists a real number r such that $r > 0$ and $f\restriction[x_0, x_0 + r]$ is non-decreasing. Then

(i) $g \cdot f$ is right differentiable in x_0, and

(ii) $(g \cdot f)'_+(x_0) = g'_+(f(x_0)) \cdot f'_+(x_0)$.

PROOF: Consider R being a real number such that $R > 0$ and $f\restriction[x_0, x_0+R]$ is non-decreasing. $x_0 \in \mathrm{dom}\, f$. For every real number r_1 such that $r_1 > 0$ there exists a real number r_0 such that $r_0 > 0$ and $[x_0, x_0 + r_0] \subseteq \mathrm{dom}([f(x_0), f(x_0) + r_1]\restriction f)$. □

(49) Suppose f is left differentiable in x_0 and g is right differentiable in $f(x_0)$ and there exists a real number r such that $r > 0$ and $f\restriction[x_0 - r, x_0]$ is non-increasing. Then

(i) $g \cdot f$ is left differentiable in x_0, and

(ii) $(g \cdot f)'_-(x_0) = g'_+(f(x_0)) \cdot f'_-(x_0)$.

PROOF: Consider R being a real number such that $R > 0$ and $f\restriction[x_0-R, x_0]$ is non-increasing. $x_0 \in \mathrm{dom}\, f$. For every real number r_1 such that $r_1 > 0$ there exists a real number r_0 such that $r_0 > 0$ and $[x_0 - r_0, x_0] \subseteq \mathrm{dom}([f(x_0), f(x_0) + r_1]\restriction f)$. □

(50) Suppose f is right differentiable in x_0 and g is left differentiable in $f(x_0)$ and there exists a real number r such that $r > 0$ and $f\restriction[x_0, x_0 + r]$ is non-increasing. Then

(i) $g \cdot f$ is right differentiable in x_0, and

(ii) $(g \cdot f)'_+(x_0) = g'_-(f(x_0)) \cdot f'_+(x_0)$.

PROOF: Consider R being a real number such that $R > 0$ and $f\restriction[x_0, x_0+R]$ is non-increasing. $x_0 \in \mathrm{dom}\, f$. For every real number r_1 such that $r_1 > 0$ there exists a real number r_0 such that $r_0 > 0$ and $[x_0, x_0 + r_0] \subseteq \mathrm{dom}([f(x_0) - r_1, f(x_0)]\restriction f)$. □

(51) Suppose f is left differentiable in x_0 and g is left differentiable in $f(x_0)$ and there exists a real number r such that $r > 0$ and $f\restriction[x_0 - r, x_0]$ is non-decreasing. Then

(i) $g \cdot f$ is left differentiable in x_0, and

(ii) $(g \cdot f)'_-(x_0) = g'_-(f(x_0)) \cdot f'_-(x_0)$.

PROOF: Consider R being a real number such that $R > 0$ and $f \restriction [x_0 - R, x_0]$ is non-decreasing. $x_0 \in \operatorname{dom} f$. For every real number r_1 such that $r_1 > 0$ there exists a real number r_0 such that $r_0 > 0$ and $[x_0 - r_0, x_0] \subseteq \operatorname{dom}([f(x_0) - r_1, f(x_0)] \restriction f)$. □

(52) CHAIN RULE:

Let us consider partial functions f, g from $\mathbb{R}$ to $\mathbb{R}$, and non empty intervals I, J. Suppose f is differentiable on interval I and g is differentiable on interval J and $f^\circ I \subseteq J$. Then

(i) $g \cdot f$ is differentiable on interval I, and

(ii) $(g \cdot f)'_I = g'_J \cdot f \cdot f'_I$.

The theorem is a consequence of (4), (5), (11), and (3).

REFERENCES

[1] Tom M. Apostol. *Mathematical Analysis*. Addison-Wesley, 1969.

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

[3] 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.

[4] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Improving real analysis in Coq: A user-friendly approach to integrals and derivatives. In Chris Hawblitzel and Dale Miller, editors, *Certified Programs and Proofs – Second International Conference, CPP 2012, Kyoto, Japan, December 13–15, 2012. Proceedings*, volume 7679 of *Lecture Notes in Computer Science*, pages 289–304. Springer, 2012. doi:10.1007/978-3-642-35308-6_22.

[5] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Formalization of real analysis: A survey of proof assistants and libraries. *Mathematical Structures in Computer Science*, 26:1196–1233, 2015.

[6] Ewa Burakowska and Beata Madras. Real function one-side differentiability. *Formalized Mathematics*, 2(**5**):653–656, 1991.

[7] Noboru Endou. Improper integral. Part I. *Formalized Mathematics*, 29(**4**):201–220, 2021. doi:10.2478/forma-2021-0019.

[8] Noboru Endou. Improper integral. Part II. *Formalized Mathematics*, 29(**4**):279–294, 2021. doi:10.2478/forma-2021-0024.

[9] Noboru Endou. Relationship between the Riemann and Lebesgue integrals. *Formalized Mathematics*, 29(**4**):185–199, 2021. doi:10.2478/forma-2021-0018.

[10] Jacques D. Fleuriot. On the mechanization of real analysis in Isabelle/HOL. In Mark Aagaard and John Harrison, editors, *Theorem Proving in Higher Order Logics*, pages 145–161. Springer Berlin Heidelberg, 2000. ISBN 978-3-540-44659-0.

[11] Ruben Gamboa. *Continuity and Differentiability*, pages 301–315. Springer US, 2000. ISBN 978-1-4757-3188-0. doi:10.1007/978-1-4757-3188-0_18.

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

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

Accepted March 31, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 23–29, 2023
DOI: 10.2478/forma-2023-0003
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part VII

Artur Korniłowicz
Institute of Computer Science
University of Białystok
Poland

Summary. In this paper problems 48, 80, 87, 89, and 124 from [7] are formalized, using the Mizar formalism [1], [2], [4]. The work is natural continuation of [5] and [3] as suggested in [6].

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes

MML identifier: NUMBER07, version: 8.1.12 5.74.1441

1. Preliminaries

From now on X denotes a set, a, b, c, k, m, n denote natural numbers, i, j denote integers, r denotes a real number, and p, p_1, p_2 denote prime numbers.

Now we state the propositions:

(1) $\gcd(m, m \cdot n) = m$.

(2) If $m \neq 1$, then m and $m \cdot n$ are not relatively prime.

(3) If $i \neq -1$ and $i \neq 1$ and $i \mid j$, then $i \nmid j + 1$.

(4) If $i \neq -1$ and $i \neq 1$ and $i \mid j$, then $i \nmid j - 1$.

(5) If $i \mid j$, then i and $j + 1$ are relatively prime.

Proof: For every integer m such that $m \mid i$ and $m \mid j + 1$ holds $m \mid 1$ by [8, (1)]. □

(6) If $i \mid j$, then i and $j - 1$ are relatively prime.

Proof: For every integer m such that $m \mid i$ and $m \mid j - 1$ holds $m \mid 1$. □

(7) If $a+b+c$ is odd and a, b, c are mutually coprime, then a is odd and b is odd and c is odd.

(8) (i) $4 \cdot n \bmod 8 = 0$, or

(ii) $4 \cdot n \bmod 8 = 4$.

(9) If $n \mid 2$, then $n = 1$ or $n = 2$.

(10) If $n \mid 6$, then $n = 1$ or $n = 2$ or $n = 3$ or $n = 6$.

(11) If $n \mid 9$, then $n = 1$ or $n = 3$ or $n = 9$.

(12) If $n \mid 10$, then $n = 1$ or $n = 2$ or $n = 5$ or $n = 10$.

(13) If $n \mid 25$, then $n = 1$ or $n = 5$ or $n = 25$.

(14) If $n \mid 26$, then $n = 1$ or $n = 2$ or $n = 13$ or $n = 26$.

(15) If $n \mid 36$, then $n = 1$ or $n = 2$ or $n = 3$ or $n = 4$ or $n = 6$ or $n = 9$ or $n = 12$ or $n = 18$ or $n = 36$.

(16) If $n \mid 50$, then $n = 1$ or $n = 2$ or $n = 5$ or $n = 10$ or $n = 25$ or $n = 50$.

(17) If $n \mid 65$, then $n = 1$ or $n = 5$ or $n = 13$ or $n = 65$.

(18) If $n \mid 82$, then $n = 1$ or $n = 2$ or $n = 41$ or $n = 82$.

(19) If $n \mid 122$, then $n = 1$ or $n = 2$ or $n = 61$ or $n = 122$.

(20) If $n \mid 145$, then $n = 1$ or $n = 5$ or $n = 29$ or $n = 145$.

(21) If $n \mid 226$, then $n = 1$ or $n = 2$ or $n = 113$ or $n = 226$.

(22) If $n \mid 325$, then $n = 1$ or $n = 5$ or $n = 13$ or $n = 25$ or $n = 65$ or $n = 325$.

(23) If $n \mid 362$, then $n = 1$ or $n = 2$ or $n = 181$ or $n = 362$.

(24) If $n \mid 485$, then $n = 1$ or $n = 5$ or $n = 97$ or $n = 485$.

(25) If $n \mid 626$, then $n = 1$ or $n = 2$ or $n = 313$ or $n = 626$.

(26) If $m \cdot n = p$, then $m = 1$ and $n = p$ or $m = p$ and $n = 1$.

(27) If $m \cdot n = 10$, then $m = 1$ and $n = 10$ or $m = 2$ and $n = 5$ or $m = 5$ and $n = 2$ or $m = 10$ and $n = 1$. The theorem is a consequence of (12).

(28) If $m \cdot n = 25$, then $m = 1$ and $n = 25$ or $m = 5$ and $n = 5$ or $m = 25$ and $n = 1$. The theorem is a consequence of (13).

(29) If $m \cdot n = 26$, then $m = 1$ and $n = 26$ or $m = 2$ and $n = 13$ or $m = 13$ and $n = 2$ or $m = 26$ and $n = 1$. The theorem is a consequence of (14).

(30) If $m \cdot n = 50$, then $m = 1$ and $n = 50$ or $m = 2$ and $n = 25$ or $m = 5$ and $n = 10$ or $m = 10$ and $n = 5$ or $m = 25$ and $n = 2$ or $m = 50$ and $n = 1$. The theorem is a consequence of (16).

(31) If $m \cdot n = 65$, then $m = 1$ and $n = 65$ or $m = 5$ and $n = 13$ or $m = 13$ and $n = 5$ or $m = 65$ and $n = 1$. The theorem is a consequence of (17).

(32) If $m \cdot n = 82$, then $m = 1$ and $n = 82$ or $m = 2$ and $n = 41$ or $m = 41$ and $n = 2$ or $m = 82$ and $n = 1$. The theorem is a consequence of (18).

(33) If $m \cdot n = 122$, then $m = 1$ and $n = 122$ or $m = 2$ and $n = 61$ or $m = 61$ and $n = 2$ or $m = 122$ and $n = 1$. The theorem is a consequence of (19).

(34) If $m \cdot n = 145$, then $m = 1$ and $n = 145$ or $m = 5$ and $n = 29$ or $m = 29$ and $n = 5$ or $m = 145$ and $n = 1$. The theorem is a consequence of (20).

(35) If $m \cdot n = 226$, then $m = 1$ and $n = 226$ or $m = 2$ and $n = 113$ or $m = 113$ and $n = 2$ or $m = 226$ and $n = 1$. The theorem is a consequence of (21).

(36) If $m \cdot n = 325$, then $m = 1$ and $n = 325$ or $m = 5$ and $n = 65$ or $m = 13$ and $n = 25$ or $m = 25$ and $n = 13$ or $m = 65$ and $n = 5$ or $m = 325$ and $n = 1$. The theorem is a consequence of (22).

(37) If $m \cdot n = 362$, then $m = 1$ and $n = 362$ or $m = 2$ and $n = 181$ or $m = 181$ and $n = 2$ or $m = 362$ and $n = 1$. The theorem is a consequence of (23).

(38) If $m \cdot n = 485$, then $m = 1$ and $n = 485$ or $m = 5$ and $n = 97$ or $m = 97$ and $n = 5$ or $m = 485$ and $n = 1$. The theorem is a consequence of (24).

(39) If $m \cdot n = 626$, then $m = 1$ and $n = 626$ or $m = 2$ and $n = 313$ or $m = 313$ and $n = 2$ or $m = 626$ and $n = 1$. The theorem is a consequence of (25).

(40) If $p_1 \neq p_2$, then $2 \leqslant p_1$ and $3 \leqslant p_2$ or $3 \leqslant p_1$ and $2 \leqslant p_2$.

2. Problem 48

Let n be a natural number. We say that n satisfies Sierpiński Problem 48 if and only if

(Def. 1) there exist natural numbers a, b, c such that $n = a + b + c$ and $a > 1$ and $b > 1$ and $c > 1$ and a, b, c are mutually coprime.

Now we state the propositions:

(41) If n is even and $n > 8$, then n satisfies Sierpiński Problem 48. The theorem is a consequence of (5) and (6).

(42) If $n > 17$, then n satisfies Sierpiński Problem 48. The theorem is a consequence of (41), (10), (4), (11), (9), (6), (5), and (3).

(43) 17 doesn't satisfy Sierpiński Problem 48. The theorem is a consequence of (7) and (1).

3. Problem 80

Now we state the propositions:

(44) Let us consider prime numbers p, q, and a natural number n. Suppose $p \cdot (p+1) + q \cdot (q+1) = n \cdot (n+1)$. Then

(i) $p = 2$ and $q = 2$ and $n = 3$, or

(ii) $p = 5$ and $q = 3$ and $n = 6$, or

(iii) $p = 3$ and $q = 5$ and $n = 6$.

The theorem is a consequence of (26).

(45) Let us consider prime numbers p, q, r. If $p \cdot (p+1) + q \cdot (q+1) = r \cdot (r+1)$, then $p = q = 2$ and $r = 3$. The theorem is a consequence of (44).

4. Problem 87

Let n be a natural number. We say that n satisfies Sierpiński Problem 87a if and only if

(Def. 2) there exist prime numbers a, b, c such that a, b, c are mutually different and $n^2 + 1 = a \cdot b \cdot c$.

We say that n satisfies Sierpiński Problem 87b if and only if

(Def. 3) there exist odd prime numbers a, b, c such that a, b, c are mutually different and $n^2 + 1 = a \cdot b \cdot c$.

Now we state the propositions:

(46) $13^2 + 1 = 2 \cdot 5 \cdot 17$.

(47) 13 satisfies Sierpiński Problem 87a. The theorem is a consequence of (46).

(48) $17^2 + 1 = 2 \cdot 5 \cdot 29$.

(49) 17 satisfies Sierpiński Problem 87a. The theorem is a consequence of (48).

(50) $21^2 + 1 = 2 \cdot 13 \cdot 17$.

(51) 21 satisfies Sierpiński Problem 87a. The theorem is a consequence of (50).

(52) $23^2 + 1 = 2 \cdot 5 \cdot 53$.

(53) 23 satisfies Sierpiński Problem 87a. The theorem is a consequence of (52).

(54) $27^2 + 1 = 2 \cdot 5 \cdot 73$.

(55) 27 satisfies Sierpiński Problem 87a. The theorem is a consequence of (54).

(56) If n satisfies Sierpiński Problem 87a and $n \leqslant 27$, then $n \in \{13, 17, 21, 23, 27\}$.

(57) $112^2 + 1 = 5 \cdot 13 \cdot 193$.

(58) 112 satisfies Sierpiński Problem 87b. The theorem is a consequence of (57).

5. Problem 89

Let us consider n. We say that n has exactly two different prime divisors if and only if

(Def. 4) there exist prime numbers p, q such that $p \neq q$ and $p \mid n$ and $q \mid n$ and for every prime number r such that $r \neq p$ and $r \neq q$ holds $r \nmid n$.

Let n be a complex number. We say that n is a product of two different primes if and only if

(Def. 5) there exist prime numbers p, q such that $p \neq q$ and $n = p \cdot q$.

Now we state the propositions:

(59) Let us consider prime numbers p, q, and natural numbers a, b. Suppose $a \neq 1$ and $b \neq 1$ and $p \cdot q = a \cdot b$. Then

(i) $p = a$ and $q = b$, or

(ii) $p = b$ and $q = a$.

(60) If n is a product of two different primes, then for every a and b such that $a \neq 1$ and $b \neq 1$ and $n = a \cdot b$ holds a is prime and b is prime.

(61) p is not a product of two different primes.

(62) If $p_1 \neq p_2$, then $p_1 \cdot p_2$ is a product of two different primes.

(63) If $a \neq 1$ and $a \neq n$ and a is not prime and $a \mid n$, then n is not a product of two different primes.

(64) $p \cdot p$ is not a product of two different primes.

(65) If n is a product of two different primes, then $n \geqslant 6$. The theorem is a consequence of (40).

Let us consider n. We say that n satisfies Sierpiński Problem 89 if and only if

(Def. 6) n is a product of two different primes and $n + 1$ is a product of two different primes and $n + 2$ is a product of two different primes.

Now we state the propositions:

(66) 33 satisfies Sierpiński Problem 89.

(67) 85 satisfies Sierpiński Problem 89.

(68) 93 satisfies Sierpiński Problem 89.

(69) 141 satisfies Sierpiński Problem 89.

(70) 201 satisfies Sierpiński Problem 89.

(71) If n satisfies Sierpiński Problem 89 and $n \leqslant 201$, then $n \in \{33, 85, 93, 141, 201\}$.

(72) There exists no n such that n satisfies Sierpiński Problem 89 and $n+1$ satisfies Sierpiński Problem 89 and $n+2$ satisfies Sierpiński Problem 89 and $n+3$ satisfies Sierpiński Problem 89.

(73) (i) $33 = 3 \cdot 11$, and

(ii) 33 has exactly two different prime divisors.

(74) (i) $34 = 2 \cdot 17$, and

(ii) 34 has exactly two different prime divisors.

(75) (i) $35 = 5 \cdot 7$, and

(ii) 35 has exactly two different prime divisors.

(76) (i) $36 = 2 \cdot 2 \cdot 3 \cdot 3$, and

(ii) 36 has exactly two different prime divisors.

The theorem is a consequence of (15).

6. Problem 124

Now we state the propositions:

(77) If $n = 28 \cdot k + 1$, then $29 \mid (2^{2 \cdot n} + 1)^2 + 2^2$.

(78) If $k > 0$ and $n = 28 \cdot k + 1$, then $(2^{2 \cdot n} + 1)^2 + 2^2$ is composite. The theorem is a consequence of (77).

(79) $\{(2^{2 \cdot n} + 1)^2 + 2^2$, where n is a natural number : $(2^{2 \cdot n} + 1)^2 + 2^2$ is composite$\}$ is infinite.

Proof: Set $X = \{(2^{2 \cdot n} + 1)^2 + 2^2$, where n is a natural number : $(2^{2 \cdot n} + 1)^2 + 2^2$ is composite$\}$. Set $n = 28 \cdot 1 + 1$. $(2^{2 \cdot n} + 1)^2 + 2^2$ is composite. X is natural-membered. For every a such that $a \in X$ there exists b such that $b > a$ and $b \in X$. $\square$

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. Elementary number theory problems. Part VI. *Formalized Mathematics*, 30(**3**):235–244, 2022. doi:10.2478/forma-2022-0019.

[4] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[5] Artur Korniłowicz and Adam Naumowicz. Elementary number theory problems. Part V. *Formalized Mathematics*, 30(**3**):229–234, 2022. doi:10.2478/forma-2022-0018.

[6] Adam Naumowicz. Dataset description: Formalization of elementary number theory in Mizar. In Christoph Benzmüller and Bruce R. Miller, editors, *Intelligent Computer Mathematics – 13th International Conference, CICM 2020, Bertinoro, Italy, July 26–31, 2020, Proceedings*, volume 12236 of *Lecture Notes in Computer Science*, pages 303–308. Springer, 2020. doi:10.1007/978-3-030-53518-6_22.

[7] Wacław Sierpiński. *250 Problems in Elementary Number Theory.* Elsevier, 1970.

[8] Li Yan, Xiquan Liang, and Junjie Zhao. Gauss lemma and law of quadratic reciprocity. *Formalized Mathematics*, 16(**1**):23–28, 2008. doi:10.2478/v10037-008-0004-4.

Accepted March 31, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 31–52, 2023
DOI: 10.2478/forma-2023-0004
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Introduction to Graph Enumerations

Sebastian Koch[1]
Mainz, Germany

Summary. In this article sets of certain subgraphs of a graph are formalized in the Mizar system [7], [1], based on the formalization of graphs in [11] briefly sketched in [12]. The main result is the spanning subgraph theorem.

MSC: 05C05 05C30 68V20

Keywords: graph enumeration; spanning tree

MML identifier: `GLENUM00`, version: `8.1.12 5.74.1441`

Introduction

Subsets of the set of all subgraphs of a graphs are rather rarely addressed directly (cf. [13], [4], [3]), but used as a tool in a wide variety of graph theory topics; e.g. they are needed for graph factorisation, graph reconstruction, random graphs, counting a special type of subgraphs and proving that every connected graph has a spanning subgraph (cf. [2], [14], [5]). The latter is proven in Section 7 of this article, together with the sharper result that we can even guarantee a spanning graph containing an arbitrary edge of the connected graph. As a necessity for that the set of all subtrees of a graph was introduced, as Jessica Enright and Piotr Rudnicki wished for in [6]. This article lays the groundwork for further formalization of any of these topics, in some sense extending and reusing [8] and [10]. It is noteworthy that the attribute `plain` from [9] was utilized here.

[1] mailto: `fly.high.android@gmail.com`

1. Subgraph Set and Subgraph Relation

From now on G, G_1, G_2 denote graphs and H denotes a subgraph of G.

Let us consider G. The functor G.allSubgraphs() yielding a graph-membered set is defined by the term

(Def. 1) {the plain subgraph of G induced by V and E, where V is a non empty subset of the vertices of G, E is a subset of the edges of G : $E \subseteq G$.edgesBetween(V)}.

We introduce the notation G.allSG() as a synonym of G.allSubgraphs(). Let G be a finite graph. One can check that G.allSG() is finite. Now we state the propositions:

(1) $G_2 \in G_1$.allSG() if and only if G_2 is a plain subgraph of G_1.

(2) $H\restriction$(the graph selectors) $\in G$.allSG(). The theorem is a consequence of (1).

(3) $G\restriction$(the graph selectors) $\in G$.allSG(). The theorem is a consequence of (2).

Let us consider G. Let V be a non empty subset of the vertices of G. The functor createGraph(V) yielding a plain subgraph of G is defined by the term

(Def. 2) createGraph($V, \emptyset,$ the function from $\emptyset$ into $V,$ the function from $\emptyset$ into V).

Let us note that createGraph(V) is edgeless. Now we state the propositions:

(4) Let us consider a non empty subset V of the vertices of G. Then createGraph(V) $\in G$.allSG().

(5) Let us consider a non empty subset V of the vertices of G, and a subgraph H of G induced by V and $\emptyset$. Then $H \approx$ createGraph(V).

(6) Let us consider a subgraph H of G with edges the edges of G removed. Then $H \approx$ createGraph(Ω_α), where α is the vertices of G. The theorem is a consequence of (5).

(7) G is edgeless if and only if $G \approx$ createGraph(Ω_α), where α is the vertices of G. The theorem is a consequence of (6).

(8) Let us consider a non empty subset V of the vertices of G_1. Suppose $V \subseteq$ the vertices of G_2. Then createGraph(V) is a subgraph of G_2.

(9) G is edgeless if and only if G.allSG() = the set of all createGraph(V) where V is a non empty subset of the vertices of G. The theorem is a consequence of (1), (7), (4), and (3).

Let us consider G. Let v be a vertex of G. The functor createGraph(v) yielding a plain subgraph of G is defined by the term

(Def. 3) createGraph($\{v\}$).

Let us note that createGraph(v) is trivial and edgeless. Now we state the propositions:

(10) Let us consider a vertex v of G. Then createGraph(v) $\in G$.allSG().

(11) Let us consider a vertex v of G, and a subgraph H of G induced by $\{v\}$ and $\emptyset$. Then $H \approx$ createGraph(v).

(12) Let us consider a vertex v of G_1. Suppose $v \in$ the vertices of G_2. Then createGraph(v) is a subgraph of G_2.

Let G be a non edgeless graph and e be an edge of G.

The functor createGraph(e) yielding a plain subgraph of G is defined by

(Def. 4) there exists a non empty subset V of the vertices of G and there exist functions S, T from $\{e\}$ into V such that it = createGraph($V, \{e\}, S, T$) and $\{$(the source of G)(e), (the target of G)(e)$\} = V$ and $S = e \dot{\longmapsto}$(the source of G)(e) and $T = e \dot{\longmapsto}$(the target of G)(e).

Let us consider a non edgeless graph G and an edge e of G. Now we state the propositions:

(13) (i) the edges of createGraph(e) $= \{e\}$, and

(ii) the vertices of createGraph(e) $= \{$(the source of G)(e), (the target of G)(e)$\}$.

(14) e joins (the source of G)(e) to (the target of G)(e) in createGraph(e). The theorem is a consequence of (13).

Let us consider a non edgeless graph G, an edge e of G, and objects e_0, v, w. Now we state the propositions:

(15) Suppose e_0 joins v to w in createGraph(e). Then

(i) $e_0 = e$, and

(ii) $v =$ (the source of G)(e), and

(iii) $w =$ (the target of G)(e).

The theorem is a consequence of (13).

(16) If e_0 joins v and w in createGraph(e), then $e_0 = e$. The theorem is a consequence of (15).

Let G be a non edgeless graph and e be an edge of G. One can check that createGraph(e) is non edgeless, non-multi, connected, and finite. Let us consider a non edgeless graph G and an edge e of G. Now we state the propositions:

(17) createGraph(e) is loopless if and only if $e \notin G$.loops(). The theorem is a consequence of (14) and (15).

(18) createGraph(e) is acyclic if and only if $e \notin G$.loops(). The theorem is a consequence of (17), (13), and (16).

(19) createGraph(e) $\in G$.allSG().

(20) Let us consider a non edgeless graph G, an edge e of G, and a subgraph H of G induced by $\{(\text{the source of } G)(e), (\text{the target of } G)(e)\}$ and $\{e\}$. Then $H \approx \text{createGraph}(e)$. The theorem is a consequence of (13).

(21) Let us consider a non edgeless graph G, an edge e of G, and a subset V of the vertices of G. Then every supergraph of createGraph(e) extended by the vertices from V is a subgraph of G.

(22) Let us consider an edgeless graph G, a graph union set S, and a graph union G' of S. Suppose for every vertex v of G, there exists an element H' of S such that $v \in$ the vertices of H'. Then G is a subgraph of G'.

(23) Let us consider a non edgeless graph G, a graph union set S, and a graph union G' of S. Suppose for every vertex v of G, there exists an element H' of S such that $v \in$ the vertices of H' and for every edge e of G, there exists an element H' of S such that createGraph(e) is a subgraph of H'. Then G is a subgraph of G'. The theorem is a consequence of (13).

(24) Let us consider an edgeless graph G, a graph union set S, and a graph union G' of S. Suppose for every vertex v of G, createGraph(v) $\in S$. Then G is a subgraph of G'. The theorem is a consequence of (22).

(25) Let us consider a non edgeless graph G, a graph union set S, and a graph union G' of S. Suppose for every vertex v of G, createGraph(v) $\in S$ and for every edge e of G, createGraph(e) $\in S$. Then G is a subgraph of G'. The theorem is a consequence of (23).

(26) Let us consider a non edgeless graph G, a set E, an edge e of G, and a subgraph H of G with edges E removed. If $e \notin E$, then createGraph(e) is a subgraph of H. The theorem is a consequence of (13).

Let us consider a non edgeless graph G, a subgraph H of G with loops removed, a graph union set S, and a graph union G' of S. Now we state the propositions:

(27) Suppose for every vertex v of G, there exists an element H' of S such that $v \in$ the vertices of H' and for every edge e of G such that $e \notin G$.loops() there exists an element H' of S such that createGraph(e) is a subgraph of H'. Then H is a subgraph of G'. The theorem is a consequence of (13) and (26).

(28) Suppose for every vertex v of G, createGraph(v) $\in S$ and for every edge e of G such that $e \notin G$.loops() holds createGraph(e) $\in S$. Then H is a subgraph of G'. The theorem is a consequence of (27).

Let us consider G. Let us observe that G.allSG() is non empty, $\cup$-tolerating, and plain. Let S be a non empty subset of G.allSG(). Let us observe that an element of S is a subgraph of G. Now we state the propositions:

(29) G_2.allSG() $\subseteq$ G_1.allSG() if and only if G_2 is a subgraph of G_1. The theorem is a consequence of (3) and (1).

(30) $G_1 \approx G_2$ if and only if G_1.allSG() = G_2.allSG(). The theorem is a consequence of (29).

Let us consider G_1 and G_2. Let F be a partial graph mapping from G_1 to G_2. The functor SG2SGFunc(F) yielding a function from G_1.allSG() into G_2.allSG() is defined by

(Def. 5) for every plain subgraph H of G_1, $it(H) = \mathrm{rng}(F \restriction H)$.

One can verify that SG2SGFunc(F) is non empty and graph-yielding and dom(SG2SGFunc(F)) is graph-membered and dom(SG2SGFunc(F)) is plain.

Now we state the proposition:

(31) Let us consider a partial graph mapping F from G_1 to G_2. If F is weak subgraph embedding, then SG2SGFunc(F) is one-to-one. The theorem is a consequence of (1).

Let G_1 be a graph, G_2 be a G_1-isomorphic graph, and F be an isomorphism between G_1 and G_2. Let us observe that SG2SGFunc(F) is one-to-one. Now we state the propositions:

(32) Let us consider a partial graph mapping F from G_1 to G_2. Suppose F is onto. Then rng SG2SGFunc(F) = G_2.allSG(). The theorem is a consequence of (1).

(33) If G_2 is G_1-directed-isomorphic, then G_1.allSG() and G_2.allSG() are directed-isomorphic. The theorem is a consequence of (32), (31), and (1).

(34) If G_2 is G_1-isomorphic, then G_1.allSG() and G_2.allSG() are isomorphic. The theorem is a consequence of (32), (31), and (1).

(35) G is a graph union of G.allSG(). The theorem is a consequence of (3) and (1).

(36) (i) G is loopless iff G.allSG() is loopless, and

(ii) G is non-multi iff G.allSG() is non-multi, and

(iii) G is non-directed-multi iff G.allSG() is non-directed-multi, and

(iv) G is simple iff G.allSG() is simple, and

(v) G is directed-simple iff G.allSG() is directed-simple, and

(vi) G is acyclic iff G.allSG() is acyclic, and

(vii) G is edgeless iff G.allSG() is edgeless.

Let G be a loopless graph. Observe that G.allSG() is loopless. Let G be a non-multi graph. Let us observe that G.allSG() is non-multi. Let G be a non-directed-multi graph. One can verify that G.allSG() is non-directed-multi. Let G be a simple graph. One can check that G.allSG() is simple.

Let G be a directed-simple graph. Let us note that G.allSG() is directed-simple. Let G be an acyclic graph. Let us observe that G.allSG() is acyclic. Let G be an edgeless graph. One can verify that G.allSG() is edgeless. Now we state the propositions:

(37) The vertices of G.allSG() $= 2^{\alpha} \setminus \{\emptyset\}$, where α is the vertices of G. The theorem is a consequence of (1).

(38) The edges of G.allSG() $= 2^{\alpha}$, where α is the edges of G. The theorem is a consequence of (1).

Let us consider G. The functor SubgraphRel(G) yielding a binary relation on G.allSG() is defined by

(Def. 6) for every elements H_1, H_2 of G.allSG(), $\langle H_1, H_2 \rangle \in it$ iff H_1 is a subgraph of H_2.

Now we state the propositions:

(39) $\langle H\restriction$(the graph selectors), $G\restriction$(the graph selectors)$\rangle \in$ SubgraphRel(G). The theorem is a consequence of (2) and (3).

(40) field SubgraphRel(G) $= G$.allSG().
PROOF: G.allSG() $\subseteq$ field SubgraphRel(G). □

(41) SubgraphRel(G) partially orders G.allSG().

Let us consider G. One can verify that SubgraphRel(G) is reflexive, antisymmetric, transitive, and partial-order. Now we state the propositions:

(42) $G\restriction$(the graph selectors) is maximal in SubgraphRel(G). The theorem is a consequence of (3), (40), (1), and (39).

(43) SubgraphRel(H) $=$ SubgraphRel(G) $|^2 H$.allSG(). The theorem is a consequence of (29) and (40).

(44) Let us consider a non empty subset S of G.allSG(), and a graph union G' of S. Suppose SubgraphRel(G) $|^2 S$ is a linear order. Let us consider a walk W of G'. Then there exists an element H of S such that W is a walk of H.
PROOF: Define $\mathcal{P}$[walk of G'] $\equiv$ there exists an element H of S such that $\$_1$ is a walk of H. For every trivial walk W of G', $\mathcal{P}[W]$. For every walk W of G' and for every object e such that $e \in W$.last().edgesInOut() and $\mathcal{P}[W]$ holds $\mathcal{P}[W$.addEdge(e)]. For every walk W of G', $\mathcal{P}[W]$. □

2. INDUCED SUBGRAPH SET

Let us consider G. The functor G.allInducedSG() yielding a subset of G.allSG() is defined by the term

(Def. 7) the set of all the plain subgraph of G induced by V where V is a non empty subset of the vertices of G.

Now we state the proposition:

(45) $G_2 \in G_1$.allInducedSG() if and only if there exists a non empty subset V of the vertices of G_1 such that G_2 is a plain subgraph of G_1 induced by V.

Let G be a vertex-finite graph. Observe that G.allInducedSG() is finite. Now we state the propositions:

(46) Let us consider a non empty subset V of the vertices of G, and a subgraph H of G induced by V. Then $H\restriction$(the graph selectors) $\in G$.allInducedSG(). The theorem is a consequence of (45).

(47) $G\restriction$(the graph selectors) $\in G$.allInducedSG(). The theorem is a consequence of (46).

Let us consider G. Observe that G.allInducedSG() is non empty, $\cup$-tolerating, and plain. Now we state the propositions:

(48) G_2.allInducedSG() $\subseteq G_1$.allInducedSG() if and only if there exists a non empty subset V of the vertices of G_1 such that G_2 is a subgraph of G_1 induced by V. The theorem is a consequence of (47) and (45).

(49) $G_1 \approx G_2$ if and only if G_1.allInducedSG() $= G_2$.allInducedSG(). The theorem is a consequence of (48).

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

(50) If F is total and onto, then G_2.allInducedSG() $\subseteq$ rng(SG2SGFunc(F) $\restriction G_1$.allInducedSG()). The theorem is a consequence of (49).

(51) If F is total and continuous, then rng(SG2SGFunc(F)$\restriction G_1$.allInducedSG()) $\subseteq G_2$.allInducedSG(). The theorem is a consequence of (45).

(52) If F is isomorphism, then rng(SG2SGFunc(F)$\restriction G_1$.allInducedSG()) $= G_2$.allInducedSG(). The theorem is a consequence of (50) and (51).

(53) If G_2 is G_1-directed-isomorphic, then G_1.allInducedSG() and G_2.allInducedSG() are directed-isomorphic. The theorem is a consequence of (52), (31), and (45).

(54) If G_2 is G_1-isomorphic, then G_1.allInducedSG() and G_2.allInducedSG() are isomorphic. The theorem is a consequence of (52), (31), and (45).

(55) G is a graph union of G.allInducedSG(). The theorem is a consequence of (47).

(56) (i) G is loopless iff G.allInducedSG() is loopless, and

(ii) G is non-multi iff G.allInducedSG() is non-multi, and

(iii) G is non-directed-multi iff G.allInducedSG() is non-directed-multi, and

(iv) G is simple iff G.allInducedSG() is simple, and

(v) G is directed-simple iff G.allInducedSG() is directed-simple, and

(vi) G is acyclic iff G.allInducedSG() is acyclic, and

(vii) G is edgeless iff G.allInducedSG() is edgeless, and

(viii) G is chordal iff G.allInducedSG() is chordal, and

(ix) G is loopfull iff G.allInducedSG() is loopfull.

Let G be a loopless graph. One can verify that G.allInducedSG() is loopless. Let G be a non-multi graph. Note that G.allInducedSG() is non-multi. Let G be a non-directed-multi graph. Observe that G.allInducedSG() is non-directed-multi. Let G be a simple graph. One can verify that G.allInducedSG() is simple. Let G be a directed-simple graph. Note that G.allInducedSG() is directed-simple. Let G be an acyclic graph. Observe that G.allInducedSG() is acyclic. Let G be an edgeless graph. One can verify that G.allInducedSG() is edgeless. Let G be a chordal graph. Note that G.allInducedSG() is chordal. Let G be a loopfull graph. Let us note that G.allInducedSG() is loopfull. Now we state the propositions:

(57) G is edgeless if and only if G.allInducedSG() = the set of all createGraph (V) where V is a non empty subset of the vertices of G. The theorem is a consequence of (9), (45), and (47).

(58) G is edgeless if and only if G.allSG() = G.allInducedSG(). The theorem is a consequence of (9), (57), and (45).

(59) The vertices of G.allInducedSG() $= 2^{\alpha} \setminus \{\emptyset\}$, where α is the vertices of G. The theorem is a consequence of (37).

3. Spanning Subgraph Set

Let us consider G. The functor G.allSpanningSG() yielding a subset of G.allSG() is defined by the term

(Def. 8) $\{H$, where H is an element of $\Omega_{G.\mathrm{allSG}()} : H$ is spanning$\}$.

We introduce the notation G.allFactors() as a synonym of G.allSpanningSG(). Now we state the propositions:

(60) $G_2 \in G_1$.allSpanningSG() if and only if G_2 is a plain, spanning subgraph of G_1. The theorem is a consequence of (1).

(61) Let us consider a spanning subgraph H of G. Then $H\restriction$(the graph selectors) $\in G$.allSpanningSG(). The theorem is a consequence of (60).

(62) $G\restriction$(the graph selectors) $\in G$.allSpanningSG(). The theorem is a consequence of (61).

(63) createGraph(Ω_α) $\in G$.allSpanningSG(), where α is the vertices of G. The theorem is a consequence of (60).

(64) Let us consider a non edgeless graph G, an edge e of G, and a plain supergraph H of createGraph(e) extended by the vertices from the vertices of G. Then $H \in G$.allSpanningSG(). The theorem is a consequence of (21) and (60).

Let G be a graph. Let us note that G.allSpanningSG() is non empty, $\cup$-tolerating, and plain. Now we state the propositions:

(65) G_2.allSpanningSG() $\subseteq G_1$.allSpanningSG() if and only if G_2 is a spanning subgraph of G_1. The theorem is a consequence of (62) and (60).

(66) $G_1 \approx G_2$ if and only if G_1.allSpanningSG() $= G_2$.allSpanningSG(). The theorem is a consequence of (65).

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

(67) Suppose rng $F_{\mathbb{V}}$ = the vertices of G_2.
Then rng(SG2SGFunc(F)$\restriction G_1$.allSpanningSG()) $\subseteq G_2$.allSpanningSG().

(68) Suppose F is onto and $F_{\mathbb{V}}$ is one-to-one and total.
Then rng(SG2SGFunc(F)$\restriction G_1$.allSpanningSG()) $= G_2$.allSpanningSG(). The theorem is a consequence of (67), (32), (1), and (60).

(69) If F is isomorphism, then rng(SG2SGFunc(F)$\restriction G_1$.allSpanningSG()) $= G_2$.allSpanningSG(). The theorem is a consequence of (68).

(70) If G_2 is G_1-directed-isomorphic, then G_1.allSpanningSG() and G_2.allSpanningSG() are directed-isomorphic. The theorem is a consequence of (69), (31), and (60).

(71) If G_2 is G_1-isomorphic, then G_1.allSpanningSG() and G_2.allSpanningSG() are isomorphic. The theorem is a consequence of (69), (31), and (60).

(72) G is a graph union of G.allSpanningSG(). The theorem is a consequence of (62).

(73) (i) G is loopless iff G.allSpanningSG() is loopless, and
(ii) G is non-multi iff G.allSpanningSG() is non-multi, and
(iii) G is non-directed-multi iff G.allSpanningSG() is non-directed-multi, and

(iv) G is simple iff G.allSpanningSG() is simple, and

(v) G is directed-simple iff G.allSpanningSG() is directed-simple, and

(vi) G is acyclic iff G.allSpanningSG() is acyclic, and

(vii) G is edgeless iff G.allSpanningSG() is edgeless.

Let G be a loopless graph. Note that G.allSpanningSG() is loopless. Let G be a non-multi graph. Observe that G.allSpanningSG() is non-multi. Let G be a non-directed-multi graph. One can verify that G.allSpanningSG() is non-directed-multi. Let G be a simple graph. Note that G.allSpanningSG() is simple.

Let G be a directed-simple graph. Observe that G.allSpanningSG() is directed-simple. Let G be an acyclic graph. One can verify that G.allSpanningSG() is acyclic. Let G be an edgeless graph. Note that G.allSpanningSG() is edgeless. Now we state the propositions:

(74) G is edgeless if and only if G.allSpanningSG() $= \{G\restriction$(the graph selectors)$\}$. The theorem is a consequence of (60) and (62).

(75) The vertices of G.allSpanningSG() $= \{$the vertices of $G\}$. The theorem is a consequence of (60).

(76) The edges of G.allSpanningSG() $= 2^{\alpha}$, where α is the edges of G. The theorem is a consequence of (38) and (60).

(77) G.allInducedSG() $\cap$ G.allSpanningSG() $= \{G\restriction$(the graph selectors)$\}$. The theorem is a consequence of (45), (60), (47), and (62).

4. Forest Subgraph Set

Let us consider G. The functor G.allForests() yielding a subset of G.allSG() is defined by the term

(Def. 9) $\{H$, where H is an element of $\Omega_{G.\mathrm{allSG}()} : H$ is acyclic$\}$.

Now we state the propositions:

(78) $G_2 \in G_1$.allForests() if and only if G_2 is a plain, acyclic subgraph of G_1. The theorem is a consequence of (1).

(79) Let us consider an acyclic subgraph H of G. Then $H\restriction$(the graph selectors) $\in G$.allForests(). The theorem is a consequence of (78).

(80) G is acyclic if and only if $G\restriction$(the graph selectors) $\in G$.allForests(). The theorem is a consequence of (79) and (78).

(81) Let us consider a non empty subset V of the vertices of G. Then createGraph(V) $\in G$.allForests().

(82) Let us consider a vertex v of G. Then createGraph(v) $\in G$.allForests().

(83) Let us consider a non edgeless graph G, and an edge e of G. Suppose $e \notin G$.loops(). Then createGraph(e) $\in G$.allForests(). The theorem is a consequence of (18) and (78).

(84) Let us consider a non edgeless graph G, an edge e of G, a subset V of the vertices of G, and a plain supergraph H of createGraph(e) extended by the vertices from V. If $e \notin G$.loops(), then $H \in G$.allForests(). The theorem is a consequence of (18), (21), and (78).

Let us consider G. Let us note that G.allForests() is non empty, $\cup$-tolerating, plain, acyclic, and simple. Now we state the propositions:

(85) H.allForests() $\subseteq G$.allForests(). The theorem is a consequence of (78).

(86) Let us consider a loopless graph G_2.
Suppose G_2.allForests() $\subseteq G_1$.allForests(). Then G_2 is a subgraph of G_1.
PROOF: The edges of $G_2 \subseteq$ the edges of G_1. □

(87) Let us consider a subgraph H of G with loops removed.
Then G.allForests() $= H$.allForests(). The theorem is a consequence of (85) and (78).

(88) Let us consider loopless graphs G_1, G_2. Then $G_1 \approx G_2$ if and only if G_1.allForests() $= G_2$.allForests(). The theorem is a consequence of (87) and (86).

(89) Let us consider a subgraph G_3 of G_1 with loops removed, and a subgraph G_4 of G_2 with loops removed. Then $G_3 \approx G_4$ if and only if G_1.allForests() $=$ G_2.allForests(). The theorem is a consequence of (87) and (88).

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

(90) If F is weak subgraph embedding,
then rng(SG2SGFunc(F)$\restriction G_1$.allForests()) $\subseteq G_2$.allForests(). The theorem is a consequence of (78) and (1).

(91) If F is one-to-one and onto, then G_2.allForests() $\subseteq$ rng(SG2SGFunc(F) $\restriction G_1$.allForests()). The theorem is a consequence of (78).

(92) If F is isomorphism, then G_2.allForests() = rng(SG2SGFunc(F) $\restriction G_1$.allForests()). The theorem is a consequence of (90) and (91).

(93) If G_2 is G_1-directed-isomorphic, then G_1.allForests() and G_2.allForests() are directed-isomorphic. The theorem is a consequence of (92), (31), and (78).

(94) If G_2 is G_1-isomorphic, then G_1.allForests() and G_2.allForests() are isomorphic. The theorem is a consequence of (92), (31), and (78).

Let us consider a subgraph G_3 of G_1 with loops removed and a subgraph G_4 of G_2 with loops removed. Now we state the propositions:

(95) If G_4 is G_3-directed-isomorphic, then G_1.allForests() and G_2.allForests() are directed-isomorphic. The theorem is a consequence of (87) and (93).

(96) If G_4 is G_3-isomorphic, then G_1.allForests() and G_2.allForests() are isomorphic. The theorem is a consequence of (87) and (94).

(97) Every subgraph of G with loops removed is a graph union of G.allForests(). The theorem is a consequence of (35), (82), (83), (13), (87), and (78).

(98) G is loopless if and only if G is a graph union of G.allForests(). The theorem is a consequence of (97).

(99) The edges of $G = G$.loops() if and only if G.allForests() is edgeless. The theorem is a consequence of (78) and (83).

(100) The edges of $G = G$.loops() if and only if G.allForests() = the set of all createGraph(V) where V is a non empty subset of the vertices of G. The theorem is a consequence of (99), (78), and (81).

(101) The vertices of G.allForests() $= 2^{\alpha} \setminus \{\emptyset\}$, where α is the vertices of G. The theorem is a consequence of (37) and (81).

5. Spanning Forest Subgraph Set

Let us consider G. The functor G.allSpanningForests() yielding a subset of G.allSG() is defined by the term

(Def. 10) $\{H$, where H is an element of $\Omega_{G.\mathrm{allSG}()} : H$ is spanning and acyclic$\}$.

Now we state the propositions:

(102) $G_2 \in G_1$.allSpanningForests() if and only if G_2 is a plain, spanning, acyclic subgraph of G_1. The theorem is a consequence of (1).

(103) G.allSpanningForests() $= G$.allSpanningSG() $\cap G$.allForests(). The theorem is a consequence of (102), (60), and (78).

(104) Let us consider a spanning, acyclic subgraph H of G. Then $H\restriction$(the graph selectors) $\in G$.allSpanningForests(). The theorem is a consequence of (102).

(105) G is acyclic if and only if $G\restriction$(the graph selectors) $\in G$.allSpanningForests(). The theorem is a consequence of (103), (80), and (62).

(106) createGraph(Ω_{α}) $\in G$.allSpanningForests(), where α is the vertices of G. The theorem is a consequence of (81), (63), and (103).

(107) Let us consider a non edgeless graph G, an edge e of G, and a plain supergraph H of createGraph(e) extended by the vertices from the vertices of G. If $e \notin G$.loops(), then $H \in G$.allSpanningForests(). The theorem is a consequence of (64), (84), and (103).

Let us consider G. One can check that G.allSpanningForests() is non empty, $\cup$-tolerating, plain, acyclic, and simple. Now we state the propositions:

(108) Let us consider a spanning subgraph H of G. Then H.allSpanningForests() $\subseteq$ G.allSpanningForests(). The theorem is a consequence of (102).

(109) Let us consider a loopless graph G_2. Suppose G_2.allSpanningForests() $\subseteq$ G_1.allSpanningForests(). Then G_2 is a spanning subgraph of G_1. The theorem is a consequence of (102), (107), and (13).

(110) Let us consider a subgraph H of G with loops removed. Then G.allSpanningForests() $=$ H.allSpanningForests(). The theorem is a consequence of (108) and (102).

(111) Let us consider loopless graphs G_1, G_2. Then $G_1 \approx G_2$ if and only if G_1.allSpanningForests() $=$ G_2.allSpanningForests(). The theorem is a consequence of (110) and (109).

(112) Let us consider a subgraph G_3 of G_1 with loops removed, and a subgraph G_4 of G_2 with loops removed. Then $G_3 \approx G_4$ if and only if G_1.allSpanningForests() $=$ G_2.allSpanningForests(). The theorem is a consequence of (110) and (111).

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

(113) Suppose F is weak subgraph embedding and rng $F_{\mathbb{V}}$ = the vertices of G_2. Then rng(SG2SGFunc(F)$\restriction G_1$.allSpanningForests()) $\subseteq$ G_2.allSpanning Forests(). The theorem is a consequence of (67), (90), and (103).

(114) Suppose F is weak subgraph embedding and onto. Then G_2.allSpanningForests() $=$ rng(SG2SGFunc(F)$\restriction G_1$.allSpanning Forests()). The theorem is a consequence of (113), (68), (91), (103), and (31).

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

(115) If G_2 is G_1-directed-isomorphic, then G_1.allSpanningForests() and G_2.allSpanningForests() are directed-isomorphic. The theorem is a consequence of (114), (31), and (102).

(116) If G_2 is G_1-isomorphic, then G_1.allSpanningForests() and G_2.allSpanningForests() are isomorphic. The theorem is a consequence of (114), (31), and (102).

Let us consider a subgraph G_3 of G_1 with loops removed and a subgraph G_4 of G_2 with loops removed. Now we state the propositions:

(117) If G_4 is G_3-directed-isomorphic, then G_1.allSpanningForests() and G_2.allSpanningForests() are directed-isomorphic. The theorem is a consequence of (110) and (115).

(118) If G_4 is G_3-isomorphic, then G_1.allSpanningForests() and G_2.allSpanningForests() are isomorphic. The theorem is a consequence of (110) and (116).

(119) Every subgraph of G with loops removed is a graph union of G.allSpanningForests(). The theorem is a consequence of (35), (106), (107), (13), (110), and (102).

(120) G is loopless if and only if G is a graph union of G.allSpanningForests(). The theorem is a consequence of (119).

(121) The edges of $G = G$.loops() if and only if G.allSpanningForests() is edgeless. The theorem is a consequence of (99), (103), and (107).

(122) The edges of $G = G$.loops() if and only if for every subgraph H of G with loops removed, G.allSpanningForests() $= \{H\restriction$(the graph selectors)$\}$. The theorem is a consequence of (102) and (104).

(123) The vertices of G.allSpanningForests() $= \{$the vertices of $G\}$. The theorem is a consequence of (103) and (75).

6. Connected Subgraph Set

Let us consider G. The functor G.allConnectedSG() yielding a subset of G.allSG() is defined by the term

(Def. 11) $\{H$, where H is an element of $\Omega_{G.\mathrm{allSG}()} : H$ is connected$\}$.

Now we state the propositions:

(124) $G_2 \in G_1$.allConnectedSG() if and only if G_2 is a plain, connected subgraph of G_1. The theorem is a consequence of (1).

(125) Let us consider a connected subgraph H of G. Then $H\restriction$(the graph selectors) $\in G$.allConnectedSG(). The theorem is a consequence of (124).

(126) G is connected if and only if $G\restriction$(the graph selectors) $\in$ G.allConnectedSG(). The theorem is a consequence of (125) and (124).

(127) Let us consider a vertex v of G.
Then createGraph(v) $\in G$.allConnectedSG().

(128) Let us consider a non edgeless graph G, and an edge e of G. Then createGraph(e) $\in G$.allConnectedSG().

Let us consider G. One can check that G.allConnectedSG() is non empty, $\cup$-tolerating, plain, and connected. Now we state the propositions:

(129) H.allConnectedSG() $\subseteq G$.allConnectedSG(). The theorem is a consequence of (124).

(130) If G_2.allConnectedSG() $\subseteq$ G_1.allConnectedSG(), then G_2 is a subgraph of G_1.

PROOF: The edges of $G_2 \subseteq$ the edges of G_1. □

(131) $G_1 \approx G_2$ if and only if G_1.allConnectedSG() = G_2.allConnectedSG(). The theorem is a consequence of (129) and (130).

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

(132) If F is total, then rng(SG2SGFunc(F)$\restriction G_1$.allConnectedSG()) $\subseteq$ G_2.allConnectedSG(). The theorem is a consequence of (124) and (1).

(133) If F is one-to-one and onto, then G_2.allConnectedSG() $\subseteq$ rng(SG2SGFunc(F)$\restriction G_1$.allConnectedSG()). The theorem is a consequence of (124).

(134) If F is isomorphism, then G_2.allConnectedSG() = rng(SG2SGFunc(F) $\restriction G_1$.allConnectedSG()). The theorem is a consequence of (132) and (133).

(135) If G_2 is G_1-directed-isomorphic, then G_1.allConnectedSG() and G_2.allConnectedSG() are directed-isomorphic. The theorem is a consequence of (134), (31), and (124).

(136) If G_2 is G_1-isomorphic, then G_1.allConnectedSG() and G_2.allConnectedSG() are isomorphic. The theorem is a consequence of (134), (31), and (124).

(137) G is a graph union of G.allConnectedSG(). The theorem is a consequence of (35), (127), (24), (128), and (25).

7. TREE SUBGRAPH SET AND SUBTREE RELATION

Let us consider G. The functor G.allTrees() yielding a subset of G.allSG() is defined by the term

(Def. 12) $\{H$, where H is an element of $\Omega_{G.\mathrm{allSG}()} : H$ is tree-like$\}$.

Now we state the propositions:

(138) $G_2 \in G_1$.allTrees() if and only if G_2 is a plain, tree-like subgraph of G_1. The theorem is a consequence of (1).

(139) G.allTrees() = G.allForests() $\cap G$.allConnectedSG(). The theorem is a consequence of (138), (78), and (124).

(140) Let us consider a tree-like subgraph H of G. Then $H\restriction$(the graph selectors) $\in G$.allTrees(). The theorem is a consequence of (138).

(141) G is tree-like if and only if $G\restriction$(the graph selectors) $\in G$.allTrees(). The theorem is a consequence of (140) and (138).

(142) Let us consider a vertex v of G. Then createGraph(v) $\in$ G.allTrees().

(143) Let us consider a non edgeless graph G, and an edge e of G. Suppose $e \notin G$.loops(). Then createGraph(e) $\in$ G.allTrees(). The theorem is a consequence of (18) and (138).

Let us consider G. Observe that G.allTrees() is non empty, $\cup$-tolerating, plain, tree-like, and simple. Now we state the propositions:

(144) H.allTrees() $\subseteq$ G.allTrees(). The theorem is a consequence of (138).

(145) Let us consider a loopless graph G_2.
Suppose G_2.allTrees() $\subseteq$ G_1.allTrees(). Then G_2 is a subgraph of G_1. The theorem is a consequence of (142), (138), (143), and (13).

(146) Let us consider a subgraph H of G with loops removed. Then G.allTrees() = H.allTrees(). The theorem is a consequence of (144) and (138).

(147) Let us consider loopless graphs G_1, G_2. Then $G_1 \approx G_2$ if and only if G_1.allTrees() = G_2.allTrees(). The theorem is a consequence of (146) and (145).

(148) Let us consider a subgraph G_3 of G_1 with loops removed, and a subgraph G_4 of G_2 with loops removed. Then $G_3 \approx G_4$ if and only if G_1.allTrees() = G_2.allTrees(). The theorem is a consequence of (146) and (147).

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

(149) If F is weak subgraph embedding,
then rng(SG2SGFunc(F)$\restriction G_1$.allTrees()) $\subseteq$ G_2.allTrees(). The theorem is a consequence of (139), (90), and (132).

(150) If F is weak subgraph embedding and onto, then G_2.allTrees() = rng(SG2SGFunc(F)$\restriction G_1$.allTrees()). The theorem is a consequence of (91), (133), (139), (149), and (31).

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

(151) If G_2 is G_1-directed-isomorphic, then G_1.allTrees() and G_2.allTrees() are directed-isomorphic. The theorem is a consequence of (150), (31), and (138).

(152) If G_2 is G_1-isomorphic, then G_1.allTrees() and G_2.allTrees() are isomorphic. The theorem is a consequence of (150), (31), and (138).

Let us consider a subgraph G_3 of G_1 with loops removed and a subgraph G_4 of G_2 with loops removed. Now we state the propositions:

(153) If G_4 is G_3-directed-isomorphic, then G_1.allTrees() and G_2.allTrees() are directed-isomorphic. The theorem is a consequence of (146) and (151).

(154) If G_4 is G_3-isomorphic, then G_1.allTrees() and G_2.allTrees() are isomorphic. The theorem is a consequence of (146) and (152).

(155) Every subgraph of G with loops removed is a graph union of G.allTrees(). The theorem is a consequence of (35), (142), (143), (13), (146), and (138).

(156) G is loopless if and only if G is a graph union of G.allTrees(). The theorem is a consequence of (155).

(157) The edges of $G = G$.loops() if and only if G.allTrees() is edgeless. The theorem is a consequence of (138) and (143).

(158) The edges of $G = G$.loops() if and only if G.allTrees() = the set of all createGraph(v) where v is a vertex of G. The theorem is a consequence of (157), (138), and (142).

Let us consider G. The functor SubtreeRel(G) yielding a binary relation on G.allTrees() is defined by the term

(Def. 13) SubgraphRel(G) $|^2$ G.allTrees().

Now we state the propositions:

(159) Let us consider plain, tree-like subgraphs H_1, H_2 of G. Then $\langle H_1, H_2 \rangle \in$ SubtreeRel(G) if and only if H_1 is a subgraph of H_2. The theorem is a consequence of (1) and (138).

(160) field SubtreeRel(G) = G.allTrees(). The theorem is a consequence of (40).

(161) SubtreeRel(G) partially orders G.allTrees(). The theorem is a consequence of (41) and (160).

Let us consider G. Let us observe that SubtreeRel(G) is reflexive, antisymmetric, transitive, and partial-order. Now we state the propositions:

(162) SubtreeRel(H) = SubtreeRel(G) $|^2$ H.allTrees(). The theorem is a consequence of (43) and (144).

(163) Let us consider a loopless graph G. Then G is edgeless if and only if SubtreeRel(G) = $\mathrm{id}_{G.\mathrm{allTrees}()}$. The theorem is a consequence of (160), (138), (159), (143), and (13).

(164) Let us consider a subgraph H of G with loops removed. Then SubtreeRel(G) = SubtreeRel(H). The theorem is a consequence of (146) and (162).

(165) The edges of $G = G$.loops() if and only if SubtreeRel(G) = $\mathrm{id}_{G.\mathrm{allTrees}()}$. The theorem is a consequence of (164), (163), and (146).

(166) G.allTrees() has the upper Zorn property w.r.t. SubtreeRel(G). The theorem is a consequence of (160), (159), (44), (35), and (138).

Let G be a connected graph.

EVERY CONNECTED GRAPH HAS A SPANNING TREE: there exists a subgraph of G which is plain, spanning, and tree-like.

Now we state the proposition:

(167) Let us consider a connected graph G, and an object e. Suppose $e \in$ (the edges of G) $\setminus$ (G.loops()). Then there exists a plain, spanning, tree-like subgraph T of G such that $e \in$ the edges of T.

8. Spanning Tree Subgraph Set

Let us consider G. The functor G.allSpanningTrees() yielding a subset of G.allSG() is defined by the term

(Def. 14) $\{H$, where H is an element of $\Omega_{G.\mathrm{allSG}()} : H$ is spanning and tree-like$\}$.

Now we state the propositions:

(168) $G_2 \in G_1$.allSpanningTrees() if and only if G_2 is plain, spanning, acyclic subgraph of G_1 and connected. The theorem is a consequence of (1).

(169) G.allSpanningTrees() $= G$.allSpanningSG() $\cap G$.allTrees(). The theorem is a consequence of (168), (60), and (138).

(170) G.allSpanningTrees() $= G$.allConnectedSG() $\cap G$.allSpanningForests(). The theorem is a consequence of (168), (102), and (124).

(171) Let us consider a spanning, acyclic subgraph H of G. Suppose H is connected. Then $H\restriction$(the graph selectors) $\in G$.allSpanningTrees(). The theorem is a consequence of (168).

(172) G is tree-like if and only if $G\restriction$(the graph selectors) $\in G$.allSpanningTrees(). The theorem is a consequence of (169), (141), and (62).

(173) G is connected if and only if G.allSpanningTrees() $\neq \emptyset$. The theorem is a consequence of (168).

Let G be a non connected graph. Let us note that G.allSpanningTrees() is empty. Let G be a connected graph. Observe that G.allSpanningTrees() is non empty, tree-like, and simple. Now we state the propositions:

(174) Let us consider a connected graph G, and a connected, spanning subgraph H of G. Then H.allSpanningTrees() $\subseteq G$.allSpanningTrees(). The theorem is a consequence of (168).

(175) Let us consider a loopless, connected graph G_2. Suppose G_2.allSpanning Trees() $\subseteq G_1$.allSpanningTrees(). Then G_2 is a spanning subgraph of G_1. The theorem is a consequence of (168) and (167).

(176) Let us consider a subgraph H of G with loops removed.
Then G.allSpanningTrees() $= H$.allSpanningTrees(). The theorem is a consequence of (174) and (168).

(177) Let us consider loopless, connected graphs G_1, G_2. Then $G_1 \approx G_2$ if and only if G_1.allSpanningTrees() $= G_2$.allSpanningTrees(). The theorem is a consequence of (176) and (175).

(178) Let us consider connected graphs G_1, G_2, a subgraph G_3 of G_1 with loops removed, and a subgraph G_4 of G_2 with loops removed. Then $G_3 \approx G_4$ if and only if G_1.allSpanningTrees() = G_2.allSpanningTrees(). The theorem is a consequence of (176) and (177).

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

(179) Suppose F is weak subgraph embedding and rng $F_{\mathbb{V}}$ = the vertices of G_2. Then rng(SG2SGFunc(F)$\restriction G_1$.allSpanningTrees()) $\subseteq$ G_2.allSpanningTrees(). The theorem is a consequence of (132), (113), and (170).

(180) Suppose F is weak subgraph embedding and onto. Then G_2.allSpanningTrees() = rng(SG2SGFunc(F)$\restriction G_1$.allSpanningTrees()). The theorem is a consequence of (179), (133), (114), (170), and (31).

(181) If G_2 is G_1-directed-isomorphic, then G_1.allSpanningTrees() and G_2.allSpanningTrees() are directed-isomorphic. The theorem is a consequence of (180), (31), and (168).

(182) If G_2 is G_1-isomorphic, then G_1.allSpanningTrees() and G_2.allSpanningTrees() are isomorphic. The theorem is a consequence of (180), (31), and (168).

Let us consider a subgraph G_3 of G_1 with loops removed and a subgraph G_4 of G_2 with loops removed. Now we state the propositions:

(183) If G_4 is G_3-directed-isomorphic, then G_1.allSpanningTrees() and G_2.allSpanningTrees() are directed-isomorphic. The theorem is a consequence of (176) and (181).

(184) If G_4 is G_3-isomorphic, then G_1.allSpanningTrees() and G_2.allSpanningTrees() are isomorphic. The theorem is a consequence of (176) and (182).

(185) Let us consider a connected graph G. Then every subgraph of G with loops removed is a graph union of G.allSpanningTrees(). The theorem is a consequence of (35), (168), (167), and (176).

(186) Every loopless, connected graph is a graph union of G.allSpanningTrees(). The theorem is a consequence of (185).

(187) G is tree-like if and only if G.allSpanningTrees() = $\{G\restriction$(the graph selectors)$\}$. The theorem is a consequence of (168) and (172).

(188) G is connected if and only if the vertices of G.allSpanningTrees() = $\{$the vertices of $G\}$. The theorem is a consequence of (123) and (170).

9. Component Subgraph Set

Let us consider G. The functor G.allComponents() yielding a subset of G.allSG() is defined by the term

(Def. 15) $\{H$, where H is an element of $\Omega_{G.\mathrm{allSG}()} : H$ is component-like$\}$.

Now we state the propositions:

(189) $G_2 \in G_1$.allComponents() if and only if G_2 is a plain component of G_1. The theorem is a consequence of (1).

(190) G.allComponents() $\subseteq G$.allInducedSG() $\cap G$.allConnectedSG(). The theorem is a consequence of (189) and (124).

(191) Let us consider a component H of G. Then $H\restriction$(the graph selectors) $\in$ G.allComponents(). The theorem is a consequence of (189).

(192) G is connected if and only if $G\restriction$(the graph selectors) $\in G$.allComponents(). The theorem is a consequence of (191) and (189).

Let us consider G. Let us observe that G.allComponents() is non empty, vertex-disjoint, edge-disjoint, $\cup$-tolerating, plain, and connected. Now we state the propositions:

(193) If G_2.allComponents() $\subseteq G_1$.allComponents(), then G_2 is a subgraph of G_1. The theorem is a consequence of (189).

(194) $G_1 \approx G_2$ if and only if G_1.allComponents() $= G_2$.allComponents(). The theorem is a consequence of (189) and (193).

(195) Let us consider a non empty, one-to-one partial graph mapping F from G_1 to G_2. Suppose F is isomorphism. Then G_2.allComponents() $=$ rng(SG2SGFunc(F)$\restriction G_1$.allComponents()). The theorem is a consequence of (189).

(196) If G_2 is G_1-directed-isomorphic, then G_1.allComponents() and G_2.allComponents() are directed-isomorphic. The theorem is a consequence of (195), (31), and (189).

(197) If G_2 is G_1-isomorphic, then G_1.allComponents() and G_2.allComponents() are isomorphic. The theorem is a consequence of (195), (31), and (189).

(198) G is a graph union of G.allComponents(). The theorem is a consequence of (35), (189), (22), (14), (13), and (23).

(199) (i) G is loopless iff G.allComponents() is loopless, and

(ii) G is non-multi iff G.allComponents() is non-multi, and

(iii) G is non-directed-multi iff G.allComponents() is non-directed-multi, and

(iv) G is simple iff G.allComponents() is simple, and

(v) G is directed-simple iff G.allComponents() is directed-simple, and

(vi) G is acyclic iff G.allComponents() is acyclic, and

(vii) G is edgeless iff G.allComponents() is edgeless, and

(viii) G is chordal iff G.allComponents() is chordal, and

(ix) G is loopfull iff G.allComponents() is loopfull.

The theorem is a consequence of (198).

Let G be a loopless graph. Observe that G.allComponents() is loopless. Let G be a non-multi graph. One can verify that G.allComponents() is non-multi. Let G be a non-directed-multi graph. Note that G.allComponents() is non-directed-multi. Let G be a simple graph. Observe that G.allComponents() is simple. Let G be a directed-simple graph. One can verify that G.allComponents() is directed-simple.

Let G be an acyclic graph. Note that G.allComponents() is acyclic. Let G be an edgeless graph. Observe that G.allComponents() is edgeless. Let G be a chordal graph. One can verify that G.allComponents() is chordal. Let G be a loopfull graph. One can check that G.allComponents() is loopfull. Now we state the propositions:

(200) G is connected if and only if G.allComponents() $= \{G\restriction$(the graph selectors)$\}$. The theorem is a consequence of (192) and (189).

(201) The vertices of G.allComponents() $= G$.componentSet().

(202) G.numComponents() $= \overline{\overline{G\text{.allComponents()}}}$.

PROOF: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a plain component H of G such that $\$_1 = H$ and $\$_2 =$ the vertices of H. For every object x such that $x \in G$.allComponents() there exists an object y such that $\mathcal{P}[x, y]$. Consider f being a function such that $\operatorname{dom} f = G$.allComponents() and for every object x such that $x \in G$.allComponents() holds $\mathcal{P}[x, f(x)]$. □

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] Ricky W. Butler and Jon A. Sjogren. A PVS graph theory library. Technical report, NASA Langley, 1998.

[4] Ching-Tsun Chou. A formal theory of undirected graphs in higher-order logic. In Thomas F. Melham and Juanito Camilleri, editors, *Higher Order Logic Theorem Proving and Its Applications, 7th International Workshop, Valletta, Malta, September 19–22, 1994, Proceedings*, volume 859 of *Lecture Notes in Computer Science*, pages 144–157. Springer, 1994. doi:10.1007/3-540-58450-1_40.

[5] Reinhard Diestel. *Graph Theory*, volume Graduate Texts in Mathematics; 173. Springer, Berlin, fifth edition, 2017. ISBN 978-3-662-53621-6.

[6] Jessica Enright and Piotr Rudnicki. Helly property for subtrees. *Formalized Mathematics*, 16(**2**):91–96, 2008. doi:10.2478/v10037-008-0013-3.

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

[8] Sebastian Koch. Miscellaneous graph preliminaries. Part I. *Formalized Mathematics*, 29 (**1**):21–38, 2021. doi:10.2478/forma-2021-0003.

[9] Sebastian Koch. Underlying simple graphs. *Formalized Mathematics*, 27(**3**):237–259, 2019. doi:10.2478/forma-2019-0023.

[10] Sebastian Koch. About graph sums. *Formalized Mathematics*, 29(**4**):249–278, 2021. doi:10.2478/forma-2021-0023.

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

[12] Gilbert Lee and Piotr Rudnicki. Alternative aggregates in Mizar. In Manuel Kauers, Manfred Kerber, Robert Miner, and Wolfgang Windsteiger, editors, *Towards Mechanized Mathematical Assistants*, pages 327–341, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. ISBN 978-3-540-73086-6. doi:10.1007/978-3-540-73086-6_26.

[13] Lars Noschinski. A graph library for Isabelle. *Mathematics in Computer Science*, 9(1): 23–39, 2015. doi:10.1007/s11786-014-0183-z.

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

Accepted March 31, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 53–57, 2023
DOI: 10.2478/forma-2023-0005
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

On the Formalization of Gram-Schmidt Process for Orthonormalizing a Set of Vectors

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In this article, we formalize the Gram-Schmidt process in the Mizar system [2], [3] (compare another formalization using Isabelle/HOL proof assistant [1]). This process is one of the most famous methods for orthonormalizing a set of vectors. The method is named after Jørgen Pedersen Gram and Erhard Schmidt [4]. There are many applications of the Gram-Schmidt process in the field of computer science, e.g., error correcting codes or cryptology [8]. First, we prove some preliminary theorems about real unitary space. Next, we formalize the definition of the Gram-Schmidt process that finds orthonormal basis. We followed [5] in the formalization, continuing work developed in [7], [6].

MSC: 65F25 94A11 97H60 68V20

Keywords: Gram-Schmidt process; orthonormal basis; linear algebra

MML identifier: `RUSUB_6`, version: `8.1.12 5.74.1441`

1. Preliminaries

Let V be a non empty RLS structure, r be a finite sequence of elements of $\mathbb{R}$, and x be a finite sequence of elements of V. The functor $r \circ x$ yielding a finite sequence of elements of V is defined by

(Def. 1) $\operatorname{len} it = \operatorname{len} x$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} x$ holds $it(i) = r_{/i} \cdot (x_{/i})$.

Now we state the proposition:

(1) Let us consider a real linear space V, a subset A of V, a finite sequence x of elements of V, and a finite sequence r of elements of $\mathbb{R}$. Suppose $\operatorname{rng} x \subseteq A$ and $\operatorname{len} x = \operatorname{len} r$. Then $\sum(r \circ x) \in \operatorname{Lin}(A)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence x of elements of V for every finite sequence r of elements of $\mathbb{R}$ such that $\$_1 = \operatorname{len} x$ and $\operatorname{rng} x \subseteq A$ and $\operatorname{len} x = \operatorname{len} r$ holds $\sum(r \circ x) \in \operatorname{Lin}(A)$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

Let us consider a real linear space V and subsets A, B of V. Now we state the propositions:

(2) If $A \subseteq$ the carrier of $\operatorname{Lin}(B)$, then $\operatorname{Lin}(A)$ is a subspace of $\operatorname{Lin}(B)$.

(3) Suppose $A \subseteq$ the carrier of $\operatorname{Lin}(B)$ and $B \subseteq$ the carrier of $\operatorname{Lin}(A)$. Then $\operatorname{Lin}(A) = \operatorname{Lin}(B)$. The theorem is a consequence of (2).

Let V be a non empty unitary space structure, u be a point of V, and x be a finite sequence of elements of V. The functor $(u|x)$ yielding a finite sequence of elements of $\mathbb{R}$ is defined by

(Def. 2) $\operatorname{len} it = \operatorname{len} x$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} x$ holds $it(i) = (u|x_{/i})$.

Now we state the propositions:

(4) Let us consider a non empty unitary space structure V, a point u of V, a finite sequence x of elements of V, and a natural number i. Suppose $1 \leqslant i \leqslant \operatorname{len} x$. Then $((u|x) \circ x)(i) = (u|x_{/i}) \cdot (x_{/i})$.

(5) Let us consider a real unitary space V, a point u of V, and a finite sequence x of elements of V. Then $(u|\sum x) = \sum(u|x)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence x of elements of V such that $\$_1 = \operatorname{len} x$ holds $(u|\sum x) = \sum(u|x)$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

(6) Let us consider a real unitary space V, a point u of V, a natural number n, and a finite sequence x of elements of V. Suppose $1 \leqslant n \leqslant \operatorname{len} x$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} x$ and $n \neq i$ holds $(u|x_{/i}) = 0$. Then $(u|\sum x) = (u|x_{/n})$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence x of elements of V such that $\$_1 = \operatorname{len} x$ and $1 \leqslant n \leqslant \operatorname{len} x$ and for every natural number i such that $1 \leqslant i \leqslant \operatorname{len} x$ and $n \neq i$ holds $(u|x_{/i}) = 0$ holds $(u|\sum x) = (u|x_{/n})$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. □

Let us consider a real unitary space H. Now we state the propositions:

(7) There exists a function F from (the carrier of H) $\times$ (the carrier of H)* into (the carrier of H)* such that for every point x of H for every finite sequence e of elements of H, there exists a finite sequence F_2 of elements of H such that $F_2 = F(x, e)$ and $F_2 = (x|e) \circ e$.
PROOF: Set $C =$ the carrier of H. Define $\mathcal{R}[\text{object}, \text{object}, \text{object}] \equiv$ there exists a point x of H and there exists a finite sequence e of elements of C such that $\$_1 = x$ and $\$_2 = e$ and there exists a finite sequence F_2 of elements of C such that $F_2 = \$_3$ and $F_2 = (x|e) \circ e$. For every objects x, y such that $x \in C$ and $y \in C^*$ there exists an object z such that $z \in C^*$ and $\mathcal{R}[x, y, z]$. Consider F being a function from $C \times C^*$ into C^* such that for every objects z, y such that $z \in C$ and $y \in C^*$ holds $\mathcal{R}[z, y, F(z, y)]$. $\square$

(8) Every orthonormal family of H is linearly independent.
PROOF: For every linear combination l of G such that $\sum l = 0_H$ holds the support of $l = \emptyset$. $\square$

2. GRAM-SCHMIDT PROCESS

Let H be a real unitary space. The functor $\mathrm{Seq}_{\mathrm{Proj}}(H)$ yielding a function from (the carrier of H) $\times$ (the carrier of H)* into (the carrier of H)* is defined by

(Def. 3) for every point x of H and for every finite sequence e of elements of H, there exists a finite sequence F_2 of elements of H such that $F_2 = it(x, e)$ and $F_2 = (x|e) \circ e$.

Now we state the proposition:

(9) Let us consider a real unitary space H, and a finite sequence x of elements of H. Suppose x is one-to-one and $\operatorname{rng} x$ is linearly independent and $1 \leqslant \operatorname{len} x$. Then there exists a finite sequence e of elements of H such that

(i) $\operatorname{len} x = \operatorname{len} e$, and

(ii) $\operatorname{rng} e$ is an orthonormal family of H, and

(iii) e is one-to-one, and

(iv) $\operatorname{Lin}(\operatorname{rng} x) = \operatorname{Lin}(\operatorname{rng} e)$, and

(v) $e_{/1} = \frac{1}{\|x_{/1}\|} \cdot (x_{/1})$, and

(vi) for every natural number k such that $1 \leqslant k < \operatorname{len} x$ there exists a finite sequence g of elements of H such that $g = (\mathrm{Seq}_{\mathrm{Proj}}(H))(\langle x_{/1+k}, e\restriction k\rangle)$ and $e_{/k+1} = \frac{1}{\|x_{/1+k} - \sum g\|} \cdot (x_{/1+k} - \sum g)$, and

(vii) for every natural number k such that $k \leqslant \operatorname{len} x$ holds $\operatorname{rng}(e\restriction k)$ is an orthonormal family of H and $e\restriction k$ is one-to-one and $\operatorname{Lin}(\operatorname{rng}(x\restriction k)) = \operatorname{Lin}(\operatorname{rng}(e\restriction k))$.

PROOF: Set C = the carrier of H. Reconsider $F_1 = \bigcup\{C^i$, where i is a natural number : $i \leqslant \operatorname{len} x\}$ as a non empty set. Set $F = \operatorname{Seq}_{\operatorname{Proj}}(H)$. Define $\mathcal{R}[\text{object}, \text{object}, \text{object}] \equiv$ there exists a C-valued finite sequence e and there exists a natural number n such that $e = \$_2$ and $n = \$_1$ and if $\operatorname{len} e < \operatorname{len} x$, then there exists a C-valued finite sequence g such that $g = F(\langle x_{/1+\operatorname{len} e}, e\rangle)$ and $\$_3 = e \frown \langle \frac{1}{\|x_{/1+\operatorname{len} e} - \sum g\|} \cdot (x_{/1+\operatorname{len} e} - \sum g)\rangle$. For every natural number n such that $1 \leqslant n < \operatorname{len} x$ for every element e of F_1, there exists an element f of F_1 such that $\mathcal{R}[n, e, f]$. Set $E_0 = \langle \frac{1}{\|x_{/1}\|} \cdot (x_{/1})\rangle$.

Consider E being a finite sequence of elements of F_1 such that $\operatorname{len} E = \operatorname{len} x$ and $E(1) = E_0$ or $\operatorname{len} x = 0$ and for every natural number n such that $1 \leqslant n < \operatorname{len} x$ holds $\mathcal{R}[n, E(n), E(n+1)]$. For every natural number k such that $k < \operatorname{len} x$ there exists a finite sequence e of elements of C such that $\operatorname{len} e = k + 1$ and $E(k+1) = e$. For every natural number k such that $1 \leqslant k < \operatorname{len} x$ there exist finite sequences f, g of elements of C such that $E(k) = f$ and $\operatorname{len} f = k$ and $g = F(\langle x_{/1+k}, f\rangle)$ and $E(k+1) = f \frown \langle \frac{1}{\|x_{/1+k} - \sum g\|} \cdot (x_{/1+k} - \sum g)\rangle$. Define $\mathcal{Q}[\text{natural number}, \text{object}, \text{object}] \equiv$ there exist finite sequences f, g of elements of C and there exists a point e_1 of H such that $E(\$_1) = f$ and $\operatorname{len} f = \$_1$ and $e_1 = \$_3$ and $g = F(\langle x_{/1+\$_1}, f\rangle)$ and $E(\$_1 + 1) = f \frown \langle e_1\rangle$ and $e_1 = \frac{1}{\|x_{/1+\$_1} - \sum g\|} \cdot (x_{/1+\$_1} - \sum g)$. For every natural number k such that $1 \leqslant k < \operatorname{len} x$ for every element e of H, there exists an element h of H such that $\mathcal{Q}[k, e, h]$. Set $e_0 = \frac{1}{\|x_{/1}\|} \cdot (x_{/1})$.

Consider e being a finite sequence of elements of H such that $\operatorname{len} e = \operatorname{len} x$ and $e(1) = e_0$ or $\operatorname{len} x = 0$ and for every natural number n such that $1 \leqslant n < \operatorname{len} x$ holds $\mathcal{Q}[n, e(n), e(n+1)]$. For every natural number n such that $1 \leqslant n < \operatorname{len} x$ there exist finite sequences f, g of elements of C such that $E(n) = f$ and $\operatorname{len} f = n$ and $g = F(\langle x_{/1+n}, f\rangle)$ and $E(n+1) = f \frown \langle e_{/n+1}\rangle$ and $e_{/n+1} = \frac{1}{\|x_{/1+n} - \sum g\|} \cdot (x_{/1+n} - \sum g)$. For every natural number n such that $1 \leqslant n \leqslant \operatorname{len} x$ holds $E(n) = e{\restriction}n$. For every natural number k such that $1 \leqslant k < \operatorname{len} x$ there exists a finite sequence g of elements of C such that $g = F(\langle x_{/1+k}, e{\restriction}k\rangle)$ and $e_{/k+1} = \frac{1}{\|x_{/1+k} - \sum g\|} \cdot (x_{/1+k} - \sum g)$. Define $\mathcal{S}[\text{natural number}] \equiv$ if $\$_1 \leqslant \operatorname{len} x$, then $\operatorname{rng}(e{\restriction}\$_1)$ is an orthonormal family of H and $e{\restriction}\$_1$ is one-to-one and $\operatorname{Lin}(\operatorname{rng}(x{\restriction}\$_1)) = \operatorname{Lin}(\operatorname{rng}(e{\restriction}\$_1))$. $\mathcal{S}[0]$. For every natural number k such that $\mathcal{S}[k]$ holds $\mathcal{S}[k+1]$. For every natural number k, $\mathcal{S}[k]$. □

Let H be a real unitary space and x be a finite sequence of elements of H. Assume x is one-to-one and $\operatorname{rng} x$ is linearly independent and $1 \leqslant \operatorname{len} x$. The functor $\operatorname{PROCESS}_{\operatorname{GramSchmidt}}(x)$ yielding a finite sequence of elements of H is defined by

(Def. 4) $\operatorname{len} x = \operatorname{len} it$ and $\operatorname{rng} it$ is an orthonormal family of H and it is one-to-one and $\operatorname{Lin}(\operatorname{rng} x) = \operatorname{Lin}(\operatorname{rng} it)$ and $it_{/1} = \frac{1}{\|x_{/1}\|} \cdot (x_{/1})$ and for every natural number k such that $1 \leqslant k < \operatorname{len} x$ there exists a finite sequence g of elements of H such that $g = (\operatorname{Seq}_{\operatorname{Proj}}(H))(\langle x_{/1+k},\ it\restriction k\rangle)$ and $it_{/k+1} = \frac{1}{\|x_{/1+k} - \sum g\|} \cdot (x_{/1+k} - \sum g)$ and for every natural number k such that $k \leqslant \operatorname{len} x$ holds $\operatorname{rng}(it\restriction k)$ is an orthonormal family of H and $it\restriction k$ is one-to-one and $\operatorname{Lin}(\operatorname{rng}(x\restriction k)) = \operatorname{Lin}(\operatorname{rng}(it\restriction k))$.

Now we state the proposition:

(10) Let us consider a real unitary space H, and a finite sequence x of elements of H. Suppose x is one-to-one and $\operatorname{rng} x$ is linearly independent and $1 \leqslant \operatorname{len} x$. Then $\operatorname{rng} \operatorname{PROCESS}_{\operatorname{GramSchmidt}}(x)$ is linearly independent. The theorem is a consequence of (8).

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

References

[1] Jesús Aransay and Jose Divasón. A formalisation in HOL of the fundamental theorem of linear algebra and its application to the solution of the least squares problem. *Journal of Automated Reasoning*, 58(4):509–535, 2017. doi:10.1007/s10817-016-9379-z.

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

[3] 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.

[4] Ward Cheney and David Kincaid. *Linear Algebra: Theory and Applications*. Jones and Bartlett publishers, 2009.

[5] David G. Luenberger. *Optimization by Vector Space Methods*. John Wiley and Sons, 1969.

[6] Kazuhisa Nakasho, Hiroyuki Okazaki, and Yasunari Shidama. Real vector space and related notions. *Formalized Mathematics*, 29(**3**):117–127, 2021. doi:10.2478/forma-2021-0012.

[7] Hiroyuki Okazaki. Formalization of orthogonal decomposition for Hilbert spaces. *Formalized Mathematics*, 30(**4**):295–299, 2022. doi:10.2478/forma-2022-0023.

[8] René Thiemann and Akihisa Yamada. Formalizing Jordan Normal Forms in Isabelle/HOL. In *Proceedings of the 5th ACM SIGPLAN Conference on Certified Programs and Proofs*, pages 88–99, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450341271. doi:10.1145/2854065.2854073.

Accepted March 31, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 59–66, 2023
DOI: 10.2478/forma-2023-0006
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Isosceles Triangular and Isosceles Trapezoidal Membership Functions Using Centroid Method

Takashi Mitsuishi
Faculty of Business and Informatics
Nagano University, Japan

Summary. Since isosceles triangular and trapezoidal membership functions [4] are easy to manage, they were applied to various fuzzy approximate reasoning [10], [13], [14]. The centroids of isosceles triangular and trapezoidal membership functions are mentioned in this article [16], [9] and formalized in [11] and [12]. Some propositions of the composition mapping ($f +\cdot g$, or `f +* g` using Mizar formalism, where f, g are affine mappings), are proved following [3], [15]. Then different notations for the same isosceles triangular and trapezoidal membership function are formalized.

We proved the agreement of the same function expressed with different parameters and formalized those centroids with parameters. In addition, various properties of membership functions on intervals where the endpoints of the domain are fixed and on general intervals are formalized in Mizar [1], [2]. Our formal development contains also some numerical results which can be potentially useful to encode either fuzzy numbers [7], or even fuzzy implications [5], [6] and extends the possibility of building hybrid rough-fuzzy approach in the future [8].

MSC: 03E72 93C42 94D05 68V20

Keywords: defuzzification; centroid method; isosceles triangular function; isosceles trapezoidal function

MML identifier: `FUZZY_7`, version: `8.1.12 5.74.1441`

1. Preliminaries

Let us consider real numbers a, b, c, d. Now we state the propositions:

(1) $[a, d] \setminus [b, c] \subseteq [a, b[\cup]c, d]$.

(2) If $a < b < c < d$, then $[a, d] \setminus [b, c] \subseteq [a, b] \cup [c, d]$.

(3) Let us consider real numbers p, q, r, s. If $p < r \leqslant s < q$, then $[r, s] \subset [p, q]$.

2. Continuous Functions

Let us consider functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(4) If f is continuous and g is continuous, then $\max(f, g)$ is continuous.

(5) If f is continuous and g is continuous, then $\min(f, g)$ is continuous.

Let us consider non empty, closed interval subsets A, B of $\mathbb{R}$. Now we state the propositions:

(6) If $B \subset A$, then $\inf A < \inf B$ or $\sup B < \sup A$.

(7) If $B \subseteq A$, then $\inf A \leqslant \inf B$ and $\sup B \leqslant \sup A$.

(8) Let us consider a real number r, and functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Then $r \cdot (f+\cdot g) = r \cdot f + \cdot r \cdot g$.
Proof: Set $F_1 = r \cdot (f+\cdot g)$. Set $F_2 = r \cdot f + \cdot r \cdot g$. For every object x such that $x \in \operatorname{dom} F_1$ holds $F_1(x) = F_2(x)$. □

From now on A denotes a non empty subset of $\mathbb{R}$. Now we state the propositions:

(9) Let us consider a real number r, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Then $(r \cdot f)\restriction A = r \cdot (f\restriction A)$.
Proof: Set $F = (r \cdot f)\restriction A$. Set $g = r \cdot (f\restriction A)$. For every object x such that $x \in \operatorname{dom} F$ holds $F(x) = g(x)$. □

(10) Let us consider a real number r, and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Suppose $A \subseteq \operatorname{dom} f$. Then $(r \cdot f)\restriction A = r \cdot (f\restriction A)$.
Proof: Set $F = (r \cdot f)\restriction A$. Set $g = r \cdot (f\restriction A)$. For every object x such that $x \in \operatorname{dom} F$ holds $F(x) = g(x)$. □

(11) Let us consider a real number s, and functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Then $f\restriction]-\infty, s] + \cdot g\restriction [s, +\infty[$ is a function from $\mathbb{R}$ into $\mathbb{R}$.

(12) Let us consider real numbers a, b, r.
Then $r \cdot (\operatorname{AffineMap}(a, b)) = \operatorname{AffineMap}(r \cdot a, r \cdot b)$.

(13) Let us consider a real number s, and functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Then
(i) $\operatorname{dom}(f\restriction]-\infty, s] + \cdot g\restriction [s, +\infty[) = \mathbb{R}$, and
(ii) $\operatorname{dom}(f\restriction]-\infty, s[+ \cdot g\restriction [s, +\infty[) = \mathbb{R}$.

(14) Let us consider real numbers a, b, c. Suppose $b > 0$ and $c > 0$. Let us consider a real number x. Then $((\operatorname{AffineMap}(\frac{b}{c}, b - \frac{a \cdot b}{c}))\restriction]-\infty, a] + \cdot (\operatorname{AffineMap}(-\frac{b}{c}, b + \frac{a \cdot b}{c}))\restriction [a, +\infty[)(x) = b - |\frac{b \cdot (x-a)}{c}|$.
Proof: For every real number x, $((\operatorname{AffineMap}(\frac{b}{c}, b - \frac{a \cdot b}{c}))\restriction]-\infty, a] + \cdot (\operatorname{AffineMap}(-\frac{b}{c}, b + \frac{a \cdot b}{c}))\restriction [a, +\infty[)(x) = b - |\frac{b \cdot (x-a)}{c}|$. □

(15) Let us consider real numbers a, b, c, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $b > 0$ and $c > 0$ and for every real number x, $f(x) = b - |\frac{b\cdot(x-a)}{c}|$. Then $f = (\mathrm{AffineMap}(\frac{b}{c}, b - \frac{a\cdot b}{c}))\restriction]-\infty, a] + \cdot(\mathrm{AffineMap}(-\frac{b}{c}, b + \frac{a\cdot b}{c}))\restriction[a, +\infty[$. The theorem is a consequence of (14).

Let us consider real numbers a, b. Now we state the propositions:

(16) Suppose $a > 0$. Then $|\,\mathrm{AffineMap}(a, b)| = -(\mathrm{AffineMap}(a, b))\restriction]-\infty, \frac{-b}{a}[+ \cdot(\mathrm{AffineMap}(a, b))\restriction[\frac{-b}{a}, +\infty[$.

PROOF: For every object x such that $x \in \mathrm{dom}\,|\,\mathrm{AffineMap}(a, b)|$ holds $|\,\mathrm{AffineMap}(a, b)|(x) = (-(\mathrm{AffineMap}(a, b))\restriction]-\infty, \frac{-b}{a}[+ \cdot(\mathrm{AffineMap}(a, b))\restriction[\frac{-b}{a}, +\infty[)(x)$. □

(17) Suppose $a < 0$. Then $|\,\mathrm{AffineMap}(a, b)| = (\mathrm{AffineMap}(a, b))\restriction]-\infty, \frac{-b}{a}[+ \cdot -(\mathrm{AffineMap}(a, b))\restriction[\frac{-b}{a}, +\infty[$.

PROOF: Set $f = (\mathrm{AffineMap}(a, b))\restriction]-\infty, \frac{-b}{a}[+ \cdot -(\mathrm{AffineMap}(a, b))\restriction[\frac{-b}{a}, +\infty[$. For every object x such that $x \in \mathrm{dom}((-(\mathrm{AffineMap}(a, b)))\restriction[\frac{-b}{a}, +\infty[)$ holds $(-(\mathrm{AffineMap}(a, b))\restriction[\frac{-b}{a}, +\infty[)(x) = ((-(\mathrm{AffineMap}(a, b)))\restriction[\frac{-b}{a}, +\infty[)(x)$. For every element x of $\mathbb{R}$, $f(x) = |\,\mathrm{AffineMap}(a, b)|(x)$. □

(18) Let us consider real numbers a, b, c, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $b > 0$ and $c > 0$ and for every real number x, $f(x) = \max(0, b - |\frac{b\cdot(x-a)}{c}|)$. Let us consider a real number x. If $x \notin [a - c, a + c]$, then $f(x) = 0$.

(19) Let us consider real numbers a, b, c, and functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a < b < c$. Then $(f\restriction]-\infty, b] + \cdot g\restriction[b, +\infty[)\restriction[a, c] = f\restriction[a, b] + \cdot g\restriction[b, c]$.

PROOF: For every object x such that $x \in \mathrm{dom}((f\restriction]-\infty, b] + \cdot g\restriction[b, +\infty[)\restriction[a, c])$ holds $((f\restriction]-\infty, b] + \cdot g\restriction[b, +\infty[)\restriction[a, c])(x) = (f\restriction[a, b] + \cdot g\restriction[b, c])(x)$. □

Let us consider real numbers a, b, c and a function f from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(20) Suppose $b > 0$ and $c > 0$. Then $((\mathrm{AffineMap}(\frac{b}{c}, b - \frac{a\cdot b}{c}))\restriction]-\infty, a] + \cdot(\mathrm{AffineMap}(-\frac{b}{c}, b + \frac{a\cdot b}{c}))\restriction[a, +\infty[)\restriction[a - c, a + c] = (\mathrm{AffineMap}(\frac{b}{c}, b - \frac{a\cdot b}{c}))\restriction[a - c, a] + \cdot(\mathrm{AffineMap}(-\frac{b}{c}, b + \frac{a\cdot b}{c}))\restriction[a, a + c]$. The theorem is a consequence of (19).

(21) Suppose $a < b < c$ and f is integrable on $[a, c]$ and $f\restriction[a, c]$ is bounded. Then

(i) f is integrable on $[a, b]$, and

(ii) f is integrable on $[b, c]$, and

(iii) $f\restriction[a, b]$ is bounded, and

(iv) $[a, b] \subseteq \mathrm{dom}\, f$, and

(v) $\int_a^c f(x)dx = \int_a^b f(x)dx + \int_b^c f(x)dx$.

(22) Let us consider real numbers a, b, c, d, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a < b < c < d$ and f is integrable on $[a, d]$ and $f\restriction[a, d]$ is bounded and for every real number x such that $x \in [a, b] \cup [c, d]$ holds $f(x) = 0$. Then $\operatorname{centroid}(f, [a, d]) = \operatorname{centroid}(f, [b, c])$.

(23) Let us consider non empty, closed interval subsets A, B of $\mathbb{R}$, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $\inf B \neq \sup B$ and $B \subseteq A$ and f is integrable on A and $f\restriction A$ is bounded and for every real number x such that $x \in A \setminus B$ holds $f(x) = 0$ and $f(\inf B) = 0$ and $f(\sup B) = 0$. Then $\operatorname{centroid}(f, A) = \operatorname{centroid}(f, B)$.

PROOF: $\inf A \leqslant \inf B$ and $\sup B \leqslant \sup A$. For every real number x such that $x \in [\inf A, \inf B] \cup [\sup B, \sup A]$ holds $f(x) = 0$. □

3. Triangular and Trapezoidal Membership Functions

Now we state the proposition:

(24) Let us consider real numbers a, c, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $c > 0$ and for every real number x, $f(x) = \max(0, 1 - |\frac{x-a}{c}|)$. Then f is a triangular fuzzy set of $\mathbb{R}$.

PROOF: Define $\mathcal{H}(\text{element of } \mathbb{R}) = (1 - |\frac{\$_1 - a}{c}|)(\in \mathbb{R})$. Consider h being a function from $\mathbb{R}$ into $\mathbb{R}$ such that for every element x of $\mathbb{R}$, $h(x) = \mathcal{H}(x)$. For every real number x, $f(x) = \max(0, \min(1, h(x)))$. □

Let us consider real numbers a, b, c and a function f from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(25) Suppose $b > 1$ and $c > 0$ and for every real number x, $f(x) = \min(1, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. Then f is trapezoidal fuzzy set of $\mathbb{R}$ and normalized fuzzy set of $\mathbb{R}$.

(26) If $b > 0$ and $c > 0$ and for every real number x, $f(x) = \max(0, b - |\frac{b\cdot(x-a)}{c}|)$, then $f = b \cdot \operatorname{TriangularFS}((a - c), a, (a + c))$.

PROOF: Set $g = b \cdot \operatorname{TriangularFS}((a - c), a, (a + c))$. For every object x such that $x \in \operatorname{dom} f$ holds $f(x) = g(x)$. □

(27) If $b > 0$ and $c > 0$ and for every real number x, $f(x) = \max(0, b - |\frac{b\cdot(x-a)}{c}|)$, then f is Lipschitzian.

PROOF: For every real number x, $f(x) = \max(0, \min(b, b \cdot (1 - |\frac{x-a}{c}|)))$. □

(28) Suppose $b > 0$ and $c > 0$ and $f\restriction[a - c, a + c] = (\operatorname{AffineMap}(\frac{b}{c}, b - \frac{a\cdot b}{c}))\restriction[\inf[a-c, a+c], \frac{b+\frac{a\cdot b}{c}-(b-\frac{a\cdot b}{c})}{\frac{b}{c}--\frac{b}{c}}] + \cdot(\operatorname{AffineMap}(-\frac{b}{c}, b+\frac{a\cdot b}{c}))\restriction[\frac{b+\frac{a\cdot b}{c}-(b-\frac{a\cdot b}{c})}{\frac{b}{c}--\frac{b}{c}},$

$\sup[a-c, a+c]]$. Then $\operatorname{centroid}(f, [a-c, a+c]) = a$.

(29) Suppose $b > 0$ and $c > 0$ and for every real number x, $f(x) = \max(0, b - |\frac{b\cdot(x-a)}{c}|)$. Then $f\restriction[a-c, a+c] = (\operatorname{AffineMap}(\frac{b}{c}, b - \frac{a\cdot b}{c}))\restriction[\inf[a-c, a+c], \frac{b+\frac{a\cdot b}{c}-(b-\frac{a\cdot b}{c})}{\frac{b}{c}--\frac{b}{c}}]+\cdot(\operatorname{AffineMap}(-\frac{b}{c}, b+\frac{a\cdot b}{c}))\restriction[\frac{b+\frac{a\cdot b}{c}-(b-\frac{a\cdot b}{c})}{\frac{b}{c}--\frac{b}{c}}, \sup[a-c, a+c]]$.

PROOF: Set $g = (\operatorname{AffineMap}(\frac{b}{c}, b - \frac{a\cdot b}{c}))\restriction[\inf[a-c, a+c], \frac{b+\frac{a\cdot b}{c}-(b-\frac{a\cdot b}{c})}{\frac{b}{c}--\frac{b}{c}}]+\cdot(\operatorname{AffineMap}(-\frac{b}{c}, b+\frac{a\cdot b}{c}))\restriction[\frac{b+\frac{a\cdot b}{c}-(b-\frac{a\cdot b}{c})}{\frac{b}{c}--\frac{b}{c}}, \sup[a-c, a+c]]$. For every object x such that $x \in \operatorname{dom}(f\restriction[a-c, a+c])$ holds $(f\restriction[a-c, a+c])(x) = g(x)$. □

(30) If $b > 0$ and $c > 0$ and for every real number x, $f(x) = \max(0, b - |\frac{b\cdot(x-a)}{c}|)$, then $\operatorname{centroid}(f, [a-c, a+c]) = a$. The theorem is a consequence of (29) and (28).

In the sequel A denotes a non empty, closed interval subset of $\mathbb{R}$. Let us consider real numbers a, b, c and a function f from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(31) If $b > 0$ and $c > 0$ and for every real number x, $f(x) = \max(0, b - |\frac{b\cdot(x-a)}{c}|)$, then f is integrable on A and $f\restriction A$ is bounded. The theorem is a consequence of (27).

(32) Suppose $b > 0$ and $c > 0$ and for every real number x, $f(x) = \max(0, b - |\frac{b\cdot(x-a)}{c}|)$. Then

(i) $f(\inf[a-c, a+c]) = 0$, and

(ii) $f(a-c) = 0$, and

(iii) $f(\sup[a-c, a+c]) = 0$, and

(iv) $f(a+c) = 0$.

(33) If $b > 0$ and $c > 0$ and $[a-c, a+c] \subseteq A$ and for every real number x, $f(x) = \max(0, b - |\frac{b\cdot(x-a)}{c}|)$, then $\operatorname{centroid}(f, A) = a$. The theorem is a consequence of (18), (32), (31), (23), and (30).

Let us consider real numbers a, b, c. Now we state the propositions:

(34) If $a < b < c$ and $b-a = c-b$, then $\operatorname{centroid}(\operatorname{TriangularFS}(a, b, c), [a, c]) = b$.

PROOF: For every real number x, $(\operatorname{TriangularFS}(a, b, c))(x) = \max(0, 1 - |\frac{1\cdot(x-b)}{b-a}|)$. $\operatorname{centroid}(\operatorname{TriangularFS}(a, b, c), [b-(b-a), b+(b-a)]) = b$. □

(35) If $a < b < c$, then $\operatorname{TriangularFS}(a, b, c)$ is integrable on A and $\operatorname{TriangularFS}(a, b, c)\restriction A$ is bounded.

Let us consider real numbers a, b, c, d. Now we state the propositions:

(36) If $a < b < c$ and $b-a = c-b$ and $d \neq 0$, then $\operatorname{centroid}(d\cdot\operatorname{TriangularFS}(a, b, c), [a, c]) = b$. The theorem is a consequence of (35) and (34).

(37) If $a < b < c < d$, then TrapezoidalFS(a, b, c, d) is integrable on A and TrapezoidalFS$(a, b, c, d)\restriction A$ is bounded.

(38) Let us consider real numbers a, b, c, d, r. If $a < b < c < d$, then $r \cdot$TrapezoidalFS(a, b, c, d) is integrable on A. The theorem is a consequence of (37).

(39) Let us consider real numbers a_1, c, a_2, d, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $c > 0$ and $d > 0$ and $a_1 < a_2$ and $f = (d \cdot \text{TrapezoidalFS}((a_1 - c), a_1, a_2, (a_2 + c)))\restriction[a_1 - c, a_2 + c]$. Then f is integrable on $[a_1 - c, a_2 + c]$. The theorem is a consequence of (38).

(40) Let us consider real numbers a, b, c, functions f, g from $\mathbb{R}$ into $\mathbb{R}$, and a partial function h from $\mathbb{R}$ to $\mathbb{R}$. Suppose $a \leqslant b \leqslant c$ and f is continuous and g is continuous and $h\restriction[a, c] = f\restriction[a, b] + \cdot g\restriction[b, c]$ and $f(b) = g(b)$ and $[a, c] \subseteq \operatorname{dom} h$. Then $h\restriction[a, c]$ is continuous.

PROOF: For every real numbers x_0, r such that $x_0 \in [a, c]$ and $0 < r$ there exists a real number s such that $0 < s$ and for every real number x_1 such that $x_1 \in [a, c]$ and $|x_1 - x_0| < s$ holds $|h(x_1) - h(x_0)| < r$. □

(41) Let us consider real numbers a, b, p, q, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a \neq p$ and $f = (\text{AffineMap}(a, b))\restriction]-\infty, \frac{q-b}{a-p}] + \cdot (\text{AffineMap}(p, q))\restriction[\frac{q-b}{a-p}, +\infty[$. Then f is Lipschitzian.

(42) Let us consider real numbers a, b, c, and functions f, g, h from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a \leqslant b \leqslant c$ and f is continuous and g is continuous and $h\restriction[a, c] = f\restriction[a, b] + \cdot g\restriction[b, c]$ and $f(b) = g(b)$. Then $\int\limits_{[a,c]} (\text{id}_{\mathbb{R}} \cdot h)(x)dx = \int\limits_{[a,b]} (\text{id}_{\mathbb{R}} \cdot f)(x)dx + \int\limits_{[b,c]} (\text{id}_{\mathbb{R}} \cdot g)(x)dx$.

PROOF: Set $G = (\text{id}_{\mathbb{R}} \cdot f)\restriction[a, b] + \cdot (\text{id}_{\mathbb{R}} \cdot g)\restriction[b, c]$. $[a, c] = \mathbb{R} \cap [a, c]$. For every object x such that $x \in \operatorname{dom}((\text{id}_{\mathbb{R}} \cdot h)\restriction[a, c])$ holds $(\text{id}_{\mathbb{R}} \cdot (h\restriction[a, c]))(x) = ((\text{id}_{\mathbb{R}} \cdot h)\restriction[a, c])(x)$. For every object x such that $x \in \operatorname{dom} G$ holds $G(x) = (\text{id}_{\mathbb{R}} \cdot (h\restriction[a, c]))(x)$. Reconsider $h_1 = h$ as a partial function from $\mathbb{R}$ to $\mathbb{R}$. $h_1\restriction[a, c]$ is continuous. □

Let us consider real numbers a, b, c, d, r. Now we state the propositions:

(43) Suppose $a < b < c < d$. Then $((\text{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a}))\restriction[a, b] + \cdot (\text{AffineMap}(0, 1))\restriction[b, c]) + \cdot (\text{AffineMap}(-\frac{1}{d-c}, \frac{d}{d-c}))\restriction[c, d] = \text{TrapezoidalFS}(a, b, c, d)\restriction[a, d]$.

PROOF: For every object x such that $x \in \operatorname{dom}(\text{TrapezoidalFS}(a, b, c, d)\restriction[a, d])$ holds $(((\text{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a}))\restriction[a, b] + \cdot (\text{AffineMap}(0, 1))\restriction[b, c]) + \cdot (\text{AffineMap}(-\frac{1}{d-c}, \frac{d}{d-c}))\restriction[c, d])(x) = (\text{TrapezoidalFS}(a, b, c, d)\restriction[a, d])(x)$. □

(44) Suppose $a < b < c < d$. Then TrapezoidalFS$(a, b, c, d) = (\text{AffineMap}(0,$

$0))\restriction \mathbb{R} \setminus]a,d[+ \cdot \mathrm{TrapezoidalFS}(a,b,c,d)\restriction [a,d]$. The theorem is a consequence of (43).

(45) Suppose $a < b < c < d$. Then $((r \cdot (\mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a})))\restriction [a,b] + \cdot (r \cdot (\mathrm{AffineMap}(0,1)))\restriction [b,c]) + \cdot (r \cdot (\mathrm{AffineMap}(-\frac{1}{d-c}, \frac{d}{d-c})))\restriction [c,d] = (r \cdot \mathrm{TrapezoidalFS}(a,b,c,d))\restriction [a,d]$.

PROOF: Set $f_1 = (\mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a}))\restriction [a,b]$. Set $f_2 = (\mathrm{AffineMap}(0, 1))\restriction [b,c]$. Set $f_3 = (\mathrm{AffineMap}(-\frac{1}{d-c}, \frac{d}{d-c}))\restriction [c,d]$. Set $F_1 = \mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a})$. Set $F_2 = \mathrm{AffineMap}(0,1)$. Set $F_3 = \mathrm{AffineMap}(-\frac{1}{d-c}, \frac{d}{d-c})$. For every object x such that $x \in \mathrm{dom}(r \cdot ((f_1 + \cdot f_2) + \cdot f_3))$ holds $(((r \cdot F_1)\restriction [a,b] + \cdot (r \cdot F_2)\restriction [b,c]) + \cdot (r \cdot F_3)\restriction [c,d])(x) = (r \cdot ((f_1 + \cdot f_2) + \cdot f_3))(x)$. $\square$

Let us consider real numbers a_1, c, a_2, d. Now we state the propositions:

(46) Suppose $c > 0$ and $d > 0$ and $a_1 < a_2$.
Then $((\mathrm{AffineMap}(\frac{d}{c}, -\frac{d}{c} \cdot (a_1 - c)))\restriction [a_1 - c, a_1] + \cdot (\mathrm{AffineMap}(0,d))\restriction [a_1, a_2]) + \cdot (\mathrm{AffineMap}(-\frac{d}{c}, \frac{d}{c} \cdot (a_2 + c)))\restriction [a_2, a_2 + c] = (d \cdot \mathrm{TrapezoidalFS}((a_1 - c), a_1, a_2, (a_2 + c)))\restriction [a_1 - c, a_2 + c]$. The theorem is a consequence of (12) and (45).

(47) Suppose $c > 0$ and $d > 0$ and $a_1 < a_2$. Then $\int_{[a_1 - c, a_1]} (\mathrm{AffineMap}(\frac{d}{c}, -\frac{d}{c} \cdot (a_1 - c)))(x)dx + \int_{[a_1, a_2]} (\mathrm{AffineMap}(0,d))(x)dx + \int_{[a_2, a_2 + c]} (\mathrm{AffineMap}(-\frac{d}{c}, \frac{d}{c} \cdot (a_2 + c)))(x)dx = d \cdot (a_2 - a_1 + c)$.

(48) Let us consider real numbers a_1, c, a_2, d, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $c > 0$ and $d > 0$ and $a_1 < a_2$ and $f\restriction [a_1 - c, a_2 + c] = ((\mathrm{AffineMap}(\frac{d}{c}, -\frac{d}{c} \cdot (a_1 - c)))\restriction [a_1 - c, a_1] + \cdot (\mathrm{AffineMap}(0,d))\restriction [a_1, a_2]) + \cdot (\mathrm{AffineMap}(-\frac{d}{c}, \frac{d}{c} \cdot (a_2 + c)))\restriction [a_2, a_2 + c]$. Then $\int_{[a_1 - c, a_2 + c]} f(x)dx = \int_{[a_1 - c, a_1]} (\mathrm{AffineMap}(\frac{d}{c}, -\frac{d}{c} \cdot (a_1 - c)))(x)dx + \int_{[a_1, a_2]} (\mathrm{AffineMap}(0,d))(x)dx + \int_{[a_2, a_2 + c]} (\mathrm{AffineMap}(-\frac{d}{c}, \frac{d}{c} \cdot (a_2 + c)))(x)dx$. The theorem is a consequence of (46).

(49) Let us consider real numbers a_1, c, a_2, d. Suppose $c > 0$ and $d > 0$ and $a_1 < a_2$. Then $\mathrm{centroid}(d \cdot \mathrm{TrapezoidalFS}((a_1 - c), a_1, a_2, (a_2 + c)), [a_1 - c, a_2 + c]) = \frac{a_1 + a_2}{2}$. The theorem is a consequence of (46), (48), and (47).

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] Ronald E. Giachetti and Robert E. Young. A parametric representation of fuzzy numbers and their arithmetic operators. *Fuzzy Sets and Systems*, 91(2):185–202, 1997. doi:10.1016/S0165-0114(97)00140-1.

[4] Eikou Gonda, Hitoshi Miyata, and Masaaki Ohkita. Self-turning of fuzzy rules with different types of MSFs (in Japanese). *Journal of Japan Society for Fuzzy Theory and Intelligent Informatics*, 16(6):540–550, 2004. doi:10.3156/jsoft.16.540.

[5] Adam Grabowski. On fuzzy negations generated by fuzzy implications. *Formalized Mathematics*, 28(**1**):121–128, 2020. doi:10.2478/forma-2020-0011.

[6] Adam Grabowski. Fuzzy implications in the Mizar system. In *30th IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 2021, Luxembourg, July 11–14, 2021*, pages 1–6. IEEE, 2021. doi:10.1109/FUZZ45933.2021.9494593.

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

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

[9] Tetsuro Katafuchi, Kiyoji Asai, and Hiroshi Fujita. Investigation of deffuzification in fuzzy inference: Proposal of a new defuzzification method (in Japanese). *Medical Imaging and Information Sciences*, 18(1):19–30, 2001. doi:10.11318/mii1984.18.19.

[10] Ebrahim H. Mamdani. Application of fuzzy algorithms for control of simple dynamic plant. *IEE Proceedings*, 121:1585–1588, 1974.

[11] Takashi Mitsuishi. Some properties of membership functions composed of triangle functions and piecewise linear functions. *Formalized Mathematics*, 29(**2**):103–115, 2021. doi:10.2478/forma-2021-0011.

[12] Takashi Mitsuishi. Definition of centroid method as defuzzification. *Formalized Mathematics*, 30(**2**):125–134, 2022. doi:10.2478/forma-2022-0010.

[13] Masaharu Mizumoto. Improvement of fuzzy control (IV)-case by product-sum-gravity method. In *Proc. 6th Fuzzy System Symposium, 1990*, pages 9–13, 1990.

[14] Timothy J. Ross. *Fuzzy Logic with Engineering Applications*. John Wiley and Sons Ltd, 2010.

[15] Luciano Stefanini and Laerte Sorini. Fuzzy arithmetic with parametric LR fuzzy numbers. In *Proceedings of the Joint 2009 International Fuzzy Systems Association World Congress and 2009 European Society of Fuzzy Logic and Technology Conference*, pages 600–605, 2009.

[16] Werner Van Leekwijck and Etienne E. Kerre. Defuzzification: Criteria and classification. *Fuzzy Sets and Systems*, 108(2):159–178, 1999.

Accepted March 31, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 67–73, 2023
DOI: 10.2478/forma-2023-0007
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Introduction to Algebraic Geometry

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

Summary. A classical algebraic geometry is study of zero points of system of multivariate polynomials [3], [7] and those zero points would be corresponding to points, lines, curves, surfaces in an affine space. In this article we give some basic definition of the area of affine algebraic geometry such as algebraic set, ideal of set of points, and those properties according to [4] in the Mizar system [5], [2].

We treat an affine space as the n-fold Cartesian product k^n as the same manner appeared in [4]. Points in this space are identified as n-tuples of elements from the set k. The formalization of points, which are n-tuples of numbers, is described in terms of a mapping from n to k, where the domain n corresponds to the set $n = \{0, 1, \ldots, n-1\}$, and the target domain k is the same as the scalar ring or field of polynomials. The same approach has been applied when evaluating multivariate polynomials using n-tuples of numbers [10].

This formalization aims at providing basic notions of the field which enable to formalize geometric objects such as algebraic curves which is used e.g. in coding theory [11] as well as further formalization of the fields [8] in the Mizar system, including the theory of polynomials [6].

MSC: 14-01 14H50 68V20

Keywords: affine algebraic set; multivariate polynomial

MML identifier: ALGGEO_1, version: 8.1.12 5.75.1447

1. Evaluation Functions Revisited

From now on A denotes a non degenerated commutative ring, R denotes a non degenerated integral domain, n denotes a non empty ordinal number, o, o_1, o_2 denote objects, X, Y denote subsets of $(\Omega_R)^n$, S, T denote subsets of

Polynom-Ring(n, R), F, G denote finite sequences of elements of the carrier of Polynom-Ring(n, R), and x denotes a function from n into R.

Let n be an ordinal number, L be a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure, and p be a polynomial of n,L. Note that the functor $\{p\}$ yields a subset of Polynom-Ring(n, L). Let f be an element of Polynom-Ring(n, L) and x be a function from n into L. The functor Eval(f, x) yielding an element of L is defined by

(Def. 1) there exists a polynomial p of n,L such that $p = f$ and $it = \mathrm{eval}(p, x)$.

Let F be a finite sequence of elements of the carrier of Polynom-Ring(n, L). The functor Eval(F, x) yielding a finite sequence of elements of the carrier of L is defined by

(Def. 2) $\mathrm{dom}\, it = \mathrm{dom}\, F$ and for every natural number i such that $i \in \mathrm{dom}\, F$ holds $it(i) = \mathrm{Eval}(F_{/i}, x)$.

Now we state the propositions:

(1) Let us consider a right zeroed, add-associative, right complementable, well unital, distributive, non trivial double loop structure L, and an ordinal number n. Then $\mathrm{Support}\, 0_n L = \emptyset$.

(2) Let us consider an ordinal number n, a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, non trivial double loop structure L, elements f, g of Polynom-Ring(n, L), and a function x from n into L. Then $\mathrm{Eval}(f + g, x) = \mathrm{Eval}(f, x) + \mathrm{Eval}(g, x)$.

(3) Let us consider an ordinal number n, a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, non trivial, commutative, associative, non empty double loop structure L, elements f, g of Polynom-Ring(n, L), and a function x from n into L. Then $\mathrm{Eval}(f \cdot g, x) = (\mathrm{Eval}(f, x)) \cdot (\mathrm{Eval}(g, x))$.

(4) Let us consider a natural number N_0, an ordinal number n, a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, non trivial, commutative, associative, non empty double loop structure L, a finite sequence F of elements of the carrier of Polynom-Ring(n, L), and a function x from n into L. Suppose $\mathrm{len}\, F = N_0 + 1$. Then $\mathrm{Eval}(F, x) = \mathrm{Eval}(F \restriction N_0, x) \frown \langle \mathrm{Eval}(F_{/\mathrm{len}\, F}, x) \rangle$.

PROOF: For every natural number k such that $1 \leqslant k \leqslant \mathrm{len}\, \mathrm{Eval}(F, x)$ holds $(\mathrm{Eval}(F, x))(k) = (\mathrm{Eval}(F \restriction N_0, x) \frown \langle \mathrm{Eval}(F_{/\mathrm{len}\, F}, x) \rangle)(k)$. □

(5) Let us consider an ordinal number n, a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, non trivial, commutative, associative, non empty double loop structure L, a finite sequence F of elements of the carrier of Polynom-Ring(n, L), and a func-

tion x from n into L. Then $\mathrm{Eval}(\sum F, x) = \sum \mathrm{Eval}(F, x)$. The theorem is a consequence of (2) and (4).

2. Monic Multivariate Polynomials with Degree 1

Let us consider n and R. Let a be a function from n into R and i be an element of n. The functor deg1Poly(a, i) yielding a polynomial of n,R is defined by the term

(Def. 3) $1\_1(i, R) - (a(i)\restriction(n, R))$.

Let us consider an element a of R and an element i of n. Now we state the propositions:

(6) (i) $(1\_1(i, R))(\mathrm{UnitBag}\, i) = 1_R$, and

(ii) $(a\restriction(n, R))(\mathrm{EmptyBag}\, n) = a$, and

(iii) $(1\_1(i, R))(\mathrm{EmptyBag}\, n) = 0_R$, and

(iv) $(a\restriction(n, R))(\mathrm{UnitBag}\, i) = 0_R$.

Proof: Set $U = \mathrm{UnitBag}\, i$. $U \neq \mathrm{EmptyBag}\, n$. □

(7) (i) $1\_1(i, R)$ is a polynomial of n,R, and

(ii) $a\restriction(n, R)$ is a polynomial of n,R.

(8) Let us consider a non zero element a of R, an element b of R, and an element i of n. Then $(a\restriction(n, R)) * 1\_1(i, R) + (b\restriction(n, R))$ is a polynomial of n,R.

(9) Let us consider an element a of R, and an element i of n. Then $\mathrm{Support}(1\_1(i, R) + (a\restriction(n, R))) \subseteq \{\mathrm{UnitBag}\, i\} \cup \{\mathrm{EmptyBag}\, n\}$.

(10) $\mathrm{degree}(\mathrm{EmptyBag}\, n) = 0$.

(11) Let us consider an element x of n. Then $\mathrm{degree}(\mathrm{UnitBag}\, x) = 1$.

(12) Let us consider an element a of R, and an element i of n. Then $\mathrm{degree}(1\_1(i, R) + (a\restriction(n, R))) = 1$. The theorem is a consequence of (9), (6), (1), (10), and (11).

3. Affine Space and Algebraic Sets from Ideal

Let us consider R and n. Let f be a polynomial of n,R. The functor Roots(f) yielding a subset of $(\Omega_R)^n$ is defined by the term

(Def. 4) $\{x$, where x is a function from n into $R : \mathrm{eval}(f, x) = 0_R\}$.

Now we state the propositions:

(13) $\mathrm{Roots}(0_n R) = (\Omega_R)^n$.

PROOF: If $o \in (\Omega_R)^n$, then $o \in \mathrm{Roots}(0_n R)$. □

(14) $\mathrm{Roots}(1\_(n, R)) = \emptyset_{(\Omega_R)^n}$.

Let us consider R, n, and S. The functor $\mathrm{Roots}(S)$ yielding a subset of $(\Omega_R)^n$ is defined by the term

(Def. 5) $\begin{cases} \{x, \text{ where } x \text{ is a function from } n \text{ into } R : \text{ for every polynomial } p \text{ of } \\ \ n,R \text{ such that } p \in S \text{ holds } \mathrm{eval}(p, x) = 0_R\}, \textbf{if } S \neq \emptyset, \\ \emptyset, \textbf{otherwise}. \end{cases}$

Now we state the proposition:

(15) Let us consider a polynomial p of n,R. Then $\mathrm{Roots}(\{p\}) = \mathrm{Roots}(p)$.

Let us consider R and n. Let I be a subset of $(\Omega_R)^n$. We say that I is algebraic set from ideal if and only if

(Def. 6) there exists an ideal J of Polynom-Ring(n, R) such that $I = \mathrm{Roots}(J)$.

Let us note that there exists a non empty subset of $(\Omega_R)^n$ which is algebraic set from ideal.

4. Algebraic Sets

Let us consider n and R. An algebraic set of n and R is an algebraic set from ideal subset of $(\Omega_R)^n$. Now we state the propositions:

(16) Let us consider non empty subsets S, T of Polynom-Ring(n, R). If $S \subseteq T$, then $\mathrm{Roots}(T) \subseteq \mathrm{Roots}(S)$.

(17) Let us consider a non empty subset S of Polynom-Ring(n, R). Then $\mathrm{Roots}(S) = \mathrm{Roots}(S\text{–ideal})$.

PROOF: $\mathrm{Roots}(S) \subseteq \mathrm{Roots}(S\text{–ideal})$. □

(18) Let us consider ideals I, J of Polynom-Ring(n, R). Then $\mathrm{Roots}(I \cup J) = \mathrm{Roots}(I) \cap \mathrm{Roots}(J)$. The theorem is a consequence of (16).

(19) Let us consider algebraic sets S, T of n and R. Then $S \cap T$ is an algebraic set of n and R. The theorem is a consequence of (18) and (17).

Let us consider A. Let F be a non empty subset of Ideals A. One can verify that the functor $\bigcup F$ yields a non empty subset of A. Now we state the propositions:

(20) Let us consider a non empty subset F of Ideals Polynom-Ring(n, R). Then $\mathrm{Roots}(\bigcup F) = \bigcap\{\mathrm{Roots}(I)$, where I is an ideal of Polynom-Ring$(n, R) : I \in F\}$.

PROOF: Set $P_1 =$ Polynom-Ring(n, R). Set $M = \{\mathrm{Roots}(I)$, where I is an ideal of $P_1 : I \in F\}$. Consider I being an object such that $I \in F$. Consider I_1 being an ideal of P_1 such that $I = I_1$. For every o such that

$o \in \mathrm{Roots}(\bigcup F)$ holds $o \in \bigcap M$. For every o such that $o \in \bigcap M$ holds $o \in \mathrm{Roots}(\bigcup F)$. □

(21) Let us consider polynomials f, g of n,R.
Then $\mathrm{Roots}(\{f * g\}) = \mathrm{Roots}(\{f\}) \cup \mathrm{Roots}(\{g\})$.
PROOF: If $o \in \mathrm{Roots}(\{f * g\})$, then $o \in \mathrm{Roots}(\{f\}) \cup \mathrm{Roots}(\{g\})$. If $o \in \mathrm{Roots}(\{f\}) \cup \mathrm{Roots}(\{g\})$, then $o \in \mathrm{Roots}(\{f * g\})$. □

Let us consider ideals I, J of Polynom-Ring(n, R). Now we state the propositions:

(22) $\mathrm{Roots}(I \cap J) = \mathrm{Roots}(I) \cup \mathrm{Roots}(J)$.
PROOF: $\mathrm{Roots}(I) \subseteq \mathrm{Roots}(I \cap J)$ and $\mathrm{Roots}(J) \subseteq \mathrm{Roots}(I \cap J)$. For every o such that $o \in \mathrm{Roots}(I \cap J)$ holds $o \in \mathrm{Roots}(I) \cup \mathrm{Roots}(J)$. □

(23) $\mathrm{Roots}(I * J) = \mathrm{Roots}(I) \cup \mathrm{Roots}(J)$.
PROOF: $\mathrm{Roots}(I \cap J) \subseteq \mathrm{Roots}(I * J)$. For every o such that $o \in \mathrm{Roots}(I * J)$ holds $o \in \mathrm{Roots}(I) \cup \mathrm{Roots}(J)$. □

5. THE COLLECTION OF ALGEBRAIC SETS

Let us consider n and R. The functor AlgSets(n, R) yielding a set is defined by the term

(Def. 7) $\{S$, where S is a subset of $(\Omega_R)^n : S$ is an algebraic set of n and $R\}$.

Now we state the proposition:

(24) Let us consider a non zero natural number m, and a subset F of AlgSets(n, R). Suppose $\overline{\overline{F}} = m$. Then $\bigcup F$ is an algebraic set of n and R.
PROOF: Define $\mathcal{P}$[natural number] ≡ for every subset G of AlgSets(n, R) such that $\overline{\overline{G}} = \$_1$ holds $\bigcup G$ is an algebraic set of n and R. For every non zero natural number m such that $\mathcal{P}[m]$ holds $\mathcal{P}[m + 1]$ by [9, (1)]. $\mathcal{P}[1]$. For every non zero natural number n, $\mathcal{P}[n]$. □

Let us consider n and R. Let a be a function from n into R. The functor polyset(a) yielding a non empty subset of Polynom-Ring(n, R) is defined by the term

(Def. 8) $\{f$, where f is a polynomial of n,R : there exists an element i of n such that $f = \mathrm{deg1Poly}(a, i)\}$.

Now we state the propositions:

(25) Let us consider a function a from n into R. Then $\mathrm{Roots}(\mathrm{polyset}(a)) = \{a\}$.
PROOF: If $o \in \mathrm{Roots}(\mathrm{polyset}(a))$, then $o \in \{a\}$ by [10, (24)], [1, (1)]. If $o \in \{a\}$, then $o \in \mathrm{Roots}(\mathrm{polyset}(a))$ by [10, (24)], [1, (1)]. □

(26) Let us consider an element x of $(\Omega_R)^n$. Then $\{x\}$ is an algebraic set of n and R. The theorem is a consequence of (25) and (17).

(27) Let us consider a non zero natural number m, and a subset P of $S_{((\Omega_R)^n)}$. Suppose $\overline{\overline{P}} = m$. Then $\bigcup P$ is an algebraic set of n and R.
PROOF: $S_{((\Omega_R)^n)} \subseteq \mathrm{AlgSets}(n, R)$. □

6. The Ideal of a Set of Points

Let us consider R, n, and X. The functor $\mathrm{Ideal}(X)$ yielding a non empty subset of Polynom-Ring(n, R) is defined by the term

(Def. 9) $\{f$, where f is a polynomial of n,$R : X \subseteq \mathrm{Roots}(f)\}$.

Now we state the proposition:

(28) $\mathrm{Ideal}(X)$ is an ideal of Polynom-Ring(n, R).

Let us consider R, n, and X. One can check that $\mathrm{Ideal}(X)$ is closed under addition as a subset of Polynom-Ring(n, R) and $\mathrm{Ideal}(X)$ is right ideal as a subset of Polynom-Ring(n, R). Now we state the propositions:

(29) If $X \subseteq Y$, then $\mathrm{Ideal}(Y) \subseteq \mathrm{Ideal}(X)$.

(30) $X = \emptyset$ if and only if $\mathrm{Ideal}(X) = \Omega_{\text{Polynom-Ring}(n,R)}$.
PROOF: If $X = \emptyset$, then $\mathrm{Ideal}(X) = \Omega_{\text{Polynom-Ring}(n,R)}$. If $\mathrm{Ideal}(X) = \Omega_{\text{Polynom-Ring}(n,R)}$, then $X = \emptyset_{(\Omega_R)^n}$. □

(31) $\{0_{\text{Polynom-Ring}(n,R)}\} \subseteq \mathrm{Ideal}(\Omega_{(\Omega_R)^n})$. The theorem is a consequence of (13).

(32) $S \subseteq \mathrm{Ideal}(\mathrm{Roots}(S))$.

(33) $X \subseteq \mathrm{Roots}(\mathrm{Ideal}(X))$.
PROOF: For every o such that $o \in X$ holds $o \in \mathrm{Roots}(\mathrm{Ideal}(X))$. □

(34) $\mathrm{Roots}(\mathrm{Ideal}(\mathrm{Roots}(S))) = \mathrm{Roots}(S)$. The theorem is a consequence of (33), (16), (32), and (30).

(35) $\mathrm{Ideal}(\mathrm{Roots}(\mathrm{Ideal}(X))) = \mathrm{Ideal}(X)$.

(36) Let us consider an algebraic set X of n and R. Then $X = \mathrm{Roots}(\mathrm{Ideal}(X))$. The theorem is a consequence of (34).

(37) Let us consider algebraic sets V, W of n and R. Then $V = W$ if and only if $\mathrm{Ideal}(V) = \mathrm{Ideal}(W)$. The theorem is a consequence of (36).

(38) Let us consider algebraic sets X, Y of n and R. If $X \subset Y$, then $\mathrm{Ideal}(Y) \subset \mathrm{Ideal}(X)$. The theorem is a consequence of (36) and (29).

(39) $\sqrt{\mathrm{Ideal}(X)} = \mathrm{Ideal}(X)$. The theorem is a consequence of (30) and (15).

7. Reducible Algebraic Sets

Let us consider R and n. Let I be an algebraic set of n and R. We say that I is reducible if and only if

(Def. 10) there exist algebraic sets V_1, V_2 of n and R such that $I = V_1 \cup V_2$ and $V_1 \subset I$ and $V_2 \subset I$.

Let V be an algebraic set of n and R. We introduce the notation V is irreducible as an antonym for V is reducible. Now we state the proposition:

(40) Let us consider a non empty algebraic set V of n and R. Then V is irreducible if and only if Ideal(V) is a prime ideal of Polynom-Ring(n, R). Proof: If Ideal(V) is a prime ideal of Polynom-Ring(n, R), then V is irreducible. If V is irreducible, then Ideal(V) is a prime ideal of Polynom-Ring (n, R). □

References

[1] Marcin Acewicz and Karol Pąk. Basic Diophantine relations. *Formalized Mathematics*, 26(**2**):175–181, 2018. doi:10.2478/forma-2018-0015.

[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] Edward J. Barbeau. *Polynomials*. Springer, 2003.

[4] William Fulton. *Algebraic Curves. An Introduction to Algebraic Geometry*. The Benjamin/Cummings Publishing Company, 1969.

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

[6] Karol Pąk. Prime representing polynomial. *Formalized Mathematics*, 29(**4**):221–228, 2021. doi:10.2478/forma-2021-0020.

[7] Piotr Rudnicki, Christoph Schwarzweller, and Andrzej Trybulec. Commutative algebra in the Mizar system. *Journal of Symbolic Computation*, 32(1/2):143–169, 2001. doi:10.1006/jsco.2001.0456.

[8] Christoph Schwarzweller. Existence and uniqueness of algebraic closures. *Formalized Mathematics*, 30(**4**):281–294, 2022. doi:10.2478/forma-2022-0022.

[9] Christoph Schwarzweller. Renamings and a condition-free formalization of Kronecker's construction. *Formalized Mathematics*, 28(**2**):129–135, 2020. doi:10.2478/forma-2020-0012.

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

[11] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer, 2008.

Accepted June 30, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 75–86, 2023
DOI: 10.2478/forma-2023-0008
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

About Regular Graphs

Sebastian Koch[1]
Mainz, Germany

Summary. In this article regular graphs, both directed and undirected, are formalized in the Mizar system [7], [2], based on the formalization of graphs as described in [10]. The handshaking lemma is also proven.

MSC: 05C07 68V20

Keywords: regular graphs

MML identifier: `GLIB_016`, version: `8.1.12 5.75.1447`

Introduction

Regular graphs, especially cubic graphs, are a cornerstone of graph theory (cf. [3], [12], [6]). In this article the concept of regular graphs is formalized (compare similar efforts using various proof-assistants [11], [5], [4]), along with some adjacent concepts, developing further some of the previous Mizar articles [8], [9]. In the first section, the directed analogue of `complete` from [1] is introduced. Sections 2 and 3 deal with the undirected and directed-regular graphs respectively. Section 4 is rather technical in nature; at its end $2m = \mathfrak{a}n$ is proven, where m and n denote the size and order of an $\mathfrak{a}$-regular graph, where $\mathfrak{a}$ can be any cardinal. Finally Section 5 introduces tools needed to formalize the combinatorial proof of the rather simple Handshaking Lemma.

[1]mailto: `fly.high.android@gmail.com`

1. Directed-complete Graphs

Let G be a graph. We say that G is directed-complete if and only if

(Def. 1) for every vertices v, w of G such that $v \neq w$ there exists an object e such that e joins v to w in G.

Let c be a non empty cardinal number. The functors: canCompleteGraph(c) and canDCompleteGraph(c) yielding graphs are defined by terms

(Def. 2) createGraph(c, $\subseteq_c \setminus (\mathrm{id}_c)$),

(Def. 3) createGraph(c, $(c \times c) \setminus (\mathrm{id}_c)$),

respectively. Observe that the vertices of canCompleteGraph(c) reduces to c and the vertices of canDCompleteGraph(c) reduces to c.

Observe that every vertex of canCompleteGraph(c) is ordinal and every vertex of canDCompleteGraph(c) is ordinal and every vertex of canCompleteGraph (ω) is natural and every vertex of canDCompleteGraph(ω) is natural.

Let n be a non zero natural number. Observe that canCompleteGraph(n) is finite and canDCompleteGraph(n) is finite and every vertex of canCompleteGraph(n) is natural and every vertex of canDCompleteGraph(n) is natural.

Let c be a non empty cardinal number. One can verify that canCompleteGraph(c) is plain, c-vertex, simple, and complete and canDCompleteGraph(c) is plain, c-vertex, directed-simple, and directed-complete. Now we state the propositions:

(1) Let us consider a non empty cardinal number c, and a vertex v of canCompleteGraph(c). Then

(i) v.inNeighbors() $= v$, and

(ii) v.outNeighbors() $= c \setminus (\mathrm{succ}\, v)$.

(2) Let us consider a vertex v of canCompleteGraph(ω). Then

(i) v.inDegree() $= v$, and

(ii) v.outDegree() $= \omega$.

The theorem is a consequence of (1).

(3) Let us consider a non zero natural number n, and a vertex v of canCompleteGraph(n). Then

(i) v.inDegree() $= v$, and

(ii) v.outDegree() $= n - v - 1$.

The theorem is a consequence of (1).

Let c be a non empty cardinal number. Let us observe that there exists a graph which is simple, c-vertex, and complete and there exists a graph which

is directed-simple, c-vertex, and directed-complete and every graph which is directed-complete is also complete and every graph which is trivial is also directed-complete and every graph which is non trivial and directed-complete is also non non-multi and non edgeless and there exists a graph which is non directed-complete. Now we state the propositions:

(4) Let us consider graphs G_1, G_2. Suppose $G_1 \approx G_2$ and G_1 is directed-complete. Then G_2 is directed-complete.

(5) Let us consider a graph G_1, and a subgraph G_2 of G_1 with loops removed. Then G_1 is directed-complete if and only if G_2 is directed-complete.

(6) Let us consider a graph G_1, and a subgraph G_2 of G_1 with directed-parallel edges removed. Then G_1 is directed-complete if and only if G_2 is directed-complete.

(7) Let us consider a graph G_1, and a directed-simple graph G_2 of G_1. Then G_1 is directed-complete if and only if G_2 is directed-complete. The theorem is a consequence of (6) and (5).

(8) Let us consider a graph G_1, and a graph G_2 given by reversing directions of the edges of G_1. Then G_1 is directed-complete if and only if G_2 is directed-complete.

Let G be a directed-complete graph. Let us note that every subgraph of G with loops removed is directed-complete and every subgraph of G with directed-parallel edges removed is directed-complete and every directed-simple graph of G is directed-complete and every graph given by reversing directions of the edges of G is directed-complete.

Let V be a set. Observe that every subgraph of G induced by V is directed-complete and every graph by adding a loop to each vertex of G in V is directed-complete. Let v, e, w be objects. Note that every supergraph of G extended by e between vertices v and w is directed-complete.

Let G be a non directed-complete graph. One can verify that every subgraph of G with loops removed is non directed-complete and every subgraph of G with directed-parallel edges removed is non directed-complete and every directed-simple graph of G is non directed-complete and every graph given by reversing directions of the edges of G is non directed-complete and every subgraph of G which is spanning is also non directed-complete.

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:

(9) If F is directed-continuous and strong subgraph embedding, then if G_2 is directed-complete, then G_1 is directed-complete.

(10) If F is directed-isomorphism, then G_1 is directed-complete iff G_2 is directed-complete. The theorem is a consequence of (9).

Let G be a directed-complete graph. Observe that every graph which is G-directed-isomorphic is also directed-complete. Now we state the propositions:

(11) Let us consider a directed-complete graph G, and a vertex v of G. Then

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

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

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

(12) Let us consider a loopless, directed-complete graph G, and a vertex v of G. Then

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

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

(iii) v.allNeighbors() = (the vertices of G) $\setminus \{v\}$.

The theorem is a consequence of (11).

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

(i) v.inDegree() $+ 1 = G$.order(), and

(ii) v.outDegree() $+ 1 = G$.order().

The theorem is a consequence of (12).

(14) Let us consider a graph G_1, and a directed graph complement G_2 of G_1 with loops. Then the edges of $G_1 = G_1$.loops() if and only if G_2 is directed-complete.

Let G be an edgeless graph. Let us observe that every directed graph complement of G with loops is directed-complete. Now we state the proposition:

(15) Let us consider a graph G_1, and a directed graph complement G_2 of G_1 with loops. Then G_1 is directed-complete if and only if the edges of $G_2 = G_2$.loops().

One can verify that there exists a graph which is loopfull and directed-complete.

Let G be a loopfull, directed-complete graph. Let us observe that every directed graph complement of G with loops is edgeless. Now we state the proposition:

(16) Let us consider a graph G_1, and a directed graph complement G_2 of G_1. Then the edges of $G_1 = G_1$.loops() if and only if G_2 is directed-complete. The theorem is a consequence of (14).

Let G be an edgeless graph. Note that every directed graph complement of G is directed-complete. Now we state the proposition:

(17) Let us consider a graph G_1, and a directed graph complement G_2 of G_1. Then G_1 is directed-complete if and only if G_2 is edgeless. The theorem is a consequence of (15).

Let G be a directed-complete graph. One can verify that every directed graph complement of G is edgeless. Let G be a non directed-complete graph. One can check that every directed graph complement of G is non edgeless.

Let G_1 be a graph and G_2 be a directed graph complement of G_1 with loops. One can verify that every graph union of G_1 and G_2 is directed-complete. Let G_2 be a directed graph complement of G_1. Note that every graph union of G_1 and G_2 is directed-complete. Now we state the propositions:

(18) Let us consider a graph G. Then G is directed-complete if and only if $((\text{the vertices of } G) \times (\text{the vertices of } G)) \setminus (\mathrm{id}_\alpha) \subseteq \mathrm{VertDomRel}(G)$, where α is the vertices of G.

(19) Let us consider a non empty set V, and a binary relation E on V. Then $\mathrm{createGraph}(V, E)$ is directed-complete if and only if $(V \times V) \setminus (\mathrm{id}_V) \subseteq E$.

2. Regular Graphs

From now on c, c_1, c_2 denote cardinal numbers, G, G_1, G_2 denote graphs, and v denotes a vertex of G.

Let us consider c and G. We say that G is c-regular if and only if

(Def. 4) for every v, $v.\mathrm{degree}() = c$.

One can check that every graph which is c-regular is also with max degree and every graph which is $(c+1)$-vertex, simple, and complete is also c-regular and there exists a graph which is simple and c-regular. Now we state the propositions:

(20) Degree of regularity is unique:
If G is c_1-regular and c_2-regular, then $c_1 = c_2$.

(21) G is c-regular if and only if every component of G is c-regular.

Let us consider c. Let us observe that there exists a graph which is non c-regular. Let G be a c-regular graph. Note that every component of G is c-regular. Now we state the propositions:

(22) Let us consider a c-regular graph G. Then
(i) $\delta(G) = c$, and
(ii) $\Delta(G) = c$.

(23) If $\delta(G) = c$ and $\bar{\Delta}(G) = c$, then G is c-regular.

Let n be a natural number. Observe that every graph which is n-regular is also locally-finite and there exists a graph which is simple, vertex-finite, and n-regular. Now we state the proposition:

(24) G is edgeless if and only if G is 0-regular.

One can verify that every graph which is edgeless is also 0-regular and every graph which is 0-regular is also edgeless. Let c be a non empty cardinal number. Let us observe that every graph which is c-regular is also non edgeless. Now we state the propositions:

(25) Let us consider a simple, c-regular graph G. Then $c \subseteq G.\mathrm{order}()$.

(26) Let us consider a natural number n, and a simple, vertex-finite, n-regular graph G_1. Then every graph complement of G_1 is $(G_1.\mathrm{order}() -' (n+1))$-regular.

(27) If there exists v such that v is isolated and G is c-regular, then $c = 0$.

(28) If there exists v such that v is endvertex and G is c-regular, then $c = 1$.

Let G be a 1-regular graph. Observe that every vertex of G is endvertex.

Now we state the proposition:

(29) Let us consider a 1-regular graph G, and a trail T of G. Suppose T is not trivial. Then there exists an object e such that

(i) e joins $T.\mathrm{first}()$ and $T.\mathrm{last}()$ in G, and

(ii) $T = G.\mathrm{walkOf}(T.\mathrm{first}(), e, T.\mathrm{last}())$.

One can verify that every graph which is 1-regular and connected is also 2-vertex, 1-edge, and complete and every graph which is simple, 2-vertex, and connected is also 1-regular. Now we state the propositions:

(30) Let us consider a partial graph mapping F from G_1 to G_2. Suppose F is isomorphism. Then G_1 is c-regular if and only if G_2 is c-regular.

(31) If $G_1 \approx G_2$ and G_1 is c-regular, then G_2 is c-regular.

(32) Let us consider a set E, and a graph G_2 given by reversing directions of the edges E of G_1. Then G_1 is c-regular if and only if G_2 is c-regular. The theorem is a consequence of (30).

Let G be a graph. We say that G is cubic if and only if

(Def. 5) G is 3-regular.

One can verify that every graph which is cubic is also 3-regular and every graph which is 3-regular is also cubic. Now we state the propositions:

(33) G is cubic if and only if for every v, $v.\mathrm{degree}() = 3$.

(34) Let us consider a partial graph mapping F from G_1 to G_2. If F is isomorphism, then G_1 is cubic iff G_2 is cubic.

(35) If $G_1 \approx G_2$ and G_1 is cubic, then G_2 is cubic.

(36) Let us consider a set E, and a graph G_2 given by reversing directions of the edges E of G_1. Then G_1 is cubic if and only if G_2 is cubic.

Let G be a graph. We say that G is regular if and only if

(Def. 6) there exists a cardinal number c such that G is c-regular.

Now we state the proposition:

(37) G is regular if and only if $\delta(G) = \bar{\Delta}(G)$. The theorem is a consequence of (22) and (23).

Let G be a locally-finite graph. One can check that G is regular if and only if the condition (Def. 7) is satisfied.

(Def. 7) there exists a natural number n such that G is n-regular.

Let c be a cardinal number. Let us note that every graph which is c-regular is also regular and every graph which is cubic is also regular and every graph which is regular is also with max degree and there exists a graph which is simple, non edgeless, finite, and regular.

Let G be a regular graph. Note that every component of G is regular. Let G be a simple, finite, regular graph. One can verify that every graph complement of G is regular. Now we state the propositions:

(38) If there exists v such that v is isolated and G is regular, then G is edgeless. The theorem is a consequence of (27).

(39) If there exists v such that v is endvertex and G is regular, then G is 1-regular. The theorem is a consequence of (28).

(40) Let us consider a partial graph mapping F from G_1 to G_2. If F is isomorphism, then G_1 is regular iff G_2 is regular. The theorem is a consequence of (30).

(41) If $G_1 \approx G_2$ and G_1 is regular, then G_2 is regular. The theorem is a consequence of (40).

(42) Let us consider a set E, and a graph G_2 given by reversing directions of the edges E of G_1. Then G_1 is regular if and only if G_2 is regular. The theorem is a consequence of (40).

3. Directed-regular Graphs

Let us consider c and G. We say that G is c-directed-regular if and only if

(Def. 8) for every v, v.inDegree() $= c$ and v.outDegree() $= c$.

Let us note that every graph which is c-directed-regular is also with max indegree and with max outdegree and every graph which is $(c+1)$-vertex, directed-simple, and directed-complete is also c-directed-regular and there exists a graph which is directed-simple and c-directed-regular. Now we state the proposition:

(43) Degree of directed regularity is unique:
If G is c_1-directed-regular and c_2-directed-regular, then $c_1 = c_2$.

Let us consider c. One can check that there exists a graph which is non c-directed-regular. Let G be a c-directed-regular graph. Observe that every component of G is c-directed-regular. Now we state the propositions:

(44) Let us consider a c-directed-regular graph G. Then
  (i) $\delta^-(G) = c$, and
  (ii) $\delta^+(G) = c$, and
  (iii) $\Delta^-(G) = c$, and
  (iv) $\Delta^+(G) = c$.

(45) If $\delta^-(G) = c$ and $\delta^+(G) = c$ and $\bar{\Delta}^-(G) = c$ and $\bar{\Delta}^+(G) = c$, then G is c-directed-regular.

(46) Let us consider a natural number n. If G is n-directed-regular, then G is $(2 \cdot n)$-regular.

Let n be a natural number. One can check that every graph which is n-directed-regular is also $(2 \cdot n)$-regular and locally-finite and there exists a graph which is directed-simple, finite, and n-directed-regular.

Let c be an infinite cardinal number. Let us note that every graph which is c-directed-regular is also c-regular. Now we state the proposition:

(47) G is edgeless if and only if G is 0-directed-regular. The theorem is a consequence of (46).

One can verify that every graph which is edgeless is also 0-directed-regular and every graph which is 0-directed-regular is also edgeless.

Let c be a non empty cardinal number. Let us observe that every graph which is c-directed-regular is also non edgeless. Now we state the propositions:

(48) Let us consider a directed-simple, c-directed-regular graph G. Then $c \subseteq G.\mathrm{order}()$.

(49) Let us consider a natural number n, and a directed-simple, vertex-finite, n-directed-regular graph G_1. Then every directed graph complement of G_1 is $(G_1.\mathrm{order}() -' (n+1))$-directed-regular.

(50) If there exists v such that v is isolated and G is c-directed-regular, then $c = 0$.

Let us consider c. Let G be a c-directed-regular graph. Let us note that every vertex of G is non endvertex and every graph which is 2-edge, 2-vertex, and directed-simple is also 1-directed-regular and complete and every graph which is trivial and 1-edge is also 1-directed-regular. Now we state the propositions:

(51) Let us consider a partial graph mapping F from G_1 to G_2. Suppose F is directed-isomorphism. Then G_1 is c-directed-regular if and only if G_2 is c-directed-regular.

(52) If $G_1 \approx G_2$ and G_1 is c-directed-regular, then G_2 is c-directed-regular.

Let G be a graph. We say that G is directed-regular if and only if

(Def. 9) there exists a cardinal number c such that G is c-directed-regular.

Now we state the proposition:

(53) G is directed-regular if and only if $\delta^-(G) = \bar{\Delta}^-(G)$ and $\delta^+(G) = \bar{\Delta}^+(G)$ and $\delta^-(G) = \delta^+(G)$. The theorem is a consequence of (44) and (45).

Let G be a locally-finite graph. One can verify that G is directed-regular if and only if the condition (Def. 10) is satisfied.

(Def. 10) there exists a natural number n such that G is n-directed-regular.

Let c be a cardinal number. Note that every graph which is c-directed-regular is also directed-regular and every graph which is directed-regular is also with max degree and there exists a graph which is directed-simple, non edgeless, finite, and directed-regular.

Let G be a directed-regular graph. Observe that every component of G is directed-regular. Let G be a directed-simple, finite, directed-regular graph. Note that every directed graph complement of G is directed-regular. Let G be a directed-regular graph. Note that every vertex of G is non endvertex. Now we state the propositions:

(54) Let us consider a partial graph mapping F from G_1 to G_2. Suppose F is directed-isomorphism. Then G_1 is directed-regular if and only if G_2 is directed-regular. The theorem is a consequence of (51).

(55) If $G_1 \approx G_2$ and G_1 is directed-regular, then G_2 is directed-regular. The theorem is a consequence of (54).

4. Counting the Edges

Now we state the propositions:

(56) Let us consider a set P, and a cardinal number c. Suppose P is mutually-disjoint and for every set A such that $A \in P$ holds $\overline{\overline{A}} = c$. Then $\overline{\overline{\bigcup P}} = c \cdot \overline{\overline{P}}$.

(57) Let us consider a non empty set X, a partition P of X, and a cardinal number c. Suppose for every element x of X, $\overline{\overline{\mathrm{EqClass}(x, P)}} = c$. Then $\overline{\overline{X}} = c \cdot \overline{\overline{P}}$. The theorem is a consequence of (56).

Let f be a function and X be a set. One can verify that $\langle f, \mathrm{id}_X \rangle$ is one-to-one.

Let f be a one-to-one function. One can verify that $f^\smile$ is one-to-one and $\curvearrowleft f$ is one-to-one.

Let X be a set and f be a function. Let us observe that $\langle \mathrm{id}_X, f \rangle$ is one-to-one.

Now we state the proposition:

(58) Let us consider a c-regular graph G. Then $2 \cdot G.\mathrm{size}() = c \cdot G.\mathrm{order}()$. The theorem is a consequence of (56).

5. The Degree Map and Degree Sequence

Let G be a graph. The functors: G.degreeMap(), G.inDegreeMap(), and G.outDegreeMap() yielding many sorted sets indexed by the vertices of G are defined by conditions

(Def. 11) for every vertex v of G, $G.\mathrm{degreeMap}()(v) = v.\mathrm{degree}()$,

(Def. 12) for every vertex v of G, $G.\mathrm{inDegreeMap}()(v) = v.\mathrm{inDegree}()$,

(Def. 13) for every vertex v of G, $G.\mathrm{outDegreeMap}()(v) = v.\mathrm{outDegree}()$,

respectively. Let us observe that G.degreeMap() is cardinal yielding and G.inDegreeMap() is cardinal yielding and G.outDegreeMap() is cardinal yielding. Now we state the propositions:

(59) Let us consider a graph G. Then

(i) $\overline{\overline{G.\mathrm{degreeMap}()}} = G.\mathrm{order}()$, and

(ii) $\overline{\overline{G.\mathrm{inDegreeMap}()}} = G.\mathrm{order}()$, and

(iii) $\overline{\overline{G.\mathrm{outDegreeMap}()}} = G.\mathrm{order}()$.

(60) Let us consider a graph G, and a vertex v of G. Then $(G.\mathrm{degreeMap}())(v) = (G.\mathrm{inDegreeMap}())(v) + (G.\mathrm{outDegreeMap}())(v)$.

Let G be a locally-finite graph. Note that G.degreeMap() is natural-valued and G.inDegreeMap() is natural-valued and G.outDegreeMap() is natural-valued.

The functors: G.degreeMap(), G.inDegreeMap(), and G.outDegreeMap() yield functions from the vertices of G into $\mathbb{N}$. Let G be a vertex-finite graph. Note that G.degreeMap() is finite and G.inDegreeMap() is finite and G.outDegreeMap() is finite. Now we state the proposition:

(61) Let us consider a cardinal number c, a trivial, c-edge graph G, and a vertex v of G. Then

(i) $G.\mathrm{inDegreeMap}() = v \mapsto\!\!\!\!\cdot\!\!\!\!\longrightarrow c$, and

(ii) $G.\mathrm{outDegreeMap}() = v \mapsto\!\!\!\!\cdot\!\!\!\!\longrightarrow c$, and

(iii) $G.\mathrm{degreeMap}() = v \mapsto\!\!\!\!\cdot\!\!\!\!\longrightarrow 2 \cdot c$.

Let G be a trivial graph. Let us note that G.degreeMap() is trivial and G.inDegreeMap() is trivial and G.outDegreeMap() is trivial. Now we state the propositions:

(62) Let us consider a graph G_2, a set V, and a supergraph G_1 of G_2 extended by the vertices from V. Then

(i) G_1.degreeMap() = G_2.degreeMap() $+\cdot$($V \setminus$ (the vertices of G_2) $\longmapsto 0$), and

(ii) G_1.inDegreeMap() = G_2.inDegreeMap() $+\cdot$($V \setminus$ (the vertices of G_2) $\longmapsto 0$), and

(iii) G_1.outDegreeMap() = G_2.outDegreeMap() $+\cdot$($V \setminus$ (the vertices of G_2) $\longmapsto 0$).

(63) Let us consider a graph G, and a component C of G. Then

(i) C.degreeMap() = G.degreeMap() $\restriction$(the vertices of C), and

(ii) C.inDegreeMap() = G.inDegreeMap() $\restriction$(the vertices of C), and

(iii) C.outDegreeMap() = G.outDegreeMap() $\restriction$(the vertices of C).

Let G be a graph and v be a denumeration of the vertices of G. Let us observe that $(G.\text{degreeMap}()) \cdot v$ is transfinite sequence-like and $(G.\text{order}())$-elements and $(G.\text{inDegreeMap}()) \cdot v$ is transfinite sequence-like and $(G.\text{order}())$-elements and $(G.\text{outDegreeMap}()) \cdot v$ is transfinite sequence-like and $(G.\text{order}())$-elements.

Let us consider a finite graph G and a denumeration v of the vertices of G. Now we state the propositions:

(64) $(G.\text{degreeMap}()) \cdot v = (G.\text{inDegreeMap}()) \cdot v + (G.\text{outDegreeMap}()) \cdot v$. The theorem is a consequence of (60).

(65) (i) $G.\text{size}() = \sum (G.\text{inDegreeMap}()) \cdot v$, and

(ii) $G.\text{size}() = \sum (G.\text{outDegreeMap}()) \cdot v$.

(66) $2 \cdot (G.\text{size}()) = \sum (G.\text{degreeMap}()) \cdot v$. The theorem is a consequence of (65) and (64).

(67) Handshaking Lemma:
Let us consider a finite graph G, and a natural number k. Suppose $k = \overline{\overline{\{w, \text{ where } w \text{ is a vertex of } G : w.\text{degree}() \text{ is not even } \}}}$. Then k is even.
Proof: Set v = the denumeration of the vertices of G. Define $\mathcal{M}$(natural number) = $((G.\text{degreeMap}()) \cdot v)(\$_1)$ mod 2. Consider m being a finite 0-sequence of $\mathbb{N}$ such that $\operatorname{len} m = \operatorname{len}(G.\text{degreeMap}()) \cdot v$ and for every natural number k such that $k \in \operatorname{len}(G.\text{degreeMap}()) \cdot v$ holds $m(k) = \mathcal{M}(k)$. □

References

[1] Broderick Arneson and Piotr Rudnicki. Chordal graphs. *Formalized Mathematics*, 14(**3**): 79–92, 2006. doi:10.2478/v10037-006-0010-3.

[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] 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.

[4] Ricky W. Butler and Jon A. Sjogren. A PVS graph theory library. Technical report, NASA Langley, 1998.

[5] Ching-Tsun Chou. A formal theory of undirected graphs in higher-order logic. In Thomas F. Melham and Juanito Camilleri, editors, *Higher Order Logic Theorem Proving and Its Applications, 7th International Workshop, Valletta, Malta, September 19–22, 1994, Proceedings*, volume 859 of *Lecture Notes in Computer Science*, pages 144–157. Springer, 1994. doi:10.1007/3-540-58450-1_40.

[6] Reinhard Diestel. *Graph Theory*, volume Graduate Texts in Mathematics; 173. Springer, Berlin, fifth edition, 2017. ISBN 978-3-662-53621-6.

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

[8] Sebastian Koch. Miscellaneous graph preliminaries. Part I. *Formalized Mathematics*, 29 (**1**):21–38, 2021. doi:10.2478/forma-2021-0003.

[9] Sebastian Koch. About graph sums. *Formalized Mathematics*, 29(**4**):249–278, 2021. doi:10.2478/forma-2021-0023.

[10] Gilbert Lee and Piotr Rudnicki. Alternative aggregates in Mizar. In Manuel Kauers, Manfred Kerber, Robert Miner, and Wolfgang Windsteiger, editors, *Towards Mechanized Mathematical Assistants*, pages 327–341, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. ISBN 978-3-540-73086-6. doi:10.1007/978-3-540-73086-6_26.

[11] Lars Noschinski. A graph library for Isabelle. *Mathematics in Computer Science*, 9(1): 23–39, 2015. doi:10.1007/s11786-014-0183-z.

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

Accepted June 30, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 87–100, 2023
DOI: 10.2478/forma-2023-0009
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part VIII

Artur Korniłowicz
Faculty of Computer Science
University of Białystok
Poland

Summary. In this paper problems 25, 86, 88, 105, 111, 137–142, and 184–185 from [12] are formalized, using the Mizar formalism [3], [1], [4]. This is a continuation of the work from [5], [6], and [2] as suggested in [8]. The automatization of selected lemmas from [11] proven in this paper as proposed in [9] could be an interesting future work.

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes; factorization

MML identifier: NUMBER08, version: 8.1.12 5.75.1447

1. Preliminaries

From now on X denotes a set, a, b, c, k, m, n denote natural numbers, i, j denote integers, r, s denote real numbers, and p, p_1, p_2, p_3, q denote prime numbers.

Let us consider n and r. Let us observe that $n-r+r$ is natural and $n+r-r$ is natural. Now we state the propositions:

(1) Let us consider natural numbers m, n. If $m < n < m+2$, then $n = m+1$.

(2) $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$.

Let us note that $\mathbb{N}_+$ is infinite. Now we state the propositions:

(3) Let us consider finite sequences f, g. Suppose $f \frown g$ is X-valued. Then

(i) f is X-valued, and

(ii) g is X-valued.

(4) Let us consider complex-valued many sorted sets f_1, f_2, f_3 indexed by X. Suppose for every object x such that $x \in X$ holds $f_1(x) = f_2(x) \cdot f_3(x)$. Then $f_1 = f_2 \cdot f_3$.

(5) If $b \neq 0$ and $c \neq 0$, then $\frac{r \cdot b + c}{b} > r$.

(6) If $m \leqslant n$, then $m! \mid n!$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ if $m \leqslant \$_1$, then $m! \mid \$_1!$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(7) If $p_1 \mid p_2$, then $p_1 = p_2$.

(8) If m and n are relatively prime, then $a \cdot n + m$ and n are relatively prime.

(9) If $n \mid 27$, then $n = 1$ or $n = 3$ or $n = 9$ or $n = 27$.

2. Problem 25

Now we state the proposition:

(10) Let us consider a function f. Then support(EmptyBag $X \mapsto f$) = support f.

Let X be a set and f be a finite-support function.

Observe that EmptyBag $X \mapsto f$ is finite-support.

Let p be a prime number and n be a non zero natural number. Observe that p-count(p^n) is non zero. Now we state the propositions:

(11) Let us consider a finite-support function b.
Then $\operatorname{dom}(b \cdot (\operatorname{CFS}(\operatorname{support} b))) = \operatorname{dom}(\operatorname{CFS}(\operatorname{support} b))$.

(12) Let us consider complex-valued functions f, g. Then $\operatorname{support}(f \cdot g) \subseteq \operatorname{support} f$.

Let f, g be finite-support, complex-valued functions. One can verify that $f \cdot g$ is finite-support. Now we state the propositions:

(13) Let us consider complex-valued functions f, g. Suppose support f = support g. Then $\operatorname{support}(f \cdot g) = \operatorname{support} f$. The theorem is a consequence of (12).

(14) Let us consider finite-support, complex-valued many sorted sets b_1, b_2 indexed by X. Suppose support b_1 = support b_2. Then $\prod(b_1 \cdot b_2) = (\prod b_1) \cdot (\prod b_2)$.

PROOF: Set $b_0 = b_1 \cdot b_2$. support b_0 = support b_1. support b_0 = support b_2. Consider f_0 being a finite sequence of elements of $\mathbb{C}$ such that $\prod b_0 = \prod f_0$ and $f_0 = b_0 \cdot (\operatorname{CFS}(\operatorname{support} b_0))$. Consider f_1 being a finite sequence of elements of $\mathbb{C}$ such that $\prod b_1 = \prod f_1$ and $f_1 = b_1 \cdot (\operatorname{CFS}(\operatorname{support} b_1))$. Consider f_2 being a finite sequence of elements of $\mathbb{C}$ such that $\prod b_2 = \prod f_2$ and $f_2 =$

$b_2 \cdot (\mathrm{CFS}(\mathrm{support}\, b_2))$. $\mathrm{dom}(b_0 \cdot (\mathrm{CFS}(\mathrm{support}\, b_0))) = \mathrm{dom}(\mathrm{CFS}(\mathrm{support}\, b_0))$. $\mathrm{dom}\, f_0 = \mathrm{dom}\, f_1$. $\mathrm{dom}\, f_0 = \mathrm{dom}\, f_2$. For every object c such that $c \in \mathrm{dom}\, f_0$ holds $f_0(c) = f_1(c) \cdot f_2(c)$. $\square$

Let n be a non zero natural number. The functor EulerFactorization(n) yielding a function is defined by

(Def. 1) $\mathrm{dom}\, it = \mathrm{support}\, \mathrm{PPF}(n)$ and for every natural number p such that $p \in \mathrm{dom}\, it$ there exists a non zero natural number c such that $c = p\text{-count}(n)$ and $it(p) = p^c - p^{c-1}$.

Observe that dom(EulerFactorization(n)) is finite and EulerFactorization(n) is $\mathbb{P}$-defined. Now we state the propositions:

(15) Let us consider a non zero natural number n, and an object p. Suppose $p \in \mathrm{dom}(\mathrm{EulerFactorization}(n))$. Then p is a prime number.

(16) Let us consider a non zero natural number n, and a natural number p. Suppose $p \in \mathrm{dom}(\mathrm{EulerFactorization}(n))$. Then there exists a non zero natural number c such that

(i) $c = p\text{-count}(n)$, and

(ii) $(\mathrm{EulerFactorization}(n))(p) = p^{c-1} \cdot (p-1)$.

Let n be a non zero natural number. Let us observe that EulerFactorization(n) is natural-valued and EulerFactorization(n) is finite-support and EulerFactorization(1) is empty. Now we state the propositions:

(17) Let us consider a non zero natural number n.
Then $\mathrm{EulerFactorization}(p^n) = p \mapsto (p^n - p^{n-1})$.

(18) $\mathrm{EulerFactorization}(p) = p \mapsto (p-1)$. The theorem is a consequence of (17).

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

(19) $\mathrm{support}\, \mathrm{EulerFactorization}(n) = \mathrm{dom}(\mathrm{EulerFactorization}(n))$. The theorem is a consequence of (15).

(20) If $n > 1$, then $\mathrm{support}\, \mathrm{EulerFactorization}(n)$ is not empty.

(21) If $n > 1$, then EulerFactorization(n) is not empty. The theorem is a consequence of (20).

Let us consider non zero natural numbers s, t. Now we state the propositions:

(22) If s and t are relatively prime, then dom(EulerFactorization(s)) misses dom(EulerFactorization(t)).

(23) Suppose s and t are relatively prime. Then $\mathrm{EmptyBag}\, \mathbb{P}+\cdot \mathrm{EulerFactorization}(s \cdot t) = (\mathrm{EmptyBag}\, \mathbb{P}+\cdot \mathrm{EulerFactorization}(s)) + (\mathrm{EmptyBag}\, \mathbb{P}+\cdot \mathrm{EulerFactorization}(t))$.

PROOF: Set $n = s \cdot t$. Set $N = \mathrm{EulerFactorization}(n)$. Set $S = \mathrm{EulerFactorization}(s)$. Set $T = \mathrm{EulerFactorization}(t)$. For every object x such that $x \in \mathbb{P}$ holds $(B{+}{\cdot}N)(x) = (B{+}{\cdot}S)(x) + (B{+}{\cdot}T)(x)$ by [7, (25), (58)], (22). □

(24) Let us consider a non zero natural number n.
Then $\mathrm{Euler}\, n = \prod(\mathrm{EmptyBag}\, \mathbb{P}{+}{\cdot}\, \mathrm{EulerFactorization}(n))$.
PROOF: Set $N = \mathrm{EulerFactorization}(n)$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every non zero natural number n such that $\mathrm{support}(B{+}{\cdot}\, \mathrm{EulerFactorization}(n)) \subseteq \mathrm{Seg}\, \$_1$ holds $\prod(B{+}{\cdot}\, \mathrm{EulerFactorization}(n)) = \mathrm{Euler}\, n$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number k, $\mathcal{P}[k]$. Set $G = B{+}{\cdot}N$. $\mathrm{support}\, G = \mathrm{support}\, N$. □

Let n be a non zero natural number. The functor $\mathrm{EulerFactorization}_1(n)$ yielding a function is defined by

(Def. 2) $\mathrm{dom}\, it = \mathrm{support}\, \mathrm{PPF}(n)$ and for every natural number p such that $p \in \mathrm{dom}\, it$ there exists a non zero natural number c such that $c = p\text{-}\mathrm{count}(n)$ and $it(p) = p^{c-1}$.

Let us observe that $\mathrm{dom}(\mathrm{EulerFactorization}_1(n))$ is finite and $\mathrm{EulerFactorization}_1(n)$ is $\mathbb{P}$-defined. Now we state the proposition:

(25) Let us consider a non zero natural number n, and an object p. Suppose $p \in \mathrm{dom}(\mathrm{EulerFactorization}_1(n))$. Then p is a prime number.

Let n be a non zero natural number. Note that $\mathrm{EulerFactorization}_1(n)$ is natural-valued and $\mathrm{EulerFactorization}_1(n)$ is finite-support. Now we state the proposition:

(26) Let us consider a non zero natural number n. Then $\mathrm{support}\, \mathrm{EulerFactorization}_1(n) = \mathrm{dom}(\mathrm{EulerFactorization}_1(n))$. The theorem is a consequence of (25).

Let n be a non zero natural number. The functor $\mathrm{EulerFactorization}_2(n)$ yielding a function is defined by

(Def. 3) $\mathrm{dom}\, it = \mathrm{support}\, \mathrm{PPF}(n)$ and for every natural number p such that $p \in \mathrm{dom}\, it$ holds $it(p) = p - 1$.

One can verify that $\mathrm{dom}(\mathrm{EulerFactorization}_2(n))$ is finite and $\mathrm{EulerFactorization}_2(n)$ is $\mathbb{P}$-defined. Now we state the proposition:

(27) Let us consider a non zero natural number n, and an object p. Suppose $p \in \mathrm{dom}(\mathrm{EulerFactorization}_2(n))$. Then p is a prime number.

Let n be a non zero natural number. Let us note that $\mathrm{EulerFactorization}_2(n)$ is natural-valued and $\mathrm{EulerFactorization}_2(n)$ is finite-support.

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

(28) $\operatorname{support}\operatorname{EulerFactorization}_2(n) = \operatorname{dom}(\operatorname{EulerFactorization}_2(n))$. The theorem is a consequence of (27).

(29) $\operatorname{EmptyBag}\mathbb{P}{+\cdot}\operatorname{EulerFactorization}(n) = (\operatorname{EmptyBag}\mathbb{P}{+\cdot}\operatorname{EulerFactorization}_1(n)) \cdot (\operatorname{EmptyBag}\mathbb{P}{+\cdot}\operatorname{EulerFactorization}_2(n))$.
PROOF: Set $N = \operatorname{EulerFactorization}(n)$. Set $S = \operatorname{EulerFactorization}_1(n)$. Set $T = \operatorname{EulerFactorization}_2(n)$. For every object x such that $x \in \mathbb{P}$ holds $(B{+\cdot}N)(x) = (B{+\cdot}S)(x) \cdot (B{+\cdot}T)(x)$. □

(30) Let us consider integer-valued finite sequences f_1, f_2. Suppose $\operatorname{len} f_1 = \operatorname{len} f_2$ and for every n such that $1 \leqslant n \leqslant \operatorname{len} f_1$ holds $f_1(n) \mid f_2(n)$. Then $\prod f_1 \mid \prod f_2$.

(31) Let us consider a non zero natural number n.
Then $\prod(\operatorname{EmptyBag}\mathbb{P}{+\cdot}\operatorname{EulerFactorization}_1(n)) \mid n$.
PROOF: Set $b_0 = \operatorname{PPF}(n)$. Set $F_1 = \operatorname{EulerFactorization}_1(n)$. Set $b_1 = B{+\cdot}F_1$. Consider f_0 being a finite sequence of elements of $\mathbb{C}$ such that $\prod b_0 = \prod f_0$ and $f_0 = b_0 \cdot (\operatorname{CFS}(\operatorname{support} b_0))$. Consider f_1 being a finite sequence of elements of $\mathbb{C}$ such that $\prod b_1 = \prod f_1$ and $f_1 = b_1 \cdot (\operatorname{CFS}(\operatorname{support} b_1))$. $\operatorname{support} b_1 = \operatorname{support} F_1$. $\operatorname{support} F_1 = \operatorname{dom} F_1$. $\operatorname{dom} f_0 = \operatorname{dom}(\operatorname{CFS}(\operatorname{support} b_0))$. $\operatorname{dom} f_1 = \operatorname{dom}(\operatorname{CFS}(\operatorname{support} b_1))$. For every natural number x such that $1 \leqslant x \leqslant \operatorname{len} f_1$ holds $f_1(x) \mid f_0(x)$. $\prod f_1 \mid \prod f_0$. □

Let f be a real-valued function and r be a real number. We say that $f \leqslant r$ if and only if

(Def. 4) for every object x such that $x \in \operatorname{dom} f$ holds $f(x) \leqslant r$.

Now we state the propositions:

(32) Let us consider a real-valued function f, and real numbers r_1, r_2. If $f \leqslant r_1 \leqslant r_2$, then $f \leqslant r_2$.

(33) Let us consider real-valued functions f, g. If $\operatorname{rng} g \subseteq \operatorname{rng} f$ and $f \leqslant n$, then $g \leqslant n$.

Let us consider extended real-valued finite sequences f, g. Now we state the propositions:

(34) If $f \frown g$ is increasing, then f is increasing and g is increasing.

(35) If $f \frown g$ is positive yielding, then f is positive yielding and g is positive yielding.

(36) Let us consider a natural-valued finite sequence f. If $f \leqslant n$ and f is increasing and positive yielding, then $\prod f \mid n!$. The theorem is a consequence of (3), (34), (35), and (6).

Let f be a natural-valued finite sequence. Note that $\operatorname{sort}_{\mathrm{a}} f$ is natural-valued and $\operatorname{sort}_{\mathrm{d}} f$ is natural-valued. Let f be an integer-valued finite sequence. One

can check that $\operatorname{sort}_{\mathrm{a}} f$ is integer-valued and $\operatorname{sort}_{\mathrm{d}} f$ is integer-valued. Let f be a rational-valued finite sequence. One can verify that $\operatorname{sort}_{\mathrm{a}} f$ is rational-valued and $\operatorname{sort}_{\mathrm{d}} f$ is rational-valued. Now we state the proposition:

(37) Let us consider binary relations P, R. Suppose $\operatorname{rng} R \subseteq \operatorname{rng} P$ and P is positive yielding. Then R is positive yielding.

Let f be a positive yielding, real-valued finite sequence. Let us observe that $\operatorname{sort}_{\mathrm{a}} f$ is positive yielding and every function which is $\mathbb{P}$-defined is also $\mathbb{N}$-defined. Now we state the propositions:

(38) Let us consider a real-valued, finite-support function f. Suppose $f \leqslant n$. Let us consider a real-valued finite sequence F. Suppose $F = (\operatorname{EmptyBag} \mathbb{P}_{+\cdot} f) \cdot (\operatorname{CFS}(\operatorname{support}(\operatorname{EmptyBag} \mathbb{P}_{+\cdot} f)))$. Then $F \leqslant n$.

(39) Let us consider a natural-valued, finite-support function f, and a real-valued finite sequence F.
Suppose $F = (\operatorname{EmptyBag} \mathbb{P}_{+\cdot} f) \cdot (\operatorname{CFS}(\operatorname{support}(\operatorname{EmptyBag} \mathbb{P}_{+\cdot} f)))$. Then F is positive yielding. The theorem is a consequence of (11).

Let us consider a natural-valued, finite-support, $\mathbb{P}$-defined function f and a real-valued finite sequence F. Now we state the propositions:

(40) Suppose f is increasing. Then suppose $F = (\operatorname{EmptyBag} \mathbb{P}_{+\cdot} f) \cdot (\operatorname{CFS}(\operatorname{support}(\operatorname{EmptyBag} \mathbb{P}_{+\cdot} f)))$. Then $\operatorname{sort}_{\mathrm{a}} F$ is one-to-one. The theorem is a consequence of (10) and (11).

(41) Suppose f is increasing. Then suppose $F = (\operatorname{EmptyBag} \mathbb{P}_{+\cdot} f) \cdot (\operatorname{CFS}(\operatorname{support}(\operatorname{EmptyBag} \mathbb{P}_{+\cdot} f)))$. Then $\operatorname{sort}_{\mathrm{a}} F$ is increasing. The theorem is a consequence of (11) and (10).

(42) Let us consider a natural-valued, finite-support, $\mathbb{P}$-defined function f. Suppose $f \leqslant n$ and f is increasing. Then $\prod(\operatorname{EmptyBag} \mathbb{P}_{+\cdot} f) \mid n!$. The theorem is a consequence of (38), (39), (41), (33), and (36).

(43) Let us consider a non zero natural number n. Then $\operatorname{EulerFactorization}_2(n) \leqslant n - 1$. The theorem is a consequence of (27).

Let n be a non zero natural number. Let us note that $\operatorname{EulerFactorization}_2(n)$ is increasing and $\operatorname{EulerFactorization}_2(n)$ is positive yielding.

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

(44) $\prod(\operatorname{EmptyBag} \mathbb{P}_{+\cdot} \operatorname{EulerFactorization}_2(n)) \mid (n-1)!$.

(45) $\operatorname{Euler} n \mid n!$. The theorem is a consequence of (24), (31), (43), (42), (10), (26), (28), (29), and (14).

(46) Let us consider an odd natural number n. Then $n \mid 2^{n!} - 1$. The theorem is a consequence of (45).

3. PROBLEM 86

Now we state the proposition:

(47) Suppose p_1, p_2, p_3 are mutually different. Then

(i) $p_1 \geqslant 2$ and $p_2 \geqslant 3$ and $p_3 \geqslant 5$, or

(ii) $p_1 \geqslant 2$ and $p_2 \geqslant 5$ and $p_3 \geqslant 3$, or

(iii) $p_1 \geqslant 3$ and $p_2 \geqslant 2$ and $p_3 \geqslant 5$, or

(iv) $p_1 \geqslant 3$ and $p_2 \geqslant 5$ and $p_3 \geqslant 2$, or

(v) $p_1 \geqslant 5$ and $p_2 \geqslant 2$ and $p_3 \geqslant 3$, or

(vi) $p_1 \geqslant 5$ and $p_2 \geqslant 3$ and $p_3 \geqslant 2$.

Let n be a natural number. We say that n satisfies Sierpiński Problem 86 if and only if

(Def. 5) there exist prime numbers p_1, p_2, p_3 such that p_1, p_2, p_3 are mutually different and $n^2 - 1 = p_1 \cdot p_2 \cdot p_3$.

Now we state the propositions:

(48) If n satisfies Sierpiński Problem 86, then $n \geqslant 6$. The theorem is a consequence of (47).

(49) Let us consider prime numbers a, b, c. If $n^2 - 1 = a \cdot b \cdot c$, then $n - 1$ is prime or $n + 1$ is prime.

(50) Suppose n satisfies Sierpiński Problem 86. Then

(i) $n - 1$ is prime and there exist prime numbers x, y such that $x \neq y$ and $n + 1 = x \cdot y$, or

(ii) $n + 1$ is prime and there exist prime numbers x, y such that $x \neq y$ and $n - 1 = x \cdot y$.

The theorem is a consequence of (49).

(51) If n satisfies Sierpiński Problem 86, then n is even. The theorem is a consequence of (50) and (48).

(52) $14^2 - 1 = 3 \cdot 5 \cdot 13$.

(53) $16^2 - 1 = 3 \cdot 5 \cdot 17$.

(54) $20^2 - 1 = 3 \cdot 7 \cdot 19$.

(55) $22^2 - 1 = 3 \cdot 7 \cdot 23$.

(56) $32^2 - 1 = 3 \cdot 11 \cdot 31$.

(57) 14 satisfies Sierpiński Problem 86. The theorem is a consequence of (52).

(58) 16 satisfies Sierpiński Problem 86. The theorem is a consequence of (53).

(59) 20 satisfies Sierpiński Problem 86. The theorem is a consequence of (54).

(60) 22 satisfies Sierpiński Problem 86. The theorem is a consequence of (55).

(61) 32 satisfies Sierpiński Problem 86. The theorem is a consequence of (56).

(62) If n satisfies Sierpiński Problem 86 and $n \leqslant 32$, then $n \in \{14, 16, 20, 22, 32\}$. The theorem is a consequence of (48).

4. Problem 184

Now we state the propositions:

(63) $3^{2 \cdot k} \equiv 1 \pmod 8$.

(64) $8 \nmid 3^n + 1$. The theorem is a consequence of (63).

(65) If $n \neq 0$ and $2^m - 3^n = 1$, then $m = 2$ and $n = 1$. The theorem is a consequence of (64).

5. Problem 185

Now we state the propositions:

(66) $3^{2 \cdot k} \equiv 1 \pmod 4$.

(67) If $2^n \bmod 4 = 2$, then $n = 1$.

(68) If $2^m - 2^n = 2$, then $m = 2$ and $n = 1$.

(69) If n is odd and $3^n - 2^m = 1$, then $n = m = 1$. The theorem is a consequence of (66) and (67).

(70) If n is even and $3^n - 2^m = 1$, then $n = 2$ and $m = 3$. The theorem is a consequence of (68).

(71) If $3^n - 2^m = 1$, then $n = m = 1$ or $n = 2$ and $m = 3$. The theorem is a consequence of (69) and (70).

6. Problem 88

Let us consider n. We say that n has unique prime divisor if and only if

(Def. 6) there exists a prime number p such that $p \mid n$ and for every prime number r such that $r \neq p$ holds $r \nmid n$.

Assume n has unique prime divisor. The only divisor of n yielding a prime number is defined by

(Def. 7) $it \mid n$ and for every prime number r such that $r \neq it$ holds $r \nmid n$.

Now we state the proposition:

(72) If n has unique prime divisor and $p \mid n$, then the only divisor of $n = p$.

Let us observe that every natural number which is prime has unique prime divisor. Now we state the proposition:

(73) The only divisor of $p = p$.

One can check that every natural number which is zero does not have unique prime divisor. Now we state the proposition:

(74) 1 does not have unique prime divisor.

Let p be a prime number. Let us observe that p^0 does not have unique prime divisor. Let k be a non zero natural number. One can verify that p^k has unique prime divisor. Now we state the propositions:

(75) If $p_1 \neq p_2$, then $p_1 \cdot p_2$ does not have unique prime divisor.

(76) If n has unique prime divisor, then there exists a non zero natural number k such that $n = (\text{the only divisor of } n)^k$.

(77) If $n > 7$, then there exists a natural number m and there exist prime numbers p, q such that $p \neq q$ and ($m = n$ or $m = n + 1$ or $m = n + 2$) and $p \mid m$ and $q \mid m$.

PROOF: Consider 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 $n = 6 \cdot k + 5$. n has unique prime divisor. $n + 1$ has unique prime divisor. $n + 2$ has unique prime divisor. □

7. PROBLEM 105

Let us consider n. We say that n has more than two different prime divisors if and only if

(Def. 8) there exist prime numbers q_1, q_2, q_3 such that q_1, q_2, q_3 are mutually different and $q_1 \mid n$ and $q_2 \mid n$ and $q_3 \mid n$.

Let n be a non zero natural number. We say that n satisfies Sierpiński Problem 105 if and only if

(Def. 9) $n - 1$ has more than two different prime divisors and $n + 1$ has more than two different prime divisors.

Now we state the proposition:

(78) If n has unique prime divisor, then n has no more than two different prime divisors.

Note that every natural number which is zero has more than two different prime divisors. Now we state the proposition:

(79) If $n > 0$ and n has more than two different prime divisors, then $n \geqslant 30$.

The theorem is a consequence of (47).

Let us note that every natural number which is prime does not have more than two different prime divisors. Let us consider p_1 and p_2. Observe that $p_1 \cdot p_2$ does not have more than two different prime divisors.

Let us consider p and n. Let us note that p^n does not have more than two different prime divisors. Let us consider p, q, m and n. Note that $p^m \cdot q^n$ does not have more than two different prime divisors. Now we state the propositions:

(80) 131 satisfies Sierpiński Problem 105.

(81) There exists no prime number p such that $p \leqslant 130$ and p satisfies Sierpiński Problem 105. The theorem is a consequence of (79).

8. Problem 111

Now we state the propositions:

(82) $1 + 3 + 3^2 + 3^3 + 3^4 = 11^2$.

(83) $m \mid p^4$ if and only if $m \in \{1, p, p^2, p^3, p^4\}$.

(84) $1 + p + p^2 + p^3 + p^4$ is a square if and only if $p = 3$.

(85) The set of positive divisors of $p^4 = \{1, p, p^2, p^3, p^4\}$. The theorem is a consequence of (83).

(86) $\{p$, where p is a prime number : $1 + p + p^2 + p^3 + p^4$ is a square$\} = \{3\}$. The theorem is a consequence of (84).

9. Problem 137

Let D be a non empty set. Let us observe that every sequence of D is total. Let f be a $(\mathbb{C} \times D)$-valued many sorted set indexed by $\mathbb{N}$ and n be a natural number. Note that $(f(n))_{\mathbf{1}}$ is complex. Let f be a $(D \times \mathbb{C})$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{2}}$ is complex.

Let f be an $(\mathbb{R} \times D)$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{1}}$ is real. Let f be a $(D \times \mathbb{R})$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{2}}$ is real. Let f be a $(\mathbb{Q} \times D)$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{1}}$ is rational. Let f be a $(D \times \mathbb{Q})$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{2}}$ is rational.

Let f be a $(\mathbb{Z} \times D)$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{1}}$ is integer. Let f be a $(D \times \mathbb{Z})$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{2}}$ is integer. Let f be an $(\mathbb{N} \times D)$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{1}}$ is natural. Let f be a $(D \times \mathbb{N})$-valued many sorted set indexed by $\mathbb{N}$. Note that $(f(n))_{\mathbf{2}}$ is natural.

Let a, b, x_1, x_2, x_3, y_1, y_2, y_3 be complex numbers. The functor recSeqCart(a, $b, x_1, x_2, x_3, y_1, y_2, y_3$) yielding a $(\mathbb{C} \times \mathbb{C})$-valued many sorted set indexed by $\mathbb{N}$ is defined by

(Def. 10) $it(0) = \langle a, b \rangle$ and for every natural number n, $it(n+1) = \langle x_1 \cdot ((it(n))_{\mathbf{1}}) + x_2 \cdot ((it(n))_{\mathbf{2}}) + x_3,\ y_1 \cdot ((it(n))_{\mathbf{1}}) + y_2 \cdot ((it(n))_{\mathbf{2}}) + y_3 \rangle$.

Let a, b, x_1, x_2, x_3, y_1, y_2, y_3 be real numbers. Let us observe that recSeqCart $(a, b, x_1, x_2, x_3, y_1, y_2, y_3)$ is $(\mathbb{R} \times \mathbb{R})$-valued. Let a, b, x_1, x_2, x_3, y_1, y_2, y_3 be rational numbers. Let us observe that recSeqCart$(a, b, x_1, x_2, x_3, y_1, y_2, y_3)$ is $(\mathbb{Q} \times \mathbb{Q})$-valued.

Let a, b, x_1, x_2, x_3, y_1, y_2, y_3 be integers. Let us observe that recSeqCart$(a, b, x_1, x_2, x_3, y_1, y_2, y_3)$ is $(\mathbb{Z} \times \mathbb{Z})$-valued. Let a, b, x_1, x_2, x_3, y_1, y_2, y_3 be natural numbers. Let us observe that recSeqCart$(a, b, x_1, x_2, x_3, y_1, y_2, y_3)$ is $(\mathbb{N} \times \mathbb{N})$-valued. Let us consider real numbers a, b, a_1, a_2, a_3, b_1, b_2, b_3 and a natural number n. Now we state the propositions:

(87) Suppose $a > 0$ and $b > 0$ and $a_3 \geqslant 0$ and $b_3 \geqslant 0$ and ($a_1 > 0$ and $a_2 \geqslant 0$ or $a_1 \geqslant 0$ and $a_2 > 0$) and ($b_1 > 0$ and $b_2 \geqslant 0$ or $b_1 \geqslant 0$ and $b_2 > 0$). Then

(i) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{1}} > 0$, and

(ii) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{2}} > 0$.

PROOF: Set $f = \text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3)$. Define $\mathcal{P}$[natural number] $\equiv (f(\$_1))_{\mathbf{1}} > 0$ and $(f(\$_1))_{\mathbf{2}} > 0$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(88) Suppose $a \geqslant 0$ and $b \geqslant 0$ and $a_1 \geqslant 0$ and $a_2 \geqslant 0$ and $a_3 \geqslant 0$ and $b_1 \geqslant 0$ and $b_2 \geqslant 0$ and $b_3 \geqslant 0$. Then

(i) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{1}} \geqslant 0$, and

(ii) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{2}} \geqslant 0$.

PROOF: Set $f = \text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3)$. Define $\mathcal{P}$[natural number] $\equiv (f(\$_1))_{\mathbf{1}} \geqslant 0$ and $(f(\$_1))_{\mathbf{2}} \geqslant 0$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(89) Let us consider real numbers a, b, a_1, a_2, a_3, b_1, b_2, b_3. Suppose $a > 0$ and $b > 0$ and $a_1 \geqslant 1$ and $a_2 > 0$ and $a_3 \geqslant 0$ and $b_1 > 0$ and $b_2 \geqslant 1$ and $b_3 \geqslant 0$. Let us consider natural numbers m, n. Suppose $m > n$. Then

(i) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(m))_{\mathbf{1}} > ((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{1}}$, and

(ii) $((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(m))_{\mathbf{2}} > ((\text{recSeqCart}(a, b, a_1, a_2, a_3, b_1, b_2, b_3))(n))_{\mathbf{2}}$.

PROOF: Set f = recSeqCart$(a, b, a_1, a_2, a_3, b_1, b_2, b_3)$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 > n$, then $(f(\$_1))_{\mathbf{1}} > (f(n))_{\mathbf{1}}$ and $(f(\$_1))_{\mathbf{2}} > (f(n))_{\mathbf{2}}$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(90) Let us consider real numbers a, b, a_1, a_2, a_3, b_1, b_2, b_3. Suppose $a > 0$ and $b > 0$ and $a_1 \geqslant 1$ and $a_2 > 0$ and $a_3 \geqslant 0$ and $b_1 > 0$ and $b_2 \geqslant 1$ and $b_3 \geqslant 0$. Then recSeqCart$(a, b, a_1, a_2, a_3, b_1, b_2, b_3)$ is one-to-one. The theorem is a consequence of (89).

(91) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $3 \cdot x^{\mathbf{2}} - 7 \cdot y^{\mathbf{2}} + 1 = 0\}$ is infinite.

PROOF: Define $\mathcal{R}$(complex number, complex number) $= 3 \cdot \$_1^{\mathbf{2}} - 7 \cdot \$_2^{\mathbf{2}} + 1$. Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $\mathcal{R}(x, y) = 0\}$. Define $\mathcal{G}$(real number, real number) $= 55 \cdot \$_1 + 84 \cdot \$_2 + 0$. Define $\mathcal{H}$(real number, real number) $= 36 \cdot \$_1 + 55 \cdot \$_2 + 0$. Define $\mathcal{P}$[object, element of $\mathbb{N} \times \mathbb{N}$, element of $\mathbb{N} \times \mathbb{N}$] $\equiv \$_3 = \langle \mathcal{G}((\$_2)_{\mathbf{1}}, (\$_2)_{\mathbf{2}}), \mathcal{H}((\$_2)_{\mathbf{1}}, (\$_2)_{\mathbf{2}})\rangle$. Set f = recSeqCart$(3, 2, 55, 84, 0, 36, 55, 0)$. Define $\mathcal{N}$[natural number] $\equiv f(\$_1) \in A$. If $\mathcal{N}[a]$, then $\mathcal{N}[a+1]$. $\mathcal{N}[a]$. rng $f \subseteq A$. f is one-to-one. $\square$

10. PROBLEM 138

One can check that there exists a set which is infinite and natural-membered. Now we state the propositions:

(92) If $i \mid p$, then $i = 1$ or $i = -1$ or $i = p$ or $i = -p$.

(93) $\{\langle x, y\rangle$, where x, y are integers : $2 \cdot x^3 + x \cdot y - 7 = 0\} = \{\langle 1, 5\rangle, \langle 7, -97\rangle, \langle -1, -9\rangle, \langle -7, -99\rangle\}$.

PROOF: Set $A = \{\langle x, y\rangle$, where x, y are integers : $2 \cdot x^3 + x \cdot y - 7 = 0\}$. Set $B = \{\langle 1, 5\rangle, \langle 7, -97\rangle, \langle -1, -9\rangle, \langle -7, -99\rangle\}$. $A \subseteq B$ by [10, (2)], (92). $\square$

(94) Let us consider a complex number r. If $r \neq 0$, then $2 \cdot (\frac{7}{r})^3 + \frac{7}{r} \cdot (r - \frac{98}{r^{\mathbf{2}}}) - 7 = 0$.

(95) If $n^3 \leqslant 98$, then $n \leqslant 4$.

(96) $\{\langle x, y\rangle$, where x, y are positive rational numbers : $2 \cdot x^3 + x \cdot y - 7 = 0\}$ is infinite.

PROOF: Define $\mathcal{R}$(rational number, rational number) $= 2 \cdot \$_1{}^3 + \$_1 \cdot \$_2 - 7$. Set $A = \{\langle x, y\rangle$, where x, y are positive rational numbers : $\mathcal{R}(x, y) = 0\}$. Define $\mathcal{G}$(natural number) $= \frac{7}{\$_1}$. Define $\mathcal{H}$(natural number) $= \$_1 - \frac{98}{\$_1^{\mathbf{2}}}$. Define $\mathcal{F}$(natural number) $= \langle \mathcal{G}(\$_1), \mathcal{H}(\$_1)\rangle$. Set $D = \mathbb{N} \setminus \{0, 1, 2, 3, 4\}$. Consider f being a many sorted set indexed by D such that for every element d of D, $f(d) = \mathcal{F}(d)$. rng $f \subseteq A$. f is one-to-one. $\square$

11. PROBLEM 139

Now we state the proposition:

(97) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $(x-1)^{\mathbf{2}}+(x+1)^{\mathbf{2}}=y^{\mathbf{2}}+1\}$ is infinite.

PROOF: Define $\mathcal{R}$(natural number, natural number) $= (\$_1-1)^{\mathbf{2}}+(\$_1+1)^{\mathbf{2}}-(\$_2^{\mathbf{2}}+1)$. Set $A=\{\langle x, y\rangle$, where x, y are positive natural numbers : $\mathcal{R}(x,y)=0\}$. Define $\mathcal{G}$(natural number, natural number) $= 3\cdot\$_1+2\cdot\$_2+0$. Define $\mathcal{H}$(natural number, natural number) $= 4\cdot\$_1+3\cdot\$_2+0$. Define $\mathcal{P}$[object, element of $\mathbb{N}\times\mathbb{N}$, element of $\mathbb{N}\times\mathbb{N}$] $\equiv \$_3 = \langle\mathcal{G}((\$_2)_{\mathbf{1}}, (\$_2)_{\mathbf{2}}), \mathcal{H}((\$_2)_{\mathbf{1}}, (\$_2)_{\mathbf{2}})\rangle$. Set $f=$ recSeqCart$(2,3,3,2,0,4,3,0)$. Define $\mathcal{N}$[natural number] $\equiv f(\$_1)\in A$. If $\mathcal{N}[a]$, then $\mathcal{N}[a+1]$. $\mathcal{N}[a]$. rng $f\subseteq A$. f is one-to-one. Define $\mathcal{R}$[natural number, natural number] $\equiv (\$_1-1)^{\mathbf{2}}+(\$_1+1)^{\mathbf{2}}=\$_2^{\mathbf{2}}+1$. Set $B=\{\langle x, y\rangle$, where x, y are positive natural numbers : $\mathcal{R}[x,y]\}$. $A=B$. □

12. PROBLEM 140

Let a be a rational number and n be a natural number. Let us observe that a^n is rational. Let i be an integer. One can verify that a^i is rational. Now we state the propositions:

(98) If $n>1$, then $3^n-3^{1-n}-2>0$.

(99) If $n>1$, then $3^n+3^{1-n}-4>0$.

(100) Let us consider complex numbers x, y. Suppose $x=\frac{3^n-3^{1-n}-2}{4}$ and $y=\frac{3^n+3^{1-n}-4}{8}$. Then $x\cdot(x+1)=4\cdot y\cdot(y+1)$.

(101) If $m<n$, then $3^m-3^{1-m}<3^n-3^{1-n}$.

(102) There exist no positive natural numbers x, y such that $x\cdot(x+1)=4\cdot y\cdot(y+1)$.

(103) $\{\langle x, y\rangle$, where x, y are positive rational numbers : $x\cdot(x+1)=4\cdot y\cdot(y+1)\}$ is infinite.

PROOF: Define $\mathcal{R}$(complex number, complex number) $= \$_1\cdot(\$_1+1)-4\cdot\$_2\cdot(\$_2+1)$. Set $A=\{\langle x, y\rangle$, where x, y are positive rational numbers : $\mathcal{R}(x,y)=0\}$. Define $\mathcal{G}$(natural number) $=\frac{3^{\$_1}-3^{1-\$_1}-2}{4}$. Define $\mathcal{H}$(natural number) $=\frac{3^{\$_1}+3^{1-\$_1}-4}{8}$. Define $\mathcal{F}$(natural number) $=\langle\mathcal{G}(\$_1), \mathcal{H}(\$_1)\rangle$. Set $D=\mathbb{N}\setminus\{0,1\}$. Consider f being a many sorted set indexed by D such that for every element d of D, $f(d)=\mathcal{F}(d)$. rng $f\subseteq A$. f is one-to-one. Define $\mathcal{R}$[complex number, complex number] $\equiv \$_1\cdot(\$_1+1)=4\cdot\$_2\cdot(\$_2+1)$. Set $B=\{\langle x, y\rangle$, where x, y are positive rational numbers : $\mathcal{R}[x,y]\}$. $A=B$. □

13. Problem 141

Now we state the propositions:

(104) If $m \neq 0$ and $p^m \mid a \cdot b$, then $p \mid a$ or $p \mid b$.

(105) If a and b are relatively prime and $p^n \mid a \cdot b$, then $p^n \mid a$ or $p^n \mid b$.

(106) If $n \neq 0$, then there exist no positive natural numbers x, y such that $x \cdot (x+1) = p^{2 \cdot n} \cdot y \cdot (y+1)$. The theorem is a consequence of (105).

14. Problem 142

Now we state the proposition:

(107) Let us consider natural numbers k, x, y. Suppose $x^{\mathbf{2}} - 2 \cdot y^{\mathbf{2}} = k$. Let us consider natural numbers t, u. If $t = x - 2 \cdot y$ and $u = x - y$, then $t^{\mathbf{2}} - 2 \cdot u^{\mathbf{2}} = -k$.

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] Adam Grabowski. Elementary number theory problems. Part VI. *Formalized Mathematics*, 30(**3**):235–244, 2022. doi:10.2478/forma-2022-0019.

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

[4] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[5] Artur Korniłowicz. Elementary number theory problems. Part IV. *Formalized Mathematics*, 30(**3**):223–228, 2022. doi:10.2478/forma-2022-0017.

[6] Artur Korniłowicz and Adam Naumowicz. Elementary number theory problems. Part V. *Formalized Mathematics*, 30(**3**):229–234, 2022. doi:10.2478/forma-2022-0018.

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

[8] Adam Naumowicz. Dataset description: Formalization of elementary number theory in Mizar. In Christoph Benzmüller and Bruce R. Miller, editors, *Intelligent Computer Mathematics – 13th International Conference, CICM 2020, Bertinoro, Italy, July 26–31, 2020, Proceedings*, volume 12236 of *Lecture Notes in Computer Science*, pages 303–308. Springer, 2020. doi:10.1007/978-3-030-53518-6_22.

[9] Adam Naumowicz. Extending numeric automation for number theory formalizations in Mizar. In Catherine Dubois and Manfred Kerber, editors, *Intelligent Computer Mathematics – 16th International Conference, CICM 2023, Cambridge, UK, September 5–8, 2023, Proceedings*, volume 14101 of *Lecture Notes in Computer Science*, pages 309–314. Springer, 2023. doi:10.1007/978-3-031-42753-4_23.

[10] Marco Riccardi. Solution of cubic and quartic equations. *Formalized Mathematics*, 17(**2**): 117–122, 2009. doi:10.2478/v10037-009-0012-z.

[11] Wacław Sierpiński. *Elementary Theory of Numbers*. PWN, Warsaw, 1964.

[12] Wacław Sierpiński. *250 Problems in Elementary Number Theory*. Elsevier, 1970.

Accepted June 30, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 101–120, 2023
DOI: 10.2478/forma-2023-0010
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Internal Direct Products and the Universal Property of Direct Product Groups

Alexander M. Nelson
Los Angeles, California
United States of America

Summary. This is a "quality of life" article concerning product groups, using the Mizar system [2], [4]. Like a Sonata, this article consists of three movements.

The first act, the slowest of the three, builds the infrastructure necessary for the rest of the article. We prove group homomorphisms map arbitrary finite products to arbitrary finite products, introduce a notion of "group yielding" families, as well as families of homomorphisms. We close the first act with defining the inclusion morphism of a subgroup into its parent group, and the projection morphism of a product group onto one of its factors.

The second act introduces the universal property of products and its consequences as found in, e.g., Kurosh [7]. Specifically, for the product of an arbitrary family of groups, we prove the center of a product group is the product of centers. More exciting, we prove for a product of a finite family groups, the commutator subgroup of the product is the product of commutator subgroups, but this is because in general: the direct sum of commutator subgroups is the subgroup of the commutator subgroup of the product group, and the commutator subgroup of the product is a subgroup of the product of derived subgroups. We conclude this act by proving a few theorems concerning the image and kernel of morphisms between product groups, as found in Hungerford [5], as well as quotients of product groups.

The third act introduces the notion of an internal direct product. Isaacs [6] points out (paraphrasing with Mizar terminology) that the internal direct product is a predicate but the external direct product is a [Mizar] functor. To our delight, we find the bulk of the "recognition theorem" (as stated by Dummit and Foote [3], Aschbacher [1], and Robinson [11]) are already formalized in the heroic work of Nakasho, Okazaki, Yamazaki, and Shidama [9], [8]. We generalize the notion of an internal product to a set of subgroups, proving it is equivalent to the internal product of a family of subgroups [10].

MSC: 20E22 68V20

Keywords: direct product of groups

MML identifier: GROUP_23, version: 8.1.12 5.75.1447

1. Preliminaries

Now we state the propositions:

(1) Let us consider sets X, Y, Z, W. Suppose $Z \neq \emptyset$ and $W \neq \emptyset$. Let us consider a function f from $X \times Y$ into Z, and a function g from $X \times Y$ into W. If for every element a of X for every element b of Y, $f(a, b) = g(a, b)$, then $f = g$.

(2) Let us consider a finite set A. Then $\mathrm{CFS}(A)$ is a many sorted set indexed by $\mathrm{Seg}\,\overline{\overline{A}}$.

(3) Let us consider non empty sets X, Y, and a function f from X into Y. Suppose f is onto. Then there exists a function g from Y into X such that $f \cdot g = \mathrm{id}_Y$.

Proof: Define $\mathcal{P}[\mathrm{object}, \mathrm{object}] \equiv \$_1 = f(\$_2)$. For every object y such that $y \in Y$ there exists an object x such that $x \in X$ and $\mathcal{P}[y, x]$. Consider g being a function from Y into X such that for every object y such that $y \in Y$ holds $\mathcal{P}[y, g(y)]$. For every element y of Y, $(f \cdot g)(y) = y$. □

Let I be a non empty set, A, B be many sorted sets indexed by I, f be a many sorted function from A into B, and i be an element of I. Let us observe that the functor $f(i)$ yields a function from $A(i)$ into $B(i)$. Let F_1, F_2 be 1-sorted yielding many sorted sets indexed by I.

A many sorted function from F_1 into F_2 is a many sorted function from the support of F_1 into the support of F_2. Let φ be a many sorted function from F_1 into F_2 and i be an element of I. Note that the functor $\varphi(i)$ yields a function from $F_1(i)$ into $F_2(i)$. Now we state the proposition:

(4) Let us consider a non empty set I, many sorted sets A, B indexed by I, and a many sorted set f indexed by I. Then f is a many sorted function from A into B if and only if for every element i of I, $f(i)$ is a function from $A(i)$ into $B(i)$.

Let I, X be sets. Observe that there exists a many sorted set indexed by I which is (2^X)-valued.

Let M be a (2^X)-valued many sorted set indexed by I. One can check that the functor $\bigcup M$ yields a subset of X. Let I be a set, J be a subset of I, and F be a many sorted set indexed by I. One can check that $F{\restriction}J$ is J-defined and total.

Let F be a 1-sorted yielding many sorted set indexed by I. Observe that $F\restriction J$ is 1-sorted yielding, J-defined, and total. Now we state the proposition:

(5) Let us consider a non empty set I, a many sorted set M indexed by I, and an object y. Then $y \in \operatorname{rng} M$ if and only if there exists an element i of I such that $y = M(i)$.

2. Sequences of Group Elements under Homomorphisms

Now we state the propositions:

(6) Let us consider groups G_1, G_2, a homomorphism φ from G_1 to G_2, a finite sequence F_1 of elements of the carrier of G_1, and a finite sequence F_2 of elements of the carrier of G_2. If $F_2 = \varphi \cdot F_1$, then $\prod F_2 = \varphi(\prod F_1)$.

PROOF: Define $\mathcal{P}[\text{finite sequence of elements of the carrier of } G_1] \equiv \varphi(\prod \$_1) = \prod \varphi \cdot \$_1$. $\mathcal{P}[\varepsilon_\alpha]$, where α is the carrier of G_1. For every finite sequence p_0 of elements of the carrier of G_1 and for every element x of the carrier of G_1 such that $\mathcal{P}[p_0]$ holds $\mathcal{P}[p_0 \frown \langle x \rangle]$. For every finite sequence p_0 of elements of the carrier of G_1, $\mathcal{P}[p_0]$. □

(7) Let us consider groups G_1, G_2, a homomorphism φ from G_1 to G_2, and a finite sequence F_1 of elements of the carrier of G_1. Then there exists a finite sequence F_2 of elements of the carrier of G_2 such that

(i) $\operatorname{len} F_1 = \operatorname{len} F_2$, and

(ii) $F_2 = \varphi \cdot F_1$, and

(iii) $\prod F_2 = \varphi(\prod F_1)$.

PROOF: Set $n_1 = \operatorname{len} F_1$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a natural number k such that $k = \$_1$ and $\$_2 = \varphi(F_1(k))$. For every natural number k such that $k \in \operatorname{Seg} n_1$ there exists an object x such that $\mathcal{P}[k, x]$. Consider p being a finite sequence such that $\operatorname{dom} p = \operatorname{Seg} n_1$ and for every natural number k such that $k \in \operatorname{Seg} n_1$ holds $\mathcal{P}[k, p(k)]$. $p = \varphi \cdot F_1$. □

(8) Let us consider groups G_1, G_2, a homomorphism φ from G_1 to G_2, a finite sequence F_1 of elements of the carrier of G_1, and a finite sequence k_1 of elements of $\mathbb{Z}$. Then there exists a finite sequence F_2 of elements of the carrier of G_2 such that

(i) $\operatorname{len} F_1 = \operatorname{len} F_2$, and

(ii) $F_2 = \varphi \cdot F_1$, and

(iii) $\prod {F_2}^{k_1} = \varphi(\prod {F_1}^{k_1})$.

PROOF: Consider F_2 being a finite sequence of elements of the carrier of G_2 such that $\operatorname{len} F_1 = \operatorname{len} F_2$ and $F_2 = \varphi \cdot F_1$ and $\prod F_2 = \varphi(\prod F_1)$. For every natural number k such that $k \in \operatorname{dom} {F_2}^{k_1}$ holds $(\varphi \cdot {F_1}^{k_1})(k) = {F_2}^{k_1}(k)$. □

3. Preliminary Work about Group-families and Group-yielding Many Sorted Sets

Let I_2 be a binary relation. We say that I_2 is group yielding if and only if

(Def. 1) for every object G such that $G \in \operatorname{rng} I_2$ holds G is a group.

One can check that every function which is group yielding is also 1-sorted yielding and every function which is group yielding is also multiplicative magma yielding. Now we state the proposition:

(9) Let us consider a set I. Then every associative, group-like multiplicative magma family of I is group yielding.

Let I be a set. One can check that there exists a many sorted set indexed by I which is group yielding and every multiplicative magma family of I which is associative and group-like is also group yielding and there exists a function which is group yielding. Now we state the proposition:

(10) Let us consider a non empty set I, a group yielding many sorted set F indexed by I, and an element i of I. Then $F(i)$ is a group.

Let I be a non empty set, i be an element of I, and F be a group yielding many sorted set indexed by I. Note that $F(i)$ is group-like, associative, unital, and non empty as a multiplicative magma. Now we state the proposition:

(11) Let us consider a set I, and a many sorted set F indexed by I. Then F is group yielding if and only if for every object i such that $i \in I$ holds $F(i)$ is a group.

Let I be a set. Let us observe that every multiplicative magma family of I which is group yielding is also group-like and associative and every group-like, associative multiplicative magma family of I is group yielding and every group yielding many sorted set indexed by I is group-like, associative, and multiplicative magma yielding.

From now on I denotes a non empty set, i denotes an element of I, F denotes a group family of I, and G denotes a group. Now we state the propositions:

(12) $\emptyset \longmapsto G$ is a group family of $\emptyset$.

(13) Let us consider a natural number n. Then $\operatorname{Seg} n \longmapsto G$ is a group family of $\operatorname{Seg} n$. The theorem is a consequence of (12).

Let G be a group and n be a natural number. One can verify that $\operatorname{Seg} n \longmapsto G$ is group yielding. Now we state the proposition:

(14) (The support of F)(i) = the carrier of $F(i)$.

The scheme *GrFamSch* deals with a non empty set I_1 and a unary functor $\mathcal{A}$ yielding a group and states that

(Sch. 1) There exists a group family $\mathcal{F}$ of I_1 such that for every element i of I_1, $\mathcal{F}(i) = \mathcal{A}(i)$.

4. Subgroup-family of a Family of Groups

Let I be a set and F, I_2 be group families of I. We say that I_2 is F-subgroup yielding if and only if

(Def. 2) for every element i of I and for every group G such that $G = F(i)$ holds $I_2(i)$ is a subgroup of G.

Now we state the propositions:

(15) Let us consider a group family S of I. Then S is F-subgroup yielding if and only if for every element i of I, $S(i)$ is a subgroup of $F(i)$.

(16) Let us consider a set I. Then every group family of I is F-subgroup yielding.

Let I be a set and F be a group family of I. Let us observe that there exists a group family of I which is F-subgroup yielding.

A subgroup family of F is an F-subgroup yielding group family of I. Let I be a non empty set, S be a subgroup family of F, and i be an element of I. Let us observe that the functor $S(i)$ yields a subgroup of $F(i)$. From now on S denotes a subgroup family of F. Now we state the proposition:

(17) Let us consider a group family S of I. Then S is a subgroup family of F if and only if for every element i of I, $S(i)$ is a subgroup of $F(i)$.

The scheme *SubFamSch* deals with a non empty set I_1 and a group family $\mathcal{F}$ of I_1 and a unary functor $\mathcal{S}$ yielding a group and states that

(Sch. 2) There exists a subgroup family S of $\mathcal{F}$ such that for every element i of I_1, $S(i) = \mathcal{S}(\mathcal{F}(i))$

provided

- for every group G, $\mathcal{S}(G)$ is a subgroup of G.

Let I be a non empty set and I_2 be a group family of I. We say that I_2 is componentwise strict if and only if

(Def. 3) for every element i of I, $I_2(i)$ is strict.

One can check that there exists a group family of I which is componentwise strict. Now we state the proposition:

(18) Let us consider a non empty set I, a group family F of I, and a subgroup family I_2 of F. Then I_2 is componentwise strict if and only if for every element i of I, $I_2(i)$ is a strict subgroup of $F(i)$.

Let I be a non empty set and F be a group family of I. One can verify that there exists a subgroup family of F which is componentwise strict. Let S be a componentwise strict subgroup family of F and i be an element of I. Note that $S(i)$ is strict as a subgroup of $F(i)$.

The scheme *StrSubFamSch* deals with a non empty set I_1 and a group family $\mathcal{F}$ of I_1 and a unary functor $\mathcal{S}$ yielding a group and states that

(Sch. 3) There exists a componentwise strict subgroup family S of $\mathcal{F}$ such that for every element i of I_1, $S(i) = \mathcal{S}(\mathcal{F}(i))$

provided

- for every group G, $\mathcal{S}(G)$ is a strict subgroup of G.

Now we state the proposition:

(19) Let us consider subgroup families A, B of F. If for every element i of I, $A(i) = B(i)$, then $A = B$.

Let I be a non empty set and F be a group family of I. The functor $\{\mathbf{1}\}_F$ yielding a componentwise strict subgroup family of F is defined by

(Def. 4) for every element i of I, $it(i) = \{\mathbf{1}\}_{F(i)}$.

The functor Ω_F yielding a componentwise strict subgroup family of F is defined by

(Def. 5) for every element i of I, $it(i) = \Omega_{F(i)}$.

Let I_2 be a subgroup family of F. We say that I_2 is normal if and only if

(Def. 6) for every element i of I, $I_2(i)$ is a normal subgroup of $F(i)$.

Let us note that there exists a subgroup family of F which is componentwise strict and normal. Let S be a normal subgroup family of F and i be an element of I. One can check that $S(i)$ is normal as a subgroup of $F(i)$.

Let S be a componentwise strict subgroup family of F. Note that $S(i)$ is strict as a subgroup of $F(i)$ and $\{\mathbf{1}\}_F$ is normal and Ω_F is normal. Let N be a normal subgroup family of F. The functor ${}^{F}/_{N}$ yielding a group family of I is defined by

(Def. 7) for every element i of I, $it(i) = {}^{F(i)}/_{N(i)}$.

Observe that ${}^{F}/_{N}$ is componentwise strict. Now we state the propositions:

(20) There exists a componentwise strict, normal subgroup family S of F such that for every element i of I, $S(i) = F(i)^{\mathrm{c}}$.

PROOF: Define $\mathcal{A}(\text{group}) = \$_1{}^{\mathrm{c}}$. Consider S being a componentwise strict subgroup family of F such that for every element i of I, $S(i) = \mathcal{A}(F(i))$. For every element i of I, $S(i)$ is a normal subgroup of $F(i)$. □

(21) Let us consider a strict multiplicative magma M. Suppose there exists an object x such that the carrier of $M = \{x\}$. Then there exists a strict, trivial group G such that $M = G$.

(22) Let us consider an empty set I, and a multiplicative magma family F of I. Then $\prod F$ is a trivial group. The theorem is a consequence of (21).

5. Inclusion Morphism

Let G, H be groups. Assume H is a subgroup of G. The functor $\mathrm{incl}(H, G)$ yielding a homomorphism from H to G is defined by the term

(Def. 8) id_α, where α is the carrier of H.

Let G be a group and H be a subgroup of G. The functor $\overset{H}{\hookrightarrow}$ yielding a homomorphism from H to G is defined by the term

(Def. 9) $\mathrm{incl}(H, G)$.

Now we state the propositions:

(23) Let us consider a group H, and an element h of H. If H is a subgroup of G, then $(\mathrm{incl}(H, G))(h) = h$.

(24) Let us consider a subgroup H of G. Then

(i) $\mathrm{incl}(H, G)$ is one-to-one, and

(ii) $\operatorname{Im} \mathrm{incl}(H, G) =$ the multiplicative magma of H.

Proof: Set $f = \mathrm{incl}(H, G)$. $\operatorname{Ker} f = \{\mathbf{1}\}_H$. □

Let G be a group and H be a subgroup of G. Let us observe that $\mathrm{incl}(H, G)$ is one-to-one. Now we state the propositions:

(25) Let us consider groups H, K. Suppose H is a subgroup of G. Let us consider a homomorphism φ from G to K. Then $\varphi\restriction$(the carrier of H) $= \varphi \cdot (\mathrm{incl}(H, G))$.

Proof: $\mathrm{dom}(\varphi\restriction(\text{the carrier of } H)) =$ the carrier of H. For every object x such that $x \in \mathrm{dom}(\varphi\restriction(\text{the carrier of } H))$ holds $(\varphi\restriction(\text{the carrier of } H))(x) = (\varphi \cdot (\mathrm{incl}(H, G)))(x)$. □

(26) Let us consider a group K, a subgroup H of G, and a homomorphism φ from G to K. Then $\varphi\restriction H = \varphi \cdot (\overset{H}{\hookrightarrow})$.

Proof: For every element h of H, $(\varphi\restriction H)(h) = (\varphi \cdot (\overset{H}{\hookrightarrow}))(h)$. □

(27) Let us consider a group G, and a strict subgroup H of G. Then $\operatorname{Im}(\overset{H}{\hookrightarrow}) = H$.

6. Families of Homomorphisms

Let G be a group, I be a non empty set, and F be a group family of I.

A homomorphism family of G and F is a many sorted function indexed by I defined by

(Def. 10) for every element i of I, $it(i)$ is a homomorphism from G to $F(i)$.

Let f be a homomorphism family of G and F and i be an element of I. One can check that the functor $f(i)$ yields a homomorphism from G to $F(i)$. In the sequel f denotes a homomorphism family of G and F. Now we state the proposition:

(28) $\langle i, f(i)\rangle \in f$.

Let I be a non empty set and F_1, F_2 be group families of I.

A homomorphism family of F_1 and F_2 is a many sorted function from F_1 into F_2 defined by

(Def. 11) for every element i of I, $it(i)$ is a homomorphism from $F_1(i)$ to $F_2(i)$.

Let i be an element of I and φ be a homomorphism family of F_1 and F_2. Note that $\varphi(i)$ is multiplicative as a function from $F_1(i)$ into $F_2(i)$. Now we state the proposition:

(29) Let us consider a non empty set I, group families A, B of I, and a many sorted set f indexed by I. Then f is a homomorphism family of A and B if and only if for every element i of I, $f(i)$ is a homomorphism from $A(i)$ to $B(i)$. The theorem is a consequence of (14).

The scheme *HomFamSch* deals with a non empty set I_1 and a group family D_1 of I_1 and a group family $\mathcal{C}$ of I_1 and a unary functor $\mathcal{A}$ yielding a function and states that

(Sch. 4) There exists a homomorphism family H of D_1 and $\mathcal{C}$ such that for every element i of I_1, $H(i) = \mathcal{A}(i)$

provided

- for every element i of I_1, $\mathcal{A}(i)$ is a homomorphism from $D_1(i)$ to $\mathcal{C}(i)$.

Now we state the proposition:

(30) Let us consider a group G, a non empty set I, a group family F of I, and a many sorted set f indexed by I. Then f is a homomorphism family of G and F if and only if for every element i of I, $f(i)$ is a homomorphism from G to $F(i)$.

The scheme *RHomFamSch* deals with a non empty set I_1 and a group D_1 and a group family $\mathcal{C}$ of I_1 and a unary functor $\mathcal{A}$ yielding a function and states that

(Sch. 5) There exists a homomorphism family H of D_1 and $\mathcal{C}$ such that for every element i of I_1, $H(i) = \mathcal{A}(i)$

provided

- for every element i of I_1, $\mathcal{A}(i)$ is a homomorphism from D_1 to $\mathcal{C}(i)$.

Now we state the proposition:

(31) Let us consider a non empty set I, group families A, B of I, and a many sorted set f indexed by I. Then f is a homomorphism family of A and B if and only if for every element i of I, $f(i)$ is a homomorphism from $A(i)$ to $B(i)$. The theorem is a consequence of (14).

7. Projection Morphisms from Product Group to Direct Factors

Now we state the proposition:

(32) Let us consider an element g of $\prod F$. Then $g(i)$ is an element of $F(i)$.

Let I be a non empty set, F be a group family of I, g be an element of $\prod F$, and i be an element of I. The functor $g_{/i}$ yielding an element of $F(i)$ is defined by the term

(Def. 12) $g(i)$.

We identify $g(i)$ with $g_{/i}$. The functor $\mathrm{proj}(F, i)$ yielding a homomorphism from $\prod F$ to $F(i)$ is defined by

(Def. 13) for every element h of $\prod F$, $it(h) = h(i)$.

Now we state the proposition:

(33) $\mathrm{proj}(F, i)$ is onto.

Proof: For every object y such that $y \in$ the carrier of $F(i)$ there exists an object x such that $x \in$ the carrier of $\prod F$ and $y = (\mathrm{proj}(F, i))(x)$. □

Let I be a non empty set, F be a group family of I, and i be an element of I. Let us observe that $\mathrm{proj}(F, i)$ is onto. Now we state the propositions:

(34) $\mathrm{proj}(\text{the support of } F, i)$ is a function from $\prod(\text{the support of } F)$ into the carrier of $F(i)$.

(35) Let us consider an element g of $\prod F$.
Then $(\mathrm{proj}(F, i))(g) = (\mathrm{proj}(\text{the support of } F, i))(g)$.

(36) $\mathrm{proj}(F, i) = \mathrm{proj}(\text{the support of } F, i)$. The theorem is a consequence of (34) and (35).

(37) Let us consider an element g of $\prod F$, and an element h of $F(i)$. Then $g +\cdot (i, h) \in \prod F$.

(38) Let us consider an element i of I, and an element g of $\prod F$. Then $g +\cdot (i, \mathbf{1}_{F(i)}) \in \mathrm{Ker}\,\mathrm{proj}(F, i)$. The theorem is a consequence of (37).

(39) Let us consider groups G_1, G_2, and a homomorphism f from G_1 to G_2. If for every element g of G_1, $f(g) = g$, then G_1 is a subgroup of G_2.
PROOF: The carrier of $G_1 \subseteq$ the carrier of G_2. Set $U_1 =$ the carrier of G_1. For every element a of U_1 and for every element b of U_1, (the multiplication of G_1)$(a, b) =$ ((the multiplication of G_2) $\restriction U_1$)(a, b). (The multiplication of G_2) $\restriction U_1$ is a binary operation on U_1. □

(40) Let us consider elements i, j of I. Suppose $i \neq j$. Then $(\mathrm{proj}(F, j)) \cdot (1\mathrm{ProdHom}(F, i)) = F(i) \to \{\mathbf{1}\}_{F(j)}$.
PROOF: Set $U =$ the carrier of $F(i)$. $\mathrm{dom}(F(i) \to \{\mathbf{1}\}_{F(j)}) = U$ and $\mathrm{dom}((\mathrm{proj}(F, j)) \cdot (1\mathrm{ProdHom}(F, i))) = U$. For every element x of U, $((\mathrm{proj}(F, j)) \cdot (1\mathrm{ProdHom}(F, i)))(x) = (F(i) \to \{\mathbf{1}\}_{F(j)})(x)$. □

(41) $(\mathrm{proj}(F, i)) \cdot (1\mathrm{ProdHom}(F, i)) = \mathrm{id}_\alpha$, where α is the carrier of $F(i)$.
PROOF: Set $U =$ the carrier of $F(i)$. For every element x of U, $((\mathrm{proj}(F, i)) \cdot (1\mathrm{ProdHom}(F, i)))(x) = x$. □

8. Universal Property of Direct Products of Groups

Let us consider a homomorphism family f of G and F. Now we state the propositions:

(42) There exists a homomorphism φ from G to $\prod F$ such that for every element g of G for every element j of I, $(f(j))(g) = (\mathrm{proj}(F, j))(\varphi(g))$.
PROOF: Define $\mathcal{P}[\mathrm{object}, \mathrm{object}] \equiv$ there exists an element g_0 of $\prod F$ such that $\$_2 = g_0$ and for every element j of I, $f(j)(\$_1) = g_0(j)$. Define $\mathcal{F} =$ the carrier of G. For every object x such that $x \in \mathcal{F}$ there exists an object y such that $y \in$ the carrier of $\prod F$ and $\mathcal{P}[x, y]$. Consider φ being a function from $\mathcal{F}$ into the carrier of $\prod F$ such that for every object x such that $x \in \mathcal{F}$ holds $\mathcal{P}[x, \varphi(x)]$. For every element g of G and for every element j of I, $\varphi(g)(j) = f(j)(g)$. For every elements a, b of G, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. For every element j of I, $(f(j))(g) = (\mathrm{proj}(F, j))(\varphi(g))$. □

(43) There exists a homomorphism φ from G to $\prod F$ such that for every element i of I, $f(i) = (\mathrm{proj}(F, i)) \cdot \varphi$.
PROOF: Consider φ being a homomorphism from G to $\prod F$ such that for every element g of G and for every element j of I, $(f(j))(g) = (\mathrm{proj}(F, j))(\varphi(g))$. For every element g of G, $((\mathrm{proj}(F, i)) \cdot \varphi)(g) = f(i)(g)$. □

(44) Let us consider a homomorphism family f of G and F, and homomorphisms φ_1, φ_2 from G to $\prod F$. Suppose for every element i of I, $f(i) = (\mathrm{proj}(F, i)) \cdot \varphi_1$ and for every element i of I, $f(i) = (\mathrm{proj}(F, i)) \cdot \varphi_2$. Then $\varphi_1 = \varphi_2$.
PROOF: For every element g of G, $\varphi_1(g) = \varphi_2(g)$. □

Let G be a group, I be a non empty set, F be a group family of I, and f be a homomorphism family of G and F. The functor $\prod f$ yielding a homomorphism from G to $\prod F$ is defined by

(Def. 14) for every element g of G and for every element i of I, $f(i)(g) = it(g)(i)$.

Let us consider an element g of G. Now we state the propositions:

(45) for every element i of I, $(\prod f)(g)(i) = \mathbf{1}_{F(i)}$ if and only if $(\prod f)(g) = \mathbf{1}_{\prod F}$.
PROOF: If for every element i of I, $(\prod f)(g)(i) = \mathbf{1}_{F(i)}$, then $(\prod f)(g) = \mathbf{1}_{\prod F}$. □

(46) $g \in \operatorname{Ker} \prod f$ if and only if for every element i of I, $g \in \operatorname{Ker} f(i)$.
PROOF: If $g \in \operatorname{Ker} \prod f$, then for every element i of I, $g \in \operatorname{Ker} f(i)$. If for every element i of I, $g \in \operatorname{Ker} f(i)$, then $g \in \operatorname{Ker} \prod f$. □

(47) Let us consider groups G_1, G_2, G_3, a homomorphism f_1 from G_1 to G_2, a homomorphism f_2 from G_2 to G_3, and an element g of G_1. Then $g \in \operatorname{Ker} f_2 \cdot f_1$ if and only if $f_1(g) \in \operatorname{Ker} f_2$.
PROOF: If $g \in \operatorname{Ker} f_2 \cdot f_1$, then $f_1(g) \in \operatorname{Ker} f_2$. If $f_1(g) \in \operatorname{Ker} f_2$, then $g \in \operatorname{Ker} f_2 \cdot f_1$. □

(48) Let us consider groups G_1, G_2, G_3, a homomorphism f_1 from G_1 to G_2, and a homomorphism f_2 from G_2 to G_3. Then the carrier of $\operatorname{Ker} f_2 \cdot f_1 = {f_1}^{-1}((\text{the carrier of } \operatorname{Ker} f_2))$.
PROOF: For every element g of G_1 such that $g \in$ the carrier of $\operatorname{Ker} f_2 \cdot f_1$ holds $g \in {f_1}^{-1}((\text{the carrier of } \operatorname{Ker} f_2))$. For every element g of G_1 such that $g \in {f_1}^{-1}((\text{the carrier of } \operatorname{Ker} f_2))$ holds $g \in$ the carrier of $\operatorname{Ker} f_2 \cdot f_1$. □

(49) The carrier of $\operatorname{Ker} \prod f = \bigcap$ the set of all the carrier of $\operatorname{Ker} f(i)$ where i is an element of I.
PROOF: Set $\mathcal{F}$ = the set of all the carrier of $\operatorname{Ker} f(i)$ where i is an element of I. $\mathcal{F} \neq \emptyset$. For every object g, $g \in \operatorname{Ker} \prod f$ iff for every set A such that $A \in \mathcal{F}$ holds $g \in A$. For every object g, $g \in \operatorname{Ker} \prod f$ iff $g \in \bigcap \mathcal{F}$. For every object g, $g \in$ the carrier of $\operatorname{Ker} \prod f$ iff $g \in \bigcap \mathcal{F}$. □

(50) Let us consider a function f, a non empty set I, and a group family F of I. Suppose $\operatorname{dom} f = I$ and for every element i of I, $f(i) \in F(i)$. Then $f \in \prod F$. The theorem is a consequence of (14).

(51) Let us consider a group family S of I, and an element g of $\prod F$. Then $g \in \prod S$ if and only if for every element i of I, $(\operatorname{proj}(F, i))(g) \in S(i)$. The theorem is a consequence of (50).

(52) Let us consider group families F_1, F_2 of I. Suppose for every element i of I, $F_1(i)$ is a subgroup of $F_2(i)$. Then $\prod F_1$ is a subgroup of $\prod F_2$.

PROOF: Define $\mathcal{A}(\text{element of } I) = (\text{incl}(F_1(\$_1), F_2(\$_1))) \cdot (\text{proj}(F_1, \$_1))$. Consider f being a homomorphism family of $\prod F_1$ and F_2 such that for every element i of I, $f(i) = \mathcal{A}(i)$. For every element g of $\prod F_1$ and for every element i of I, $f(i)(g) = g(i)$. Consider φ being a homomorphism from $\prod F_1$ to $\prod F_2$ such that for every element g of $\prod F_1$ and for every element i of I, $(f(i))(g) = (\text{proj}(F_2, i))(\varphi(g))$. For every element g of $\prod F_1$, $\varphi(g) = g$. □

Let I be a non empty set, F be a group family of I, and S be a subgroup family of F. The functor $\prod S$ yielding a strict subgroup of $\prod F$ is defined by the term

(Def. 15) $\prod S$.

Now we state the propositions:

(53) $\operatorname{Im}\text{proj}(F, i) =$ the multiplicative magma of $F(i)$.
PROOF: For every object g such that $g \in$ the carrier of $F(i)$ holds $g \in$ the carrier of $\operatorname{Im}\text{proj}(F, i)$. □

(54) Let us consider componentwise strict subgroup families F_1, F_2 of F. Suppose for every element i of I, $\operatorname{Im}\text{proj}(F_1, i)$ is a subgroup of $\operatorname{Im}\text{proj}(F_2, i)$. Then $\prod F_1$ is a strict subgroup of $\prod F_2$. The theorem is a consequence of (53) and (52).

(55) Let us consider a strict subgroup G of $\prod F$, and S. Suppose for every element i of I, $S(i) = \text{Im}(\text{proj}(F, i)) \cdot (\overset{G}{\hookrightarrow})$. Let us consider a homomorphism family f of G and S. Suppose for every element i of I, $f(i) = (\text{proj}(F, i)) \cdot (\overset{G}{\hookrightarrow})$. Then $\prod f = \text{id}_\alpha$, where α is the carrier of G.
PROOF: For every element g of G and for every element i of I, $((\text{proj}(F, i)) \cdot (\overset{G}{\hookrightarrow}))(g) = ((\text{proj}(F, i)) \cdot (\prod f))(g)$. For every element g of $\prod F$ such that $g \in G$ holds $(\prod f)(g) = g$. For every object x such that $x \in$ the carrier of G holds $(\prod f)(x) = x$. □

(56) Let us consider groups G_1, G_2, a homomorphism φ from G_1 to G_2, and an element x of G_1. Suppose $x \in$ the commutators of G_1. Then $\varphi(x) \in$ the commutators of G_2.

(57) Let us consider groups G_1, G_2, G_3, a homomorphism f_1 from G_1 to G_2, a homomorphism f_2 from G_2 to G_3, and an element g of G_1. Then $(f_2 \cdot f_1)(g) = f_2(f_1(g))$.

(58) Let us consider groups G_1, G_2, a subgroup H of G_2, a homomorphism f_1 from G_1 to G_2, and a homomorphism f_2 from G_1 to H. If $f_1 = f_2$, then $\operatorname{Im} f_1 = \operatorname{Im} f_2$.
PROOF: For every element g of G_2, $g \in \operatorname{Im} f_1$ iff $g \in \operatorname{Im} f_2$. □

(59) Let us consider elements a, b of $\prod F$, and i. Then $[a, b](i) = [a_{/i}, b_{/i}]$.

The scheme *SubFamEx* deals with a non empty set I_1 and a group family $\mathcal{F}$ of I_1 and a binary predicate $\mathcal{P}$ and states that

(Sch. 6) There exists a subgroup family S of $\mathcal{F}$ such that for every element i of I_1, $\mathcal{P}[i, S(i)]$

provided

- for every element i of I_1, there exists a subgroup j of $\mathcal{F}(i)$ such that $\mathcal{P}[i, j]$.

Now we state the propositions:

(60) Let us consider a many sorted set A indexed by I. Suppose for every element i of I, $A(i)$ is a subset of $F(i)$. Then $\prod A$ is a subset of $\prod F$.
PROOF: For every object x such that $x \in \prod A$ holds $x \in$ the carrier of $\prod F$. □

(61) Let us consider a normal subgroup family S of F. Then $\prod S$ is a normal subgroup of $\prod F$.
PROOF: For every element g of $\prod F$, $(\prod S)^g$ is a subgroup of $\prod S$. □

Let I be a non empty set, F be a group family of I, and S be a normal subgroup family of F. Note that $\prod S$ is normal as a subgroup of $\prod F$.

9. Commutator Subgroup and Center of Product Groups

Now we state the proposition:

(62) Let us consider a group family Z of I. If for every element i of I, $Z(i) = \mathrm{Z}(F(i))$, then $\mathrm{Z}(\prod F) = \prod Z$.
PROOF: For every element a of $\prod F$, $a \in \prod Z$ iff for every element b of $\prod F$, $a \cdot b = b \cdot a$. For every element a of $\prod F$, $a \in \prod Z$ iff $a \in \mathrm{Z}(\prod F)$. For every element i of I, $Z(i)$ is a subgroup of $F(i)$. □

Let us consider a subgroup family D of F. Now we state the propositions:

(63) If for every element i of I, $D(i) = F(i)^{\mathrm{c}}$, then $(\prod F)^{\mathrm{c}}$ is a strict subgroup of $\prod D$.
PROOF: For every elements a, b of $\prod F$, $[a, b] \in \prod D$. □

(64) If for every element i of I, $D(i) = F(i)^{\mathrm{c}}$, then $\operatorname{sum} D$ is a strict subgroup of $(\prod F)^{\mathrm{c}}$.
PROOF: For every element g of $\prod F$ such that $g \in \operatorname{sum} D$ holds $g \in (\prod F)^{\mathrm{c}}$. □

(65) Let us consider a finite, non empty set I, a group family F of I, and a subgroup family D of F. Suppose for every element i of I, $D(i) = F(i)^{\mathrm{c}}$. Then $(\prod F)^{\mathrm{c}} = \prod D$. The theorem is a consequence of (64) and (63).

10. Quotients of Product Groups

Let I be a non empty set, F_1, F_2 be group families of I, and f be a homomorphism family of F_1 and F_2. The functor $\prod f$ yielding a homomorphism from $\prod F_1$ to $\prod F_2$ is defined by

(Def. 16) for every element i of I, $(\mathrm{proj}(F_2, i)) \cdot it = f(i) \cdot (\mathrm{proj}(F_1, i))$.

The functor $\operatorname{Ker} f$ yielding a componentwise strict, normal subgroup family of F_1 is defined by

(Def. 17) for every element i of I, $it(i) = \operatorname{Ker}(f(i)$ **qua** homomorphism from $F_1(i)$ to $F_2(i))$.

The functor $\operatorname{Im} f$ yielding a componentwise strict subgroup family of F_2 is defined by

(Def. 18) for every element i of I, $it(i) = \operatorname{Im}(f(i)$ **qua** homomorphism from $F_1(i)$ to $F_2(i))$.

Let us consider group families F_1, F_2 of I and a homomorphism family f of F_1 and F_2. Now we state the propositions:

(66) $\operatorname{Ker} \prod f = \prod \operatorname{Ker} f$.

Proof: For every element g of $\prod F_1$, $g \in \operatorname{Ker} \prod f$ iff $g \in \prod \operatorname{Ker} f$. □

(67) $\operatorname{Im} \prod f = \prod \operatorname{Im} f$.

Proof: For every element g of $\prod F_2$, $g \in \operatorname{Im} \prod f$ iff $g \in \prod \operatorname{Im} f$. □

(68) Let us consider a componentwise strict, normal subgroup family S of F. Then $\prod {}^{F}/_{\prod S}$ and $\prod({}^{F}/_{S})$ are isomorphic.

Proof: Define $\mathcal{A}$(element of I) = the canonical homomorphism onto cosets of $S(\$_1)$. For every element i of I, $\mathcal{A}(i)$ is a homomorphism from $F(i)$ to $({}^{F}/_{S})(i)$. Consider f being a homomorphism family of F and ${}^{F}/_{S}$ such that for every element i of I, $f(i) = \mathcal{A}(i)$. $\operatorname{Ker} f = S$. $\operatorname{Ker} \prod f = \prod S$. $\operatorname{Im} f = {}^{F}/_{S}$. $\operatorname{Im} \prod f = \prod \operatorname{Im} f$. □

11. Internal Direct Products

Let I be a set, G be a group, and I_2 be a homomorphism family of I and G. We say that I_2 is normal if and only if

(Def. 19) for every object i such that $i \in I$ holds $I_2(i)$ is a normal subgroup of G.

We say that I_2 is componentwise strict if and only if

(Def. 20) for every object i such that $i \in I$ holds $I_2(i)$ is a strict subgroup of G.

Let us consider a non empty set I, a group G, and a homomorphism family F of I and G. Now we state the propositions:

(69) F is normal if and only if for every element i of I, $F(i)$ is a normal subgroup of G.

(70) F is componentwise strict if and only if for every element i of I, $F(i)$ is a strict subgroup of G.

Let I be a set and G be a group. Note that there exists a homomorphism family of I and G which is componentwise strict and normal.

Let I be a non empty set, F be a homomorphism family of I and G, and i be an element of I. Note that the functor $F(i)$ yields a subgroup of G. Let F be a normal homomorphism family of I and G. One can check that $F(i)$ is normal as a subgroup of G. Now we state the propositions:

(71) Let us consider subgroups H_1, H_2 of G. Suppose $[H_1, H_2] = \{\mathbf{1}\}_G$. Let us consider elements a, b of G. If $a \in H_1$ and $b \in H_2$, then $a \cdot b = b \cdot a$.

(72) Let us consider a normal subgroup N of G, and elements a, b of G. If $a \in N$, then $a^b \in N$.

(73) Let us consider normal subgroups H, K of G. Suppose $H \cap K = \{\mathbf{1}\}_G$. Let us consider elements h, k of G. If $h \in H$ and $k \in K$, then $h \cdot k = k \cdot h$.
PROOF: $[h, k] \in H \cap K$. □

(74) Let us consider a normal homomorphism family F of I and G, and a subset A of G. Suppose $A = \bigcup\{$the carrier of $F(i)$, where i is an element of $I\}$. Then there exists a strict, normal subgroup N of G such that $N = \mathrm{gr}(A)$.
PROOF: Reconsider $N = \mathrm{gr}(A)$ as a strict subgroup of G. For every element i of I, the carrier of $F(i) \subseteq$ the carrier of N. For every element a of G, N^a is a subgroup of N. □

Let I be a set, J be a subset of I, and F be a group yielding many sorted set indexed by I. One can verify that $F{\restriction}J$ is group yielding, J-defined, and total.

Now we state the proposition:

(75) Let us consider a set I, a homomorphism family F of I and G, and a set J. If $J \subseteq I$, then $F{\restriction}J$ is a homomorphism family of J and G.
PROOF: For every object j such that $j \in J$ holds $(F{\restriction}J)(j)$ is a subgroup of G. □

Let I be a set, G be a group, F be a homomorphism family of I and G, and J be a subset of I. Note that the functor $F{\restriction}J$ yields a homomorphism family of J and G. One can check that $F{\restriction}J$ is group yielding. Now we state the propositions:

(76) Let us consider a normal homomorphism family F of I and G, a subset A of G, and an element i of I. Suppose $A = \bigcup\{$the carrier of $F(j)$, where j is an element of $I : i \neq j\}$. Then there exists a strict, normal subgroup

N of G such that $N = \mathrm{gr}(A)$. The theorem is a consequence of (75), (69), and (74).

(77) Let us consider a non empty subset J of I, and a normal homomorphism family F of I and G. Then $F\restriction J$ is a normal homomorphism family of J and G.

PROOF: For every element j of J, $(F\restriction J)(j)$ is a normal subgroup of G. □

(78) Let us consider a set I, a subset J of I, and a normal homomorphism family F of I and G. Then $F\restriction J$ is a normal homomorphism family of J and G.

PROOF: For every object i such that $i \in J$ holds $(F\restriction J)(i)$ is a normal subgroup of G. □

Let I be a set, J be a subset of I, G be a group, and F be a normal homomorphism family of I and G. Let us note that $F\restriction J$ is normal as a homomorphism family of J and G. Now we state the proposition:

(79) Let us consider a set I, a subset J of I, and a componentwise strict homomorphism family F of I and G. Then $F\restriction J$ is a componentwise strict homomorphism family of J and G.

PROOF: For every object i such that $i \in J$ holds $(F\restriction J)(i)$ is a strict subgroup of G. □

Let I be a set, J be a subset of I, G be a group, and F be a componentwise strict homomorphism family of I and G. Let us note that $F\restriction J$ is componentwise strict as a homomorphism family of J and G. Now we state the propositions:

(80) Let us consider a set I, and a subset J of I. Suppose J is empty. Let us consider a normal homomorphism family F of I and G. Then the support of $F\restriction J = \emptyset \longmapsto 2^{\alpha}$, where α is the carrier of G.

(81) Let us consider a set I, a subset J of I, a normal homomorphism family F of I and G, and a subset A of G. Suppose $A = \bigcup$(the support of $F\restriction J$). Then there exists a strict, normal subgroup N of G such that $N = \mathrm{gr}(A)$.

(82) Let us consider a set I, a normal homomorphism family F of I and G, and a subset A of G. Suppose $A = \bigcup$(the support of F). Then there exists a strict, normal subgroup N of G such that $N = \mathrm{gr}(A)$. The theorem is a consequence of (81).

(83) Every componentwise strict homomorphism family of I and G is $(\mathrm{SubGr}\, G)$-valued. The theorem is a consequence of (5) and (70).

Let I be a non empty set and G be a group. Let us observe that every componentwise strict homomorphism family of I and G is $(\mathrm{SubGr}\, G)$-valued. Let I be a set and F be a 1-sorted yielding many sorted set indexed by I. An element of F is an element of the support of F. Now we state the proposition:

(84) Let us consider a group family F of I, an element g of F, and an element i of I. Then $g(i)$ is an element of $F(i)$. The theorem is a consequence of (14).

Let I be a non empty set, G be a group, and F be a homomorphism family of I and G. Observe that every element of F is (the carrier of G)-valued and every element of $\prod F$ is I-defined, relation-like, and function-like and every element of $\prod F$ is I-defined, (the carrier of G)-valued, and total. Now we state the proposition:

(85) Let us consider a set I, a group G, and a homomorphism family F of I and G. Then the support of F is (2^{α})-valued, where α is the carrier of G. The theorem is a consequence of (14).

Let I be a set, G be a group, and F be a homomorphism family of I and G. Observe that the support of F is $(2^{(\text{the carrier of } G)})$-valued. Now we state the propositions:

(86) Let us consider a group G, a finite subset S of $\operatorname{SubGr} G$, and a natural number n. Suppose $n = \overline{\overline{S}}$. Then $\operatorname{CFS}(S)$ is a homomorphism family of $\operatorname{Seg} n$ and G.

PROOF: For every object y such that $y \in \operatorname{rng} \operatorname{CFS}(S)$ holds y is a subgroup of G. $\operatorname{CFS}(S)$ is a group family of $\operatorname{Seg} n$. For every object i such that $i \in \operatorname{Seg} n$ holds $(\operatorname{CFS}(S))(i)$ is a subgroup of G. □

(87) Let us consider a group G, a finite subset N of the normal subgroups of G, and a natural number n. Suppose $n = \overline{\overline{N}}$. Then $\operatorname{CFS}(N)$ is a normal homomorphism family of $\operatorname{Seg} n$ and G.

PROOF: For every object i such that $i \in \operatorname{Seg} n$ holds $(\operatorname{CFS}(N))(i)$ is a normal subgroup of G. □

(88) Let us consider a group G, an empty set I, and a homomorphism family F of I and G. Then $\operatorname{gr}(\bigcup(\text{the support of } F)) = \{\mathbf{1}\}_G$.

Let G be a group, I be a set, F be a homomorphism family of I and G, and i be an object. Assume $i \in I$. The functor $F_{/i}$ yielding a subgroup of G is defined by the term

(Def. 21) $F(i)$.

We say that G is an internal product of F if and only if

(Def. 22) for every object i such that $i \in I$ holds $F(i)$ is a normal subgroup of G and the multiplicative magma of $G = \operatorname{gr}(\bigcup(\text{the support of } F))$ and for every object i such that $i \in I$ for every strict, normal subgroup N of G such that $N = \operatorname{gr}(\bigcup(\text{the support of } F \restriction I \setminus \{j, \text{ where } j \text{ is an element of } I : F(i) = F(j)\}))$ holds $F_{/i} \cap N = \{\mathbf{1}\}_G$.

Now we state the propositions:

(89) Let us consider a group G, an empty set I, and a homomorphism family F of I and G. Then G is an internal product of F if and only if G is trivial. The theorem is a consequence of (88).

(90) Let us consider a group G, a non empty set I, and a homomorphism family F of I and G. Then G is an internal product of F if and only if for every element i of I, $F(i)$ is a normal subgroup of G and the multiplicative magma of $G = \mathrm{gr}(\bigcup(\text{the support of } F))$ and for every element i of I and for every subset J of I such that $J = I \setminus \{j$, where j is an element of $I : F(i) = F(j)\}$ for every strict, normal subgroup N of G such that $N = \mathrm{gr}(\bigcup(\text{the support of } F\restriction J))$ holds $F(i) \cap N = \{\mathbf{1}\}_G$.

Let G be a group, I be a set, and F be a normal homomorphism family of I and G. One can check that G is an internal product of F if and only if the condition (Def. 23) is satisfied.

(Def. 23) the multiplicative magma of $G = \mathrm{gr}(\bigcup(\text{the support of } F))$ and for every object i such that $i \in I$ for every strict, normal subgroup N of G such that $N = \mathrm{gr}(\bigcup(\text{the support of } F\restriction I \setminus \{j$, where j is an element of $I : F(i) = F(j)\}))$ holds $F_{/i} \cap N = \{\mathbf{1}\}_G$.

Let us consider a group G, a non empty set I, and a normal homomorphism family F of I and G. Now we state the propositions:

(91) G is an internal product of F if and only if the multiplicative magma of $G = \mathrm{gr}(\bigcup(\text{the support of } F))$ and for every element i of I and for every subset J of I such that $J = I \setminus \{j$, where j is an element of $I : F(i) = F(j)\}$ for every strict, normal subgroup N of G such that $N = \mathrm{gr}(\bigcup(\text{the support of } F\restriction J))$ holds $F(i) \cap N = \{\mathbf{1}\}_G$. The theorem is a consequence of (90).

(92) Suppose F is one-to-one. Then G is an internal product of F if and only if the multiplicative magma of $G = \mathrm{gr}(\bigcup(\text{the support of } F))$ and for every element i of I and for every subset J of I such that $J = I \setminus \{i\}$ for every strict, normal subgroup N of G such that $N = \mathrm{gr}(\bigcup(\text{the support of } F\restriction J))$ holds $F(i) \cap N = \{\mathbf{1}\}_G$. The theorem is a consequence of (91).

(93) The celebrated "Recognition Theorem", see Aschbacher [1, (1.9)], Hungerford [5, (1.8.6)], Robinson [11, (1.4.7.ii)]:
Let us consider a strict group G, a non empty set I, and a normal homomorphism family F of I and G. Suppose F is one-to-one. Then G is an internal product of F if and only if F is an internal direct sum components of G and I.
Proof: For every element i of I and for every subset J of I, the support of $F\restriction J = (\text{the support of } F)\restriction J$. If G is an internal product of F, then F is an internal direct sum components of G and I. If F is an internal direct sum components of G and I, then G is an internal product of F. □

Let G be a group and $\mathcal{F}$ be a subset of $\mathrm{SubGr}\, G$. We say that G is an internal product of $\mathcal{F}$ if and only if

(Def. 24) for every strict subgroup H of G such that $H \in \mathcal{F}$ holds H is a normal subgroup of G and there exists a subset A of G such that $A = \bigcup\{U_3$, where U_3 is a subset of G : there exists a strict subgroup H of G such that $H \in \mathcal{F}$ and $U_3 =$ the carrier of $H\}$ and the multiplicative magma of $G = \mathrm{gr}(A)$ and for every strict subgroup H of G such that $H \in \mathcal{F}$ for every subset A of G such that $A = \bigcup\{U_4$, where U_4 is a subset of G : there exists a strict subgroup K of G such that $K \in \mathcal{F}$ and $U_4 =$ the carrier of K and $K \neq H\}$ holds $H \cap \mathrm{gr}(A) = \{\mathbf{1}\}_G$.

Let H be a strict subgroup of G. We say that H is an internal product of $\mathcal{F}$ if and only if

(Def. 25) for every strict subgroup H_1 of G such that $H_1 \in \mathcal{F}$ holds H_1 is a normal subgroup of H and there exists a subset A of G such that $A = \bigcup\{U_3$, where U_3 is a subset of G : there exists a strict subgroup H of G such that $H \in \mathcal{F}$ and $U_3 =$ the carrier of $H\}$ and $H = \mathrm{gr}(A)$ and for every strict subgroup H_1 of G such that $H_1 \in \mathcal{F}$ for every subset A of G such that $A = \bigcup\{U_4$, where U_4 is a subset of G : there exists a strict subgroup K of G such that $K \in \mathcal{F}$ and $U_4 =$ the carrier of K and $K \neq H_1\}$ holds $H_1 \cap \mathrm{gr}(A) = \{\mathbf{1}\}_G$.

Now we state the propositions:

(94) G is a subgroup of Ω_G.

(95) Let us consider a group G, and a subgroup H of G. Suppose H is a normal subgroup of Ω_G. Then H is a normal subgroup of G. The theorem is a consequence of (94).

(96) Let us consider a group G, and a subset $\mathcal{F}$ of $\mathrm{SubGr}\, G$. Then G is an internal product of $\mathcal{F}$ if and only if Ω_G is an internal product of $\mathcal{F}$. The theorem is a consequence of (95).

(97) Let us consider a group G, a non empty set I, a componentwise strict homomorphism family F of I and G, and a subset $\mathcal{F}$ of $\mathrm{SubGr}\, G$. Suppose $\mathcal{F} = \mathrm{rng}\, F$. Then $\bigcup\{A$, where A is a subset of G : there exists a strict subgroup H of G such that $H \in \mathcal{F}$ and $A =$ the carrier of $H\} = \bigcup($the support of $F)$. The theorem is a consequence of (5) and (14).

(98) Let us consider a group G, a non empty set I, a componentwise strict homomorphism family F of I and G, and a subset $\mathcal{F}$ of $\mathrm{SubGr}\, G$. Suppose $\mathcal{F} = \mathrm{rng}\, F$. Let us consider a strict subgroup H of G, and an element i of I. Suppose $H = F(i)$. Let us consider a subset J of I. Suppose $J = I \setminus \{j$, where j is an element of $I : F(i) = F(j)\}$. Then $\bigcup\{A$, where A is a subset of G : there exists a strict subgroup K of G such that $K \in$

$\mathcal{F}$ and $A =$ the carrier of K and $K \neq H\} = \bigcup$(the support of $F\restriction J$).

PROOF: Set $X = \{A$, where A is a subset of $G:$ there exists a strict subgroup K of G such that $K \in \mathcal{F}$ and $A =$ the carrier of K and $K \neq H\}$. For every object x, $x \in X$ iff $x \in \operatorname{rng}$(the support of $F\restriction J$). □

(99) Let us consider a group G, a non empty set I, a componentwise strict homomorphism family F of I and G, and a subset $\mathcal{F}$ of $\operatorname{SubGr} G$. Suppose $\mathcal{F} = \operatorname{rng} F$. Then G is an internal product of F if and only if G is an internal product of $\mathcal{F}$. The theorem is a consequence of (5), (97), (69), (81), (98), and (70).

ACKNOWLEDGEMENT: Dedicated in loving memory of Paul Sirri. "Each man is a spark in the darkness. Would that we all burn as bright."

REFERENCES

[1] Michael Aschbacher. *Finite Group Theory*, volume 10. Cambridge University Press, 2000.

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

[3] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley and Sons, Third edition, 2004.

[4] 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.

[5] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag New York Inc., Seattle, Washington USA, Department of Mathematics University of Washington edition, 1974.

[6] I. Martin Isaacs. *Finite Group Theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, 2008.

[7] Aleksandr Gennadievich Kurosh. *The Theory of Groups*, volume 1. Chelsea Publishing Company, 1955.

[8] Kazuhisa Nakasho, Hiroyuki Okazaki, Hiroshi Yamazaki, and Yasunari Shidama. Equivalent expressions of direct sum decomposition of groups. *Formalized Mathematics*, 23(**1**): 67–73, 2015. doi:10.2478/forma-2015-0006.

[9] Kazuhisa Nakasho, Hiroshi Yamazaki, Hiroyuki Okazaki, and Yasunari Shidama. Definition and properties of direct sum decomposition of groups. *Formalized Mathematics*, 23 (**1**):15–27, 2015. doi:10.2478/forma-2015-0002.

[10] Alexander M. Nelson. Characteristic subgroups. *Formalized Mathematics*, 30(**2**):79–91, 2022. doi:10.2478/forma-2022-0007.

[11] Derek Robinson. *A Course in the Theory of Groups*. Springer New York, 2012.

Accepted June 30, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 121–130, 2023
DOI: 10.2478/forma-2023-0011
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Normal Extensions

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In this article we continue the formalization of field theory in Mizar [1], [2], [4], [3]. We introduce normal extensions: an (algebraic) extension E of F is normal if every polynomial of F that has a root in E already splits in E. We proved characterizations (for finite extensions) by minimal polynomials [7], splitting fields, and fixing monomorphisms [6], [5]. This required extending results from [11] and [12], in particular that $F[T] = \{p(a_1, \dots a_n) \mid p \in F[X],\ a_i \in T\}$ and $F(T) = F[T]$ for finite algebraic $T \subseteq E$. We also provided the counterexample that $\mathcal{Q}(\sqrt[3]{2})$ is not normal over $\mathcal{Q}$ (compare [13]).

MSC: 12F05 68V20

Keywords: normal extension; fixing monomorphisms

MML identifier: FIELD_13, version: 8.1.12 5.75.1447

1. Preliminaries

Let Y be a non empty set and y_1, y_2, y_3 be elements of Y. Note that the functor $\{y_1, y_2, y_3\}$ yields a subset of Y. Let R be an integral domain and p, q be constant polynomials over R. Note that $p * q$ is constant. Let R be a ring. Note that every ring extension of R is R-homomorphic and R-monomorphic.

Let F be a field, p be a non constant element of the carrier of Polynom-Ring F, and E be a splitting field of p. Let us observe that $\mathrm{Roots}(E, p)$ is non empty. Let R be a ring, S be a ring extension of R, and T be a ring extension of S. One can check that there exists a homomorphism from S to T which is R-fixing and there exists a monomorphism of S and T which is R-fixing. Now we state the propositions:

(1) Let us consider a ring R, a subring S of R, a non empty finite sequence F of elements of the carrier of R, and a non empty finite sequence G of elements of the carrier of S. If $F = G$, then $\prod F = \prod G$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non empty finite sequence F of elements of the carrier of R for every non empty finite sequence G of elements of the carrier of S such that $\operatorname{len} F = \$_1$ and $F = G$ holds $\prod F = \prod G$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $n = \operatorname{len} F$. □

(2) Let us consider a field F, and a non empty finite sequence G of elements of the carrier of Polynom-Ring F. Then $\prod G = \mathbf{0}.F$ if and only if there exists an element i of $\operatorname{dom} G$ such that $G(i) = \mathbf{0}.F$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non empty finite sequence G of elements of the carrier of Polynom-Ring F such that $\operatorname{len} G = \$_1$ and for every element i of $\operatorname{dom} G$, $G(i) \neq \mathbf{0}.F$ holds $\prod G \neq \mathbf{0}.F$. $\mathcal{P}[1]$. For every natural number k such that $k \geqslant 1$ holds $\mathcal{P}[k]$. □

(3) Let us consider a field F, and a non empty finite sequence G of elements of the carrier of Polynom-Ring F. Suppose for every element i of $\operatorname{dom} G$, $G(i) \neq \mathbf{0}.F$. Let us consider a polynomial q over F. Suppose $q = \prod G$. Let us consider an element i of $\operatorname{dom} G$, and a polynomial p over F. If $p = G(i)$, then $\deg(p) \leqslant \deg(q)$. The theorem is a consequence of (2).

(4) Let us consider a field F, an extension E of F, a non empty finite sequence G of elements of the carrier of Polynom-Ring F, and a polynomial q over F. Suppose $q = \prod G$. Let us consider an element a of E. Suppose there exists an element i of $\operatorname{dom} G$ and there exists a polynomial p over F such that $p = G(i)$ and $\operatorname{ExtEval}(p, a) = 0_E$. Then $\operatorname{ExtEval}(q, a) = 0_E$.

(5) Let us consider a field F, a non empty finite sequence G of elements of the carrier of Polynom-Ring F, and a non constant polynomial q over F. Suppose $q = \prod G$. Then q splits in F if and only if for every element i of $\operatorname{dom} G$ and for every polynomial p over F such that $p = G(i)$ holds p is constant or p splits in F.

(6) Let us consider a field F, an extension E of F, a non empty finite sequence G of elements of the carrier of Polynom-Ring F, and a non constant polynomial q over F. Suppose $q = \prod G$. Then q splits in E if and only if for every element i of $\operatorname{dom} G$ and for every polynomial p over F such that $p = G(i)$ holds p is constant or p splits in E. The theorem is a consequence of (1) and (5).

(7) Let us consider a field F, an extension E of F, a non constant polynomial p over F, and a non zero polynomial q over F. If $p * q$ splits in E, then p splits in E.

(8) Let us consider a natural number n, a field F, an extension E of F, a polynomial p of n,F, and a polynomial q of n,E. If $p = q$, then Support q = Support p.

(9) Let us consider a natural number n, a field F, an extension E of F, a polynomial p of n,F, a polynomial q of n,E, and a function x from n into E. If $p = q$, then $\mathrm{ExtEval}(p, x) = \mathrm{eval}(q, x)$.

PROOF: Consider F_3 being a finite sequence of elements of the carrier of S such that $\mathrm{ExtEval}(p, x) = \sum F_3$ and $\mathrm{len}\, F_3 = \mathrm{len}\, \mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p)$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, F_3$ holds $F_3(i) = (p \cdot (\mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p)))i)(\in S) \cdot (\mathrm{eval}((\mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, p))_{/i}, x))$. Consider F_4 being a finite sequence of elements of the carrier of S such that $\mathrm{len}\, F_4 = \mathrm{len}\, \mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, q)$ and $\mathrm{eval}(q, x) = \sum F_4$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \mathrm{len}\, F_4$ holds $F_{4/i} = q \cdot (\mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, q))_{/i} \cdot (\mathrm{eval}((\mathrm{SgmX}(\mathrm{BagOrder}\, n, \mathrm{Support}\, q))_{/i}, x))$. For every natural number i such that $i \in \mathrm{dom}\, F_3$ holds $F_4(i) = F_3(i)$. □

(10) Let us consider a natural number n, a field F, an extension E of F, an element a of F, and an element b of E. If $a = b$, then $a\restriction(n, F) = b\restriction(n, E)$.

(11) Let us consider a field F, an extension E_1 of F, and a field E_2. If $E_1 \approx E_2$, then E_2 is an extension of F.

(12) Let us consider fields F_1, F_2, and a product of linear polynomials p of F_1. If $F_1 \approx F_2$, then p is a product of linear polynomials of F_2.

(13) Let us consider a field F, an extension E of F, a polynomial p over F, a polynomial q over E, an element a of F, and an element b of E. If $p = q$ and $a = b$, then $a \cdot p = b \cdot q$.

(14) Let us consider fields F_1, F_2, a polynomial p over F_1, an element a of F_1, a polynomial q over F_2, and an element b of F_2. If $F_1 \approx F_2$, then if $p = q$ and $a = b$, then $a \cdot p = b \cdot q$. The theorem is a consequence of (13).

(15) Let us consider a field F, extensions E_1, E_2 of F, and a polynomial p over F. If $E_1 \approx E_2$, then if p splits in E_1, then p splits in E_2. The theorem is a consequence of (12) and (14).

(16) Let us consider a field F, extensions E_1, E_2 of F, and a non constant element p of the carrier of Polynom-Ring F. Suppose $E_1 \approx E_2$. If E_1 is a splitting field of p, then E_2 is a splitting field of p. The theorem is a consequence of (11) and (15).

(17) Let us consider a field F, and a linear element p of the carrier of Polynom-Ring F. Then F is a splitting field of p.

Let F be a field and E be an extension of F. Let us observe that there exists

a subset of E which is non empty, finite, and F-algebraic. Let a be an F-algebraic element of E. Let us observe that $\{a\}$ is F-algebraic as a subset of E.

Let T_1, T_2 be F-algebraic subsets of E. One can verify that $T_1 \cup T_2$ is F-algebraic as a subset of E. Let T_1 be an F-algebraic subset of E and T_2 be a subset of E. Let us observe that $T_1 \cap T_2$ is F-algebraic as a subset of E and $T_1 \setminus T_2$ is F-algebraic as a subset of E. Let T be a non empty, F-algebraic subset of E.

Note that an element of T is an element of E. Let us note that every element of T is F-algebraic. Let E_1, E_2 be extensions of F, h be a function from E_1 into E_2, and T be a subset of E_1. Observe that the functor $h^\circ T$ yields a subset of E_2. Now we state the propositions:

(18) Let us consider a field F, an extension E of F, a subset T_1 of E, a subset T_2 of E, an extension E_1 of $\mathrm{FAdj}(F, T_2)$, and a subset T_3 of E_1. Suppose $E_1 = E$ and $T_1 = T_3$. Then $\mathrm{FAdj}(F, T_1 \cup T_2) = \mathrm{FAdj}(\mathrm{FAdj}(F, T_2), T_3)$.
PROOF: $T_1 \cup T_2 \subseteq$ the carrier of $\mathrm{FAdj}(\mathrm{FAdj}(F, T_2), T_3)$. □

(19) Let us consider a field F, an extension E of F, an E-extending extension K of F, a finite, F-algebraic subset T_1 of E, and a subset T_2 of K. If $T_1 = T_2$, then $\mathrm{FAdj}(F, T_1) = \mathrm{FAdj}(F, T_2)$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite, F-algebraic subset T_1 of E for every subset T_2 of K such that $\overline{\overline{T_1}} = \$_1$ and $T_1 = T_2$ holds $\mathrm{FAdj}(F, T_1) = \mathrm{FAdj}(F, T_2)$. $\mathcal{P}[0]$ by [14, (3)]. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{T_1}} = n$. □

(20) Let us consider fields F_1, F_2, an element p_1 of the carrier of Polynom-Ring F_1, an element p_2 of the carrier of Polynom-Ring F_2, an extension E_1 of F_1, and an extension E_2 of F_2. Suppose $E_1 = E_2$ and $p_1 = p_2$. Then $\mathrm{Roots}(E_1, p_1) = \mathrm{Roots}(E_2, p_2)$.

(21) Let us consider a field F, extensions E, K of F, an extension U_1 of E, an extension U_2 of K, a subset T_1 of U_1, and a subset T_2 of U_2. Suppose $U_1 = U_2$ and $T_1 = T_2$ and $E \approx K$. Then $\mathrm{FAdj}(E, T_1) = \mathrm{FAdj}(K, T_2)$.
PROOF: $\mathrm{FAdj}(E, T_1)$ is a subfield of $\mathrm{FAdj}(K, T_2)$. $\mathrm{FAdj}(K, T_2)$ is a subfield of $\mathrm{FAdj}(E, T_1)$ by [9, (37)], [10, (7)], [11, (35),(37)]. □

(22) Let us consider a field F, an extension E of F, an E-extending extension K of F, a subset T_1 of K, and a finite subset T_2 of K. Suppose $T_1 \subseteq T_2$ and $E \approx \mathrm{FAdj}(F, T_1)$. Then $\mathrm{FAdj}(E, T_2) = \mathrm{FAdj}(F, T_2)$. The theorem is a consequence of (21) and (18).

(23) Let us consider a field F_1, a non constant element p_1 of the carrier of Polynom-Ring F_1, an extension F_2 of F_1, a non constant element p_2 of the carrier of Polynom-Ring F_2, a splitting field E of p_2, and an F_1-algebraic subset T of F_2. Suppose $T \subseteq \mathrm{Roots}(E, p_2)$ and $F_2 \approx \mathrm{FAdj}(F_1, T)$.

If $p_1 = p_2$, then E is a splitting field of p_1. The theorem is a consequence of (19).

(24) Let us consider a field F, an extension E of F, an F-extending extension K of E, and a non constant element p of the carrier of Polynom-Ring F. If p splits in E, then $\mathrm{Roots}(K, p) = \mathrm{Roots}(E, p)$.

(25) Let us consider a field F_1, an F_1-homomorphic field F_2, a homomorphism h from F_1 to F_2, and an element a of F_1. Then $(\mathrm{PolyHom}(h))(\mathrm{X}-a) = \mathrm{X}-h(a)$.

(26) Let us consider a field F_1, an F_1-isomorphic, F_1-homomorphic field F_2, an isomorphism h between F_1 and F_2, an extension E_1 of F_1, an extension E_2 of F_2, an element a of E_1, an element b of E_2, and an irreducible element p of the carrier of Polynom-Ring F_1. Suppose $\mathrm{ExtEval}(p, a) = 0_{E_1}$ and $\mathrm{ExtEval}((\mathrm{PolyHom}(h))(p), b) = 0_{E_2}$. Then $(\Psi(a, b, h, p))(a) = b$. The theorem is a consequence of (25).

2. Preliminaries about Ring Adjunctions

Let R_1, R_2 be rings. One can check that $R_1 \approx R_2$ if and only if the condition (Def. 1) is satisfied.

(Def. 1) R_1 is a subring of R_2 and R_2 is a subring of R_1.

Now we state the propositions:

(27) Let us consider a ring R. Then $R \approx R$.

(28) Let us consider rings R_1, R_2. If $R_1 \approx R_2$, then $R_2 \approx R_1$.

(29) Let us consider rings R_1, R_2, R_3. If $R_1 \approx R_2$ and $R_2 \approx R_3$, then $R_1 \approx R_3$.

(30) Let us consider a ring R, a ring extension S of R, and subsets T_1, T_2 of S. Suppose $T_1 \subseteq T_2$. Then $\mathrm{RAdj}(R, T_1)$ is a subring of $\mathrm{RAdj}(R, T_2)$.

(31) Let us consider a ring R, a ring extension S of R, subsets T_1, T_2 of S, a ring extension S_1 of $\mathrm{RAdj}(R, T_2)$, and a subset T_3 of S_1. Suppose $S_1 = S$ and $T_1 = T_3$. Then $\mathrm{RAdj}(R, T_1 \cup T_2) = \mathrm{RAdj}(\mathrm{RAdj}(R, T_2), T_3)$.

PROOF: $T_1 \cup T_2 \subseteq$ the carrier of $\mathrm{RAdj}(\mathrm{RAdj}(F, T_2), T_3)$. $\mathrm{RAdj}(F, T_2)$ is a subring of $\mathrm{RAdj}(F, T_1 \cup T_2)$. □

(32) Let us consider a ring R, a ring extension S of R, and a subset T of S. Then $\mathrm{RAdj}(R, T) \approx R$ if and only if T is a subset of R.

Let n be a natural number, R, S be non degenerated commutative rings, and x be a function from n into S. The functor $\mathrm{HomExtEval}(x, R)$ yielding a function from Polynom-Ring(n, R) into S is defined by

(Def. 2) for every polynomial p of n,R, $it(p) = \mathrm{ExtEval}(p, x)$.

Let R be a non degenerated commutative ring and S be a commutative ring extension of R. Let us observe that HomExtEval(x, R) is additive, multiplicative, and unity-preserving. Now we state the proposition:

(33) Let us consider a natural number n, and a field F. Then every extension of F is (Polynom-Ring(n, F))-homomorphic.

Let n be a natural number and F be a field. One can check that there exists an extension of F which is (Polynom-Ring(n, F))-homomorphic. Now we state the proposition:

(34) Let us consider a natural number n, fields F, E, and a function x from n into E. Then rng HomExtEval(x, F) = the set of all ExtEval(p, x) where p is a polynomial of n,F.

Let n be a natural number, F be a field, E be an extension of F, and x be a function from n into E. The functor ImageHomExtEval(x, F) yielding a strict double loop structure is defined by

(Def. 3) the carrier of it = rng HomExtEval(x, F) and the addition of it = (the addition of E) $\restriction$ rng HomExtEval(x, F) and the multiplication of it = (the multiplication of E) $\restriction$ rng HomExtEval(x, F) and the one of $it = 1_E$ and the zero of $it = 0_E$.

One can check that ImageHomExtEval(x, F) is non degenerated and ImageHomExtEval(x, F) is Abelian, add-associative, right zeroed, and right complementable and ImageHomExtEval(x, F) is commutative, associative, well unital, and distributive. Now we state the proposition:

(35) Let us consider a natural number n, a field F, an extension E of F, and a function x from n into E. Then F is a subring of ImageHomExtEval(x, F). The theorem is a consequence of (10), (9), and (34).

Let F be a field, T be a finite subset of F, and x be a function from $\overline{\overline{T}}$ into F. We say that x is T-evaluating if and only if

(Def. 4) x is one-to-one and rng $x = T$.

Let us note that there exists a function from $\overline{\overline{T}}$ into F which is T-evaluating and every function from $\overline{\overline{T}}$ into F which is T-evaluating is also T-valued and one-to-one. Now we state the propositions:

(36) Let us consider a field F, an extension E of F, a non empty, finite subset T of E, a bag b of $\overline{\overline{T}}$, and a T-evaluating function x from $\overline{\overline{T}}$ into E. Then eval$(b, x) \in$ the carrier of RAdj(F, T).

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every bag b of $\overline{\overline{T}}$ such that $\overline{\overline{\text{support } b}} = \$_1$ for every T-evaluating function x from $\overline{\overline{T}}$ into E, eval$(b, x) \in$ the carrier of RAdj(F, T). Set $n = \overline{\overline{T}}$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{\text{support } b}} = n$. $\square$

(37) Let us consider a field F, an extension E of F, a non empty, finite subset T of E, a polynomial p of $\overline{\overline{T}}$,F, and a T-evaluating function x from $\overline{\overline{T}}$ into E. Then $\mathrm{ExtEval}(p, x) \in$ the carrier of $\mathrm{RAdj}(F, T)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every polynomial p of $\overline{\overline{T}}$,F such that $\overline{\overline{\mathrm{Support}\, p}} = \$_1$ holds $\mathrm{ExtEval}(p, x) \in$ the carrier of $\mathrm{RAdj}(F, T)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. □

Let us consider a field F, an extension E of F, a non empty, finite subset T of E, and a T-evaluating function x from $\overline{\overline{T}}$ into E. Now we state the propositions:

(38) $\mathrm{RAdj}(F, T) = \mathrm{ImageHomExtEval}(x, F)$. The theorem is a consequence of (35).

(39) The carrier of $\mathrm{RAdj}(F, T) =$ the set of all $\mathrm{ExtEval}(p, x)$ where p is a polynomial of $\overline{\overline{T}}$,F. The theorem is a consequence of (38) and (34).

(40) Let us consider a field F, an extension E of F, and a finite subset T of E. If T is F-algebraic, then $\mathrm{FAdj}(F, T) = \mathrm{RAdj}(F, T)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every field F for every extension E of F for every finite subset T of E such that $\overline{\overline{T}} = \$_1$ holds if T is F-algebraic, then $\mathrm{FAdj}(F, T) = \mathrm{RAdj}(F, T)$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{T}} = n$. □

3. On Fixing Monomorphisms

Let R be a ring and S be a ring extension of R. Note that there exists a homomorphism of S which is R-fixing and there exists a monomorphism of S which is R-fixing and there exists an automorphism of S which is R-fixing. Now we state the propositions:

(41) Let us consider a field F, an extension E of F, an extension K of E, an element p of the carrier of Polynom-Ring F, and an F-fixing homomorphism h from E to K. Then $(\mathrm{PolyHom}(h))(p) = p$.

(42) Let us consider a field F, an extension E of F, an extension K of E, an element p of the carrier of Polynom-Ring F, an element a of E, and an F-fixing homomorphism h from E to K. Then $h(\mathrm{ExtEval}(p, a)) = \mathrm{ExtEval}(p, h(a))$. The theorem is a consequence of (41).

(43) Let us consider a field F, an extension E of F, an F-fixing monomorphism h of E, and a non zero element p of the carrier of Polynom-Ring F. Then $h^{\circ}(\mathrm{Roots}(E, p)) = \mathrm{Roots}(E, p)$.

(44) Let us consider a field F, an F-algebraic extension E of F, and an F-fixing monomorphism h of E. Then the carrier of $E \subseteq \mathrm{rng}\, h$. The theorem

is a consequence of (43).

(45) Let us consider a field F, and an F-algebraic extension E of F. Then every F-fixing monomorphism of E is an automorphism of E. The theorem is a consequence of (44).

Let F be a field and E be an F-algebraic extension of F. Let us observe that every F-fixing monomorphism of E is isomorphism. Now we state the propositions:

(46) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, and an F-algebraic subset T of E. Then $h^{\circ}T$ is F-algebraic. The theorem is a consequence of (42).

(47) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, a non empty, finite subset T of E, a bag b of $\overline{\overline{T}}$, and a T-evaluating function x from $\overline{\overline{T}}$ into E. Then $h(\mathrm{eval}(b,x)) \in$ the carrier of $\mathrm{RAdj}(F, h^{\circ}T)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every bag b of $\overline{\overline{T}}$ such that $\overline{\overline{\mathrm{support}\, b}} = \$_1$ for every T-evaluating function x from $\overline{\overline{T}}$ into E, $h(\mathrm{eval}(b, x)) \in$ the carrier of $\mathrm{RAdj}(F, h^{\circ}T)$. Set $n = \overline{\overline{T}}$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{\mathrm{support}\, b}} = n$. □

(48) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, a non empty, finite subset T of E, a polynomial p of $\overline{\overline{T}}$,F, and a T-evaluating function x from $\overline{\overline{T}}$ into E. Then $h(\mathrm{ExtEval}(p,x)) \in$ the carrier of $\mathrm{RAdj}(F, h^{\circ}T)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every polynomial p of $\overline{\overline{T}}$,F such that $\overline{\overline{\mathrm{Support}\, p}} = \$_1$ holds $h(\mathrm{ExtEval}(p,x)) \in$ the carrier of $\mathrm{RAdj}(F, h^{\circ}T)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. $\mathcal{P}[0]$ by [8, (5), (16)]. For every natural number k, $\mathcal{P}[k]$. □

(49) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, and a non empty, finite, F-algebraic subset T of E. Then $h^{\circ}(\text{the carrier of } \mathrm{FAdj}(F,T)) \subseteq$ the carrier of $\mathrm{FAdj}(F, h^{\circ}T)$. The theorem is a consequence of (46), (40), and (48).

(50) Let us consider a field F, an extension E of F, an E-extending extension K of F, and a finite, F-algebraic subset T of K. Suppose $T \subseteq$ the carrier of E. Then $\mathrm{FAdj}(F,T)$ is a subfield of E. The theorem is a consequence of (19).

(51) Let us consider a field F, an extension E of F, an E-extending extension

K of F, an F-fixing homomorphism h from E to (K **qua** extension of E), and a finite, F-algebraic subset T of E. Suppose $h^\circ T \subseteq$ the carrier of E. Then $\mathrm{FAdj}(F, h^\circ T)$ is a subfield of E. The theorem is a consequence of (42) and (19).

(52) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, and a non empty, finite, F-algebraic subset T of E. Suppose $h^\circ T \subseteq$ the carrier of E. Then $h^\circ(\text{the carrier of } \mathrm{FAdj}(F, T)) \subseteq$ the carrier of E. The theorem is a consequence of (51) and (49).

(53) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, and a non constant element p of the carrier of Polynom-Ring F. Suppose p splits in E. Then $h^\circ(\mathrm{Roots}(E, p)) \subseteq$ the carrier of E. The theorem is a consequence of (42) and (24).

4. NORMAL EXTENSIONS

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

(Def. 5) E is F-algebraic and for every irreducible element p of the carrier of Polynom-Ring F such that p has a root in E holds p splits in E.

Let us observe that every extension of F which is F-normal is also F-algebraic and every extension of F which is F-quadratic is also F-normal and every algebraic closure of F is F-normal and there exists an extension of F which is F-algebraic and F-normal and $\mathrm{FAdj}(\mathbb{F}_\mathbb{Q}, \{\sqrt[3]{2}\})$ is non $(\mathbb{F}_\mathbb{Q})$-normal. Now we state the proposition:

(54) Let us consider a field F, and an F-algebraic extension E of F. Then E is F-normal if and only if for every element a of E, $\mathrm{MinPoly}(a, F)$ splits in E.

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

(55) E is F-normal if and only if there exists a non constant element p of the carrier of Polynom-Ring F such that E is a splitting field of p.

(56) E is F-normal if and only if for every extension K of E, every F-fixing monomorphism of E and K is an automorphism of E.

Let F be a field and p be a non constant element of the carrier of Polynom-Ring F. One can verify that every splitting field of p is F-normal. Now we state the propositions:

(57) Let us consider a field F, an extension E of F, and an F-algebraic element a of E. Then $\mathrm{FAdj}(F, \{a\})$ is F-normal if and only if $\mathrm{MinPoly}(a, F)$ splits in $\mathrm{FAdj}(F, \{a\})$.

(58) Let us consider a field F, an extension E of F, and a non empty, finite, F-algebraic subset T of E. Then $\mathrm{FAdj}(F, T)$ is F-normal if and only if for every element a of T, $\mathrm{MinPoly}(a, F)$ splits in $\mathrm{FAdj}(F, T)$. The theorem is a consequence of (3), (6), and (4).

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

[4] 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.

[5] Serge Lang. *Algebra*. Springer Verlag, 2002 (Revised Third Edition).

[6] Knut Radbruch. *Algebra I*. Lecture Notes, University of Kaiserslautern, Germany, 1991.

[7] Piotr Rudnicki, Christoph Schwarzweller, and Andrzej Trybulec. Commutative algebra in the Mizar system. *Journal of Symbolic Computation*, 32(1/2):143–169, 2001. doi:10.1006/jsco.2001.0456.

[8] Christoph Schwarzweller. Artin's theorem towards the existence of algebraic closures. *Formalized Mathematics*, 30(**3**):199–207, 2022. doi:10.2478/forma-2022-0014.

[9] Christoph Schwarzweller. Existence and uniqueness of algebraic closures. *Formalized Mathematics*, 30(**4**):281–294, 2022. doi:10.2478/forma-2022-0022.

[10] Christoph Schwarzweller. Field extensions and Kronecker's construction. *Formalized Mathematics*, 27(**3**):229–235, 2019. doi:10.2478/forma-2019-0022.

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

[12] Christoph Schwarzweller. Splitting fields. *Formalized Mathematics*, 29(**3**):129–139, 2021. doi:10.2478/forma-2021-0013.

[13] Christoph Schwarzweller and Sara Burgoa. Splitting fields for the rational polynomials x^2-2, x^2+x+1, x^3-1, and x^3-2. *Formalized Mathematics*, 30(**1**):23–30, 2022. doi:10.2478/forma-2022-0003.

[14] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Algebraic extensions. *Formalized Mathematics*, 29(**1**):39–48, 2021. doi:10.2478/forma-2021-0004.

Accepted June 30, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 131–141, 2023
DOI: 10.2478/forma-2023-0012
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Antiderivatives and Integration[1]

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

Summary. In this paper, we introduce indefinite integrals [8] (antiderivatives) and proof integration by substitution in the Mizar system [2], [3]. In our previous article [15], we have introduced an indefinite-like integral, but it is inadequate because it must be an integral over the whole set of real numbers and in some sense it causes some duplication in the Mizar Mathematical Library [13]. For this reason, to define the antiderivative for a function, we use the derivative of an arbitrary interval as defined recently in [7]. Furthermore, antiderivatives are also used to modify the integration by substitution and integration by parts.

In the first section, we summarize the basic theorems on continuity and derivativity (for interesting survey of formalizations of real analysis in another proof-assistants like ACL2 [12], Isabelle/HOL [11], Coq [4], see [5]). In the second section, we generalize some theorems that were noticed during the formalization process. In the last section, we define the antiderivatives and formalize the integration by substitution and the integration by parts. We referred to [1] and [6] in our development.

MSC: 26A06 68V20

Keywords: antiderivative; integration by substitution

MML identifier: `INTEGR26`, version: `8.1.12 5.75.1447`

1. Basic Theorems on Continuity and Derivativity

From now on h, h_1 denote 0-convergent, non-zero sequences of real numbers and c, c_1 denote constant sequences of real numbers. Let us observe that every subset of $\mathbb{R}$ which is open interval is also open. Now we state the propositions:

[1]This work was supported by JSPS KAKENHI 23K11242.

(1) Let us consider an interval I. If $\inf I \in I$, then $\inf I = \inf I$.

(2) Let us consider an interval subset I of $\mathbb{R}$. If $\sup I \in I$, then $\sup I = \sup I$.

(3) Let us consider real numbers a, b, and an interval I. If a, $b \in I$, then $[a, b] \subseteq I$.

Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$ and real numbers a, b. Now we state the propositions:

(4) Suppose $a < b$ and $[a, b[\subseteq \operatorname{dom} f$ and $f \restriction [a, b[$ is continuous and f is differentiable on $]a, b[$ and $f'_{\restriction]a,b[}$ is right convergent in a. Then

(i) f is right differentiable in a, and

(ii) $f'_+(a) = \lim_{a^+} f'_{\restriction]a,b[}$.

PROOF: Consider e being a real number such that $a < e < b$. For every h and c such that $\operatorname{rng} c = \{a\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom} f$ and for every natural number n, $h(n) > 0$ holds $h^{-1} \cdot ((f_*(h + c)) - (f_*c))$ is convergent and $\lim(h^{-1} \cdot ((f_*(h + c)) - (f_*c))) = \lim_{a^+} f'_{\restriction]a,b[}$. □

(5) Suppose $a < b$ and $]a, b] \subseteq \operatorname{dom} f$ and $f \restriction]a, b]$ is continuous and f is differentiable on $]a, b[$ and $f'_{\restriction]a,b[}$ is left convergent in b. Then

(i) f is left differentiable in b, and

(ii) $f'_-(b) = \lim_{b^-} f'_{\restriction]a,b[}$.

PROOF: Consider e being a real number such that $a < e < b$. For every h and c such that $\operatorname{rng} c = \{b\}$ and $\operatorname{rng}(h + c) \subseteq \operatorname{dom} f$ and for every natural number n, $h(n) < 0$ holds $h^{-1} \cdot ((f_*(h + c)) - (f_*c))$ is convergent and $\lim(h^{-1} \cdot ((f_*(h + c)) - (f_*c))) = \lim_{b^-} f'_{\restriction]a,b[}$. □

(6) Let us consider real numbers a, b, x, a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and an interval I. Suppose $\inf I \leqslant a$ and $b \leqslant \sup I$ and $I \subseteq \operatorname{dom} f$ and $f \restriction I$ is continuous and $x \in]a, b[$. Then f is continuous in x.

(7) Let us consider an open subset X of $\mathbb{R}$, and partial functions f, F from $\mathbb{R}$ to $\mathbb{R}$. Suppose $X \subseteq \operatorname{dom} f$ and $f \restriction X$ is continuous. Let us consider a real number x. If $x \in X$, then f is continuous in x.

Let us consider real numbers a, b, x and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(8) Suppose $a \leqslant x < b$ and $]a, b[\subseteq \operatorname{dom} f$ and f is right convergent in x. Then

(i) $f \restriction]a, b[$ is right convergent in x, and

(ii) $\lim_{x^+}(f \restriction]a, b[) = \lim_{x^+} f$.

PROOF: For every real number r such that $x < r$ there exists a real number g such that $g < r$ and $x < g$ and $g \in \operatorname{dom}(f \restriction]a, b[)$. For every real number

r such that $0 < r$ there exists a real number d such that $x < d$ and for every real number x_1 such that $x_1 < d$ and $x < x_1$ and $x_1 \in \operatorname{dom}(f\restriction]a, b[)$ holds $|(f\restriction]a, b[)(x_1) - \lim_{x^+} f| < r$. □

(9) Suppose $a < x \leqslant b$ and $]a, b[\subseteq \operatorname{dom} f$ and f is left convergent in x. Then

(i) $f\restriction]a, b[$ is left convergent in x, and

(ii) $\lim_{x^-}(f\restriction]a, b[) = \lim_{x^-} f$.

PROOF: For every real number r such that $r < x$ there exists a real number g such that $r < g < x$ and $g \in \operatorname{dom}(f\restriction]a, b[)$. For every real number r such that $0 < r$ there exists a real number d such that $d < x$ and for every real number x_1 such that $d < x_1 < x$ and $x_1 \in \operatorname{dom}(f\restriction]a, b[)$ holds $|(f\restriction]a, b[)(x_1) - \lim_{x^-} f| < r$. □

(10) Suppose $[a, b] \subseteq \operatorname{dom} f$ and $f\restriction [a, b]$ is continuous and $x \in [a, b[$. Then

(i) f is right convergent in x, and

(ii) $\lim_{x^+}(f\restriction]a, b[) = f(x)$.

PROOF: For every real number r such that $x < r$ there exists a real number g such that $g < r$ and $x < g$ and $g \in \operatorname{dom} f$. For every real number r such that $0 < r$ there exists a real number s such that $x < s$ and for every real number x_1 such that $x_1 < s$ and $x < x_1$ and $x_1 \in \operatorname{dom} f$ holds $|f(x_1) - f(x)| < r$. For every real number r such that $0 < r$ there exists a real number s such that $x < s$ and for every real number x_1 such that $x_1 < s$ and $x < x_1$ and $x_1 \in \operatorname{dom}(f\restriction]a, b[)$ holds $|(f\restriction]a, b[)(x_1) - f(x)| < r$. $f\restriction]a, b[$ is right convergent in x and $\lim_{x^+}(f\restriction]a, b[) = \lim_{x^+} f$. □

(11) Suppose $[a, b] \subseteq \operatorname{dom} f$ and $f\restriction [a, b]$ is continuous and $x \in]a, b]$. Then

(i) f is left convergent in x, and

(ii) $\lim_{x^-}(f\restriction]a, b[) = f(x)$.

PROOF: For every real number r such that $r < x$ there exists a real number g such that $r < g < x$ and $g \in \operatorname{dom} f$. For every real number r such that $0 < r$ there exists a real number s such that $s < x$ and for every real number x_1 such that $s < x_1 < x$ and $x_1 \in \operatorname{dom} f$ holds $|f(x_1) - f(x)| < r$. For every real number r such that $0 < r$ there exists a real number s such that $s < x$ and for every real number x_1 such that $s < x_1 < x$ and $x_1 \in \operatorname{dom}(f\restriction]a, b[)$ holds $|(f\restriction]a, b[)(x_1) - f(x)| < r$. $f\restriction]a, b[$ is left convergent in x and $\lim_{x^-}(f\restriction]a, b[) = \lim_{x^-} f$. □

Let us consider a real number x, a partial function f from $\mathbb{R}$ to $\mathbb{R}$, a non empty interval I, and a subset X of $\mathbb{R}$. Now we state the propositions:

(12) If $I \subseteq X$ and $x \in I$ and $x \neq \sup I$, then f is right differentiable in x iff $f\restriction X$ is right differentiable in x.

(13) If $I \subseteq X$ and $x \in I$ and $x \neq \inf I$, then f is left differentiable in x iff $f\restriction X$ is left differentiable in x.

(14) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, an open subset I of $\mathbb{R}$, and a subset X of $\mathbb{R}$. Suppose $I \subseteq X$. Then f is differentiable on I if and only if $f\restriction X$ is differentiable on I.

Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, a non empty interval I, and a subset X of $\mathbb{R}$. Now we state the propositions:

(15) If $I \subseteq X$, then f is differentiable on interval I iff $f\restriction X$ is differentiable on interval I. The theorem is a consequence of (1), (12), (2), (13), and (14).

(16) If $I \subseteq X$ and f is differentiable on interval I, then $f'_I = (f\restriction X)'_I$. The theorem is a consequence of (15), (1), and (2).

(17) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and non empty intervals I, J. Suppose f is differentiable on interval I and $J \subseteq I$ and $\inf J < \sup J$. Then $f'_I\restriction J = f'_J$.
PROOF: For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom}(f'_I\restriction J)$ holds $(f'_I\restriction J)(x) = f'_J(x)$. □

2. Generalization of Previous Theorems

Now we state the propositions:

(18) Let us consider extended real numbers a, b. If $a < b$, then there exists a real number c such that $a < c < b$.

(19) Let us consider extended real numbers p, q, and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Suppose f is differentiable on $]p, q[$ and for every real number x such that $x \in]p, q[$ holds $f'(x) = 0$. Then $f\restriction]p, q[$ is constant.

(20) Let us consider extended real numbers p, q, and partial functions f_1, f_2 from $\mathbb{R}$ to $\mathbb{R}$. Suppose f_1 is differentiable on $]p, q[$ and f_2 is differentiable on $]p, q[$ and for every real number x such that $x \in]p, q[$ holds ${f_1}'(x) = {f_2}'(x)$. Then

(i) $(f_1 - f_2)\restriction]p, q[$ is constant, and

(ii) there exists a real number r such that for every real number x such that $x \in]p, q[$ holds $f_1(x) = f_2(x) + r$.

The theorem is a consequence of (19).

Let us consider extended real numbers p, q and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(21) Suppose f is differentiable on $]p, q[$ and for every real number x such that $x \in]p, q[$ holds $0 < f'(x)$. Then $f\restriction]p, q[$ is increasing.

(22) Suppose f is differentiable on $]p,q[$ and for every real number x such that $x \in]p,q[$ holds $f'(x) < 0$. Then $f\restriction]p,q[$ is decreasing.

(23) Suppose f is differentiable on $]p,q[$ and for every real number x such that $x \in]p,q[$ holds $0 \leqslant f'(x)$. Then $f\restriction]p,q[$ is non-decreasing.

(24) Suppose f is differentiable on $]p,q[$ and for every real number x such that $x \in]p,q[$ holds $f'(x) \leqslant 0$. Then $f\restriction]p,q[$ is non-increasing.

(25) Let us consider an open subset X of $\mathbb{R}$, a real number x_0, and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Suppose $x_0 \in X$ and f is differentiable on X. Then $f'(x_0) = (f\restriction X)'(x_0)$.

PROOF: Consider N being a neighbourhood of x_0 such that $N \subseteq \operatorname{dom}(f\restriction X)$ and there exists a linear function L and there exists a rest R such that $(f\restriction X)'(x_0) = L(1)$ and for every real number x such that $x \in N$ holds $(f\restriction X)(x) - (f\restriction X)(x_0) = L(x-x_0) + R(x-x_0)$. Consider L being a linear function, R being a rest such that $(f\restriction X)'(x_0) = L(1)$ and for every real number x such that $x \in N$ holds $(f\restriction X)(x) - (f\restriction X)(x_0) = L(x-x_0) + R(x-x_0)$. For every real number x such that $x \in N$ holds $f(x) - f(x_0) = L(x-x_0) + R(x-x_0)$. □

(26) Let us consider real numbers a, b, and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Suppose $a < b$ and $[a,b] \subseteq \operatorname{dom} f$ and $f\restriction[a,b]$ is continuous. Then there exists a partial function F from $\mathbb{R}$ to $\mathbb{R}$ such that

(i) $]a,b[\subseteq \operatorname{dom} F$, and

(ii) for every real number x such that $x \in]a,b[$ holds $F(x) = \int_a^x f(x)dx$, and

(iii) F is differentiable on $]a,b[$, and

(iv) $F'_{\restriction]a,b[} = f\restriction]a,b[$.

PROOF: Consider x_0 being a real number such that $a < x_0 < b$. Consider F being a partial function from $\mathbb{R}$ to $\mathbb{R}$ such that $]a,b[\subseteq \operatorname{dom} F$ and for every real number x such that $x \in]a,b[$ holds $F(x) = \int_a^x f(x)dx$ and F is differentiable in x_0 and $F'(x_0) = f(x_0)$. For every real number x such that $x \in]a,b[$ holds $F\restriction]a,b[$ is differentiable in x. For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom} F'_{\restriction]a,b[}$ holds $F'_{\restriction]a,b[}(x) = (f\restriction]a,b[)(x)$. □

(27) Let us consider real numbers a, b, and partial functions f, F from $\mathbb{R}$ to $\mathbb{R}$. Suppose $a < b$ and $[a,b] \subseteq \operatorname{dom} f$ and $f\restriction[a,b]$ is continuous and $]a,b[\subseteq \operatorname{dom} F$ and for every real number x such that $x \in]a,b[$ holds

$F(x) = \int_a^x f(x)dx$. Then

(i) F is differentiable on $]a, b[$, and

(ii) $F'_{\restriction]a,b[} = f \restriction]a, b[$.

PROOF: Consider G being a partial function from $\mathbb{R}$ to $\mathbb{R}$ such that $]a, b[\subseteq \operatorname{dom} G$ and for every real number x such that $x \in]a, b[$ holds $G(x) = \int_a^x f(x)dx$ and G is differentiable on $]a, b[$ and $G'_{\restriction]a,b[} = f \restriction]a, b[$. For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom}(F \restriction]a, b[)$ holds $(F \restriction]a, b[)(x) = (G \restriction]a, b[)(x)$. □

3. Antiderivatives and Related Theorems

Let f, F be partial functions from $\mathbb{R}$ to $\mathbb{R}$ and I be a non empty interval. We say that F is antiderivative of f on I if and only if

(Def. 1) F is differentiable on interval I and $F'_I = f \restriction I$.

Now we state the propositions:

(28) Let us consider partial functions f, F, g, G from $\mathbb{R}$ to $\mathbb{R}$, and a non empty interval I. Suppose F is antiderivative of f on I and G is antiderivative of g on I. Then

(i) $F + G$ is antiderivative of $f + g$ on I, and

(ii) $F - G$ is antiderivative of $f - g$ on I.

(29) Let us consider partial functions f, F from $\mathbb{R}$ to $\mathbb{R}$, a non empty interval I, and a real number r. If F is antiderivative of f on I, then $r \cdot F$ is antiderivative of $r \cdot f$ on I.

Let us consider partial functions f, g, F, G from $\mathbb{R}$ to $\mathbb{R}$ and a non empty interval I. Now we state the propositions:

(30) If F is antiderivative of f on I and G is antiderivative of g on I, then $F \cdot G$ is antiderivative of $f \cdot G + F \cdot g$ on I.

(31) Suppose F is antiderivative of f on I and G is antiderivative of g on I and for every set x such that $x \in I$ holds $G(x) \neq 0$. Then $\frac{F}{G}$ is antiderivative of $\frac{f \cdot G - F \cdot g}{G \cdot G}$ on I.

(32) Let us consider real numbers a, b, and partial functions f, F from $\mathbb{R}$ to $\mathbb{R}$. Suppose $a \leqslant b$ and $[a, b] \subseteq \operatorname{dom} f$ and $f \restriction [a, b]$ is continuous and $[a, b] \subseteq \operatorname{dom} F$ and for every real number x such that $x \in [a, b]$ holds

$F(x) = \int_a^x f(x)dx$. Let us consider a real number x. Suppose $x \in]a, b[$. Then

(i) F is differentiable in x, and

(ii) $F'(x) = f(x)$.

PROOF: Set $O =]a, b[$. Define $\mathcal{G}_0$(real number) $= (\int_a^{\$_1} f(x)dx)(\in \mathbb{R})$. Consider G_1 being a function from $\mathbb{R}$ into $\mathbb{R}$ such that for every element h of $\mathbb{R}$, $G_1(h) = \mathcal{G}_0(h)$. Reconsider $G = G_1 \restriction O$ as a partial function from $\mathbb{R}$ to $\mathbb{R}$. For every real number x such that $x \in O$ holds G is differentiable in x and $G'(x) = f(x)$ by (6), [9, (10),(11)]. For every real number x such that $x \in]a, b[$ holds F is differentiable in x and $F'(x) = f(x)$ by [14, (2)]. □

Let us consider real numbers a, b and partial functions f, F from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(33) Suppose $a \leqslant b$ and $[a, b] \subseteq \operatorname{dom} f$ and $f \restriction [a, b]$ is bounded and f is integrable on $[a, b]$ and $[a, b] = \operatorname{dom} F$ and for every real number x such that $x \in [a, b]$ holds $F(x) = \int_a^x f(x)dx$. Then F is Lipschitzian.

PROOF: Consider r_0 being a real number such that for every object x such that $x \in [a, b] \cap \operatorname{dom} f$ holds $|f(x)| \leqslant r_0$. Reconsider $r = \max(r_0, 1)$ as a real number. For every real numbers p, q such that p, $q \in [a, b]$ and $p \leqslant q$ holds f is integrable on $[p, q]$ and $f \restriction [p, q]$ is bounded. For every real numbers x_1, x_2 such that x_1, $x_2 \in \operatorname{dom} F$ holds $|F(x_1) - F(x_2)| \leqslant r \cdot |x_1 - x_2|$ by [10, (20),(23)]. □

(34) Suppose $a < b$ and $[a, b] \subseteq \operatorname{dom} f$ and $f \restriction [a, b]$ is continuous and $[a, b] \subseteq \operatorname{dom} F$ and for every real number x such that $x \in [a, b]$ holds $F(x) = \int_a^x f(x)dx$. Then $F'_{\restriction]a,b[}$ is right convergent in a and left convergent in b.

PROOF: For every real number x such that $x \in]a, b[$ holds $F \restriction]a, b[$ is differentiable in x. For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom} F'_{\restriction]a,b[}$ holds $F'_{\restriction]a,b[}(x) = (f \restriction]a, b[)(x)$. For every real number r such that $a < r$ there exists a real number g such that $g < r$ and $a < g$ and $g \in \operatorname{dom} F'_{\restriction]a,b[}$. For every real number g_1 such that $0 < g_1$ there exists a real number r such that $a < r$ and for every real number r_1 such that $r_1 < r$ and $a < r_1$ and $r_1 \in \operatorname{dom} F'_{\restriction]a,b[}$ holds $|F'_{\restriction]a,b[}(r_1) - f(a)| < g_1$. For every real number r such that $r < b$ there exists a real number g such that $r < g < b$ and $g \in \operatorname{dom} F'_{\restriction]a,b[}$. For every real number g_1 such that $0 < g_1$ there exists

a real number r such that $r < b$ and for every real number r_1 such that $r < r_1 < b$ and $r_1 \in \operatorname{dom} F'_{\restriction]a,b[}$ holds $|F'_{\restriction]a,b[}(r_1) - f(b)| < g_1$. $\square$

(35) Suppose $a < b$ and $[a,b] \subseteq \operatorname{dom} f$ and $f \restriction [a,b]$ is continuous and $[a,b] \subseteq \operatorname{dom} F$ and for every real number x such that $x \in [a,b]$ holds $F(x) = \int_a^x f(x)dx$. Then

(i) F is right differentiable in a, and

(ii) $F'_+(a) = \lim_{a^+} F'_{\restriction]a,b[}$.

PROOF: For every real number x such that $x \in]a,b[$ holds $F \restriction]a,b[$ is differentiable in x. $F'_{\restriction]a,b[}$ is right convergent in a. For every real number x such that $x \in [a,b]$ holds $(F \restriction [a,b])(x) = \int_a^x f(x)dx$. $F \restriction [a,b[$ is Lipschitzian. $\square$

(36) Suppose $a < b$ and $[a,b] \subseteq \operatorname{dom} f$ and $f \restriction [a,b]$ is continuous and $[a,b] \subseteq \operatorname{dom} F$ and for every real number x such that $x \in [a,b]$ holds $F(x) = \int_a^x f(x)dx$. Then

(i) F is left differentiable in b, and

(ii) $F'_-(b) = \lim_{b^-} F'_{\restriction]a,b[}$.

PROOF: For every real number x such that $x \in]a,b[$ holds $F \restriction]a,b[$ is differentiable in x. $F'_{\restriction]a,b[}$ is left convergent in b. For every real number x such that $x \in [a,b]$ holds $(F \restriction [a,b])(x) = \int_a^x f(x)dx$. $F \restriction]a,b]$ is Lipschitzian. $\square$

(37) Suppose $a < b$ and $[a,b] \subseteq \operatorname{dom} f$ and $f \restriction [a,b]$ is continuous and $[a,b] \subseteq \operatorname{dom} F$ and for every real number x such that $x \in [a,b]$ holds $F(x) = \int_a^x f(x)dx$. Then

(i) F is differentiable on interval $[a,b]$, and

(ii) $F'_{[a,b]} = f \restriction [a,b]$.

PROOF: Reconsider $I = [a,b]$ as a non empty interval. If $\inf I \in I$, then F is right differentiable in $\inf I$. If $\sup I \in I$, then F is left differentiable in $\sup I$. For every real number x such that $x \in]a,b[$ holds $F \restriction]a,b[$ is differentiable in x. $F'_{\restriction]a,b[} = f \restriction]a,b[$. For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom} F'_{[a,b]}$ holds $F'_{[a,b]}(x) = (f \restriction [a,b])(x)$. $\square$

(38) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and real numbers a, b. Then $\int_b^a f(x)dx = -\int_a^b f(x)dx$.

(39) Let us consider real numbers a, b, and partial functions f, F from $\mathbb{R}$ to $\mathbb{R}$. Suppose $a < b$ and $[a,b] \subseteq \operatorname{dom} f$ and $f\restriction[a,b]$ is continuous and $[a,b] \subseteq \operatorname{dom} F$ and for every real number x such that $x \in [a,b]$ holds $F(x) = \int_a^x f(x)dx$. Let us consider a real number x. Suppose $x \in]a,b[$. Then

(i) F is differentiable in x, and

(ii) $F'(x) = f(x)$.

The theorem is a consequence of (37).

(40) Let us consider real numbers a, b, and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Suppose $a < b$ and $[a,b] \subseteq \operatorname{dom} f$ and $f\restriction[a,b]$ is continuous. Then there exists a partial function F from $\mathbb{R}$ to $\mathbb{R}$ such that

(i) F is antiderivative of f on $[a,b]$, and

(ii) for every real number x such that $x \in [a,b]$ holds $F(x) = \int_a^x f(x)dx$.

The theorem is a consequence of (37).

(41) Let us consider a real number c, partial functions f, F, G from $\mathbb{R}$ to $\mathbb{R}$, and a non empty interval I. Suppose $I \subseteq \operatorname{dom} f$ and F is antiderivative of f on I and $I \subseteq \operatorname{dom} G$ and for every real number x such that $x \in I$ holds $G(x) = F(x) + c$. Then G is antiderivative of f on I.

PROOF: Reconsider $c_0 = c$ as an element of $\mathbb{R}$. Define $\mathcal{F}(\text{element of } \mathbb{R}) = c_0$. Consider F_0 being a function from $\mathbb{R}$ into $\mathbb{R}$ such that for every element x of $\mathbb{R}$, $F_0(x) = \mathcal{F}(x)$. $F\restriction I$ is differentiable on interval I. G is differentiable on interval I. □

(42) Let us consider partial functions f, F from $\mathbb{R}$ to $\mathbb{R}$, and non empty intervals I, J. Suppose $\inf I < \sup I$ and $I \subseteq J$ and F is antiderivative of f on J. Then F is antiderivative of f on I.

(43) Let us consider real numbers a, b, a partial function f from $\mathbb{R}$ to $\mathbb{R}$, and a partition D of $[a,b]$. Suppose $a < b$ and f is differentiable on interval $[a,b]$ and $f'_{[a,b]}$ is bounded. Then $\operatorname{lower\_sum}(f'_{[a,b]} \restriction [a,b], D) \leqslant f(b) - f(a) \leqslant \operatorname{upper\_sum}(f'_{[a,b]} \restriction [a,b], D)$.

(44) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, real numbers a, b, and a non empty interval I. Suppose a, $b \in I$ and $a < b$ and f is differentiable

on interval I and f'_I is integrable on $[a,b]$ and f'_I is bounded. Then

(i) $\int_a^b f'_{[a,b]}(x)dx = f(b) - f(a)$, and

(ii) $\int_a^b f'_I(x)dx = f(b) - f(a)$.

The theorem is a consequence of (3) and (17).

(45) Let us consider a partial function f from $\mathbb{R}$ to $\mathbb{R}$, a real number a, and a non empty interval I. Suppose f is differentiable on interval I and $a \in I$. Then $\int_a^a f'_I(x)dx = 0$. The theorem is a consequence of (3).

(46) Let us consider partial functions f, F, G from $\mathbb{R}$ to $\mathbb{R}$, and a non empty interval I. Suppose F is antiderivative of f on I and G is antiderivative of f on I. Then there exists a real number c such that for every real number x such that $x \in I$ holds $F(x) = G(x) + c$. The theorem is a consequence of (42), (1), (2), and (18).

(47) Integration by substitution:
Let us consider real numbers a, b, p, q, and partial functions f, g from $\mathbb{R}$ to $\mathbb{R}$. Suppose $a < b$ and $p < q$ and $[a,b] \subseteq \operatorname{dom} f$ and $f\restriction[a,b]$ is continuous and g is differentiable on interval $[p,q]$ and $g'_{[p,q]}$ is integrable on $[p,q]$ and $g'_{[p,q]}$ is bounded and $\operatorname{rng}(g\restriction[p,q]) \subseteq [a,b]$ and $g(p) = a$ and $g(q) = b$. Then $\int_a^b f(x)dx = \int_p^q (f \cdot g \cdot g'_{[p,q]})(x)dx$. The theorem is a consequence of (37).

(48) Let us consider real numbers a, b, and partial functions f, g from $\mathbb{R}$ to $\mathbb{R}$. Suppose $a < b$ and f is differentiable on interval $[a,b]$ and g is differentiable on interval $[a,b]$ and $f'_{[a,b]}$ is integrable on $[a,b]$ and $f'_{[a,b]}$ is bounded and $g'_{[a,b]}$ is integrable on $[a,b]$ and $g'_{[a,b]}$ is bounded. Then $\int_a^b (f'_{[a,b]} \cdot g)(x)dx = f(b) \cdot g(b) - f(a) \cdot g(a) - \int_a^b (f \cdot g'_{[a,b]})(x)dx$.

References

[1] Tom M. Apostol. *Calculus*, volume I. John Wiley & Sons, second edition, 1967.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in*

Computer Science, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[3] 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.

[4] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Improving real analysis in Coq: A user-friendly approach to integrals and derivatives. In Chris Hawblitzel and Dale Miller, editors, *Certified Programs and Proofs – Second International Conference, CPP 2012, Kyoto, Japan, December 13–15, 2012. Proceedings*, volume 7679 of *Lecture Notes in Computer Science*, pages 289–304. Springer, 2012. doi:10.1007/978-3-642-35308-6_22.

[5] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Formalization of real analysis: A survey of proof assistants and libraries. *Mathematical Structures in Computer Science*, 26:1196–1233, 2015.

[6] Richard Courant and Edward James McShane. *Differential and Integral Calculus*. John Wiley & Sons, 1988.

[7] Noboru Endou. Differentiation on interval. *Formalized Mathematics*, 31(1):9–21, 2023. doi:10.2478/forma-2023-0002.

[8] Noboru Endou. Improper integral. Part II. *Formalized Mathematics*, 29(**4**):279–294, 2021. doi:10.2478/forma-2021-0024.

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

[10] Noboru Endou, Yasunari Shidama, and Masahiko Yamazaki. Integrability and the integral of partial functions from $\mathbb{R}$ into $\mathbb{R}$. *Formalized Mathematics*, 14(**4**):207–212, 2006. doi:10.2478/v10037-006-0023-y.

[11] Jacques D. Fleuriot. On the mechanization of real analysis in Isabelle/HOL. In Mark Aagaard and John Harrison, editors, *Theorem Proving in Higher Order Logics*, pages 145–161. Springer Berlin Heidelberg, 2000. ISBN 978-3-540-44659-0.

[12] Ruben Gamboa. *Continuity and Differentiability*, pages 301–315. Springer US, 2000. ISBN 978-1-4757-3188-0. doi:10.1007/978-1-4757-3188-0_18.

[13] Adam Grabowski and Christoph Schwarzweller. On duplication in mathematical repositories. In Serge Autexier, Jacques Calmet, David Delahaye, Patrick D. F. Ion, Laurence Rideau, Renaud Rioboo, and Alan P. Sexton, editors, *Intelligent Computer Mathematics, 10th International Conference, AISC 2010, 17th Symposium, Calculemus 2010, and 9th International Conference, MKM 2010, Paris, France, July 5–10, 2010. Proceedings*, volume 6167 of *Lecture Notes in Computer Science*, pages 300–314. Springer, 2010. doi:10.1007/978-3-642-14128-7_26.

[14] Sora Otsuki, Pauline N. Kawamoto, and Hiroshi Yamazaki. A simple example for linear partial differential equations and its solution using the method of separation of variables. *Formalized Mathematics*, 27(**1**):25–34, 2019. doi:10.2478/forma-2019-0003.

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

Accepted June 30, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 143–150, 2023
DOI: 10.2478/forma-2023-0013
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Embedding Principle for Rings and Abelian Groups

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

Summary. The article concerns about formalizing a certain lemma on embedding of algebraic structures in the Mizar system, claiming that if a ring A is embedded in a ring B then there exists a ring C which is isomorphic to B and includes A as a subring. This construction applies to algebraic structures such as Abelian groups and rings.

MSC: 13B25 68V20

Keywords: Abelian group; ring; embedding

MML identifier: RING_EMB, version: 8.1.14 5.76.1452

Introduction

The article concerns about formalizing a certain lemma on embedding of algebraic structures in the Mizar system [2], [3], along with the lemma appeared in the book [12] at §13 of Chapter 1. The lemma claims that if a ring A is embedded in a ring B then there exists a ring C which is isomorphic to B and includes A as a subring [11]. A basic idea to prove the lemma is that for given monomorphism φ from A to B, one can obtain such ring C by introducing the addition and multiplication on the set $(B \setminus \varphi(A)) \cup A$, while B does not meet A. The same argument has already been discussed and formalized in [9] in line with field extensions [10] (recently reused to formalize algebraic closures, see e.g. [8]).

We treat here a general case, namely the case of B meets A, it is enough to create a set X which does not meet A and $X \cong B \setminus \varphi(A)$ and construct a new

ring C from the set $(X \cong B \setminus \varphi(A)) \cup A$. The formalized lemma can be applied to another algebraic structures such as Abelian groups as shown in the article as well with the same formulation of rings [6].

We need the following 3 steps required for precise arguments and formalization to construct the target object C:

Step 1. Prepare a set X which does not meet A and isomorphic to $B \setminus \varphi(A)$ as set-theoretical. The step is coded in Theorem 1 and 2;

Step 2. Make a $X \setminus S$ a ring as C, corresponds to Theorem 7 and 12 for rings and for Abelian groups, respectively;

Step 3. Construct an isomorphism $G : A \xrightarrow{\sim} C$ such that $\iota = G \circ \varphi$ is an identity mapping. Corresponding formal counterparts are Theorem 9 and 14 for rings and for Abelian groups, respectively.

As a consequence of the principle, taking Polynom-Ring(A) as B, we have a polynomial ring over A with indeterminate X and includes A as a subring, say $A[X] = C$. Here Polynom-Ring(A) is existing formalized ring of polynomials [4], which is constructed by sequences. An indeterminate X is defined by the image of $(0, 1, 0, 0, \cdots) \in$ Polynom-Ring(A) by the map G of Step 3. Some of the Mizar functors had to be defined additionally as we used the groups not in their multiplicative version [1], [7], which is more common in the Mizar Mathematical Library, but in the additive setting [5].

1. Preliminaries from Set Theory

From now on a denotes a non empty set and b, x, o denote objects.

Now we state the propositions:

(1) There exists an object b such that for every set x, $\langle x, b \rangle \notin a$.

(2) Let us consider non empty sets a, b. Then there exists a non empty set c such that

(i) $a \cap c = \emptyset$, and

(ii) there exists a function f such that f is one-to-one and $\operatorname{dom} f = b$ and $\operatorname{rng} f = c$.

Proof: Consider d being an object such that for every set x, $\langle x, d \rangle \notin a$. Set $C = b \times \{d\}$. Consider f being a function such that f is one-to-one and $\operatorname{dom} f = b$ and $\operatorname{rng} f = C$. $a \cap C = \emptyset$. $\square$

2. EMBEDDING PRINCIPLE APPLIED TO RINGS

Now we state the proposition:

(3) Let us consider a ring A, a non empty set X, a function f from A into X, and elements a, b of X. Suppose f is bijective. Then $f((\text{the addition of } A)((f^{-1})(a), (f^{-1})(b)))$ is an element of X.

Let A be a ring, X be a non empty set, f be a function from A into X, and a, b be elements of X. Assume f is bijective. The functor addemb(f, a, b) yielding an element of X is defined by the term

(Def. 1) $f((\text{the addition of } A)((f^{-1})(a), (f^{-1})(b)))$.

Now we state the proposition:

(4) Let us consider a ring A, a non empty set X, a function f from A into X, and elements a, b, c of X. Suppose f is bijective. Then addemb$(f, a,$ addemb $(f, b, c)) =$ addemb$(f,$ addemb$(f, a, b), c)$.

Let A be a ring, X be a non empty set, and f be a function from A into X. The functor addemb(f) yielding a binary operation on X is defined by

(Def. 2) for every elements a, b of X, $it(a, b) =$ addemb(f, a, b).

Now we state the proposition:

(5) Let us consider a ring A, a non empty set X, a function f from A into X, and elements a, b of X. Suppose f is bijective. Then $f((\text{the multiplication of } A)((f^{-1})(a), (f^{-1})(b)))$ is an element of X.

Let A be a ring, X be a non empty set, f be a function from A into X, and a, b be elements of X. Assume f is bijective. The functor multemb(f, a, b) yielding an element of X is defined by the term

(Def. 3) $f((\text{the multiplication of } A)((f^{-1})(a), (f^{-1})(b)))$.

The functor multemb(f) yielding a binary operation on X is defined by

(Def. 4) for every elements a, b of X, $it(a, b) =$ multemb(f, a, b).

The functor embRing(f) yielding a strict, non empty double loop structure is defined by the term

(Def. 5) $\langle X,$ addemb$(f),$ multemb$(f), f(1_A), f(0_A)\rangle$.

Now we state the propositions:

(6) Let us consider a ring A, a non empty set X, and a function f from A into X. If f is bijective, then embRing(f) is a ring.

PROOF: Reconsider $Z_1 = \langle X,$ addemb$(f),$ multemb$(f), f(1_A), f(0_A)\rangle$ as a non empty double loop structure. For every elements v, w of Z_1, $v+w = w+v$. For every elements u, v, w of Z_1, $u+(v+w) = (u+v)+w$. For every element v of Z_1, $v+0_{Z_1} = v$. Every element of Z_1 is right complementable. For every elements a, b, v of Z_1, $(a+b)\cdot v = a\cdot v + b\cdot v$. For every elements

a, b, v of Z_1, $v \cdot (a+b) = v \cdot a + v \cdot b$ and $(a+b) \cdot v = a \cdot v + b \cdot v$. For every elements a, b, v of Z_1, $(a \cdot b) \cdot v = a \cdot (b \cdot v)$. For every element v of Z_1, $v \cdot (1_{Z_1}) = v$ and $1_{Z_1} \cdot v = v$. □

(7) Let us consider a commutative ring A, a non empty set X, and a function f from A into X. If f is bijective, then embRing(f) is a commutative ring.
PROOF: embRing(f) is commutative. □

(8) Let us consider rings A, B, and a function i from A into B. Suppose i inherits ring homomorphism and $i = \mathrm{id}_A$. Then A is a subring of B.
PROOF: For every object o such that $o \in$ the carrier of A holds $o \in$ the carrier of B. The addition of $A =$ (the addition of B) $\restriction$ (the carrier of A). The multiplication of $A =$ (the multiplication of B) $\restriction$ (the carrier of A). □

(9) Let us consider rings A, B, and a function f from A into B. Suppose f is monomorphic and $\Omega_B \setminus (\operatorname{rng} f) \neq \emptyset$. Then there exists a ring C and there exists a set X and there exists a function h and there exists a function G from B into C such that $X \cap \Omega_A = \emptyset$ and h is one-to-one and $\operatorname{dom} h = \Omega_B \setminus (\operatorname{rng} f)$ and $\operatorname{rng} h = X$ and $\Omega_C = X \cup \Omega_A$ and A is a subring of C and G inherits ring isomorphism and $\mathrm{id}_A = G \cdot f$.
PROOF: Consider X being a non empty set such that $\Omega_A \cap X = \emptyset$ and there exists a function h such that h is one-to-one and $\operatorname{dom} h = \Omega_B \setminus (\operatorname{rng} f)$ and $\operatorname{rng} h = X$. Consider h being a function such that h is one-to-one and $\operatorname{dom} h = \Omega_B \setminus (\operatorname{rng} f)$ and $\operatorname{rng} h = X$ and $\Omega_A \cap X = \emptyset$.

Define $\mathcal{P}$[element of B, element of $\Omega_A \cup X$] $\equiv$ \$1 $\in \operatorname{rng} f$ and (f^{-1})(\$1) = \$2 or \$1 $\notin \operatorname{rng} f$ and \$2 $= h$(\$1). Set $C_1 = \Omega_A \cup X$. Consider g being a function from the carrier of B into C_1 such that for every element x of B, $\mathcal{P}[x, g(x)]$. g is bijective. Reconsider $C = \mathrm{embRing}(g)$ as a non empty ring. Reconsider $G = g$ as a function from B into C. G is linear. For every o such that $o \in \Omega_A$ holds $(G \cdot f)(o) = o$. A is a subring of C. □

3. Embedding Principle Applied to Abelian Groups

Let G be an Abelian group. A subgroup of G is an Abelian group defined by

(Def. 6) the carrier of $it \subseteq$ the carrier of G and the addition of $it =$ (the addition of G) $\restriction$ (the carrier of it) and $0_{it} = 0_G$.

Let G, H be Abelian groups and f be a homomorphism from G to H. The functor Im f yielding a strict additive loop structure is defined by

(Def. 7) the carrier of $it = \operatorname{rng} f$ and the addition of $it =$ (the addition of H) $\restriction$ $\operatorname{rng} f$ and the zero of $it = 0_H$.

Now we state the proposition:

(10) Let us consider an Abelian group A, a non empty set X, a function f from A into X, and elements a, b of X. Suppose f is bijective. Then $f((\text{the addition of } A)((f^{-1})(a), (f^{-1})(b)))$ is an element of X.

Let A be an Abelian group, X be a non empty set, f be a function from A into X, and a, b be elements of X. Assume f is bijective. The functor $\mathrm{addemb}(f, a, b)$ yielding an element of X is defined by the term

(Def. 8) $f((\text{the addition of } A)((f^{-1})(a), (f^{-1})(b)))$.

Now we state the proposition:

(11) Let us consider an Abelian group A, a non empty set X, a function f from A into X, and elements a, b, c of X. Suppose f is bijective. Then $\mathrm{addemb}(f, a, \mathrm{addemb}(f, b, c)) = \mathrm{addemb}(f, \mathrm{addemb}(f, a, b), c)$.

Let A be an Abelian group, X be a non empty set, and f be a function from A into X. The functor $\mathrm{addemb}(f)$ yielding a binary operation on X is defined by

(Def. 9) for every elements a, b of X, $it(a, b) = \mathrm{addemb}(f, a, b)$.

The functor $\mathrm{embAbGr}(f)$ yielding a strict, non empty additive loop structure is defined by the term

(Def. 10) $\langle X, \mathrm{addemb}(f), f(0_A)\rangle$.

Now we state the propositions:

(12) Let us consider an Abelian group A, a non empty set X, and a function f from A into X. If f is bijective, then $\mathrm{embAbGr}(f)$ is an Abelian group.
PROOF: Reconsider $Z_1 = \langle X, \mathrm{addemb}(f), f(0_A)\rangle$ as a non empty additive loop structure. For every elements v, w of Z_1, $v + w = w + v$. For every elements u, v, w of Z_1, $u + (v + w) = (u + v) + w$. For every element v of Z_1, $v + 0_{Z_1} = v$. Every element of Z_1 is right complementable. □

(13) Let us consider Abelian groups A, B, and a homomorphism i from A to B. If $i = \mathrm{id}_A$, then A is a subgroup of B.
PROOF: For every object o such that $o \in$ the carrier of A holds $o \in$ the carrier of B. The addition of $A =$ (the addition of B) $\restriction$ (the carrier of A). □

(14) Let us consider Abelian groups A, B, and a homomorphism f from A to B. Suppose f is one-to-one and $\Omega_B \setminus (\mathrm{rng}\, f) \neq \emptyset$. Then there exists an Abelian group C and there exists a set X and there exists a function h and there exists a function G from B into C such that $X \cap \Omega_A = \emptyset$ and h is one-to-one and $\mathrm{dom}\, h = \Omega_B \setminus (\mathrm{rng}\, f)$ and $\mathrm{rng}\, h = X$ and $\Omega_C = X \cup \Omega_A$ and A is a subgroup of C and G is a homomorphism from B to C and $\mathrm{id}_A = G \cdot f$.
PROOF: Consider X being a non empty set such that $\Omega_A \cap X = \emptyset$ and there

exists a function h such that h is one-to-one and $\operatorname{dom} h = \Omega_B \setminus (\operatorname{rng} f)$ and $\operatorname{rng} h = X$. Consider h being a function such that h is one-to-one and $\operatorname{dom} h = \Omega_B \setminus (\operatorname{rng} f)$ and $\operatorname{rng} h = X$ and $\Omega_A \cap X = \emptyset$. Define $\mathcal{P}$[element of B, element of $\Omega_A \cup X$] $\equiv$ $\$_1 \in \operatorname{rng} f$ and $(f^{-1})(\$_1) = \$_2$ or $\$_1 \notin \operatorname{rng} f$ and $\$_2 = h(\$_1)$. Set $C_1 = \Omega_A \cup X$.

Consider g being a function from the carrier of B into C_1 such that for every element x of B, $\mathcal{P}[x, g(x)]$. g is bijective. Reconsider $C = \operatorname{embAbGr}(g)$ as a non empty Abelian group. Reconsider $G = g$ as a function from B into C. G is additive. For every o such that $o \in \Omega_A$ holds $(G \cdot f)(o) = o$. A is a subgroup of C. □

4. Relation with Polynomial Rings

Now we state the proposition:

(15) Let us consider a bag b of 0. Then

(i) $\operatorname{dom} b = \emptyset$, and

(ii) $b = \operatorname{EmptyBag} \emptyset$, and

(iii) $\operatorname{rng} b = 0$, and

(iv) $\operatorname{EmptyBag} \emptyset = \emptyset \longmapsto 0$, and

(v) $\operatorname{Bags} \emptyset = \{\operatorname{EmptyBag} \emptyset\}$.

From now on R denotes a right zeroed, add-associative, right complementable, Abelian, well unital, distributive, associative, non trivial, non trivial double loop structure. Now we state the propositions:

(16) Let us consider a polynomial f of $0,R$. Then

(i) $\operatorname{dom} f = \operatorname{Bags} 0$, and

(ii) $\operatorname{Bags} 0 = \{\emptyset\}$, and

(iii) $\operatorname{rng} f = \{f(\operatorname{EmptyBag} 0)\}$.

The theorem is a consequence of (15).

(17) Every polynomial of $0,R$ is constant.

(18) Let us consider a polynomial f of $0,R$. Then there exists an element a of R such that $f = a\restriction(0, R)$. The theorem is a consequence of (17).

Let us consider R. The functor $1\_1(R)$ yielding a sequence of R is defined by the term

(Def. 11) $\mathbf{0}.R +\cdot (1, 1_R)$.

Now we state the proposition:

(19) Let us consider a non degenerated commutative ring R.
Then Support $1\_1(R) = \{1\}$.
PROOF: For every o such that $o \in$ Support $1\_1(R)$ holds $o \in \{1\}$. For every o such that $o \in \{1\}$ holds $o \in$ Support $1\_1(R)$. □

Let us consider R. One can verify that $1\_1(R)$ is finite-Support. Now we state the propositions:

(20) Leading-Monomial $1\_1(R) = 1\_1(R)$.

(21) Let us consider an element m of R. Then $\mathrm{eval}(1\_1(R), m) = m$. The theorem is a consequence of (20).

In the sequel R denotes a non degenerated commutative ring. Now we state the propositions:

(22) Let us consider an element p_0 of Polynom-Ring$(0, R)$. Then p_0 is not a polynomial over Polynom-Ring$(0, R)$.

(23) Let us consider a non degenerated commutative ring R.
Then Polynom-Ring Polynom-Ring$(0, R)$ and Polynom-Ring$(1, R)$ are isomorphic.

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

(24) $\Omega_{\text{Polynom-Ring } R} \setminus (\mathrm{rng}(R \overset{\text{canHom}}{\hookrightarrow} \text{Polynom-Ring } R)) \neq \emptyset$.

(25) There exists a non degenerated ring P_1 and there exists a set X and there exists a function h and there exists a function G from Polynom-Ring R into P_1 such that R is a subring of P_1.
And G inherits ring isomorphism and $\mathrm{id}_R = G \cdot (R \overset{\text{canHom}}{\hookrightarrow} \text{Polynom-Ring } R)$ and $X \cap \Omega_R = \emptyset$ and h is one-to-one and $\mathrm{dom}\, h = \Omega_{\text{Polynom-Ring } R} \setminus (\mathrm{rng}(R \overset{\text{canHom}}{\hookrightarrow} \text{Polynom-Ring } R))$ and $\mathrm{rng}\, h = X$ and $\Omega_{P_1} = X \cup \Omega_R$. The theorem is a consequence of (24) and (9).

(26) $\Omega_{\text{Polynom-Ring}(0,R)} \cap \Omega_{\text{Polynom-Ring Polynom-Ring}(0,R)} = \emptyset$. The theorem is a consequence of (22).

(27) Let us consider a non degenerated ring R. Then there exists a non degenerated ring P_1 and there exists a set X and there exists a function h and there exists a function G from Polynom-Ring Polynom-Ring$(0, R)$ into P_1 such that Polynom-Ring$(0, R)$ is a subring of P_1.
And G inherits ring isomorphism and $\mathrm{id}_{\text{Polynom-Ring}(0,R)} = G \cdot (\text{Polynom-Ring}(0, R) \overset{\text{canHom}}{\hookrightarrow} \text{Polynom-Ring Polynom-Ring}(0, R))$ and $X \cap \Omega_{\text{Polynom-Ring}(0,R)} = \emptyset$ and h is one-to-one and $\mathrm{dom}\, h = \Omega_{\text{Polynom-Ring Polynom-Ring}(0,R)} \setminus (\mathrm{rng}(\text{Polynom-Ring}(0, R) \overset{\text{canHom}}{\hookrightarrow} \text{Polynom-Ring Polynom-Ring}(0, R)))$ and $\mathrm{rng}\, h = X$ and $\Omega_{P_1} = X \cup \Omega_{\text{Polynom-Ring}(0,R)}$.

Let us consider R. Let A be an R-monomorphic commutative ring and x be an element of A. We say that x is indeterminate if and only if

(Def. 12) there exists a function g from Polynom-Ring R into A such that g is isomorphism and $x = g(1\_1(R))$.

Now we state the proposition:

(28) Let us consider a non degenerated commutative ring R. Then there exists an element X of Polynom-Ring R such that

(i) X is indeterminate, and

(ii) $X = 1\_1(R)$.

References

[1] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to Commutative Algebra*, volume 2. Addison-Wesley Reading, 1969.

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

[3] 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.

[4] Edward J. Barbeau. *Polynomials*. Springer, 2003.

[5] Adam Grabowski and Christoph Schwarzweller. On duplication in mathematical repositories. In Serge Autexier, Jacques Calmet, David Delahaye, Patrick D. F. Ion, Laurence Rideau, Renaud Rioboo, and Alan P. Sexton, editors, *Intelligent Computer Mathematics, 10th International Conference, AISC 2010, 17th Symposium, Calculemus 2010, and 9th International Conference, MKM 2010, Paris, France, July 5–10, 2010. Proceedings*, volume 6167 of *Lecture Notes in Computer Science*, pages 300–314. Springer, 2010. doi:10.1007/978-3-642-14128-7_26.

[6] 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.

[7] Piotr Rudnicki, Christoph Schwarzweller, and Andrzej Trybulec. Commutative algebra in the Mizar system. *Journal of Symbolic Computation*, 32(1/2):143–169, 2001. doi:10.1006/jsco.2001.0456.

[8] Christoph Schwarzweller. Existence and uniqueness of algebraic closures. *Formalized Mathematics*, 30(**4**):281–294, 2022. doi:10.2478/forma-2022-0022.

[9] Christoph Schwarzweller. On monomorphisms and subfields. *Formalized Mathematics*, 27(**2**):133–137, 2019. doi:10.2478/forma-2019-0014.

[10] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Algebraic extensions. *Formalized Mathematics*, 29(**1**):39–48, 2021. doi:10.2478/forma-2021-0004.

[11] Yasushige Watase. Ring of endomorphisms and modules over a ring. *Formalized Mathematics*, 30(**3**):211–221, 2022. doi:10.2478/forma-2022-0016.

[12] Oscar Zariski and Pierre Samuel. *Commutative Algebra I*. Springer, 2nd edition, 1975.

Accepted November 21, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 151–159, 2023
DOI: 10.2478/forma-2023-0014
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

On Fuzzy Negations and Laws of Contraposition. Lattice of Fuzzy Negations

Adam Grabowski
Faculty of Computer Science
University of Białystok
Poland

Summary. This the next article in the series formalizing the book of Baczyński and Jayaram "Fuzzy Implications". We define the laws of contraposition connected with various fuzzy negations, and in order to make the cluster registration mechanism fully working, we construct some more non-classical examples of fuzzy implications. Finally, as the testbed of the reuse of lattice-theoretical approach, we introduce the lattice of fuzzy negations and show its basic properties.

MSC: 03B52 68V20

Keywords: fuzzy implication; contrapositive symmetry; fuzzy negation

MML identifier: FUZIMPL4, version: 8.1.14 5.76.1452

Introduction

The main aim of this Mizar article was to implement a formal counterpart of the handbook of fuzzy implications [1]. This is the next submission in the series formalizing this volume, following, among others, [5]. We define the laws of contraposition with the connection to various fuzzy negations [6]. Developing the approach proposed in [7], we deal with the part of Chapter 1.5, pp. 20–23 [1].

In the first section we introduce Mizar attributes [2] which define contrapositive symmetry (also in its weaker, left- and right-side form) with respect to the given fuzzy negation, in Section 2 we recall the notion of fuzzy negation,

taking into account the fact that if its converse is just the function (denoted in the Mizar formalism by $R^\smile$) implies their surjectivity or injectivity.

Section 3, 4, and 5 formalize complete proofs of lemmas and corollaries 1.5.3–1.5.9 from Chapter 1.5 [1]. The sixth section introduces two fuzzy implications introduced by Drewniak [3], which were not formalized in Mizar before: I_{I3} and I_{I4}, needed to formulate Example 1.5.10. Section 7 shows how nine basic fuzzy implications are connected with contrapositive symmetry. Most of these properties, once proven formally, can be obtained by the Mizar checker without any additional references, only by virtue of cluster registrations mechanism. These registrations in the Mizar code can be treated as the formal counterpart of Table 1.9, p. 29 from Baczyński and Jayaram book, quoted below.

Fuzzy implication I	(CP)	(L-CP)	(R-CP)
I_{LK}	N_{C}	N_{C}	N_{C}
I_{GD}	$\times$	$\times$	N_{D1}
I_{RC}	N_{C}	N_{C}	N_{C}
I_{KD}	N_{C}	N_{C}	N_{C}
I_{GG}	$\times$	$\times$	N_{D1}
I_{RS}	N_{C}	N_{C}	N_{C}
I_{YG}	$\times$	$\times$	N_{D1}
I_{WB}	$\times$	$\times$	N_{D2}
I_{FD}	N_{C}	N_{C}	N_{C}

Additionally, in the final section we introduce the lattice of all fuzzy negations and show its basic properties [9], partially formulating and proving Theorem 1.4.3, p. 14. We wanted to avoid duplication of lattice-theoretical notions (ordering vs. lattice suprema and infima) [11], and the availability of min and max operations for various (formally distinct) classes of functions was an issue we had to cope with [12].

Our work makes a step towards the formalization of fuzzy sets and fuzzy numbers [4], [15] in the computerized proof assistant [8], [10]; see [13] and [14] for another interesting effort in this direction.

1. Laws of Contraposition

Let L be a non empty 1-sorted structure and a, b be elements of L. Let us note that the functor $\{a, b\}$ yields a subset of L. One can verify that there exists a fuzzy negation which is decreasing.

Let N be a fuzzy negation and I be a binary operation on $[0, 1]$. We say that I satisfies contraposition property w.r.t. N if and only if

(Def. 1) for every elements x, y of $[0,1]$, $I(x,y) = I(N(y),N(x))$.

We say that I satisfies left contraposition property w.r.t. N if and only if

(Def. 2) for every elements x, y of $[0,1]$, $I(N(x),y) = I(N(y),x)$.

We say that I satisfies right contraposition property w.r.t. N if and only if

(Def. 3) for every elements x, y of $[0,1]$, $I(x,N(y)) = I(y,N(x))$.

2. Fuzzy Negations Revisited

Now we state the proposition:

(1) $N_C = (\mathrm{AffineMap}(-1,1))\restriction[0,1]$.

Proof: Set $N = N_C$. Set $f = (\mathrm{AffineMap}(-1,1))\restriction[0,1]$. For every object x such that $x \in \operatorname{dom} N$ holds $f(x) = N(x)$. □

Note that N_C is continuous and N_C is strong and there exists a fuzzy negation which is strict and there exists a fuzzy negation which is strong. Every fuzzy negation which is satisfying (N3) is also decreasing and every fuzzy negation which is decreasing is also satisfying (N3).

Observe that every unary operation on $[0,1]$ is $\mathbb{R}$-defined and real-valued and every real-valued function which is $\mathbb{R}$-defined and decreasing is also one-to-one. Every unary operation on $[0,1]$ which is decreasing is also one-to-one and every fuzzy negation is non-increasing and every fuzzy negation which is strict is also one-to-one. Now we state the proposition:

(2) Let us consider a function R. If $R^\smile$ is a function, then R is one-to-one.

Let us consider fuzzy negations N_1, N_2. Now we state the propositions:

(3) If ${N_1}^\smile = N_2$, then N_1 is one-to-one.

(4) If ${N_1}^\smile = N_2$, then N_1 is onto.

Proof: N_2 is one-to-one. For every object y such that $y \in [0,1]$ there exists an object x such that $x \in [0,1]$ and $y = N_1(x)$. □

(5) Let us consider a binary operation I on $[0,1]$, a strict fuzzy negation N, and a fuzzy negation N_1. Suppose $N^\smile = N_1$. Then I satisfies left contraposition property w.r.t. N if and only if I satisfies right contraposition property w.r.t. N_1.

Proof: N is onto. If I satisfies left contraposition property w.r.t. N, then I satisfies right contraposition property w.r.t. N_1. For every elements x, y of $[0,1]$, $I(N(x),y) = I(N(y),x)$. □

3. Proposition 1.5.3

Let us consider a binary operation I on $[0,1]$ and a strong fuzzy negation N. Now we state the propositions:

(6) If I satisfies contraposition property w.r.t. N, then I satisfies left contraposition property w.r.t. N.

(7) If I satisfies left contraposition property w.r.t. N, then I satisfies right contraposition property w.r.t. N.

(8) If I satisfies right contraposition property w.r.t. N, then I satisfies contraposition property w.r.t. N.

(9) I satisfies contraposition property w.r.t. N if and only if I satisfies left contraposition property w.r.t. N.

(10) I satisfies contraposition property w.r.t. N if and only if I satisfies right contraposition property w.r.t. N.

4. Lemma 1.5.4

Let us consider a binary operation I on $[0,1]$ and a fuzzy negation N. Now we state the propositions:

(11) If I satisfies (I1) and contraposition property w.r.t. N, then I satisfies (I2).
Proof: For every elements x, y, z of $[0,1]$ such that $y \leqslant z$ holds $I(x,y) \leqslant I(x,z)$. □

(12) If I satisfies (I2) and contraposition property w.r.t. N, then I satisfies (I1).
Proof: For every elements x, y, z of $[0,1]$ such that $x \leqslant y$ holds $I(x,z) \geqslant I(y,z)$. □

(13) If I satisfies (LB) and contraposition property w.r.t. N, then I satisfies (RB).

(14) If I satisfies (RB) and contraposition property w.r.t. N, then I satisfies (LB).

(15) If I satisfies (NP) and contraposition property w.r.t. N, then $N = N_I$ and N_I is strong.

(16) If I satisfies (NP) and contraposition property w.r.t. N, then I satisfies (I3), (I4), and (I5). The theorem is a consequence of (15).

(17) Let us consider a binary operation I on $[0,1]$. Suppose I satisfies (NP). If N_I is not strong, then for every fuzzy negation N, I does not satisfy contraposition property w.r.t. N.

5. Lemma 1.5.6 and Corollaries

Let us consider a binary operation I on $[0,1]$ and a strong fuzzy negation N. Now we state the propositions:

(18) If $N = N_I$, then if I satisfies contraposition property w.r.t. N, then I satisfies (NP).

(19) If $N = N_I$, then if I satisfies (EP), then I satisfies (I3), (I4), (I5), (NP), and contraposition property w.r.t. N. The theorem is a consequence of (18) and (16).

Let us consider a binary operation I on $[0,1]$ and a fuzzy negation N. Now we state the propositions:

(20) If I satisfies contraposition property w.r.t. N, then I satisfies (I1) iff I satisfies (I2).

(21) If I satisfies contraposition property w.r.t. N, then I satisfies (LB) iff I satisfies (RB).

(22) If I satisfies contraposition property w.r.t. N, then if N is strong, then I satisfies (NP) iff $N = N_I$.

(23) If I satisfies contraposition property w.r.t. N, (I1), and (NP), then $I \in \mathcal{FI}$ and $N_I = N$ and N is strong. The theorem is a consequence of (20), (16), and (15).

(24) Let us consider fuzzy implication I satisfying (NP) and (EP). Then N_I is strong if and only if I satisfies contraposition property w.r.t. (N_I).

6. Some Further Examples of Fuzzy Implications

The functor I_{I3} yielding a binary operation on $[0,1]$ is defined by

(Def. 4) for every elements x, y of $[0,1]$, if $x = 0$ or $y \neq 0$, then $it(x,y) = 1$ and if $x \neq 0$ and $y = 0$, then $it(x,y) = 0$.

One can verify that I_{I3} is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak. Now we state the proposition:

(25) $N_{I_{\mathrm{I3}}} = N_{\mathrm{D1}}$.

Let us note that I_{I3} satisfies (EP) but does not satisfy (NP) and I_{I3} satisfies contraposition property w.r.t. $(N_{I_{\mathrm{I3}}})$.

The functor I_{I4} yielding a binary operation on $[0,1]$ is defined by

(Def. 5) for every elements x, y of $[0,1]$, if $x \neq 1$ or $y = 1$, then $it(x,y) = 1$ and if $x = 1$ and $y \neq 1$, then $it(x,y) = 0$.

One can verify that I_{I4} is antitone w.r.t. 1st coordinate, isotone w.r.t. 2nd coordinate, 00-dominant, 11-dominant, and 10-weak. Now we state the proposition:

(26) $N_{I_{\mathrm{I4}}} = N_{\mathrm{D2}}$.

Let us note that I_{I4} satisfies (EP) but does not satisfy (NP) and I_{I4} satisfies contraposition property w.r.t. $(N_{I_{\mathrm{I4}}})$.

7. Contrapositive Symmetry w.r.t. the Natural Negation

Let I be a fuzzy implication. We say that I satisfies contraposition property if and only if

(Def. 6) I satisfies contraposition property w.r.t. (N_I).

We say that I satisfies left contraposition property if and only if

(Def. 7) I satisfies left contraposition property w.r.t. (N_I).

We say that I satisfies right contraposition property if and only if

(Def. 8) I satisfies right contraposition property w.r.t. (N_I).

Observe that I_{LK} satisfies left contraposition property w.r.t. (N_C), right contraposition property w.r.t. (N_C), and contraposition property w.r.t. (N_C) and I_{LK} satisfies left contraposition property, right contraposition property, and contraposition property. I_{GD} satisfies right contraposition property w.r.t. (N_{D1}) and I_{GD} satisfies right contraposition property.

Note that I_{RC} satisfies contraposition property w.r.t. (N_C), left contraposition property w.r.t. (N_C), and right contraposition property w.r.t. (N_C) and I_{RC} satisfies contraposition property, left contraposition property, and right contraposition property. I_{KD} satisfies contraposition property w.r.t. (N_C) and I_{KD} satisfies left contraposition property w.r.t. (N_C) and I_{KD} satisfies right contraposition property w.r.t. (N_C) and I_{KD} satisfies contraposition property, left contraposition property, and right contraposition property.

Let us observe I_{GG} satisfies right contraposition property w.r.t. (N_{D1}) and I_{GG} satisfies right contraposition property. Now we state the proposition:

(27) I_{RS} satisfies left contraposition property w.r.t. (N_C).

One can check that I_{RS} satisfies contraposition property w.r.t. (N_C), left contraposition property w.r.t. (N_C), and right contraposition property w.r.t. (N_C). Now we state the proposition:

(28) Let us consider a decreasing fuzzy negation N. Then I_{RS} satisfies contraposition property w.r.t. N.

Proof: Set $I = I_{\mathrm{RS}}$.

For every elements x, y of $[0,1]$, $I(x,y) = I(N(y), N(x))$. □

Let us observe that I_{YG} satisfies right contraposition property w.r.t. (N_{D1}) and I_{YG} satisfies right contraposition property. I_{WB} satisfies right contraposition property w.r.t. (N_{D2}) and I_{WB} satisfies right contraposition property.

Note that I_{FD} satisfies contraposition property w.r.t. (N_C), left contraposition property w.r.t. (N_C), and right contraposition property w.r.t. (N_C) and I_{FD} satisfies contraposition property, left contraposition property, and right contraposition property.

8. Fuzzy Lattice Revisited

Now we state the propositions:

(29) FuzzyLattice $[0,1]$ is a complete, Heyting, distributive lattice.

(30) the set of all f where f is a fuzzy negation $\subseteq [0,1]^{[0,1]}$.

Let N_1, N_2 be fuzzy negations. The functors: $\max(N_1, N_2)$ and $\min(N_1, N_2)$ yielding fuzzy negations are defined by conditions

(Def. 9) there exist functions f, g from $[0,1]$ into $\mathbb{R}$ such that $f = N_1$ and $g = N_2$ and $\max(N_1, N_2) = \max(f, g)$,

(Def. 10) there exist functions f, g from $[0,1]$ into $\mathbb{R}$ such that $f = N_1$ and $g = N_2$ and $\min(N_1, N_2) = \min(f, g)$,

respectively. The functor FuzzyNegations yielding a strict, full relational substructure of FuzzyLattice $[0,1]$ is defined by

(Def. 11) the carrier of it = the set of all $\mathcal{N}$ where $\mathcal{N}$ is a fuzzy negation.

Observe that FuzzyNegations is non empty, reflexive, transitive, and antisymmetric. Now we state the proposition:

(31) Let us consider fuzzy negations N_1, N_2.
Then $\max(N_1, N_2) = \mathbf{max}_{\mathbb{R}^{[0,1]}}(N_1, N_2)$.
Proof: Set $A = [0,1]$. Set $\mathcal{F} = \max(N_1, N_2)$. Set $m = \mathbf{max}_{\mathbb{R}^{[0,1]}}(N_1, N_2)$. Consider f_1 being a function such that $m = f_1$ and $\operatorname{dom} f_1 = A$ and $\operatorname{rng} f_1 \subseteq \mathbb{R}$. For every object x such that $x \in [0,1]$ holds $\mathcal{F}(x) = m(x)$. □

Let us consider fuzzy negations N_1, N_2 and membership functions f_2, g_2 of $[0,1]$. Now we state the propositions:

(32) If $N_1 = f_2$ and $N_2 = g_2$, then $\max(N_1, N_2) = \max(f_2, g_2)$.

(33) If $N_1 = f_2$ and $N_2 = g_2$, then $\min(N_1, N_2) = \min(f_2, g_2)$.

(34) Let us consider fuzzy negations N_1, N_2.
Then $\min(N_1, N_2) = \mathbf{min}_{\mathbb{R}^{[0,1]}}(N_1, N_2)$.
Proof: Set $A = [0,1]$. Set $\mathcal{F} = \min(N_1, N_2)$. Set $m = \mathbf{min}_{\mathbb{R}^{[0,1]}}(N_1, N_2)$. Consider f_1 being a function such that $m = f_1$ and $\operatorname{dom} f_1 = A$ and $\operatorname{rng} f_1 \subseteq \mathbb{R}$. For every object x such that $x \in [0,1]$ holds $\mathcal{F}(x) = m(x)$. □

Note that FuzzyNegations is join-inheriting and FuzzyNegations is meet-inheriting.

Let us consider elements $\mathcal{N}_1$, $\mathcal{N}_2$ of FuzzyNegations and fuzzy negations N_1, N_2. Now we state the propositions:

(35) If $N_1 = \mathcal{N}_1$ and $N_2 = \mathcal{N}_2$, then $\mathcal{N}_1 \sqcup \mathcal{N}_2 = \max(N_1, N_2)$. The theorem is a consequence of (32).

(36) If $N_1 = \mathcal{N}_1$ and $N_2 = \mathcal{N}_2$, then $\mathcal{N}_1 \sqcap \mathcal{N}_2 = \min(N_1, N_2)$. The theorem is a consequence of (33).

References

[1] Michał Baczyński and Balasubramaniam Jayaram. *Fuzzy Implications*. Springer Publishing Company, Incorporated, 2008. doi:10.1007/978-3-540-69082-5.

[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] Józef Drewniak. Invariant fuzzy implications. *Soft Computing*, 10:506–513, 2006.

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

[5] Adam Grabowski. Formal introduction to fuzzy implications. *Formalized Mathematics*, 25(**3**):241–248, 2017. doi:10.1515/forma-2017-0023.

[6] Adam Grabowski. On fuzzy negations generated by fuzzy implications. *Formalized Mathematics*, 28(**1**):121–128, 2020. doi:10.2478/forma-2020-0011.

[7] Adam Grabowski. Fuzzy implications in the Mizar system. In *30th IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 2021, Luxembourg, July 11–14, 2021*, pages 1–6. IEEE, 2021. doi:10.1109/FUZZ45933.2021.9494593.

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

[9] Adam Grabowski. Lattice theory for rough sets – a case study with Mizar. *Fundamenta Informaticae*, 147(2–3):223–240, 2016. doi:10.3233/FI-2016-1406.

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

[11] Adam Grabowski and Takashi Mitsuishi. Formalizing lattice-theoretical aspects of rough and fuzzy sets. In D. Ciucci, G. Wang, S. Mitra, and W.Z. Wu, editors, *Rough Sets and Knowledge Technology – 10th International Conference held as part of the International Joint Conference on Rough Sets (IJCRS), Tianjin, PR China, November 20–23, 2015, Proceedings*, volume 9436 of *Lecture Notes in Artificial Intelligence*, pages 347–356. Springer, 2015. doi:10.1007/978-3-319-25754-9_31.

[12] Adam Grabowski and Christoph Schwarzweller. On duplication in mathematical repositories. In Serge Autexier, Jacques Calmet, David Delahaye, Patrick D. F. Ion, Laurence Rideau, Renaud Rioboo, and Alan P. Sexton, editors, *Intelligent Computer Mathematics, 10th International Conference, AISC 2010, 17th Symposium, Calculemus 2010, and 9th International Conference, MKM 2010, Paris, France, July 5–10, 2010. Proceedings*, volume 6167 of *Lecture Notes in Computer Science*, pages 300–314. Springer, 2010. doi:10.1007/978-3-642-14128-7_26.

[13] Takashi Mitsuishi. Definition of centroid method as defuzzification. *Formalized Mathe-*

matics, 30(**2**):125–134, 2022. doi:10.2478/forma-2022-0010.

[14] Takashi Mitsuishi. Isosceles triangular and isosceles trapezoidal membership functions using centroid method. *Formalized Mathematics*, 31(1):59–66, 2023. doi:10.2478/forma-2023-0006.

[15] Lotfi Zadeh. Fuzzy sets. *Information and Control*, 8(3):338–353, 1965. doi:10.1016/S0019-9958(65)90241-X.

Accepted November 21, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 161–169, 2023
DOI: 10.2478/forma-2023-0015
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part IX

Artur Korniłowicz
Faculty of Computer Science
University of Białystok
Poland

Summary. This paper continues the formalization of chosen problems defined in the book "250 Problems in Elementary Number Theory" by Wacław Sierpiński.

MSC: 11A41 68V20

Keywords: number theory; divisibility; primes; factorization

MML identifier: NUMBER09, version: 8.1.14 5.76.1452

Introduction

In this paper, problems 62 from Section III, 91, 125 from Section IV, 143, 146, 147, 158, 166, 178, 180, and 181 from Section V of [10] are formalized, using the Mizar formalism [1, 2, 4]. It contributes to the project for the formalization of problems defined in [7].

In the preliminary section, we provide some very technical lemmas, mainly about powers of complex numbers, which are helpful for this and future formalizations. To formulate the statement of Problem 62 the operation ArProg introduced in [3] is used. Some useful theorems about primeness of products of elements of finite sequences are proven.

Problem 91 is devoted to decomposing some Mersenne numbers [9] into products of primes or arbitrary integers. For justification of the primeness of Mersenne(17) and Mersenne(19) we formalized the lemma

$$\forall_{p,q\in\mathbb{P}}\ p \text{ is odd} \wedge q|\text{Mersenne}(p) \Rightarrow \exists_{k\in\mathbb{N}}\ q = 2\cdot k\cdot p + 1.$$

The proof of Problem 143 concerning solutions of the equation $x^2-Dy^2=z^2$ in positive integers x, y, z for arbitrary integer D presented in the book has been split into three cases depending on the sign of the parameter D.

The proof of Problem 158 about infiniteness of the number of solutions of the equation $\frac{x}{y}+\frac{y}{z}+\frac{z}{t}+\frac{t}{z}=1$ in integers x, y, z, t relies on the infiniteness of the range of an injective function with infinite domain, where as the function we use $f : A \to \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$, where A is the set of all integers greater than 1 and for every integer $n>1$, $f(n)=[-n^2, n^2\cdot(n^2-1), (n^2-1)^2, -n\cdot(n^2-1)]$.

Problem 166 about representing number $\frac{1}{2}$ as a sum of reciprocals of a finite number of squares of positive integers is formulated as just one example of such decomposition, as

$$\frac{1}{2}=\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{6^2}+\frac{1}{7^2}+\frac{1}{9^2}+\frac{1}{12^2}+\frac{1}{14^2}+\frac{1}{21^2}+\frac{1}{36^2}+\frac{1}{45^2}+\frac{1}{60^2}$$

and its proof is evident to the Mizar verifier due to built-in arithmetic processing.

Problem 180 about solutions (in positive integers) of the equation $y\cdot(y+1)=x\cdot(x+1)\cdot(x+2)$ is formulated as equations $2\cdot(2+1)=1\cdot(1+1)\cdot(1+2)$ and $14\cdot(14+1)=5\cdot(5+1)\cdot(5+2)$ with shapes which mimic the structure of the problem. Its proof is also obvious to the Mizar verifier due to built-in arithmetic processing [8].

The proof of Problem 181 about infiniteness of the number of solutions of the equation $1+x^2+y^2=z^2$ in positive integers x, y, z uses the same technique as we used in the proof of Problem 158 where $f : \mathbb{N}_+ \to \mathbb{N}_+\times\mathbb{N}_+\times\mathbb{N}_+$ such that for every positive integer n, $f(n)=[2\cdot n, 2\cdot n^2, 2\cdot n^2+1]$.

1. Preliminaries

From now on X denotes a set, a, b, c, k, m, n denote natural numbers, i, j denote integers, r, s denote real numbers, p, p_1, p_2, p_3 denote prime numbers, and z denotes a complex number. Now we state the propositions:

(1) $z^{11}=z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z$.

(2) $z^{12}=z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z$. The theorem is a consequence of (1).

(3) $z^{13}=z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z$. The theorem is a consequence of (2).

(4) $z^{14}=z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z$. The theorem is a consequence of (3).

(5) $z^{15}=z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z\cdot z$. The theorem is a consequence of (4).

(6) $z^{16} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (5).

(7) $z^{17} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (6).

(8) $z^{18} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (7).

(9) $z^{19} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (8).

(10) $z^{20} = z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z \cdot z$. The theorem is a consequence of (9).

(11) If $n \geqslant 2$, then there exists a positive natural number k such that $2^n - 1 = 4 \cdot k - 1$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \geqslant 2$, then there exists a positive natural number k such that $2^{\$_1} - 1 = 4 \cdot k - 1$. $\mathcal{P}[2]$. For every natural number j such that $2 \leqslant j$ holds if $\mathcal{P}[j]$, then $\mathcal{P}[j+1]$. For every natural number i such that $2 \leqslant i$ holds $\mathcal{P}[i]$. □

2. PROBLEM 62

Let X be a set. We say that X is included in a segment if and only if

(Def. 1) there exists a natural number k such that $X \subseteq \operatorname{Seg} k$.

Note that every set which is empty is also included in a segment.

Let n be a non zero natural number. Let us note that $\{n\}$ is included in a segment and there exists a set which is non empty and included in a segment and every set which is included in a segment is also finite and natural-membered and every finite, natural-membered set which has non empty elements is also included in a segment.

Let a, r be natural numbers. Observe that $\operatorname{ArProg}(a, r)$ is natural-valued.

Let us consider i. The functor Coprimes(i) yielding a subset of $\mathbb{Z}$ is defined by the term

(Def. 2) $\{j$, where j is an integer : i and j are relatively prime$\}$.

Now we state the proposition:

(12) Let us consider an included in a segment set X. If $X \subseteq \mathbb{P}$ and $p \mid \prod \operatorname{Sgm} X$, then $p \in X$.

Let us consider natural numbers a, b and a non zero natural number m. Now we state the propositions:

(13) Suppose a and b are relatively prime. Then $\prod \mathrm{Sgm}\{p$, where p is a prime number : $p \mid m$ and $p \mid a\}$ and $\prod \mathrm{Sgm}\{q$, where q is a prime number : $q \mid m$ and $q \mid b\}$ are relatively prime. The theorem is a consequence of (12).

(14) $\prod \mathrm{Sgm}\{p$, where p is a prime number : $p \mid m$ and $p \mid a\}$ and $\prod \mathrm{Sgm}\{r$ where r is a prime number : $r \mid m$ and $r \nmid a$ and $r \nmid b\}$ are relatively prime. The theorem is a consequence of (12).

(15) Suppose a and b are relatively prime. Then $\prod \mathrm{Sgm}\{q$, where q is a prime number : $q \mid m$ and $q \mid b\}$ and $\prod \mathrm{Sgm}\{r$, where r is a prime number : $r \mid m$ and $r \nmid a$ and $r \nmid b\}$ are relatively prime. The theorem is a consequence of (14).

(16) Let us consider an included in a segment set X. If $a \in X$, then $a \mid \prod \mathrm{Sgm}\, X$.

(17) Let us consider non zero natural numbers a, m. Suppose a and b are relatively prime. Then $\mathrm{rng}\,\mathrm{ArProg}(b, a) \cap \mathrm{Coprimes}(m)$ is infinite.

PROOF: Set $P_1 = \{p$, where p is a prime number : $p \mid m$ and $p \mid a\}$. Set $R_1 = \{r$, where r is a prime number : $r \mid m$ and $r \nmid a$ and $r \nmid b\}$. Set $P = \prod \mathrm{Sgm}\, P_1$. Set $R = \prod \mathrm{Sgm}\, R_1$. $a \cdot P \cdot R + b$ and m are relatively prime. Set $g = \mathrm{ArProg}(b, a)$. Set $X = \mathrm{rng}\, g \cap \mathrm{Coprimes}(m)$. For every natural number x such that $x \in X$ there exists a natural number y such that $y > x$ and $y \in X$ by [3, (7)], [5, (64)]. □

3. PROBLEM 91

Let n be a complex number. We say that n is a product of two primes if and only if

(Def. 3) there exist prime numbers p_1, p_2 such that $n = p_1 \cdot p_2$.

We introduce the notation n is not a product of two primes as an antonym for n is a product of two primes.

One can check that every prime number is not a product of two primes. Let us consider p_1 and p_2. One can verify that $p_1 \cdot p_2$ is a product of two primes. Now we state the propositions:

(18) If $a \neq 1$ and $a \neq n$ and a is not prime and $a \mid n$, then n is not a product of two primes.

(19) If n is a product of two primes, then $n \geqslant 4$.

(20) If c is a product of two different primes, then c is a product of two primes.

Let us consider p_1, p_2, and p_3. One can check that $p_1 \cdot p_2 \cdot p_3$ is not a product of two primes. Now we state the propositions:

(21) If n is a product of two primes, then for every a and b such that $a \neq 1$ and $b \neq 1$ and $n = a \cdot b$ holds a is prime and b is prime.

(22) If $2^n - 1$ is prime and $2^n + 1$ is prime, then $n = 2$.

Let n be a zero natural number. Note that M_n is zero. Let n be a non zero natural number. Let us note that M_n is odd. Now we state the propositions:

(23) Let us consider prime numbers p, q. Suppose p is odd and $q \mid M_p$. Then there exists a natural number k such that $q = 2 \cdot k \cdot p + 1$.

(24) M_{17} is prime. The theorem is a consequence of (23).

(25) M_{19} is prime. The theorem is a consequence of (23).

(26) $\{2^n - 1$, where n is a natural number : $2^n - 1 \leqslant 10^6$ and $2^n - 1$ is a product of two primes$\} = \{2^4 - 1, 2^9 - 1, 2^{11} - 1\}$.
PROOF: Set $A = \{2^n - 1 : 2^n - 1 \leqslant 10^6$ and $2^n - 1$ is a product of two primes$\}$. Set $B = \{2^4 - 1, 2^9 - 1, 2^{11} - 1\}$. $A \subseteq B$ by [6, (7)], (9). $B \subseteq A$. □

Let us consider n. We say that n has at least three different divisors if and only if

(Def. 4) there exist natural numbers q_1, q_2, q_3 such that q_1, q_2, q_3 are mutually different and $q_1 > 1$ and $q_2 > 1$ and $q_3 > 1$ and $q_1 \mid n$ and $q_2 \mid n$ and $q_3 \mid n$.

Observe that every natural number which has more than two different prime divisors has also at least three different divisors and every natural number which has more than two different prime divisors is also not a product of two primes.

Now we state the propositions:

(27) If n has more than two different prime divisors, then n is not a product of two different primes.

(28) If n is even and $n > 4$, then $2^n - 1$ has at least three different divisors. The theorem is a consequence of (22).

4. PROBLEM 125

Now we state the propositions:

(29) If Fermat m = Fermat n, then $m = n$.

(30) If $m < n$, then Fermat $m <$ Fermat n.

(31) If $m \leqslant n$, then Fermat $m \leqslant$ Fermat n. The theorem is a consequence of (30).

(32) If $i \equiv j \pmod{j}$, then $j \mid i$.

(33) $i \cdot n \equiv n \pmod{n}$.

(34) If $a \mid m^k + 1$, then $a \mid (a \cdot n + m)^k + 1$.

(35) $17 \mid (34 \cdot k + 2)^{2^2} + 1$. The theorem is a consequence of (34).

(36) $17 \mid (34 \cdot k + 4)^{2^1} + 1$. The theorem is a consequence of (34).

(37) $17 \mid (34 \cdot k + 6)^{2^3} + 1$. The theorem is a consequence of (34).

(38) $17 \mid (34 \cdot k + 8)^{2^2} + 1$. The theorem is a consequence of (34).

(39) $17 \mid (34 \cdot k + 10)^{2^3} + 1$. The theorem is a consequence of (34).

(40) $17 \mid (34 \cdot k + 12)^{2^3} + 1$. The theorem is a consequence of (34).

(41) $17 \mid (34 \cdot k + 14)^{2^3} + 1$. The theorem is a consequence of (34).

(42) $17 \mid (34 \cdot k + 20)^{2^3} + 1$. The theorem is a consequence of (34).

(43) $17 \mid (34 \cdot k + 22)^{2^3} + 1$. The theorem is a consequence of (34).

(44) $17 \mid (34 \cdot k + 24)^{2^3} + 1$. The theorem is a consequence of (34).

(45) $17 \mid (34 \cdot k + 26)^{2^2} + 1$. The theorem is a consequence of (34).

(46) $17 \mid (34 \cdot k + 28)^{2^3} + 1$. The theorem is a consequence of (34).

(47) $17 \mid (34 \cdot k + 30)^{2^1} + 1$. The theorem is a consequence of (34).

(48) $17 \mid (34 \cdot k + 32)^{2^2} + 1$. The theorem is a consequence of (34).

(49) If $1 < a \leqslant 100$, then there exists a positive natural number n such that $n \leqslant 6$ and $a^{2^n} + 1$ is composite. The theorem is a consequence of (37), (38), (39), (40), (41), (42), (43), (44), (45), (46), (47), (48), (35), and (36).

5. Problem 143

Now we state the proposition:

(50) Let us consider an integer D. Then $\{\langle x, y, z\rangle$, where x, y, z are positive natural numbers : $x^{\mathbf{2}} - D \cdot y^{\mathbf{2}} = z^{\mathbf{2}}\}$ is infinite.

6. Problem 146

Now we state the propositions:

(51) (i) $n^{\mathbf{2}} \bmod 8 = 0$, or

(ii) $n^{\mathbf{2}} \bmod 8 = 1$, or

(iii) $n^{\mathbf{2}} \bmod 8 = 4$.

(52) Let us consider natural numbers x, y, z. Then $x^{\mathbf{2}} - 2 \cdot y^{\mathbf{2}} + 8 \cdot z \neq 3$. The theorem is a consequence of (51).

7. PROBLEM 147

Now we state the proposition:

(53) $\{\langle x, y\rangle$, where x, y are natural numbers : $y^{\mathbf{2}} - x\cdot(x+1)\cdot(x+2)\cdot(x+3) = 1\} = \{\langle x, y\rangle$, where x, y are natural numbers : $y = x^{\mathbf{2}} + 3\cdot x + 1\}$.
PROOF: Set $A = \{\langle x, y\rangle$, where x, y are natural numbers : $y^{\mathbf{2}} - x\cdot(x+1)\cdot(x+2)\cdot(x+3) = 1\}$. Set $B = \{\langle x, y\rangle$, where x, y are natural numbers : $y = x^{\mathbf{2}} + 3\cdot x + 1\}$. $A \subseteq B$. Consider x, y being natural numbers such that $a = \langle x, y\rangle$ and $y = x^{\mathbf{2}} + 3\cdot x + 1$. $\square$

8. PROBLEM 158

Now we state the propositions:

(54) Let us consider positive real numbers a, b, c, d. If $\frac{a}{b} < 1$ and $\frac{c}{d} < 1$, then $\frac{a}{b}\cdot\frac{c}{d} < 1$.

(55) Let us consider positive natural numbers x, y, z, t. Then $\frac{x}{y} + \frac{y}{z} + \frac{z}{t} + \frac{t}{x} \neq 1$. The theorem is a consequence of (54).

Let n be a natural number. The functor $\langle n, \infty)_{\mathbb{N}}$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 5) $\mathbb{N} \setminus (\mathbb{Z}_n)$.

Let us consider n. One can check that $\langle n, \infty)_{\mathbb{N}}$ is infinite. Now we state the propositions:

(56) $k \in \langle n, \infty)_{\mathbb{N}}$ if and only if $n \leqslant k$.
PROOF: If $k \in \langle n, \infty)_{\mathbb{N}}$, then $n \leqslant k$. $\square$

(57) $n + k \in \langle n, \infty)_{\mathbb{N}}$.

(58) $n \in \langle n, \infty)_{\mathbb{N}}$.

(59) If $k > 0$, then $n \notin \langle n + k, \infty)_{\mathbb{N}}$. The theorem is a consequence of (56).

Let us consider n. Let us note that every element of $\langle n, \infty)_{\mathbb{N}}$ is n or greater and there exists a natural number which is n or greater. Now we state the proposition:

(60) Let us consider an n or greater natural number k. Then $k \in \langle n, \infty)_{\mathbb{N}}$.

Let us consider n. Let k be a non zero natural number. Observe that $k \cdot n$ is n or greater. Let k be an n or greater natural number. One can verify that $k - n$ is natural. Now we state the proposition:

(61) $\{\langle x, y, z, t\rangle$, where x, y, z, t are integers : $\frac{x}{y} + \frac{y}{z} + \frac{z}{t} + \frac{t}{x} = 1\}$ is infinite.
PROOF: Set $G_2 = \langle 2, \infty)_{\mathbb{N}}$. Set $A = \{\langle x, y, z, t\rangle$, where x, y, z, t are integers : $\frac{x}{y} + \frac{y}{z} + \frac{z}{t} + \frac{t}{x} = 1\}$. Define $\mathcal{V}$(natural number) $= -\$_1^{\mathbf{2}}$. Define $\mathcal{Y}$(natural

number) = $\$_1^{\mathbf{2}} \cdot (\$_1^{\mathbf{2}} - 1)$. Define $\mathcal{Z}$(natural number) = $(\$_1^{\mathbf{2}} - 1)^{\mathbf{2}}$. Define $\mathcal{T}$(natural number) = $-\$_1 \cdot (\$_1^{\mathbf{2}} - 1)$. Define $\mathcal{F}$(element of G_2) = $\langle \mathcal{V}(\$_1), \mathcal{Y}(\$_1), \mathcal{Z}(\$_1), \mathcal{T}(\$_1) \rangle$. Consider f being a many sorted set indexed by G_2 such that for every element d of G_2, $f(d) = \mathcal{F}(d)$. rng $f \subseteq A$. f is one-to-one. □

9. Problem 166

Now we state the proposition:

(62) $\frac{1}{2} = \frac{1}{2^{\mathbf{2}}} + \frac{1}{3^{\mathbf{2}}} + \frac{1}{4^{\mathbf{2}}} + \frac{1}{6^{\mathbf{2}}} + \frac{1}{7^{\mathbf{2}}} + \frac{1}{9^{\mathbf{2}}} + \frac{1}{12^{\mathbf{2}}} + \frac{1}{14^{\mathbf{2}}} + \frac{1}{21^{\mathbf{2}}} + \frac{1}{36^{\mathbf{2}}} + \frac{1}{45^{\mathbf{2}}} + \frac{1}{60^{\mathbf{2}}}$.

10. Problem 178

Now we state the proposition:

(63) $(n+1)^3 + (n+2)^3 + (n+3)^3 + (n+4)^3 \neq (n+5)^3$.

11. Problem 180

Now we state the proposition:

(64) (i) $2 \cdot (2+1) = 1 \cdot (1+1) \cdot (1+2)$, and

(ii) $14 \cdot (14+1) = 5 \cdot (5+1) \cdot (5+2)$.

12. Problem 181

Now we state the proposition:

(65) $\{\langle x, y, z \rangle$, where x, y, z are positive natural numbers : $1 + x^{\mathbf{2}} + y^{\mathbf{2}} = z^{\mathbf{2}}\}$ is infinite.

Proof: Set $A = \{\langle x, y, z \rangle$, where x, y, z are positive natural numbers : $1 + x^{\mathbf{2}} + y^{\mathbf{2}} = z^{\mathbf{2}}\}$. Define $\mathcal{V}$(natural number) = $2 \cdot \$_1$. Define $\mathcal{Y}$(natural number) = $2 \cdot \$_1^{\mathbf{2}}$. Define $\mathcal{Z}$(natural number) = $2 \cdot \$_1^{\mathbf{2}} + 1$. Define $\mathcal{F}$(natural number) = $\langle \mathcal{V}(\$_1), \mathcal{Y}(\$_1), \mathcal{Z}(\$_1) \rangle$. Consider f being a many sorted set indexed by $\mathbb{N}_+$ such that for every element d of $\mathbb{N}_+$, $f(d) = \mathcal{F}(d)$. rng $f \subseteq A$. f is one-to-one. □

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. Elementary number theory problems. Part VI. *Formalized Mathematics*, 30(**3**):235–244, 2022. doi:10.2478/forma-2022-0019.

[4] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[5] Artur Korniłowicz. Elementary number theory problems. Part IV. *Formalized Mathematics*, 30(**3**):223–228, 2022. doi:10.2478/forma-2022-0017.

[6] Artur Korniłowicz and Dariusz Surowik. Elementary number theory problems. Part II. *Formalized Mathematics*, 29(**1**):63–68, 2021. doi:10.2478/forma-2021-0006.

[7] Adam Naumowicz. Dataset description: Formalization of elementary number theory in Mizar. In Christoph Benzmüller and Bruce R. Miller, editors, *Intelligent Computer Mathematics – 13th International Conference, CICM 2020, Bertinoro, Italy, July 26–31, 2020, Proceedings*, volume 12236 of *Lecture Notes in Computer Science*, pages 303–308. Springer, 2020. doi:10.1007/978-3-030-53518-6_22.

[8] Adam Naumowicz. Extending numeric automation for number theory formalizations in Mizar. In Catherine Dubois and Manfred Kerber, editors, *Intelligent Computer Mathematics – 16th International Conference, CICM 2023, Cambridge, UK, September 5–8, 2023, Proceedings*, volume 14101 of *Lecture Notes in Computer Science*, pages 309–314. Springer, 2023. doi:10.1007/978-3-031-42753-4_23.

[9] Wacław Sierpiński. *Elementary Theory of Numbers*. PWN, Warsaw, 1964.

[10] Wacław Sierpiński. *250 Problems in Elementary Number Theory*. Elsevier, 1970.

Accepted November 21, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 171–180, 2023
DOI: 10.2478/forma-2023-0016
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part X – Diophantine Equations

Artur Korniłowicz
Faculty of Computer Science
University of Białystok
Poland

Summary. This paper continues the formalization of problems defined in the book "250 Problems in Elementary Number Theory" by Wacław Sierpiński.

MSC: 11A41 11D72 68V20

Keywords: number theory; Diophantine equations

MML identifier: `NUMBER10`, version: `8.1.14 5.76.1452`

Introduction

In this paper, Problems 84, 94, 99 from Section IV, 170, 173, 174, 175, 177, 179, 186, 187, 189, 190, 193, 194, 197, and 199 from Section V of [10] are formalized, using the Mizar formalism [1]. It contributes to the project announced in [6].

Some of the problems in the book are formulated in terms of *positive integers*. To represent such numbers in the Mizar Mathematical Library [2], we use notions either `positive Integer` or `positive Nat` or `non zero Nat`, which are automatically understood as equivalent due to the built-in processing of adjectives by the Mizar checker.

For proving the infiniteness of the set of pairs of consecutive primes that are not twin primes (Problem 84), we implemented the operation $\max\langle 0, 6\cdot n+1\rangle_{\mathbb{P}}$, which represents the largest prime $\leqslant 6n+1$ denoted as p_{k_n} in the book. We noted a small misprint in the proof presented in the book in the equation $(6n+5)+(6n+1)=4$ – it should be $(6n+5)-(6n+1)=4$.

Problem 179 asks about all rational solutions of the equation

$$(x+1)^3+(x+2)^3+(x+3)^3+(x+4)^3=(x+10)^3.$$

We generalized the problem to real numbers and presented the only solution $x = 10$ in reals, which is also the only solution in rationals. Moreover, we computed that the substitution $x = t + 10$ proposed in the book results in the equation $t(t^2 + 30t + 230) = 0$.

The infiniteness of sets defined in Problems 189, 190, and 199 is proven using function `recSeqCart` [4] with parameters adequate to given problems.

Problem 197 is devoted to the existence of solutions of the equation

$$x_1 + x_2 + \cdots + x_n = x_1 x_2 \cdots x_n$$

in positive integers. In the case of $n > 2$, the proof in the book proposes $x_{n-1} = 1$, but we computed that x_{n-1} must be equal to 2.

Proofs of other problems are straightforward formalizations of solutions given in the book, by means of available development of number theory in Mizar [9], using ellipsis [3] extensively, looking forward for more advanced automatization of arithmetical calculations [7].

1. Preliminaries

From now on a, b, c, k, m, n denote natural numbers, i, j, x, y denote integers, p, q denote prime numbers, and r, s denote real numbers. Now we state the propositions:

(1) Let us consider natural numbers i, j. If $i < j$, then there exists a positive natural number k such that $j = i + k$.

(2) Let us consider a positive yielding, integer-valued finite sequence f. Then $\prod f \geqslant 1$.

Proof: Define $\mathcal{P}[\text{set}] \equiv$ for every positive yielding, integer-valued finite sequence F such that $F = \$_1$ holds $\prod F \geqslant 1$. For every finite sequence p of elements of $\mathbb{Z}$ and for every element x of $\mathbb{Z}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p^\frown \langle x \rangle]$. For every finite sequence p of elements of $\mathbb{Z}$, $\mathcal{P}[p]$. □

(3) If $m \geqslant 2$ and $n \geqslant 2$, then $m \cdot n$ is composite.

(4) If $p \nmid n$, then n and p are relatively prime.

(5) $-1 \bmod p = p - 1$.

2. Problem 84

Let r, s be complex numbers. We say that r and s are twin if and only if

(Def. 1) $|s - r| = 2$.

One can verify that the predicate is irreflexive and symmetric. Now we state the proposition:

(6) If $r \leqslant s$, then r and s are twin iff $s - r = 2$.

Let us consider n. The functor $\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 2) $\{a$, where a is a natural number : $a \leqslant 6 \cdot n + 1\}$.

Now we state the propositions:

(7) $a \leqslant 6 \cdot n + 1$ if and only if $a \in \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$.

(8) $\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \subseteq \mathbb{Z}_{6 \cdot n + 2}$.

Let us consider n. Observe that $\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$ is non empty and finite. Now we state the propositions:

(9) If $m \leqslant n$, then $\langle 0, 6 \cdot m + 1 \rangle_{\mathbb{N}} \subseteq \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$. The theorem is a consequence of (7).

(10) If $m < n$, then $\langle 0, 6 \cdot m + 1 \rangle_{\mathbb{N}} \subset \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$. The theorem is a consequence of (9) and (7).

(11) If $\langle 0, 6 \cdot m + 1 \rangle_{\mathbb{N}} = \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}}$, then $m = n$. The theorem is a consequence of (10).

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

(12) $2 \in \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P}$.

(13) $3 \in \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P}$.

(14) $5 \in \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P}$.

(15) $7 \in \langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P}$.

Let n be a non zero natural number. Observe that $\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P}$ is non empty.

The functor $\max\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{P}}$ yielding a prime number is defined by the term

(Def. 3) $\max(\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{N}} \cap \mathbb{P})$.

Now we state the propositions:

(16) Let us consider non zero natural numbers m, n. Suppose $m \leqslant n$. Then $\max\langle 0, 6 \cdot m + 1 \rangle_{\mathbb{P}} \leqslant \max\langle 0, 6 \cdot n + 1 \rangle_{\mathbb{P}}$. The theorem is a consequence of (9).

(17) $\max\langle 0, 6 \cdot 20 + 1 \rangle_{\mathbb{P}} = \max\langle 0, 6 \cdot 19 + 1 \rangle_{\mathbb{P}}$.
PROOF: Set $a = 20$. Set $b = 19$. Set $X = \langle 0, 6 \cdot a + 1 \rangle_{\mathbb{N}}$. Set $B = \max\langle 0, 6 \cdot b + 1 \rangle_{\mathbb{P}}$. $B \leqslant 6 \cdot b + 1$. For every extended real x such that $x \in X \cap \mathbb{P}$ holds $x \leqslant B$. $\square$

(18) $\langle 0, 6 \cdot 1 + 1 \rangle_{\mathbb{N}} = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

(19) $\max\langle 0, 6 \cdot 1 + 1 \rangle_{\mathbb{P}} = 7$.

(20) If $\mathrm{pr}(m) = \mathrm{pr}(n)$, then $m = n$.

Let p be a natural number. Assume p is prime. The functor primeindex(p) yielding an element of $\mathbb{N}$ is defined by

(Def. 4) $\mathrm{pr}(it) = p$.

Now we state the propositions:

(21) If primeindex(p) = primeindex(q), then $p = q$.

(22) primeindex(2) = 0.

(23) primeindex(3) = 1.

(24) primeindex(5) = 2.

(25) primeindex(7) = 3.

(26) primeindex(11) = 4.

(27) primeindex(13) = 5.

(28) If $n > 0$, then $p < \mathrm{pr}(n + \mathrm{primeindex}(p))$.

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

(29) $\mathrm{pr}(1 + \mathrm{primeindex}(\max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}})) \geqslant 6 \cdot n + 5$. The theorem is a consequence of (28).

(30) $\mathrm{pr}(1 + \mathrm{primeindex}(\max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}})) - \max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}} \geqslant 4$. The theorem is a consequence of (7) and (29).

(31) $\max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}}$ and $\mathrm{pr}(1 + \mathrm{primeindex}(\max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}}))$ are not twin. The theorem is a consequence of (28), (30), and (6).

(32) Let us consider a non zero natural number m. Suppose $6 \cdot m + 1$ is prime. Then $6 \cdot m + 1 = \max\langle 0, 6 \cdot m + 1\rangle_{\mathbb{P}}$. The theorem is a consequence of (7).

Let us consider non zero natural numbers m, n. Now we state the propositions:

(33) If $6 \cdot n + 1$ is prime and $m < n$, then $\max\langle 0, 6 \cdot m + 1\rangle_{\mathbb{P}} < \max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}}$. The theorem is a consequence of (16), (32), and (7).

(34) Suppose $6 \cdot m + 1$ is prime and $6 \cdot n + 1$ is prime and $\max\langle 0, 6 \cdot m + 1\rangle_{\mathbb{P}} = \max\langle 0, 6 \cdot n + 1\rangle_{\mathbb{P}}$. Then $m = n$. The theorem is a consequence of (33).

The functor $\{6n + 1 : n \in \mathbb{N}\}_{\mathbb{P}}$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 5) $\{6 \cdot n + 1$, where n is a natural number : $6 \cdot n + 1$ is prime$\}$.

Note that $\{6n + 1 : n \in \mathbb{N}\}_{\mathbb{P}}$ has non empty elements. Now we state the proposition:

(35) $\{6n + 1 : n \in \mathbb{N}\}_{\mathbb{P}} \subseteq \mathbb{P}$.

One can check that $\{6n + 1 : n \in \mathbb{N}\}_{\mathbb{P}}$ is infinite. Now we state the proposition:

(36) $\{\langle p, q\rangle$, where p, q are prime numbers : p and q are not twin$\}$ is infinite. Proof: Set $A = \{\langle p, q\rangle$, where p, q are prime numbers : p and q are not twin$\}$. Define $\mathcal{S}$(non zero natural number) = $\max\langle 0, 6 \cdot \$_1 + 1\rangle_{\mathbb{P}}$. Define $\mathcal{F}$(non zero natural number) = $\langle \mathcal{S}(\$_1), \mathrm{pr}(1 + \mathrm{primeindex}(\mathcal{S}(\$_1)))\rangle$.

Define $\mathcal{P}$[natural number, object] $\equiv$ there exists a non zero natural number n such that $n = \$_1$ and $\$_2 = \mathcal{F}(n)$. Set $P = \{6n + 1 : n \in \mathbb{N}\}_{\mathbb{P}}$. Define $\mathcal{C}$(element of P) = $(\$_1 - 1 \operatorname{div} 6)(\in \mathbb{N})$. Consider C being a function

from P into $\mathbb{N}$ such that for every element p of P, $C(p) = \mathcal{C}(p)$. C is one-to-one. Reconsider $D = \operatorname{rng} C$ as an infinite subset of $\mathbb{N}$. For every element d of D, $6 \cdot d + 1$ is prime. For every element i of D, there exists an object j such that $\mathcal{P}[i, j]$. Consider f being a many sorted set indexed by D such that for every element d of D, $\mathcal{P}[d, f(d)]$. $\operatorname{rng} f \subseteq A$. f is one-to-one. □

3. Problem 94

Let c be a complex number. We say that c is a product of three different primes if and only if

(Def. 6) there exist prime numbers p, q, r such that p, q, r are mutually different and $c = p \cdot q \cdot r$.

Now we state the propositions:

(37) If $n > 4$, then there exists a natural number k such that $n = 2 \cdot k$ and $k > 2$ or $n = 2 \cdot k + 1$ and $k > 1$.

(38) If $n > 4$, then there exists a natural number m such that $n < m < 2 \cdot n$ and m is a product of two different primes. The theorem is a consequence of (37) and (3).

(39) If $n > 15$, then there exists a natural number m such that $n < m < 2 \cdot n$ and m is a product of three different primes. The theorem is a consequence of (3).

4. Problem 99

Now we state the proposition:

(40) $5 \mid 2^{4 \cdot n+2} + 1$.

Let us consider n. Note that $\frac{1}{5} \cdot (2^{4 \cdot n+2} + 1)$ is natural. Now we state the proposition:

(41) If $n > 1$, then $\frac{1}{5} \cdot (2^{4 \cdot n+2} + 1)$ is composite. The theorem is a consequence of (40) and (3).

5. Problem 170

Now we state the proposition:

(42) $\{\langle x, y, z\rangle$, where x, y, z are integers : $x + y + z = 3$ and $x^3 + y^3 + z^3 = 3\} = \{\langle 1, 1, 1\rangle, \langle -5, 4, 4\rangle, \langle 4, -5, 4\rangle, \langle 4, 4, -5\rangle\}$.

PROOF: Set $A = \{\langle x, y, z\rangle$, where x, y, z are integers : $x + y + z = 3$ and $x^3 + y^3 + z^3 = 3\}$. Set $B = \{\langle 1, 1, 1\rangle, \langle -5, 4, 4\rangle, \langle 4, -5, 4\rangle, \langle 4, 4, -5\rangle\}$. $A \subseteq B$ by [8, (2)]. □

6. Problem 173

Now we state the proposition:

(43) Let us consider positive natural numbers m, n. Then there exist integers a, b, c such that $\{\langle x, y\rangle$, where x, y are natural numbers : $a \cdot x + b \cdot y = c\} = \{\langle m, n\rangle\}$.

Proof: Consider a being a prime number such that $a > m + n$. Consider b being a prime number such that $b > a$. Set $A = \{\langle x, y\rangle$, where x, y are natural numbers : $a \cdot x + b \cdot y = c\}$. Set $B = \{\langle m, n\rangle\}$. $A \subseteq B$. $\square$

7. Problem 174

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

(44) $\overline{\overline{\{\langle x, y\rangle, \text{ where } x, y \text{ are positive natural numbers} : x + y = m + 1\}}} = m$.

Proof: Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $x + y = m + 1\}$. $\operatorname{Seg} m \approx A$. $\square$

(45) There exist positive natural numbers a, b, c such that $\overline{\overline{\{\langle x, y\rangle, \text{ where } x, y \text{ are positive natural numbers} : a \cdot x + b \cdot y = c\}}} = m$.

The theorem is a consequence of (44).

8. Problem 175

Now we state the proposition:

(46) Let us consider a positive natural number m. Then $\overline{\overline{\{\langle x, y\rangle, \text{ where } x, y \text{ are positive natural numbers} : x^2 + y^2 + 2 \cdot x \cdot y - m \cdot x - m \cdot y - m - 1 = 0\}}} = m$.

The theorem is a consequence of (44).

9. Problem 177

Let b, e be real numbers and n be a natural number. The functor powersFS(b, e, n) yielding a finite sequence of elements of $\mathbb{R}$ is defined by

(Def. 7) $\operatorname{len} it = n$ and for every natural number i such that $1 \leqslant i \leqslant n$ holds $it(i) = (b + i)^e$.

Now we state the propositions:

(47) $\operatorname{powersFS}(-(k+1), r, 2 \cdot (k+1)) = (\langle(-k)^r\rangle \frown \operatorname{powersFS}(-k, r, 2 \cdot k)) \frown \langle(k+1)^r\rangle$.

(48) Let us consider a positive natural number k. Then $\mathrm{powersFS}(-(k+1), r, 2 \cdot (k+1)-1) = (\langle(-k)^r\rangle \frown \mathrm{powersFS}(-k, r, 2 \cdot k - 1)) \frown \langle k^r\rangle$.

(49) $\sum \mathrm{powersFS}(-k, 3, 2 \cdot k) = k^3$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \sum \mathrm{powersFS}(-\$_1, 3, 2 \cdot \$_1) = {\$_1}^3$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(50) Let us consider a positive natural number k. Then $\sum \mathrm{powersFS}(-k, 3, 2 \cdot k - 1) = 0$.
PROOF: Define $\mathcal{P}[\text{non zero natural number}] \equiv \sum \mathrm{powersFS}(-\$_1, 3, 2 \cdot \$_1 - 1) = 0$. $\mathcal{P}[1]$. For every non zero natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every non zero natural number n, $\mathcal{P}[n]$. □

(51) Let us consider a positive natural number n. Then there exists an integer x and there exists a natural number y such that $\sum \mathrm{powersFS}(x, 3, n) = y^3$.
The theorem is a consequence of (49) and (50).

10. PROBLEM 179

Now we state the proposition:

(52) Let us consider a real number x. Then $(x+1)^3 + (x+2)^3 + (x+3)^3 + (x+4)^3 = (x+10)^3$ if and only if $x = 10$.
PROOF: If $(x+1)^3 + (x+2)^3 + (x+3)^3 + (x+4)^3 = (x+10)^3$, then $x = 10$. □

11. PROBLEM 186

Now we state the proposition:

(53) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $2^x + 1 = y^{\mathbf{2}}\} = \{\langle 3, 3\rangle\}$.
PROOF: Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $2^x + 1 = y^{\mathbf{2}}\}$. $A \subseteq \{\langle 3, 3\rangle\}$ by [11, (36)]. □

12. PROBLEM 187

Now we state the proposition:

(54) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $2^x - 1 = y^{\mathbf{2}}\} = \{\langle 1, 1\rangle\}$.
PROOF: Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $2^x - 1 = y^{\mathbf{2}}\}$. $A \subseteq \{\langle 1, 1\rangle\}$ by [5, (11)]. □

13. Problem 189

Now we state the propositions:

(55) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $(2\cdot x+1)^{\mathbf{2}}-2\cdot y^{\mathbf{2}}+1=0\}$ is infinite.

Proof: Define $\mathcal{R}$(complex number, complex number) $= (2\cdot \$_1+1)^{\mathbf{2}}-2\cdot \$_2^{\mathbf{2}}+1$. Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $\mathcal{R}(x, y) = 0\}$. Set $f =$ recSeqCart$(3, 5, 3, 2, 1, 4, 3, 2)$. Define $\mathcal{N}$[natural number] $\equiv f(\$_1) \in A$. If $\mathcal{N}[a]$, then $\mathcal{N}[a+1]$. $\mathcal{N}[a]$. rng $f \subseteq A$. $\square$

(56) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $x^{\mathbf{2}} + (x+1)^{\mathbf{2}} = y^{\mathbf{2}}\}$ is infinite. The theorem is a consequence of (55).

14. Problem 190

Now we state the propositions:

(57) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $3\cdot x^{\mathbf{2}}+3\cdot x-y^{\mathbf{2}}+1=0\}$ is infinite.

Proof: Define $\mathcal{R}$(complex number, complex number) $= 3\cdot \$_1^{\mathbf{2}}+3\cdot \$_1-\$_2^{\mathbf{2}}+1$. Set $A = \{\langle x, y\rangle$, where x, y are positive natural numbers : $\mathcal{R}(x, y) = 0\}$. Set $f =$ recSeqCart$(7, 13, 7, 4, 3, 12, 7, 6)$. Define $\mathcal{N}$[natural number] $\equiv f(\$_1) \in A$. If $\mathcal{N}[a]$, then $\mathcal{N}[a+1]$. $\mathcal{N}[a]$. rng $f \subseteq A$. $\square$

(58) $\{\langle x, y\rangle$, where x, y are positive natural numbers : $(x+1)^3 - x^3 = y^{\mathbf{2}}\}$ is infinite. The theorem is a consequence of (57).

15. Problem 193

Now we state the propositions:

(59) If i is even, then $i^{\mathbf{2}} \bmod 8 = 0$ or $i^{\mathbf{2}} \bmod 8 = 4$.

(60) If i is odd, then $i^{\mathbf{2}} \bmod 8 = 1$.

(61) (i) $i^{\mathbf{2}} \bmod 8 = 0$, or

(ii) $i^{\mathbf{2}} \bmod 8 = 1$, or

(iii) $i^{\mathbf{2}} \bmod 8 = 4$.

(62) If $p = 4 \cdot k + 3$ and $p \mid i^{\mathbf{2}} + j^{\mathbf{2}}$, then $p \mid i$ and $p \mid j$.

(63) $x^2 - y^3 \neq 7$. The theorem is a consequence of (59) and (60).

16. PROBLEM 194

Now we state the proposition:

(64) Let us consider an odd natural number c. Then $x^2 - y^3 \neq (2 \cdot c)^3 - 1$. The theorem is a consequence of (60) and (59).

17. PROBLEM 197

Let f, g be positive yielding finite sequences. Let us note that $f^\frown g$ is positive yielding. Let x be a positive real number. Let us note that $\langle x \rangle$ is positive yielding. Let x, y be positive real numbers. Let us note that $\langle x, y \rangle$ is positive yielding. Now we state the proposition:

(65) If $n > 0$, then there exists a positive yielding finite sequence f of elements of $\mathbb{N}$ such that $\operatorname{len} f = n$ and $\sum f = \prod f$.

18. PROBLEM 199

Now we state the propositions:

(66) Let us consider positive natural numbers x, y. Suppose $y \cdot (3 \cdot y - 1) = x \cdot (x + 1)$. Then $\operatorname{Polygon}(3, x) = \operatorname{Polygon}(5, y)$.

(67) Let us consider positive natural numbers m, n, and a natural number s. If $\operatorname{Polygon}(s, m) = \operatorname{Polygon}(s, n)$ and $s \geqslant 2$, then $m = n$.

(68) $\{\langle x, y \rangle$, where x, y are positive natural numbers : $y \cdot (3 \cdot y - 1) - x \cdot (x + 1) = 0\}$ is infinite.

PROOF: Define $\mathcal{R}(\text{complex number}, \text{complex number}) = \$_2 \cdot (3 \cdot \$_2 - 1) - \$_1 \cdot (\$_1 + 1)$. Set $A = \{\langle x, y \rangle$, where x, y are positive natural numbers : $\mathcal{R}(x, y) = 0\}$. Set $f = \operatorname{recSeqCart}(1, 1, 7, 12, 1, 4, 7, 1)$. Define $\mathcal{N}[\text{natural number}] \equiv f(\$_1) \in A$. If $\mathcal{N}[a]$, then $\mathcal{N}[a + 1]$. $\mathcal{N}[a]$. $\operatorname{rng} f \subseteq A$. $\square$

(69) $\{n$, where n is a 3-gonal natural number : n is 5-gonal$\}$ is infinite.

PROOF: Set $A = \{n$, where n is a 3-gonal natural number : n is 5-gonal$\}$. Set $B = \{\langle x, y \rangle$, where x, y are positive natural numbers : $y \cdot (3 \cdot y - 1) - x \cdot (x + 1) = 0\}$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a positive natural number n such that $n = (\$_1)_{\mathbf{1}}$ and $\$_2 = \operatorname{Polygon}(3, n)$. For every object e such that $e \in B$ there exists an object u such that $\mathcal{P}[e, u]$. Consider f being a function such that $\operatorname{dom} f = B$ and for every object e such that $e \in B$ holds $\mathcal{P}[e, f(e)]$. f is one-to-one. $\operatorname{rng} f \subseteq A$. $\square$

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] Artur Korniłowicz. Elementary number theory problems. Part VIII. *Formalized Mathematics*, 31(1):87–100, 2023. doi:10.2478/forma-2023-0009.

[5] Artur Korniłowicz. Elementary number theory problems. Part IX. *Formalized Mathematics*, 31(1):161–169, 2023. doi:10.2478/forma-2023-0015.

[6] Adam Naumowicz. Dataset description: Formalization of elementary number theory in Mizar. In Christoph Benzmüller and Bruce R. Miller, editors, *Intelligent Computer Mathematics – 13th International Conference, CICM 2020, Bertinoro, Italy, July 26–31, 2020, Proceedings*, volume 12236 of *Lecture Notes in Computer Science*, pages 303–308. Springer, 2020. doi:10.1007/978-3-030-53518-6_22.

[7] Adam Naumowicz. Extending numeric automation for number theory formalizations in Mizar. In Catherine Dubois and Manfred Kerber, editors, *Intelligent Computer Mathematics – 16th International Conference, CICM 2023, Cambridge, UK, September 5–8, 2023, Proceedings*, volume 14101 of *Lecture Notes in Computer Science*, pages 309–314. Springer, 2023. doi:10.1007/978-3-031-42753-4_23.

[8] Marco Riccardi. Solution of cubic and quartic equations. *Formalized Mathematics*, 17(**2**): 117–122, 2009. doi:10.2478/v10037-009-0012-z.

[9] Wacław Sierpiński. *Elementary Theory of Numbers*. PWN, Warsaw, 1964.

[10] Wacław Sierpiński. *250 Problems in Elementary Number Theory*. Elsevier, 1970.

[11] Rafał Ziobro. Prime factorization of sums and differences of two like powers. *Formalized Mathematics*, 24(**3**):187–198, 2016. doi:10.1515/forma-2016-0015.

Accepted November 21, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 181–192, 2023
DOI: 10.2478/forma-2023-0017
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Multidimensional Measure Space and Integration[1]

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

Yasunari Shidama
Karuizawa Hotch 244-1
Nagano, Japan

Summary. This paper introduces multidimensional measure spaces and the integration of functions on these spaces in Mizar. Integrals on the multidimensional Cartesian product measure space are defined and appropriate formal apparatus to deal with this notion is provided as well.

MSC: 28A35 68V20

Keywords: measure in product spaces; iterated integral

MML identifier: `MEASUR13`, version: `8.1.14 5.76.1452`

Introduction

In this paper, using the Mizar system [1], [11], we introduce multidimensional measure spaces and the integration ([14], [2]) of functions on these spaces (for interesting survey of formalizations of real analysis in another proof-assistants like ACL2 [10], Isabelle/HOL [9], Coq [3], see [4]). It is the continuation of the mechanisation of this topic as developed in [5] and [8]. In constructing measures on multidimensional spaces [12], we constructed a finite sequence of Cartesian product spaces of sets in Section 1. In Section 2, using Fubini's Theorem [6], we have constructed measures on general multidimensional spaces by introducing

[1]This work was supported by JSPS KAKENHI 23K11242.

measures one by one into the finite sequence of direct product spaces obtained in Section 1. In Section 3, integrals on the m-dimensional Cartesian product measure space obtained in Section 2 are presented, and the concept of sequentially integrable, which is useful in considering integrability [7] for functions on multidimensional spaces, is introduced and its effectiveness is shown.

1. Preliminaries

Let m, n be non zero natural numbers and X be a non-empty, m-elements finite sequence. Assume $n \leqslant m$. The functor $\mathrm{ElmFin}(X, n)$ yielding a non empty set is defined by the term

(Def. 1) $X(n)$.

Let m be a natural number. A family of σ-fields of X is an m-elements finite sequence defined by

(Def. 2) for every natural number i such that $i \in \operatorname{Seg} m$ holds $it(i)$ is a σ-field of subsets of $X(i)$.

Now we state the proposition:

(1) Let us consider non zero natural numbers m, n, a non-empty, m-elements finite sequence X, and a family of σ-fields S of X. If $n \leqslant m$, then $S(n)$ is a σ-field of subsets of $\mathrm{ElmFin}(X, n)$.

Let m be a non zero natural number and X be a non-empty, m-elements finite sequence. The functor $\prod_{\mathrm{FinS}} X$ yielding a non-empty, m-elements finite sequence is defined by

(Def. 3) $it(1) = X(1)$ and for every non zero natural number i such that $i < m$ holds $it(i+1) = it(i) \times X(i+1)$.

The functor $\prod_{\mathrm{FS}} X$ yielding a set is defined by the term

(Def. 4) $(\prod_{\mathrm{FinS}} X)(m)$.

Observe that $\prod_{\mathrm{FS}} X$ is non empty. Now we state the proposition:

(2) Let us consider a non zero natural number m, a natural number k, and a non-empty, m-elements finite sequence X. If $k \leqslant m$, then $X \restriction k$ is a non-empty, k-elements finite sequence.

Let m, n be non zero natural numbers and X be a non-empty, m-elements finite sequence. Assume $n \leqslant m$. The functor $\mathrm{SubFin}(X, n)$ yielding a non-empty, n-elements finite sequence is defined by the term

(Def. 5) $X \restriction n$.

Let S be a family of σ-fields of X. Assume $n \leqslant m$. The functor $\mathrm{SubFin}(S, n)$ yielding a family of σ-fields of $\mathrm{SubFin}(X, n)$ is defined by the term

(Def. 6) $S \restriction n$.

Assume $n \leqslant m$. The functor $\mathrm{ElmFin}(S, n)$ yielding a σ-field of subsets of $\mathrm{ElmFin}(X, n)$ is defined by the term

(Def. 7) $S(n)$.

Let m be a non zero natural number. Note that a family of σ-fields of X is a family of semialgebras of X. Let S be a family of σ-fields of X.

A family of σ-measures of S is an m-elements finite sequence defined by

(Def. 8) for every natural number i such that $i \in \operatorname{Seg} m$ there exists a σ-field S_3 of subsets of $X(i)$ such that $S_3 = S(i)$ and $it(i)$ is a σ-measure on S_3.

Let m, n be non zero natural numbers and M be a family of σ-measures of S. Assume $n \leqslant m$. The functor $\mathrm{SubFin}(M, n)$ yielding a family of σ-measures of $\mathrm{SubFin}(S, n)$ is defined by the term

(Def. 9) $M \restriction n$.

Assume $n \leqslant m$. The functor $\mathrm{ElmFin}(M, n)$ yielding a σ-measure on $\mathrm{ElmFin}(S, n)$ is defined by the term

(Def. 10) $M(n)$.

Now we state the proposition:

(3) Let us consider non zero natural numbers m, i, j, k, and a non-empty, m-elements finite sequence X. Suppose $i \leqslant j \leqslant k \leqslant m$.
Then $(\prod_{\mathrm{FinS}} \mathrm{SubFin}(X, j))(i) = (\prod_{\mathrm{FinS}} \mathrm{SubFin}(X, k))(i)$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $1 \leqslant \$_1 \leqslant j$, then $(\prod_{\mathrm{FinS}} \mathrm{SubFin}(X, j))(\$_1) = (\prod_{\mathrm{FinS}} \mathrm{SubFin}(X, k))(\$_1)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. $\square$

Let us consider non zero natural numbers m, n and a non-empty, m-elements finite sequence X. Now we state the propositions:

(4) If $n \leqslant m$, then $(\prod_{\mathrm{FinS}} X)(n) = (\prod_{\mathrm{FinS}} \mathrm{SubFin}(X, n))(n)$. The theorem is a consequence of (3).

(5) If $n < m$, then $(\prod_{\mathrm{FinS}} X)(n+1) = (\prod_{\mathrm{FinS}} \mathrm{SubFin}(X, n))(n) \times \mathrm{ElmFin}(X, n+1)$. The theorem is a consequence of (4).

(6) Let us consider a non zero natural number n, and a non-empty, $(n+1)$-elements finite sequence X. Then $\prod_{\mathrm{FS}} X = \prod_{\mathrm{FS}} \mathrm{SubFin}(X, n) \times \mathrm{ElmFin}(X, n+1)$. The theorem is a consequence of (4).

Let us consider non zero natural numbers m, n, k and a non-empty, m-elements finite sequence X. Now we state the propositions:

(7) If $k \leqslant n \leqslant m$, then $\mathrm{SubFin}(X, k) = \mathrm{SubFin}(\mathrm{SubFin}(X, n), k)$.

(8) If $k \leqslant n \leqslant m$, then $\mathrm{ElmFin}(X, k) = \mathrm{ElmFin}(\mathrm{SubFin}(X, n), k)$.

Let us consider non zero natural numbers m, n and a non-empty, m-elements finite sequence X. Now we state the propositions:

(9) If $n < m$, then $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, n+1) = \prod_{\mathrm{FS}} \mathrm{SubFin}(X, n) \times \mathrm{ElmFin}(X, n+1)$. The theorem is a consequence of (8), (6), and (7).

(10) If $n < m$, then $(\prod_{\mathrm{FinS}} \mathrm{SubFin}(X, n+1))(n+1) = (\prod_{\mathrm{FinS}} \mathrm{SubFin}(X, n))(n) \times \mathrm{ElmFin}(X, n+1)$. The theorem is a consequence of (9).

(11) Let us consider non zero natural numbers n, i, a non-empty, $(n+1)$-elements finite sequence X, and a family of σ-fields S of X. Suppose $i \leqslant n$. Then $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, i) = \prod_{\mathrm{FS}} \mathrm{SubFin}(\mathrm{SubFin}(X, n), i)$. The theorem is a consequence of (7).

(12) Let us consider non zero natural numbers m, n, k, a non-empty, m-elements finite sequence X, and a family of σ-fields S of X. Suppose $k \leqslant n \leqslant m$. Then $\mathrm{ElmFin}(S, k) = \mathrm{ElmFin}(\mathrm{SubFin}(S, n), k)$.

(13) Let us consider non zero natural numbers m, n, k, a non-empty, m-elements finite sequence X, a non-empty, n-elements finite sequence Y, and a family of σ-fields S of X. Suppose $n \leqslant m$ and $Y = X{\restriction}n$. Then $\mathrm{SubFin}(S, n)$ is a family of σ-fields of Y.

PROOF: For every natural number i such that $i \in \mathrm{Seg}\, n$ holds $(\mathrm{SubFin}(S, n))(i)$ is a σ-field of subsets of $Y(i)$. □

(14) Let us consider non zero natural numbers m, n, k, a non-empty, m-elements finite sequence X, and a family of σ-fields S of X. Suppose $k \leqslant n \leqslant m$. Then $\mathrm{SubFin}(S, k) = \mathrm{SubFin}(\mathrm{SubFin}(S, n), k)$.

(15) Let us consider a non zero natural number m, and a non-empty, m-elements finite sequence X. Then there exists a function F from $\prod_{\mathrm{FS}} X$ into $\prod X$ such that F is one-to-one and onto.

PROOF: Define $\mathcal{P}[\text{non zero natural number}] \equiv$ for every non-empty, $\$_1$-elements finite sequence X, there exists a function F from $\prod_{\mathrm{FS}} X$ into $\prod X$ such that F is one-to-one and onto. $\mathcal{P}[1]$ by [13, (2)]. For every non zero natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every non zero natural number n, $\mathcal{P}[n]$. □

(16) Let us consider non zero natural numbers m, n, a non-empty, m-elements finite sequence X, and a family P of semialgebras of $\prod_{\mathrm{FinS}} X$. Suppose $n \leqslant m$. Then $P(n)$ is a semialgebra of sets of $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, n)$. The theorem is a consequence of (4).

Let us consider non zero natural numbers m, n, k, a non-empty, m-elements finite sequence X, a family of σ-fields S of X, and a family of σ-measures M of S. Now we state the propositions:

(17) If $k \leqslant n \leqslant m$, then $\mathrm{ElmFin}(M, k) = \mathrm{ElmFin}(\mathrm{SubFin}(M, n), k)$.

(18) If $k \leqslant n \leqslant m$, then $\mathrm{SubFin}(M, k) = \mathrm{SubFin}(\mathrm{SubFin}(M, n), k)$.

2. CONSTRUCTION OF m-DIMENSIONAL MEASURE SPACE

Let m be a non zero natural number, X be a non-empty, m-elements finite sequence, and S be a family of σ-fields of X. The functor $\sigma\mathrm{FldFS}_{\mathrm{Prod}}(S)$ yielding a family of σ-fields of $\prod_{\mathrm{FinS}} X$ is defined by

(Def. 11) $it(1) = S(1)$ and for every non zero natural number i such that $i < m$ there exists a σ-field S_3 of subsets of $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, i)$ such that $S_3 = it(i)$ and $it(i+1) = \sigma(\mathrm{MeasRect}(S_3, \mathrm{ElmFin}(S, i+1)))$.

Now we state the proposition:

(19) Let us consider non zero natural numbers m, n, a non-empty, m-elements finite sequence X, and a family of σ-fields S of X. Suppose $n \leqslant m$. Then $(\sigma\mathrm{FldFS}_{\mathrm{Prod}}(S))(n)$ is a σ-field of subsets of $(\prod_{\mathrm{FinS}} X)(n)$.

Let m be a non zero natural number, X be a non-empty, m-elements finite sequence, and S be a family of σ-fields of X. The functor $\prod_{\mathrm{Field}} S$ yielding a σ-field of subsets of $\prod_{\mathrm{FS}} X$ is defined by the term

(Def. 12) $(\sigma\mathrm{FldFS}_{\mathrm{Prod}}(S))(m)$.

Now we state the propositions:

(20) Let us consider non zero natural numbers m, n, k, a non-empty, m-elements finite sequence X, and a family of σ-fields S of X. Suppose $k \leqslant n \leqslant m$. Then $(\sigma\mathrm{FldFS}_{\mathrm{Prod}}(S))(k) = (\sigma\mathrm{FldFS}_{\mathrm{Prod}}(\mathrm{SubFin}(S, n)))(k)$. PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $1 \leqslant \$_1 \leqslant n$, then $(\sigma\mathrm{FldFS}_{\mathrm{Prod}}(S))(\$_1) = (\sigma\mathrm{FldFS}_{\mathrm{Prod}}(\mathrm{SubFin}(S, n)))(\$_1)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i, $\mathcal{P}[i]$. $\square$

(21) Let us consider non zero natural numbers m, n, a non-empty, m-elements finite sequence X, and a family of σ-fields S of X. Suppose $n < m$. Then $\prod_{\mathrm{Field}} \mathrm{SubFin}(S, n+1) = \sigma(\mathrm{MeasRect}(\prod_{\mathrm{Field}} \mathrm{SubFin}(S, n), \mathrm{ElmFin}(S, n+1)))$. The theorem is a consequence of (8), (12), (7), and (20).

Let m be a non zero natural number, X be a non-empty, m-elements finite sequence, S be a family of σ-fields of X, and M be a family of σ-measures of S. The functor $\sigma\mathrm{MesFS}_{\mathrm{Prod}}(M)$ yielding a family of σ-measures of $\sigma\mathrm{FldFS}_{\mathrm{Prod}}(S)$ is defined by

(Def. 13) $it(1) = M(1)$ and for every non zero natural number i such that $i < m$ there exists a σ-measure M_3 on $\prod_{\mathrm{Field}} \mathrm{SubFin}(S, i)$ such that $M_3 = it(i)$ and $it(i+1) = \mathrm{Prod}\,\sigma\text{-Meas}(M_3, \mathrm{ElmFin}(M, i+1))$.

Now we state the proposition:

(22) Let us consider non zero natural numbers m, n, a non-empty, m-elements finite sequence X, a family of σ-fields S of X, and a family of σ-measures

M of S. Suppose $n \leqslant m$. Then $(\sigma\mathrm{MesFS}_{\mathrm{Prod}}(M))(n)$ is a σ-measure on $\prod_{\mathrm{Field}} \mathrm{SubFin}(S, n)$.

PROOF: Set $P_1 = \sigma\mathrm{MesFS}_{\mathrm{Prod}}(M)$. Define $\mathcal{L}$[natural number] $\equiv$ if $1 \leqslant \$_1 \leqslant m$, then there exists a non zero natural number k such that $k = \$_1$ and $P_1(\$_1)$ is a σ-measure on $\prod_{\mathrm{Field}} \mathrm{SubFin}(S, k)$. For every natural number i such that $\mathcal{L}[i]$ holds $\mathcal{L}[i+1]$. For every natural number n, $\mathcal{L}[n]$. □

Let m be a non zero natural number, X be a non-empty, m-elements finite sequence, S be a family of σ-fields of X, and M be a family of σ-measures of S. The functor $\mathrm{Measure}_{\mathrm{Prod}}(M)$ yielding a σ-measure on $\prod_{\mathrm{Field}} S$ is defined by the term

(Def. 14) $(\sigma\mathrm{MesFS}_{\mathrm{Prod}}(M))(m)$.

We say that M is σ-finite if and only if

(Def. 15) for every natural number i such that $i \in \mathrm{Seg}\, m$ there exists a non empty set X_2 and there exists a σ-field S_3 of subsets of X_2 and there exists a σ-measure M_3 on S_3 such that $X_2 = X(i)$ and $S_3 = S(i)$ and $M_3 = M(i)$ and M_3 is σ-finite.

Now we state the propositions:

(23) Let us consider non zero natural numbers m, n, k, a non-empty, m-elements finite sequence X, a family of σ-fields S of X, and a family of σ-measures M of S. Suppose $k \leqslant n \leqslant m$. Then $(\sigma\mathrm{MesFS}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)))(k) = (\sigma\mathrm{MesFS}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k)))(k)$. The theorem is a consequence of (7), (14), (8), (12), and (17).

(24) Let us consider non zero natural numbers m, n, a non-empty, m-elements finite sequence X, a family of σ-fields S of X, and a family of σ-measures M of S. Suppose $n \leqslant m$. Then $(\sigma\mathrm{MesFS}_{\mathrm{Prod}}(M))(n) = \mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n))$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ if $1 \leqslant \$_1 \leqslant m$, then there exists a non zero natural number k such that $k = \$_1$ and $(\sigma\mathrm{MesFS}_{\mathrm{Prod}}(M))(\$_1) = \mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k))$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every natural number i, $\mathcal{P}[i]$. □

(25) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, and a family of σ-measures M of S. Then $\mathrm{Measure}_{\mathrm{Prod}}(M) = \mathrm{Prod}\,\sigma\text{-Meas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), \mathrm{ElmFin}(M, n+1))$. The theorem is a consequence of (24).

(26) Let us consider a non empty set X, a field S of subsets of X, a set sequence E of S, and a natural number i. Then (the partial unions of E)$(i) \in S$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ (the partial unions of E)$(\$_1) \in S$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every

natural number n, $\mathcal{P}[n]$. $\square$

(27) Let us consider non empty sets X, Y, a σ-field S_1 of subsets of X, a σ-field S_2 of subsets of Y, a σ-measure M_1 on S_1, and a σ-measure M_2 on S_2. Suppose M_1 is σ-finite and M_2 is σ-finite. Then $\mathrm{ProdMeas}(M_1, M_2)$ is σ-finite.

PROOF: Set $M = \mathrm{ProdMeas}(M_1, M_2)$. Consider E_1 being a set sequence of S_1 such that for every natural number n, $M_1(E_1(n)) < +\infty$ and $\bigcup E_1 = X$. Consider E_2 being a set sequence of S_2 such that for every natural number n, $M_2(E_2(n)) < +\infty$ and $\bigcup E_2 = Y$. Set F_1 = the partial unions of E_1. Set F_2 = the partial unions of E_2. Define $\mathcal{G}(\text{natural number}) = (F_1(\$_1) \times F_2(\$_1))(\in \sigma(\mathrm{MeasRect}(S_1, S_2)))$. Consider E being a function from $\mathbb{N}$ into $\sigma(\mathrm{MeasRect}(S_1, S_2))$ such that for every element i of $\mathbb{N}$, $E(i) = \mathcal{G}(i)$.

For every natural number i, $E(i) = F_1(i) \times F_2(i)$. For every natural number i, $E(i) \in \sigma(\mathrm{MeasRect}(S_1, S_2))$. For every object z, $z \in \bigcup E$ iff $z \in X \times Y$. Define $\mathcal{Q}[\text{natural number}] \equiv M_1(F_1(\$_1)), M_2(F_2(\$_1)) \in \mathbb{R}$. For every natural number i such that $\mathcal{Q}[i]$ holds $\mathcal{Q}[i+1]$. For every natural number i, $\mathcal{Q}[i]$. For every natural number i, $M(E(i)) < +\infty$. $\square$

(28) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, and a family of σ-measures M of S. Then $\mathrm{Measure}_{\mathrm{Prod}}(M) = \mathrm{ProdMeas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), \mathrm{ElmFin}(M, n+1))$. The theorem is a consequence of (25).

(29) Let us consider a non zero natural number m, a non-empty, m-elements finite sequence X, a family of σ-fields S of X, and a family of σ-measures M of S. Suppose M is σ-finite. Then $\mathrm{Measure}_{\mathrm{Prod}}(M)$ is σ-finite.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non zero natural number n for every non-empty, n-elements finite sequence X for every family of σ-fields S of X for every family of σ-measures M of S such that M is σ-finite and $\$_1 = n$ holds $\mathrm{Measure}_{\mathrm{Prod}}(M)$ is σ-finite. $\mathcal{P}[1]$. For every non zero natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. For every non zero natural number k, $\mathcal{P}[k]$. $\square$

Let us consider non zero natural numbers m, n, a non-empty, m-elements finite sequence X, a family of σ-fields S of X, and a family of σ-measures M of S. Now we state the propositions:

(30) If $n \leqslant m$ and M is σ-finite, then $\mathrm{SubFin}(M, n)$ is σ-finite.

PROOF: Set $X_6 = \mathrm{SubFin}(X, n)$. Set $S_6 = \mathrm{SubFin}(S, n)$. Set $M_6 = \mathrm{SubFin}(M, n)$. For every natural number j such that $j \in \mathrm{Seg}\, n$ there exists a non empty set X_3 and there exists a σ-field S_4 of subsets of X_3 and there exists a σ-measure M_4 on S_4 such that $X_3 = X_6(j)$ and $S_4 = S_6(j)$ and $M_4 = M_6(j)$ and M_4 is σ-finite. $\square$

(31) If $n \leqslant m$ and M is σ-finite, then $\mathrm{ElmFin}(M, n)$ is σ-finite.

3. Integrability of Functions on $(n+1)$-dimensional Space

Now we state the propositions:

(32) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, a family of σ-measures M of S, and a partial function f from $\prod_{\mathrm{FS}} X$ to $\overline{\mathbb{R}}$. Suppose f is integrable on $\mathrm{Measure}_{\mathrm{Prod}}(M)$. Then there exists a partial function g from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, n) \times \mathrm{ElmFin}(X, n+1)$ to $\overline{\mathbb{R}}$ such that

(i) $f = g$, and

(ii) g is integrable on $\mathrm{ProdMeas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), \mathrm{ElmFin}(M, n+1))$, and

(iii) $\int f \,\mathrm{d}\, \mathrm{Measure}_{\mathrm{Prod}}(M) = \int g \,\mathrm{d}\, \mathrm{ProdMeas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), \mathrm{ElmFin}(M, n+1))$.

The theorem is a consequence of (28), (6), and (21).

(33) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, a family of σ-measures M of S, a partial function f from $\prod_{\mathrm{FS}} X$ to $\overline{\mathbb{R}}$, and a partial function g from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, n) \times \mathrm{ElmFin}(X, n+1)$ to $\overline{\mathbb{R}}$.

Suppose M is σ-finite and f is integrable on $\mathrm{Measure}_{\mathrm{Prod}}(M)$ and $f = g$ and for every element y of $\mathrm{ElmFin}(X, n+1)$, $(\mathrm{Integral1}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), |g|))(y) < +\infty$. Then

(i) for every element y of $\mathrm{ElmFin}(X, n+1)$, $\mathrm{ProjPMap2}(g, y)$ is integrable on $\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n))$, and

(ii) for every element V of $\mathrm{ElmFin}(S, n+1)$, $\mathrm{Integral1}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), g)$ is V-measurable, and

(iii) $\mathrm{Integral1}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), g)$ is integrable on $\mathrm{ElmFin}(M, n+1)$, and

(iv) $\int g \,\mathrm{d}\, \mathrm{ProdMeas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), \mathrm{ElmFin}(M, n+1)) = \int \mathrm{Integral1}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), g) \,\mathrm{d}\, \mathrm{ElmFin}(M, n+1)$, and

(v) $\mathrm{Integral1}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), g) \in$ the L^1 functionsof $\mathrm{ElmFin}(M, n+1)$.

Proof: There exists a partial function g_0 from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, n) \times \mathrm{ElmFin}(X, n+1)$ to $\overline{\mathbb{R}}$ such that $f = g_0$ and g_0 is integrable on $\mathrm{ProdMeas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, n)), \mathrm{ElmFin}(M, n+1))$ and $\int f \,\mathrm{d}\, \mathrm{Measure}_{\mathrm{Prod}}(M) = \int g_0$

d ProdMeas(Measure$_{\mathrm{Prod}}$(SubFin(M,n)), ElmFin$(M,n+1)$). For every natural number j such that $j \in \operatorname{Seg} n$ there exists a non empty set X_3 and there exists a σ-field S_4 of subsets of X_3 and there exists a σ-measure m_1 on S_4 such that $X_3 = (\mathrm{SubFin}(X,n))(j)$ and $S_4 = (\mathrm{SubFin}(S,n))(j)$ and $m_1 = (\mathrm{SubFin}(M,n))(j)$ and m_1 is σ-finite. Measure$_{\mathrm{Prod}}$(SubFin(M,n)) is σ-finite. □

Let n be a non zero natural number, X be a non-empty, $(n+1)$-elements finite sequence, f be a partial function from $\prod_{\mathrm{FS}} X$ to $\overline{\mathbb{R}}$, and x be an element of $\prod_{\mathrm{FS}}$ SubFin(X,n). The functor ProjPMap1(f,x) yielding a partial function from ElmFin$(X,n+1)$ to $\overline{\mathbb{R}}$ is defined by

(Def. 16) there exists a partial function g from $\prod_{\mathrm{FS}}$ SubFin$(X,n) \times$ ElmFin$(X,n+1)$ to $\overline{\mathbb{R}}$ such that $f = g$ and $it =$ ProjPMap1(g,x).

Now we state the propositions:

(34) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, and a family of σ-measures M of S. Then $\prod_{\mathrm{Field}} S = \sigma(\mathrm{MeasRect}(\prod_{\mathrm{Field}} \mathrm{SubFin}(S,n), \mathrm{ElmFin}(S,n+1)))$. The theorem is a consequence of (21).

(35) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, a family of σ-measures M of S, a partial function f from $\prod_{\mathrm{FS}} X$ to $\overline{\mathbb{R}}$, and a partial function f_3 from $\prod_{\mathrm{FS}}$ SubFin$(X,n) \times$ ElmFin$(X,n+1)$ to $\overline{\mathbb{R}}$.

Suppose M is σ-finite and $f = f_3$ and f is integrable on Measure$_{\mathrm{Prod}}(M)$ and for every element x of $\prod_{\mathrm{FS}}$ SubFin(X,n), (Integral2(ElmFin$(M,n+1)$, $|f_3|$))$(x) < +\infty$. Then

(i) $\int f \mathrm{d}\,\mathrm{Measure}_{\mathrm{Prod}}(M) = \int f_3 \,\mathrm{d}\,\mathrm{ProdMeas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M,n)), \mathrm{ElmFin}(M,n+1))$, and

(ii) for every element x of $\prod_{\mathrm{FS}}$ SubFin(X,n), ProjPMap1(f_3,x) is integrable on ElmFin$(M,n+1)$, and

(iii) for every element U of $\prod_{\mathrm{Field}}$ SubFin(S,n), Integral2(ElmFin$(M,n+1)$, f_3) is U-measurable, and

(iv) Integral2(ElmFin$(M,n+1)$, f_3) is integrable on Measure$_{\mathrm{Prod}}$(SubFin(M,n)), and

(v) $\int f_3 \,\mathrm{d}\,\mathrm{ProdMeas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M,n)), \mathrm{ElmFin}(M,n+1)) = \int \mathrm{Integral2}(\mathrm{ElmFin}(M,n+1), f_3) \,\mathrm{d}\,\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M,n))$, and

(vi) Integral2(ElmFin$(M,n+1)$, f_3) $\in$ theL^1 functions of Measure$_{\mathrm{Prod}}$(SubFin(M,n)).

The theorem is a consequence of (6), (28), (29), (30), (31), and (21).

(36) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, a family of σ-measures M of S, a partial function f from $\prod_{\mathrm{FS}} X$ to $\overline{\mathbb{R}}$, a partial function f_1 from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X,n) \times \mathrm{ElmFin}(X,n+1)$ to $\overline{\mathbb{R}}$, and a partial function f_2 from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X,n+1)$ to $\overline{\mathbb{R}}$. Suppose M is σ-finite and $f = f_1$ and $f = f_2$ and f is integrable on $\mathrm{Measure}_{\mathrm{Prod}}(M)$ and for every element x of $\prod_{\mathrm{FS}} \mathrm{SubFin}(X,n)$, $(\mathrm{Integral2}(\mathrm{ElmFin}(M,n+1),|f_1|))(x) < +\infty$. Then $\int f_2 \,\mathrm{d}\, \mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M,n+1)) = \int \mathrm{Integral2}(\mathrm{ElmFin}(M,n+1), f_1) \,\mathrm{d}\, \mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M,n))$. The theorem is a consequence of (35).

(37) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, a family of σ-measures M of S, a partial function f from $\prod_{\mathrm{FS}} X$ to $\overline{\mathbb{R}}$, an element E of $\prod_{\mathrm{Field}} S$, and a partial function g from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X,n) \times \mathrm{ElmFin}(X,n+1)$ to $\overline{\mathbb{R}}$.

Suppose M is σ-finite and $E = \mathrm{dom}\, f$ and f is E-measurable and $f = g$. Then g is integrable on $\mathrm{ProdMeas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M,n)), \mathrm{ElmFin}(M,n+1))$ iff $\int \mathrm{Integral2}(\mathrm{ElmFin}(M,n+1),|g|) \,\mathrm{d}\, \mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M,n)) < +\infty$. The theorem is a consequence of (6), (34), (30), (29), and (31).

Let n be a non zero natural number, X be a non-empty, $(n+1)$-elements finite sequence, S be a family of σ-fields of X, M be a family of σ-measures of S, and f be a partial function from $\prod_{\mathrm{FS}} X$ to $\overline{\mathbb{R}}$. The functor $\mathrm{Integral}_{\mathrm{FS}}(M,f)$ yielding an $(n+1)$-elements finite sequence is defined by

(Def. 17) $it(1) = f$ and for every natural number i such that $1 \leqslant i < n+1$ there exists a non zero natural number k and there exists a partial function g from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X,k) \times \mathrm{ElmFin}(X,k+1)$ to $\overline{\mathbb{R}}$ such that $k = n+1-i$ and $g = it(i)$ and $it(i+1) = \mathrm{Integral2}(\mathrm{ElmFin}(M,k+1), g)$.

We say that f is sequentially integrable on M if and only if

(Def. 18) for every non zero natural number k such that $k < n+1$ there exists a partial function G from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X,k+1)$ to $\overline{\mathbb{R}}$ and there exists a partial function H from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X,k)$ to $\overline{\mathbb{R}}$ such that $G = (\mathrm{Integral}_{\mathrm{FS}}(M,f))(n+1-k)$ and $H = (\mathrm{Integral}_{\mathrm{FS}}(\mathrm{SubFin}(M,k+1),|G|))(2)$ and for every element x of $\prod_{\mathrm{FS}} \mathrm{SubFin}(X,k)$, $H(x) < +\infty$.

Now we state the propositions:

(38) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, a family of σ-measures M of S, and a partial function f from $\prod_{\mathrm{FS}} X$ to $\overline{\mathbb{R}}$.

Suppose M is σ-finite and f is sequentially integrable on M and f is integrable on $\mathrm{Measure}_{\mathrm{Prod}}(M)$. Let us consider a non zero natural number k. Suppose $k < n+1$. Then there exists a partial function g from

$\prod_{\mathrm{FS}} \mathrm{SubFin}(X, k+1)$ to $\overline{\mathbb{R}}$ such that

(i) $g = (\mathrm{Integral}_{\mathrm{FS}}(M, f))(n+1-k)$, and

(ii) g is integrable on $\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k+1))$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ if $1 \leqslant \$_1 < n+1$, then there exists a non zero natural number j and there exists a partial function g from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, j+1)$ to $\overline{\mathbb{R}}$ such that $j = n+1-\$_1$ and $g = (\mathrm{Integral}_{\mathrm{FS}}(M, f))(\$_1)$ and g is integrable on $\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, j+1))$. $\mathcal{P}[1]$. For every non zero natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every non zero natural number k, $\mathcal{P}[k]$. □

(39) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, a family of σ-measures M of S, a partial function f from $\prod_{\mathrm{FS}} X$ to $\overline{\mathbb{R}}$, and a partial function g from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, n) \times \mathrm{ElmFin}(X, n+1)$ to $\overline{\mathbb{R}}$. Suppose $f = g$. Then

(i) $(\mathrm{Integral}_{\mathrm{FS}}(M, f))(1) = f$, and

(ii) $(\mathrm{Integral}_{\mathrm{FS}}(M, f))(2) = \mathrm{Integral2}(\mathrm{ElmFin}(M, n+1), g)$.

(40) Let us consider a non zero natural number n, a non-empty, $(n+1)$-elements finite sequence X, a family of σ-fields S of X, a family of σ-measures M of S, and a partial function f from $\prod_{\mathrm{FS}} X$ to $\overline{\mathbb{R}}$. Suppose M is σ-finite and f is sequentially integrable on M and f is integrable on $\mathrm{Measure}_{\mathrm{Prod}}(M)$. Let us consider a non zero natural number k.

Suppose $k < n$. Then there exists a partial function F_5 from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, k) \times \mathrm{ElmFin}(X, k+1)$ to $\overline{\mathbb{R}}$ and there exists a partial function G_2 from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, k+1)$ to $\overline{\mathbb{R}}$ and there exists a function F_4 from $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, k)$ into $\overline{\mathbb{R}}$ such that $G_2 = F_5$ and $G_2 = (\mathrm{Integral}_{\mathrm{FS}}(M, f))(n+1-k)$ and $F_4 = (\mathrm{Integral}_{\mathrm{FS}}(M, f))(n+1-(k-1))$ and $F_4 = \mathrm{Integral2}(\mathrm{ElmFin}(M, k+1), F_5)$ and G_2 is integrable on $\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k+1))$ and $\int G_2 \,\mathrm{d}\, \mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k+1)) = \int F_5 \,\mathrm{d}\, \mathrm{ProdMeas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k)), \mathrm{ElmFin}(M, k+1))$ and for every element x of $\prod_{\mathrm{FS}} \mathrm{SubFin}(X, k)$, $\mathrm{ProjPMap1}(F_5, x)$ is integrable on $\mathrm{ElmFin}(M, k+1)$.

For every element U of $\prod_{\mathrm{Field}} \mathrm{SubFin}(S, k)$, F_4 is U-measurable and F_4 is integrable on $\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k))$ and $\int F_5 \,\mathrm{d}\, \mathrm{ProdMeas}(\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k)), \mathrm{ElmFin}(M, k+1)) = \int F_4 \,\mathrm{d}\, \mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k))$ and $F_4 \in$ the L^1 functions of $\mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k))$ and $\int G_2 \,\mathrm{d}\, \mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k+1)) = \int F_4 \,\mathrm{d}\, \mathrm{Measure}_{\mathrm{Prod}}(\mathrm{SubFin}(M, k))$.

The theorem is a consequence of (7), (8), (14), (12), (18), (17), (30), (38), (9), (6), (39), (35), and (36).

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

[3] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Improving real analysis in Coq: A user-friendly approach to integrals and derivatives. In Chris Hawblitzel and Dale Miller, editors, *Certified Programs and Proofs – Second International Conference, CPP 2012, Kyoto, Japan, December 13–15, 2012. Proceedings*, volume 7679 of *Lecture Notes in Computer Science*, pages 289–304. Springer, 2012. doi:10.1007/978-3-642-35308-6_22.

[4] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Formalization of real analysis: A survey of proof assistants and libraries. *Mathematical Structures in Computer Science*, 26:1196–1233, 2015.

[5] Noboru Endou. Improper integral. Part II. *Formalized Mathematics*, 29(**4**):279–294, 2021. doi:10.2478/forma-2021-0024.

[6] Noboru Endou. Fubini's theorem on measure. *Formalized Mathematics*, 25(**1**):1–29, 2017. doi:10.1515/forma-2017-0001.

[7] Noboru Endou. Fubini's theorem. *Formalized Mathematics*, 27(**1**):67–74, 2019. doi:10.2478/forma-2019-0007.

[8] Noboru Endou. Absolutely integrable functions. *Formalized Mathematics*, 30(**1**):31–51, 2022. doi:10.2478/forma-2022-0004.

[9] Jacques D. Fleuriot. On the mechanization of real analysis in Isabelle/HOL. In Mark Aagaard and John Harrison, editors, *Theorem Proving in Higher Order Logics*, pages 145–161. Springer Berlin Heidelberg, 2000. ISBN 978-3-540-44659-0.

[10] Ruben Gamboa. *Continuity and Differentiability*, pages 301–315. Springer US, 2000. ISBN 978-1-4757-3188-0. doi:10.1007/978-1-4757-3188-0_18.

[11] Adam Grabowski and Christoph Schwarzweller. Translating mathematical vernacular into knowledge repositories. In Michael Kohlhase, editor, *Mathematical Knowledge Management*, volume 3863 of *Lecture Notes in Computer Science*, pages 49–64. Springer, 2006. doi:10.1007/11618027_4. 4th International Conference on Mathematical Knowledge Management, Bremen, Germany, MKM 2005, July 15–17, 2005, Revised Selected Papers.

[12] Johannes Hölzl and Armin Heller. Three chapters of measure theory in Isabelle/HOL. In Marko C. J. D. van Eekelen, Herman Geuvers, Julien Schmaltz, and Freek Wiedijk, editors, *Interactive Theorem Proving (ITP 2011)*, volume 6898 of *LNCS*, pages 135–151, 2011.

[13] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. Cartesian products of family of real linear spaces. *Formalized Mathematics*, 19(**1**):51–59, 2011. doi:10.2478/v10037-011-0009-2.

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

Accepted November 21, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 193–203, 2023
DOI: 10.2478/forma-2023-0018
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Conway Numbers – Formal Introduction

Karol Pąk
Faculty of Computer Science
University of Białystok
Poland

Summary. Surreal numbers, a fascinating mathematical concept introduced by John Conway, have attracted considerable interest due to their unique properties. In this article, we formalize the basic concept of surreal numbers close to the original Conway's convention in the field of combinatorial game theory. We define surreal numbers with the pre-order in the Mizar system which satisfy the following condition: $x \leqslant y$ iff $L_x \ll \{y\} \wedge \{x\} \ll R_y$.

MSC: 03H05 12J15 68V20

Keywords: surreal numbers; Conway's game; Mizar

MML identifier: SURREAL0, version: 8.1.14 5.76.1456

Introduction

The surreal numbers have been discovered by J. Conway and they are described in the 0th part of his book [1]. Using a remarkably simple set of rules, he showed that a rich algebraic structure, as totally ordered proper class that form an ordered field could be constructed. However, his construction combines transfinite induction recursion [2] with properties of proper classes, and has been challenged from a formal point of view. We have chosen to construct surreal numbers based on transfinite induction (for recent quite sophisticated use of these second order statements, see [10] and [11]), in contrast to the formalisation in other systems [7], [9].

Imitating the induction recursion in the Mizar system, and, at the same time, to come as close as possible to the Conway convention with a non anti-symmetric pre-order we have extracted an additional fundamental step. We introduce the

functor of $\mathrm{Day}_R\alpha$ for a given ordinal α and relation R as well as the properties of the pre-order on a set D which will play the role of the Dayα, independently. Then we extract the crucial dependencies between Dayα and the pre-order to remove parameters and finally define the concept of surreal numbers in the Mizar system [6].

The formalization follows [1], [3], [4], [5] and is an independent approach to that introduced by R. Nittka [8].

1. Construction of Games on α-Day

From now on α, α_1, α_2, β, β_1, β_2, γ, θ denote ordinal numbers, R, S denote binary relations, and a, b, c, o, l, r denote objects. Let x be an object. We introduce the notation L_x as a synonym of $(x)_{\mathbf{1}}$ and R_x as a synonym of $(x)_{\mathbf{2}}$.

Note that the functor L_x yields a set. Let us observe that the functor R_x yields a set. Let us consider a and b. Let θ be a set. We say that $a \leqslant_\theta b$ if and only if

(Def. 1) $\langle a, b\rangle \in \theta$.

We introduce the notation $b \succeq_\theta a$ as a synonym of $a \leqslant_\theta b$.

Let L, R be sets. We say that $L \ggcurly_\theta R$ if and only if

(Def. 2) if $l \in L$ and $r \in R$, then $l \succeq_\theta r$.

We say that $L \llcurly_\theta R$ if and only if

(Def. 3) if $l \in L$ and $r \in R$, then not $l \succeq_\theta r$.

Let us consider α. The functor Games(α) yielding a set is defined by

(Def. 4) there exists a transfinite sequence L such that $it = L(\alpha)$ and $\operatorname{dom} L = \operatorname{succ}\alpha$ and for every θ such that $\theta \in \operatorname{succ}\alpha$ holds $L(\theta) = 2^{\bigcup \operatorname{rng}(L\restriction\theta)} \times 2^{\bigcup \operatorname{rng}(L\restriction\theta)}$.

Let us note that Games(α) is non empty and relation-like. Now we state the propositions:

(1) If $\alpha \subseteq \beta$, then Games(α) $\subseteq$ Games(β).

Proof: Consider L_1 being a transfinite sequence such that Games(α) $= L_1(\alpha)$ and $\operatorname{dom} L_1 = \operatorname{succ}\alpha$ and for every ordinal number θ such that $\theta \in \operatorname{succ}\alpha$ holds $L_1(\theta) = 2^{\bigcup \operatorname{rng}(L_1\restriction\theta)} \times 2^{\bigcup \operatorname{rng}(L_1\restriction\theta)}$. Consider L_2 being a transfinite sequence such that Games(β) $= L_2(\beta)$ and $\operatorname{dom} L_2 = \operatorname{succ}\beta$ and for every ordinal number θ such that $\theta \in \operatorname{succ}\beta$ holds $L_2(\theta) = 2^{\bigcup \operatorname{rng}(L_2\restriction\theta)} \times 2^{\bigcup \operatorname{rng}(L_2\restriction\theta)}$.

Define $\mathcal{P}$[ordinal number] $\equiv$ if $\$_1 \subseteq \alpha$, then $L_1(\$_1) = L_2(\$_1)$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. $\operatorname{rng}(L_1\restriction\alpha) \subseteq \operatorname{rng}(L_2\restriction\beta)$. $\square$

(2) $\mathrm{Games}(0) = \{\langle \emptyset, \emptyset \rangle\}$.

(3) Let us consider a transfinite sequence L, and θ. Suppose $\mathrm{dom}\, L = \mathrm{succ}\, \theta$ and for every α such that $\alpha \in \mathrm{succ}\, \theta$ holds $L(\alpha) = 2^{\bigcup \mathrm{rng}(L \restriction \alpha)} \times 2^{\bigcup \mathrm{rng}(L \restriction \alpha)}$. If $\alpha \in \mathrm{succ}\, \theta$, then $L(\alpha) = \mathrm{Games}(\alpha)$.

PROOF: Consider L_0 being a transfinite sequence such that $\mathrm{Games}(\theta) = L_0(\theta)$ and $\mathrm{dom}\, L_0 = \mathrm{succ}\, \theta$ and for every ordinal number α such that $\alpha \in \mathrm{succ}\, \theta$ holds $L_0(\alpha) = 2^{\bigcup \mathrm{rng}(L_0 \restriction \alpha)} \times 2^{\bigcup \mathrm{rng}(L_0 \restriction \alpha)}$. Define $\mathcal{P}$[ordinal number] $\equiv$ if $\$_1 \subseteq \theta$, then $L_0(\$_1) = L(\$_1)$.

For every ordinal number α such that for every ordinal number γ such that $\gamma \in \alpha$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\alpha]$. For every ordinal number α, $\mathcal{P}[\alpha]$. □

(4) $o \in \mathrm{Games}(\theta)$ if and only if o is pair and for every a such that $a \in \mathrm{L}_o \cup \mathrm{R}_o$ there exists α such that $\alpha \in \theta$ and $a \in \mathrm{Games}(\alpha)$.

PROOF: Consider L being a transfinite sequence such that $\mathrm{Games}(\theta) = L(\theta)$ and $\mathrm{dom}\, L = \mathrm{succ}\, \theta$ and for every α such that $\alpha \in \mathrm{succ}\, \theta$ holds $L(\alpha) = 2^{\bigcup \mathrm{rng}(L \restriction \alpha)} \times 2^{\bigcup \mathrm{rng}(L \restriction \alpha)}$. If $o \in \mathrm{Games}(\theta)$, then o is pair and for every object x such that $x \in \mathrm{L}_o \cup \mathrm{R}_o$ there exists an ordinal number β such that $\beta \in \theta$ and $x \in \mathrm{Games}(\beta)$. $\mathrm{L}_o \cup \mathrm{R}_o \subseteq \bigcup \mathrm{rng}(L \restriction \theta)$. □

Let us consider α. The functor $\mathrm{BeforeGames}(\alpha)$ yielding a subset of $\mathrm{Games}(\alpha)$ is defined by

(Def. 5) $a \in it$ iff there exists θ such that $\theta \in \alpha$ and $a \in \mathrm{Games}(\theta)$.

Now we state the proposition:

(5) If $\alpha \subseteq \beta$, then $\mathrm{BeforeGames}(\alpha) \subseteq \mathrm{BeforeGames}(\beta)$.

Let us consider θ and R. The functor $\mathrm{Day}_R\theta$ yielding a subset of $\mathrm{Games}(\theta)$ is defined by

(Def. 6) there exists a transfinite sequence L such that $it = L(\theta)$ and $\mathrm{dom}\, L = \mathrm{succ}\, \theta$ and for every α such that $\alpha \in \mathrm{succ}\, \theta$ holds $L(\alpha) = \{x,$ where x is an element of $\mathrm{Games}(\alpha) : \mathrm{L}_x \subseteq \bigcup \mathrm{rng}(L \restriction \alpha)$ and $\mathrm{R}_x \subseteq \bigcup \mathrm{rng}(L \restriction \alpha)$ and $\mathrm{L}_x \ll_R \mathrm{R}_x\}$.

2. CONSTRUCTION OF PREORDER ON THE α-DAY

Let us consider R. We say that R is almost **No** order if and only if

(Def. 7) there exists θ such that $R \subseteq \mathrm{Day}_R\theta \times \mathrm{Day}_R\theta$.

Now we state the propositions:

(6) Let us consider a transfinite sequence L. Suppose $\mathrm{dom}\, L = \mathrm{succ}\, \theta$ and for every α such that $\alpha \in \mathrm{succ}\, \theta$ holds $L(\alpha) = \{x,$ where x is an element of $\mathrm{Games}(\alpha) : \mathrm{L}_x \subseteq \bigcup \mathrm{rng}(L \restriction \alpha)$ and $\mathrm{R}_x \subseteq \bigcup \mathrm{rng}(L \restriction \alpha)$ and $\mathrm{L}_x \ll_R \mathrm{R}_x\}$. If $\alpha \in \mathrm{succ}\, \theta$, then $L(\alpha) = \mathrm{Day}_R\alpha$.

PROOF: Consider L_0 being a transfinite sequence such that $\mathrm{Day}_R\delta = L_0(\delta)$ and $\mathrm{dom}\, L_0 = \mathrm{succ}\,\delta$ and for every ordinal number α such that $\alpha \in \mathrm{succ}\,\delta$ holds $L_0(\alpha) = \{x$, where x is an element of $\mathrm{Games}(\alpha) : \mathrm{L}_x \subseteq \bigcup \mathrm{rng}(L_0\restriction\alpha)$ and $\mathrm{R}_x \subseteq \bigcup \mathrm{rng}(L_0\restriction\alpha)$ and $\mathrm{L}_x \ll_R \mathrm{R}_x\}$.

Define $\mathcal{P}$[ordinal number] $\equiv$ if $\$_1 \subseteq \delta$, then $L_0(\$_1) = L(\$_1)$. For every ordinal number α such that for every ordinal number γ such that $\gamma \in \alpha$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\alpha]$. For every α, $\mathcal{P}[\alpha]$. □

(7) Let us consider an element x of $\mathrm{Games}(\theta)$. Then $x \in \mathrm{Day}_R\theta$ if and only if $\mathrm{L}_x \ll_R \mathrm{R}_x$ and for every o such that $o \in \mathrm{L}_x \cup \mathrm{R}_x$ there exists α such that $\alpha \in \theta$ and $o \in \mathrm{Day}_R\alpha$.

PROOF: Consider L being a transfinite sequence such that $\mathrm{Day}_R\theta = L(\theta)$ and $\mathrm{dom}\, L = \mathrm{succ}\,\theta$ and for every α such that $\alpha \in \mathrm{succ}\,\theta$ holds $L(\alpha) = \{x$, where x is an element of $\mathrm{Games}(\alpha) : \mathrm{L}_x \subseteq \bigcup \mathrm{rng}(L\restriction\alpha)$ and $\mathrm{R}_x \subseteq \bigcup \mathrm{rng}(L\restriction\alpha)$ and $\mathrm{L}_x \ll_R \mathrm{R}_x\}$. If $\alpha \in \mathrm{Day}_R\theta$, then $\mathrm{L}_\alpha \ll_R \mathrm{R}_\alpha$ and for every object x such that $x \in \mathrm{L}_\alpha \cup \mathrm{R}_\alpha$ there exists an ordinal number β such that $\beta \in \theta$ and $x \in \mathrm{Day}_R\beta$. $\mathrm{L}_\alpha \cup \mathrm{R}_\alpha \subseteq \bigcup \mathrm{rng}(L\restriction\theta)$. □

(8) $\mathrm{Day}_R 0 = \mathrm{Games}(0)$. The theorem is a consequence of (2) and (7).

(9) If $\alpha \subseteq \beta$, then $\mathrm{Day}_R\alpha \subseteq \mathrm{Day}_R\beta$. The theorem is a consequence of (7) and (1).

Let us consider R and α. Let us note that $\mathrm{Day}_R\alpha$ is non empty. Now we state the proposition:

(10) Suppose $\beta \subseteq \alpha$ and $R \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha)) = S \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha))$. Then $\mathrm{Day}_R\beta = \mathrm{Day}_S\beta$. The theorem is a consequence of (5).

Let us consider R and o. Assume there exists θ such that $o \in \mathrm{Day}_R\theta$. The functor $\mathfrak{born}_R o$ yielding an ordinal number is defined by

(Def. 8) $o \in \mathrm{Day}_R it$ and for every θ such that $o \in \mathrm{Day}_R\theta$ holds $it \subseteq \theta$.

Now we state the propositions:

(11) Suppose $R \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha)) = S \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha))$. If $a \in \mathrm{Day}_R\alpha$, then $\mathfrak{born}_R a = \mathfrak{born}_S a$. The theorem is a consequence of (10).

(12) If $o \in \mathrm{Games}(\theta)$ and $o \notin \mathrm{Day}_R\theta$, then $o \notin \mathrm{Day}_R\alpha$.

PROOF: Define $\mathcal{P}$[ordinal number] $\equiv$ for every object x for every ordinal number θ such that $x \in (\mathrm{Games}(\theta)) \setminus (\mathrm{Day}_R\theta)$ holds $x \notin \mathrm{Day}_R\$_1$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. □

Let us consider R, α, and β. The functor $\mathrm{OpenProd}_R(\alpha, \beta)$ yielding a binary relation on $\mathrm{Day}_R\alpha$ is defined by

(Def. 9) for every elements x, y of $\mathrm{Day}_R\alpha$, $\langle x, y\rangle \in it$ iff $\mathfrak{born}_R x$, $\mathfrak{born}_R y \in \alpha$ or $\mathfrak{born}_R x = \alpha$ and $\mathfrak{born}_R y \in \beta$ or $\mathfrak{born}_R x \in \beta$ and $\mathfrak{born}_R y = \alpha$.

The functor $\mathrm{ClosedProd}_R(\alpha, \beta)$ yielding a binary relation on $\mathrm{Day}_R\alpha$ is defined by

(Def. 10) for every elements x, y of $\mathrm{Day}_R\alpha$, $\langle x, y\rangle \in it$ iff $\mathfrak{born}_R x$, $\mathfrak{born}_R y \in \alpha$ or $\mathfrak{born}_R x = \alpha$ and $\mathfrak{born}_R y \subseteq \beta$ or $\mathfrak{born}_R x \subseteq \beta$ and $\mathfrak{born}_R y = \alpha$.

Now we state the propositions:

(13) Suppose $\alpha_1 \in \alpha_2$ or $\alpha_1 = \alpha_2$ and $\beta_1 \subseteq \beta_2$. Then $\mathrm{OpenProd}_R(\alpha_1, \beta_1) \subseteq \mathrm{OpenProd}_R(\alpha_2, \beta_2)$. The theorem is a consequence of (9).

(14) Suppose $R \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha)) = S \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha))$. Then $\mathrm{OpenProd}_R(\alpha, \beta) = \mathrm{OpenProd}_S(\alpha, \beta)$.
PROOF: $\mathrm{Day}_R\alpha = \mathrm{Day}_S\alpha$. If $\langle x, y\rangle \in \mathrm{OpenProd}_R(\alpha, \beta)$, then $\langle x, y\rangle \in \mathrm{OpenProd}_S(\alpha, \beta)$. $\mathfrak{born}_R x = \mathfrak{born}_S x$ and $\mathfrak{born}_R y = \mathfrak{born}_S y$. □

(15) Suppose $R \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha)) = S \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha))$. Then $\mathrm{ClosedProd}_R(\alpha, \beta) = \mathrm{ClosedProd}_S(\alpha, \beta)$.
PROOF: $\mathrm{Day}_R\alpha = \mathrm{Day}_S\alpha$. If $\langle x, y\rangle \in \mathrm{ClosedProd}_R(\alpha, \beta)$, then $\langle x, y\rangle \in \mathrm{ClosedProd}_S(\alpha, \beta)$. $\mathfrak{born}_R x = \mathfrak{born}_S x$ and $\mathfrak{born}_R y = \mathfrak{born}_S y$. □

(16) $\mathrm{OpenProd}_R(\alpha, \beta) \subseteq \mathrm{ClosedProd}_R(\alpha, \beta)$.

(17) Suppose $\alpha_1 \in \alpha_2$ or $\alpha_1 = \alpha_2$ and $\beta_1 \subseteq \beta_2$. Then $\mathrm{ClosedProd}_R(\alpha_1, \beta_1) \subseteq \mathrm{ClosedProd}_R(\alpha_2, \beta_2)$. The theorem is a consequence of (9).

(18) If $\beta \in \gamma$, then $\mathrm{ClosedProd}_R(\alpha, \beta) \subseteq \mathrm{OpenProd}_R(\alpha, \gamma)$.

(19) If $\alpha \in \beta$, then $\mathrm{ClosedProd}_R(\alpha, \beta) \subseteq \mathrm{OpenProd}_R(\alpha, \beta)$.

Let X, R be sets. We say that R preserves **No** comparison on X if and only if

(Def. 11) for every objects a, b such that $\langle a, b\rangle \in X$ holds $a \leqslant_R b$ iff $\mathrm{L}_a \ll_R \{b\}$ and $\{a\} \ll_R \mathrm{R}_b$.

Now we state the propositions:

(20) Suppose R is almost **No** order and S is almost **No** order and $R \cap \mathrm{OpenProd}_R(\alpha, \beta) = S \cap \mathrm{OpenProd}_S(\alpha, \beta)$. Then $R \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha)) = S \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha))$.
PROOF: Consider R_0 being an ordinal number such that $R \subseteq \mathrm{Day}_R R_0 \times \mathrm{Day}_R R_0$. Consider S_0 being an ordinal number such that $S \subseteq \mathrm{Day}_S S_0 \times \mathrm{Day}_S S_0$. If $\langle y, z\rangle \in R \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha))$, then $\langle y, z\rangle \in S \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha))$.

Consider A_4 being an ordinal number such that $A_4 \in \alpha$ and $y \in \mathrm{Games}(A_4)$. Consider A_5 being an ordinal number such that $A_5 \in \alpha$ and $z \in \mathrm{Games}(A_5)$. $\mathrm{Day}_S A_4 \subseteq \mathrm{Day}_S\alpha$ and $\mathrm{Day}_S A_5 \subseteq \mathrm{Day}_S\alpha$. $y \in \mathrm{Day}_S A_4$ and $z \in \mathrm{Day}_S A_5$. □

(21) Suppose R is almost **No** order and S is almost **No** order and $R \cap \mathrm{OpenProd}_R(\alpha, \beta) = S \cap \mathrm{OpenProd}_S(\alpha, \beta)$ and R preserves **No** comparison on $\mathrm{ClosedProd}_R(\alpha, \beta)$ and S preserves **No** comparison on $\mathrm{ClosedProd}_S(\alpha, \beta)$. Then $R \cap \mathrm{ClosedProd}_R(\alpha, \beta) = S \cap \mathrm{ClosedProd}_S(\alpha, \beta)$. The theorem is a consequence of (16) and (19).

(22) Suppose R is almost **No** order and S is almost **No** order and $R \cap \mathrm{OpenProd}_R(\alpha, 0) = S \cap \mathrm{OpenProd}_S(\alpha, 0)$ and R preserves **No** comparison on $\mathrm{ClosedProd}_R(\alpha, \beta)$ and S preserves **No** comparison on $\mathrm{ClosedProd}_S(\alpha, \beta)$. Then $R \cap \mathrm{ClosedProd}_R(\alpha, \beta) = S \cap \mathrm{ClosedProd}_S(\alpha, \beta)$.

PROOF: Define $\mathcal{P}[\text{ordinal number}] \equiv$ if $\$_1 \subseteq \beta$, then $R \cap \mathrm{ClosedProd}_R(\alpha, \$_1) = S \cap \mathrm{ClosedProd}_S(\alpha, \$_1)$. $R \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha)) = S \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha))$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. □

(23) Suppose R is almost **No** order and S is almost **No** order and R preserves **No** comparison on $\mathrm{ClosedProd}_R(\alpha, \beta)$ and S preserves **No** comparison on $\mathrm{ClosedProd}_S(\alpha, \beta)$. Then $R \cap \mathrm{ClosedProd}_R(\alpha, \beta) = S \cap \mathrm{ClosedProd}_S(\alpha, \beta)$.

PROOF: Define $\mathcal{P}[\text{ordinal number}] \equiv$ if $\$_1 \in \alpha$, then $R \cap \mathrm{ClosedProd}_R(\$_1, \$_1) = S \cap \mathrm{ClosedProd}_S(\$_1, \$_1)$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. $R \cap \mathrm{OpenProd}_R(\alpha, 0) \subseteq S \cap \mathrm{OpenProd}_S(\alpha, 0)$. $S \cap \mathrm{OpenProd}_S(\alpha, 0) \subseteq R \cap \mathrm{OpenProd}_R(\alpha, 0)$. □

(24) Let us consider transfinite sequences L_3, L_4. Suppose $\mathrm{dom}\, L_3 = \mathrm{dom}\, L_4$ and for every α such that $\alpha \in \mathrm{dom}\, L_3$ holds there exist ordinal numbers a, b and there exists a binary relation R such that $R = L_4(\alpha)$ and $L_3(\alpha) = \mathrm{ClosedProd}_R(a, b)$ and $L_4(\alpha)$ is a binary relation and for every binary relation R such that $R = L_4(\alpha)$ holds R preserves **No** comparison on $L_3(\alpha)$ and $R \subseteq L_3(\alpha)$. Then

(i) $\bigcup \mathrm{rng}\, L_4$ is a binary relation, and

(ii) for every R such that $R = \bigcup \mathrm{rng}\, L_4$ holds R preserves **No** comparison on $\bigcup \mathrm{rng}\, L_3$ and $R \subseteq \bigcup \mathrm{rng}\, L_3$ and for every ordinal numbers α, a, b and for every S such that $\alpha \in \mathrm{dom}\, L_3$ and $S = L_4(\alpha)$ and $L_3(\alpha) = \mathrm{ClosedProd}_S(a, b)$ holds $R \cap (\mathrm{BeforeGames}(a) \times \mathrm{BeforeGames}(a)) = S \cap (\mathrm{BeforeGames}(a) \times \mathrm{BeforeGames}(a))$.

PROOF: $\bigcup \mathrm{rng}\, L_4$ is relation-like. $R \subseteq \bigcup \mathrm{rng}\, L_3$. R preserves **No** comparison on $\bigcup \mathrm{rng}\, L_3$. $R \cap (\mathrm{BeforeGames}(a) \times \mathrm{BeforeGames}(a)) \subseteq S \cap (\mathrm{BeforeGames}(a) \times \mathrm{BeforeGames}(a))$. $S \cap (\mathrm{BeforeGames}(a) \times \mathrm{BeforeGames}(a)) \subseteq R \cap (\mathrm{BeforeGames}(a) \times \mathrm{BeforeGames}(a))$. □

(25) $\langle a, b\rangle \in (\mathrm{ClosedProd}_R(\alpha,\beta)) \setminus (\mathrm{OpenProd}_R(\alpha,\beta))$ if and only if $a, b \in \mathrm{Day}_R\alpha$ and ($\mathfrak{born}_R a = \alpha$ and $\mathfrak{born}_R b = \beta$ or $\mathfrak{born}_R a = \beta$ and $\mathfrak{born}_R b = \alpha$).
PROOF: If $\langle a, b\rangle \in (\mathrm{ClosedProd}_R(\alpha,\beta)) \setminus (\mathrm{OpenProd}_R(\alpha,\beta))$, then $a, b \in \mathrm{Day}_R\alpha$ and ($\mathfrak{born}_R a = \alpha$ and $\mathfrak{born}_R b = \beta$ or $\mathfrak{born}_R a = \beta$ and $\mathfrak{born}_R b = \alpha$). $\langle a, b\rangle \notin \mathrm{OpenProd}_R(\alpha,\beta)$. □

(26) Suppose R preserves **No** comparison on $\mathrm{OpenProd}_R(\alpha,\beta)$ and $R \subseteq \mathrm{OpenProd}_R(\alpha,\beta)$. Then there exists S such that

(i) $R \subseteq S$, and

(ii) S preserves **No** comparison on $\mathrm{ClosedProd}_S(\alpha,\beta)$, and

(iii) $S \subseteq \mathrm{ClosedProd}_S(\alpha,\beta)$.

PROOF: Set $C_1 = \{\langle x, y\rangle$, where x, y are elements of $\mathrm{Day}_R\alpha : (\mathfrak{born}_R x = \beta$ and $\mathfrak{born}_R y = \alpha$ or $\mathfrak{born}_R x = \alpha$ and $\mathfrak{born}_R y = \beta)$ and $\mathrm{L}_x \ll_R \{y\}$ and $\{x\} \ll_R \mathrm{R}_y\}$. C_1 is relation-like. Reconsider $R_1 = R \cup C_1$ as a binary relation. $R_1 \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha)) \subseteq R \cap (\mathrm{BeforeGames}(\alpha) \times \mathrm{BeforeGames}(\alpha))$. $R_1 \subseteq \mathrm{ClosedProd}_R(\alpha,\beta)$. R_1 preserves **No** comparison on $\mathrm{ClosedProd}_R(\alpha,\beta)$. □

(27) Suppose there exists R such that R preserves **No** comparison on $\mathrm{OpenProd}_R(\alpha,\emptyset)$ and $R \subseteq \mathrm{OpenProd}_R(\alpha,\emptyset)$. Then there exists S such that

(i) S preserves **No** comparison on $\mathrm{ClosedProd}_S(\alpha,\beta)$, and

(ii) $S \subseteq \mathrm{ClosedProd}_S(\alpha,\beta)$.

PROOF: Define $\mathcal{P}$[ordinal number] ≡ there exists a binary relation R such that R preserves **No** comparison on $\mathrm{ClosedProd}_R(\alpha,\$_1)$ and $R \subseteq \mathrm{ClosedProd}_R(\alpha,\$_1)$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. □

(28) There exists R such that

(i) R preserves **No** comparison on $\mathrm{ClosedProd}_R(\alpha,\beta)$, and

(ii) $R \subseteq \mathrm{ClosedProd}_R(\alpha,\beta)$.

PROOF: Define $\mathcal{P}$[ordinal number] ≡ for every ordinal number β, there exists a binary relation R such that R preserves **No** comparison on $\mathrm{ClosedProd}_R(\$_1,\beta)$ and $R \subseteq \mathrm{ClosedProd}_R(\$_1,\beta)$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. □

(29) If $\alpha \in \beta$, then $\mathrm{ClosedProd}_R(\alpha,\alpha) = \mathrm{OpenProd}_R(\alpha,\beta)$.
PROOF: $\mathrm{ClosedProd}_R(\alpha,\alpha) \subseteq \mathrm{ClosedProd}_R(\alpha,\beta)$. $\mathrm{ClosedProd}_R(\alpha,\beta) \subseteq \mathrm{ClosedProd}_R(\alpha,\alpha)$. $\mathrm{ClosedProd}_R(\alpha,\beta) \subseteq \mathrm{OpenProd}_R(\alpha,\beta)$. $\mathrm{OpenProd}_R(\alpha,\beta) \subseteq \mathrm{ClosedProd}_R(\alpha,\beta)$. □

(30) If $\alpha \subseteq \beta$, then $\mathrm{ClosedProd}_R(\alpha, \alpha) \subseteq \mathrm{ClosedProd}_R(\beta, \beta)$. The theorem is a consequence of (17).

3. The Preorder on the α-Day

Let us consider α. The functor $\mathbf{No}_{\mathrm{Ord}}\alpha$ yielding a binary relation is defined by

(Def. 12) *it* preserves **No** comparison on $\mathrm{Day}_{it}\alpha \times \mathrm{Day}_{it}\alpha$ and $it \subseteq \mathrm{Day}_{it}\alpha \times \mathrm{Day}_{it}\alpha$.

Note that $\mathbf{No}_{\mathrm{Ord}}\alpha$ is almost **No** order. The functor $\mathrm{Day}\alpha$ yielding a non empty subset of $\mathrm{Games}(\alpha)$ is defined by the term

(Def. 13) $\mathrm{Day}_{\mathbf{No}_{\mathrm{Ord}}\alpha}\alpha$.

4. Surreal Number as a Special Type of Abstract Game

Let us consider o. We say that o is surreal if and only if

(Def. 14) there exists α such that $o \in \mathrm{Day}\alpha$.

Let us note that $\langle \emptyset, \emptyset \rangle$ is surreal and there exists a set which is surreal. Let α be an ordinal number. Note that every element of $\mathrm{Day}\alpha$ is surreal. A surreal number is a surreal set. In the sequel x, y, z, t, r, l denote surreal numbers and X, Y, Z denote sets.

The functor $\mathbf{0_{No}}$ yielding a surreal number is defined by the term

(Def. 15) $\langle \emptyset, \emptyset \rangle$.

Note that every surreal number is pair and every set which is surreal is also non empty.

Let X be a set. We say that X is surreal-membered if and only if

(Def. 16) if $o \in X$, then o is surreal.

One can check that there exists a set which is surreal-membered. Let us consider x. Observe that $\{x\}$ is surreal-membered and L_x is surreal-membered as a set and R_x is surreal-membered as a set. Let X, Y be surreal-membered sets. One can check that $X \cup Y$ is surreal-membered and $X \setminus Y$ is surreal-membered and $X \cap Y$ is surreal-membered and there exists a set which is non empty and surreal-membered.

5. The Preorder of Surreal Numbers

Let us consider x and y. We say that $x \leqslant y$ if and only if

(Def. 17) there exists α such that $x \leqslant_{\mathbf{No}_{\mathrm{Ord}}\alpha} y$.

Now we state the propositions:

(31) Let us consider ordinal numbers α, β, X. Suppose $X \subseteq \alpha$ and $X \subseteq \beta$. Then $\mathbf{No}_{\mathrm{Ord}}\alpha \cap (\mathrm{BeforeGames}(X) \times \mathrm{BeforeGames}(X)) = \mathbf{No}_{\mathrm{Ord}}\beta \cap (\mathrm{BeforeGames}(X) \times \mathrm{BeforeGames}(X))$. The theorem is a consequence of (17), (23), (29), and (20).

(32) Suppose $\alpha \subseteq \beta$. Then $\mathrm{ClosedProd}_{\mathbf{No}_{\mathrm{Ord}}\alpha}(\alpha, \alpha) = \mathrm{ClosedProd}_{\mathbf{No}_{\mathrm{Ord}}\beta}(\alpha, \alpha)$. The theorem is a consequence of (31) and (15).

(33) $\langle a, b\rangle \in \mathrm{ClosedProd}_{\mathbf{No}_{\mathrm{Ord}}\alpha}(\alpha, \alpha)$ if and only if $a, b \in \mathrm{Day}\alpha$.

(34) Suppose $\alpha \subseteq \beta$. Then $\mathbf{No}_{\mathrm{Ord}}\alpha = \mathbf{No}_{\mathrm{Ord}}\beta \cap \mathrm{ClosedProd}_{\mathbf{No}_{\mathrm{Ord}}\beta}(\alpha, \alpha)$. The theorem is a consequence of (30) and (23).

(35) If $\alpha \subseteq \beta$, then $\mathrm{Day}\alpha \subseteq \mathrm{Day}\beta$. The theorem is a consequence of (31), (10), and (9).

(36) If $o \in \mathrm{Day}_{\mathbf{No}_{\mathrm{Ord}}\alpha}\beta$ and $\beta \subseteq \alpha$, then $o \in \mathrm{Day}\beta$. The theorem is a consequence of (31) and (10).

Let us consider x. The functor $\mathfrak{born}\, x$ yielding an ordinal number is defined by

(Def. 18) $x \in \mathrm{Day}\mathit{it}$ and for every θ such that $x \in \mathrm{Day}\theta$ holds $\mathit{it} \subseteq \theta$.

Now we state the propositions:

(37) $\mathfrak{born}\, x = \emptyset$ if and only if $x = \mathbf{0_{No}}$. The theorem is a consequence of (2) and (8).

(38) If $x \in \mathrm{Day}\alpha$, then $\mathfrak{born}\, x = \mathfrak{born}_{\mathbf{No}_{\mathrm{Ord}}\alpha} x$. The theorem is a consequence of (36), (31), and (11).

(39) If $a \leqslant_{\mathbf{No}_{\mathrm{Ord}}\alpha} b$ and $a, b \in \mathrm{Day}\beta$, then $a \leqslant_{\mathbf{No}_{\mathrm{Ord}}\beta} b$. The theorem is a consequence of (33), (32), (34), (30), and (23).

(40) $x \leqslant y$ if and only if for every α such that $x, y \in \mathrm{Day}\alpha$ holds $x \leqslant_{\mathbf{No}_{\mathrm{Ord}}\alpha} y$. The theorem is a consequence of (39) and (35).

Let L, R be sets. We say that $L \succeq R$ if and only if

(Def. 19) for every l and r such that $l \in L$ and $r \in R$ holds $r \leqslant l$.

Let R, L be sets. We introduce the notation $L \preceq R$ as a synonym of $R \succeq L$.

Let L, R be sets. We say that $L \ll R$ if and only if

(Def. 20) for every l and r such that $l \in L$ and $r \in R$ holds $r \not\leqslant l$.

We introduce the notation $R \gg L$ as a synonym of $L \ll R$. Now we state the propositions:

(41) Let us consider sets X_1, X_2, Y. If $X_1 \ll Y$ and $X_2 \ll Y$, then $X_1 \cup X_2 \ll Y$.

(42) Let us consider sets X, Y_1, Y_2. If $X \ll Y_1$ and $X \ll Y_2$, then $X \ll Y_1 \cup Y_2$.

(43) $x \leqslant y$ if and only if $\mathrm{L}_x \ll \{y\}$ and $\{x\} \ll \mathrm{R}_y$.

PROOF: Consider A_3 being an ordinal number such that $x \in \mathrm{Day} A_3$. Consider A_4 being an ordinal number such that $y \in \mathrm{Day} A_4$. Set $\alpha = A_3 \cup A_4$. $\mathrm{Day} A_3 \subseteq \mathrm{Day}\alpha$. $\mathrm{Day} A_4 \subseteq \mathrm{Day}\alpha$. Set $S = \mathbf{No}_{\mathrm{Ord}}\alpha$. If $x \leqslant y$, then $\mathrm{L}_x \ll \{y\}$ and $\{x\} \ll \mathrm{R}_y$. $\langle x, y \rangle \in \mathrm{ClosedProd}_S(\alpha, \alpha)$. $\mathrm{L}_x \ll_S \{y\}$. $\{x\} \ll_S \mathrm{R}_y$. □

(44) Let us consider sets X_1, X_2, Y_1, Y_2. Suppose for every x such that $x \in X_1$ there exists y such that $y \in X_2$ and $x \leqslant y$ and for every x such that $x \in Y_2$ there exists y such that $y \in Y_1$ and $y \leqslant x$ and $x = \langle X_1, Y_1 \rangle$ and $y = \langle X_2, Y_2 \rangle$. Then $x \leqslant y$. The theorem is a consequence of (43).

(45) $\mathrm{L}_x \ll \mathrm{R}_x$. The theorem is a consequence of (7), (35), (36), and (40).

(46) Let us consider sets X, Y, and α. Then $\langle X, Y \rangle \in \mathrm{Day}\alpha$ if and only if $X \ll Y$ and for every object o such that $o \in X \cup Y$ there exists θ such that $\theta \in \alpha$ and $o \in \mathrm{Day}\theta$. The theorem is a consequence of (45), (7), (36), (4), (33), (31), and (10).

(47) Suppose X is surreal-membered. Then there exists an ordinal number M such that for every o such that $o \in X$ there exists an ordinal number α such that $\alpha \in M$ and $o \in \mathrm{Day}\alpha$.

PROOF: Define $\mathcal{P}[\mathrm{object}, \mathrm{object}] \equiv \$_1$ is a surreal number and for every surreal number z such that $z = \$_1$ holds $\$_2 = \mathfrak{b}\mathrm{orn}\, z$. For every objects x, y, z such that $\mathcal{P}[x, y]$ and $\mathcal{P}[x, z]$ holds $y = z$. Consider O_2 being a set such that for every object z, $z \in O_2$ iff there exists an object y such that $y \in X$ and $\mathcal{P}[y, z]$. For every set x such that $x \in O_2$ holds x is ordinal. □

REFERENCES

[1] John Horton Conway. *On Numbers and Games*. A K Peters Ltd., Natick, MA, second edition, 2001. ISBN 1-56881-127-6.

[2] Peter Dybjer. A general formulation of simultaneous inductive-recursive definitions in type theory. *The Journal of Symbolic Logic*, 65(2):525–549, 2000. doi:10.2307/2586554.

[3] Philip Ehrlich. Conway names, the simplicity hierarchy and the surreal number tree. *Journal of Logic and Analysis*, 3(1):1–26, 2011. doi:10.4115/jla.2011.3.1.

[4] Philip Ehrlich. The absolute arithmetic continuum and the unification of all numbers great and small. *The Bulletin of Symbolic Logic*, 18(1):1–45, 2012. doi:10.2178/bsl/1327328438.

[5] Philp Ehrlich. Number systems with simplicity hierarchies: A generalization of Conway's theory of surreal numbers. *Journal of Symbolic Logic*, 66(3):1231–1258, 2001. doi:10.2307/2695104.

[6] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Mizar in a nutshell. *Journal of Formalized Reasoning*, 3(2):153–245, 2010.

[7] Lionel Elie Mamane. Surreal numbers in Coq. In Jean-Christophe Filliâtre, Christine

Paulin-Mohring, and Benjamin Werner, editors, *Types for Proofs and Programs, TYPES 2004*, volume 3839 of *LNCS*, pages 170–185. Springer, 2004. doi:10.1007/11617990_11.

[8] Robin Nittka. Conway's games and some of their basic properties. *Formalized Mathematics*, 19(**2**):73–81, 2011. doi:10.2478/v10037-011-0013-6.

[9] Steven Obua. Partizan games in Isabelle/HOLZF. In Kamel Barkaoui, Ana Cavalcanti, and Antonio Cerone, editors, *Theoretical Aspects of Computing – ICTAC 2006*, volume 4281 of *LNCS*, pages 272–286. Springer, 2006.

[10] Karol Pąk. Prime representing polynomial. *Formalized Mathematics*, 29(**4**):221–228, 2021. doi:10.2478/forma-2021-0020.

[11] Karol Pąk. Prime representing polynomial with 10 unknowns. *Formalized Mathematics*, 30(**4**):255–279, 2022. doi:10.2478/forma-2022-0021.

Accepted December 12, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 205–213, 2023
DOI: 10.2478/forma-2023-0019
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Integration of Game Theoretic and Tree Theoretic Approaches to Conway Numbers

Karol Pąk
Faculty of Computer Science
University of Białystok
Poland

Summary. In this article, we develop our formalised concept of Conway numbers as outlined in [9]. We focus mainly pre-order properties, birthday arithmetic contained in the Chapter 1, *Properties of Order and Equality* of John Conway's seminal book. We also propose a method for the selection of class representatives respecting the relation defined by the pre-ordering in order to facilitate combining the results obtained for the original and tree-theoretic definitions of Conway numbers.

MSC: 12J15 03H05 68V20

Keywords: surreal numbers; Conway's game; Mizar

MML identifier: SURREALO, version: 8.1.14 5.76.1456

Introduction

We present a formal analysis of the contents of Chapter 1, *Properties of Order and Equality* of John Conway's seminal book. This section focuses on the pre-order structure of Conway numbers.

Then, using the developed concept of Conway numbers, we thoroughly analyse the properties of surreal birthday arithmetic. We prove the *The Simplicity Theorem* (see Theorem 11 on p. 23 [3]) which can be expressed informally as follows *when x is given as a number, it is always the* simplest *number lying between the L_x and the R_x, where* simplest *means earliest created*. It also makes it easier to manipulate birthday numbers in the context of pre-ordering surreal numbers.

In the final part, we select the representatives of the equivalence classes that are defined by the relation equivalence relation $\approx$ on surreal numbers such that $x \approx y$ iff $x \leqslant y$ and $y \leqslant x$. Representatives have a minimum-birthday as well as minimal-birthday as well as the left and right components of each representative having the smallest cardinality and such representatives as members.

The formalisation is mainly based on [3, 4, 5, 6], but also uses selected ideas proposed in [1, 2, 10].

1. Preorder of Surreal Numbers

From now on α, β, γ, θ denote ordinal numbers, X denotes a set, o denotes an object, and x, y, z, t, r, l denote surreal numbers.

The functor $\mathbf{1_{No}}$ yielding a surreal number is defined by the term

(Def. 1) $\langle\{\mathbf{0_{No}}\}, \emptyset\rangle$.

Now we state the propositions:

(1) If $y \in \mathrm{L}_x \cup \mathrm{R}_x$, then $\mathfrak{born}\, y \in \mathfrak{born}\, x$.

(2) $\mathrm{L}_x \neq \{x\} \neq \mathrm{R}_x$. The theorem is a consequence of (1).

(3) Preorder of Surreal Numbers – Reflexivity, Conway Ch. 1 Th. 0(iii):
$x \leqslant x$.
Proof: Define $\mathcal{P}$[ordinal number] $\equiv$ for every surreal number x such that $x \in \mathrm{Day}\$_1$ holds $x \leqslant x$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. $\square$

(4) Preorder of Surreal Numbers – Transitivity, Conway Ch. 1 Th. 1:
If $x \leqslant y \leqslant z$, then $x \leqslant z$.
Proof: Define $\mathcal{P}$[ordinal number] $\equiv$ for every surreal numbers x, y, z such that $x \leqslant y \leqslant z$ and $(\mathfrak{born}\, x \oplus \mathfrak{born}\, y) \oplus \mathfrak{born}\, z \subseteq \$_1$ holds $x \leqslant z$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. $\square$

(5) $\mathrm{L}_x \preceq \{x\} \preceq \mathrm{R}_x$.
Proof: Define $\mathcal{P}$[ordinal number] $\equiv$ for every surreal number x such that $\mathfrak{born}\, x \subseteq \$_1$ holds $\mathrm{L}_x \preceq \{x\} \preceq \mathrm{R}_x$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. $\square$

(6) Preorder of Surreal Numbers – Total, Conway Ch. 1 Th. 2(ii): If $y \not\leqslant x$, then $x \leqslant y$. The theorem is a consequence of (5) and (4).

(7) If α is finite, then Dayα is finite.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ Day$\$_1$ is finite. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. $\square$

(8) If $\mathfrak{b}\mathrm{orn}\, x$ is finite, then L_x is finite and R_x is finite.
PROOF: Day$\mathfrak{b}\mathrm{orn}\, x$ is finite. $\mathrm{L}_x \cup \mathrm{R}_x \subseteq$ Day$\mathfrak{b}\mathrm{orn}\, x$. $\square$

Let us consider x and y. Let us note that the predicate $x \leqslant y$ is reflexive and connected. We introduce the notation $y \geqslant x$ as a synonym of $x \leqslant y$.

2. Equivalence Relation of Preorder

Let us consider x and y. We say that $x \approx y$ if and only if

(Def. 2) $x \leqslant y \leqslant x$.

Note that the predicate is reflexive and symmetric. Now we state the propositions:

(9) If $x \leqslant y < z$, then $x < z$.

(10) If $x \approx y$ and $y \approx z$, then $x \approx z$.

(11) CONWAY CH. 1 TH. 2(I):
$\mathrm{L}_x \ll \{x\} \ll \mathrm{R}_x$.
PROOF: $\mathrm{L}_x \ll \{x\}$. $\square$

(12) Let us consider a non empty, surreal-membered set S. Suppose S is finite. Then there exist surreal numbers M_3, M_2 such that

(i) M_3, $M_2 \in S$, and

(ii) for every x such that $x \in S$ holds $M_3 \leqslant x \leqslant M_2$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non empty, surreal-membered set S such that $\$_1 = \overline{\overline{S}}$ there exist surreal numbers M_3, M_2 such that M_3, $M_2 \in S$ and for every x such that $x \in S$ holds $M_3 \leqslant x \leqslant M_2$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [8, (55)]. For every natural number n, $\mathcal{P}[n]$. $\square$

(13) Suppose $x < y$. Then

(i) there exists a surreal number x_2 such that $x_2 \in \mathrm{R}_x$ and $x < x_2 \leqslant y$, or

(ii) there exists a surreal number y_3 such that $y_3 \in \mathrm{L}_y$ and $x \leqslant y_3 < y$.

The theorem is a consequence of (11).

(14) Suppose $\mathrm{L}_y \ll \{x\} \ll \mathrm{R}_y$. Then $\langle\, \mathrm{L}_x \cup \mathrm{L}_y,\ \mathrm{R}_x \cup \mathrm{R}_y \,\rangle$ is a surreal number.
PROOF: Consider α being an ordinal number such that $x \in$ Dayα. Consider β being an ordinal number such that $y \in$ Dayβ. Set $X = \mathrm{L}_x \cup \mathrm{L}_y$. Set

$Y = \mathrm{R}_x \cup \mathrm{R}_y$. $X \ll Y$. For every object x such that $x \in X \cup Y$ there exists an ordinal number θ such that $\theta \in \alpha \cup \beta$ and $x \in \mathrm{Day}\theta$. $\square$

(15) Suppose $\mathrm{L}_y \ll \{x\} \ll \mathrm{R}_y$ and $z = \langle\, \mathrm{L}_x \cup \mathrm{L}_y,\ \mathrm{R}_x \cup \mathrm{R}_y \,\rangle$. Then $x \approx z$. The theorem is a consequence of (11).

Now we state the propositions:

(16) The Simplicity Theorem for Surreal Numbers:
Suppose $\mathrm{L}_y \ll \{x\} \ll \mathrm{R}_y$ and for every z such that $\mathrm{L}_y \ll \{z\} \ll \mathrm{R}_y$ holds $\mathfrak{born}\, x \subseteq \mathfrak{born}\, z$. Then $x \approx y$.
Proof: Set $X = \mathrm{L}_x \cup \mathrm{L}_y$. Set $Y = \mathrm{R}_x \cup \mathrm{R}_y$. Reconsider $z = \langle X, Y \rangle$ as a surreal number. $\mathrm{L}_x \ll \{x\} \ll \mathrm{R}_x$. $\mathrm{L}_y \ll \{y\} \ll \mathrm{R}_y$. $\mathrm{L}_z \ll \{z\} \ll \mathrm{R}_z$. $\mathrm{L}_x \ll \{z\}$. $\{x\} \ll \mathrm{R}_z$. $\mathrm{L}_y \ll \{z\}$. $x \approx z$. $\{y\} \ll \mathrm{R}_z$. $\{z\} \ll \mathrm{R}_y$. $\mathrm{L}_z \ll \{y\}$. $\square$

(17) If $X \ll \{x\}$ and $x \leqslant y$, then $X \ll \{y\}$. The theorem is a consequence of (4).

(18) If $\{x\} \ll X$ and $y \leqslant x$, then $\{y\} \ll X$. The theorem is a consequence of (4).

(19) If $x \approx y$, then $\langle\, \mathrm{L}_x \cup \mathrm{L}_y,\ \mathrm{R}_x \cup \mathrm{R}_y \,\rangle$ is a surreal number. The theorem is a consequence of (11), (17), (18), and (14).

(20) If $x \approx y$ and $z = \langle\, \mathrm{L}_x \cup \mathrm{L}_y,\ \mathrm{R}_x \cup \mathrm{R}_y \,\rangle$, then $x \approx z$. The theorem is a consequence of (11), (17), (18), and (15).

(21) $\{x\} \ll \{y\}$ if and only if $x < y$.

(22) $\langle \{x\}, \{y\} \rangle$ is a surreal number if and only if $x < y$. The theorem is a consequence of (21).

(23) Let us consider a surreal number M_2. Suppose for every y such that $y \in \mathrm{L}_x$ holds $y \leqslant M_2$ and $M_2 \in \mathrm{L}_x$. Then

(i) $\langle\, \{M_2\},\ \mathrm{R}_x \,\rangle$ is a surreal number, and

(ii) for every y such that $y = \langle\, \{M_2\},\ \mathrm{R}_x \,\rangle$ holds $y \approx x$ and $\mathfrak{born}\, y \subseteq \mathfrak{born}\, x$.

Proof: $\{M_2\} \ll \mathrm{R}_x$. For every object o such that $o \in \{M_2\} \cup \mathrm{R}_x$ there exists θ such that $\theta \in \mathfrak{born}\, x$ and $o \in \mathrm{Day}\theta$. For every surreal number x_1 such that $x_1 \in \mathrm{L}_x$ there exists a surreal number y_1 such that $y_1 \in \mathrm{L}_y$ and $x_1 \leqslant y_1$. For every surreal number x_1 such that $x_1 \in \mathrm{L}_y$ there exists a surreal number y_1 such that $y_1 \in \mathrm{L}_x$ and $x_1 \leqslant y_1$. $\square$

(24) Let us consider a surreal number M_3. Suppose for every y such that $y \in \mathrm{R}_x$ holds $M_3 \leqslant y$ and $M_3 \in \mathrm{R}_x$. Then

(i) $\langle\, \mathrm{L}_x,\ \{M_3\} \rangle$ is a surreal number, and

(ii) for every y such that $y = \langle \mathrm{L}_x, \{M_3\}\rangle$ holds $y \approx x$ and $\mathfrak{born}\, y \subseteq \mathfrak{born}\, x$.

PROOF: $\mathrm{L}_x \ll \{M_3\}$. For every object o such that $o \in \mathrm{L}_x \cup \{M_3\}$ there exists θ such that $\theta \in \mathfrak{born}\, x$ and $o \in \mathrm{Day}\theta$. For every surreal number x_1 such that $x_1 \in \mathrm{R}_y$ there exists a surreal number y_1 such that $y_1 \in \mathrm{R}_x$ and $y_1 \leqslant x_1$. For every surreal number x_1 such that $x_1 \in \mathrm{R}_x$ there exists a surreal number y_1 such that $y_1 \in \mathrm{R}_y$ and $y_1 \leqslant x_1$. □

(25) If $x \leqslant y$ and $z = \langle \{x, y\}, X\rangle$ and $t = \langle \{y\}, X\rangle$, then $z \approx t$. The theorem is a consequence of (23).

(26) If $z = \langle \{x, y\}, X\rangle$, then $\langle \{x\}, X\rangle$ is a surreal number.
PROOF: Set $b = \mathfrak{born}\, z$. $\{x\} \ll X$. For every object o such that $o \in \{x\} \cup X$ there exists θ such that $\theta \in b$ and $o \in \mathrm{Day}\theta$. □

(27) If $x \leqslant y$ and $z = \langle X, \{x, y\}\rangle$ and $t = \langle X, \{x\}\rangle$, then $z \approx t$. The theorem is a consequence of (24).

(28) If $z = \langle X, \{x, y\}\rangle$, then $\langle X, \{x\}\rangle$ is a surreal number.
PROOF: Set $b = \mathfrak{born}\, z$. $X \ll \{x\}$. For every object o such that $o \in X \cup \{x\}$ there exists θ such that $\theta \in b$ and $o \in \mathrm{Day}\theta$. □

Let X, Y be sets. We say that $X \lessdot Y$ if and only if

(Def. 3) for every surreal number x such that $x \in X$ there exist surreal numbers y_1, y_2 such that y_1, $y_2 \in Y$ and $y_1 \leqslant x \leqslant y_2$.

One can verify that the predicate is reflexive.

We say that $X \leftrightarrow Y$ if and only if

(Def. 4) $X \lessdot Y$ and $Y \lessdot X$.

One can verify that the predicate is reflexive and symmetric.

Now we state the propositions:

(29) Let us consider sets X_1, X_2, Y_1, Y_2. Suppose $X_1 \leftrightarrow X_2$ and $Y_1 \leftrightarrow Y_2$ and $x = \langle X_1, Y_1\rangle$ and $y = \langle X_2, Y_2\rangle$. Then $x \approx y$.

(30) Let us consider sets X, Y. If $X \subseteq Y$, then $X \lessdot Y$.

(31) Let us consider sets X_1, X_2, Y_1, Y_2. If $X_1 \lessdot X_2$ and $Y_1 \lessdot Y_2$, then $X_1 \cup Y_1 \lessdot X_2 \cup Y_2$.

(32) If $x \approx y$, then $\{x\} \lessdot \{y\}$.

3. Representative of Equivalence Class With a Unique Set of Properties

Let x be a surreal number. The functor $\mathfrak{born}_{\approx}x$ yielding an ordinal number is defined by

(Def. 5) there exists a surreal number y such that $\mathfrak{born}\, y = it$ and $y \approx x$ and for every surreal number y such that $y \approx x$ holds $it \subseteq \mathfrak{born}\, y$.

The functor $\mathfrak{Born}_{\approx}x$ yielding a surreal-membered set is defined by

(Def. 6) $y \in it$ iff $y \approx x$ and $y \in \mathrm{Day}\mathfrak{born}_{\approx}x$.

One can check that $\mathfrak{Born}_{\approx}x$ is non empty. Let α be a non empty, surreal-membered set. We say that x is α-smallest if and only if

(Def. 7) $x \in \alpha$ and for every y such that $y \in \alpha$ and $y \approx x$ holds $\overline{\overline{\mathrm{L}_x}} \oplus \overline{\overline{\mathrm{R}_x}} \subseteq \overline{\overline{\mathrm{L}_y}} \oplus \overline{\overline{\mathrm{R}_y}}$.

Observe that there exists a surreal number which is α-smallest. Now we state the propositions:

(33) If $x \approx y$, then $\mathfrak{born}_{\approx}x = \mathfrak{born}_{\approx}y$. The theorem is a consequence of (4).

(34) If $x \approx y$, then $\mathfrak{Born}_{\approx}x = \mathfrak{Born}_{\approx}y$.

(35) If $y \in \mathfrak{Born}_{\approx}x$, then $\mathfrak{born}\, y = \mathfrak{born}_{\approx}y = \mathfrak{born}_{\approx}x$. The theorem is a consequence of (33).

(36) $\langle \emptyset, \mathrm{Day}\alpha \rangle, \langle \mathrm{Day}\alpha, \emptyset \rangle \in (\mathrm{Daysucc}\, \alpha) \setminus (\mathrm{Day}\alpha)$. The theorem is a consequence of (11).

From now on n denotes a natural number. Let α be a set. The functor made of α yielding a surreal-membered set is defined by

(Def. 8) $o \in it$ iff o is surreal and $\mathrm{L}_o \cup \mathrm{R}_o \subseteq \alpha$.

Let α be an ordinal number. The functor $\mathrm{unique}_{\mathbf{No}}\mathrm{op}(\alpha)$ yielding a transfinite sequence is defined by

(Def. 9) $\mathrm{dom}\, it = \mathrm{succ}\, \alpha$ and for every ordinal number β such that $\beta \in \mathrm{succ}\, \alpha$ holds $it(\beta) \subseteq \mathrm{Day}\beta$ and for every x, $x \in it(\beta)$ iff $x \in \bigcup \mathrm{rng}(it \restriction \beta)$ or $\beta = \mathfrak{born}_{\approx}x$ and there exists a non empty, surreal-membered set Y such that $Y = \mathfrak{Born}_{\approx}x \cap$ made of $\bigcup \mathrm{rng}(it \restriction \beta)$ and $x =$ the Y-smallest surreal number.

Let us consider o. One can verify that $(\mathrm{unique}_{\mathbf{No}}\mathrm{op}(\alpha))(o)$ is surreal-membered. Now we state the propositions:

(37) Suppose $\alpha \subseteq \beta$. Then $\mathrm{unique}_{\mathbf{No}}\mathrm{op}(\beta) \restriction \mathrm{succ}\, \alpha = \mathrm{unique}_{\mathbf{No}}\mathrm{op}(\alpha)$.
PROOF: Define $\mathcal{P}[\text{transfinite sequence}, \text{ordinal number}, \text{surreal number}] \equiv \$_3 \in \bigcup \mathrm{rng}\, \$_1$ or $\$_2 = \mathfrak{born}_{\approx}\$_3$ and there exists a non empty, surreal-membered set Y such that $Y = \mathfrak{Born}_{\approx}\$_3 \cap$ made of $\bigcup \mathrm{rng}\, \$_1$ and $\$_3 =$

the Y-smallest surreal number. Define $\mathcal{H}$(transfinite sequence) = $\{e$, where e is an element of Daydom $\$_1$: for every x such that $x = e$ holds $\mathcal{P}[\$_1, \operatorname{dom} \$_1, x]\}$. Set $S_1 = \operatorname{unique}_{\mathbf{No}}\operatorname{op}(\alpha)$. Set $S = \operatorname{unique}_{\mathbf{No}}\operatorname{op}(\beta)$. Set $S_2 = S\restriction \operatorname{succ} \alpha$. $\operatorname{dom} S_1 = \operatorname{succ} \alpha$ and for every ordinal number β and for every transfinite sequence L_1 such that $\beta \in \operatorname{succ} \alpha$ and $L_1 = S_1\restriction\beta$ holds $S_1(\beta) = \mathcal{H}(L_1)$. $\operatorname{dom} S_2 = \operatorname{succ} \alpha$ and for every ordinal number γ and for every transfinite sequence L_2 such that $\gamma \in \operatorname{succ} \alpha$ and $L_2 = S_2\restriction\gamma$ holds $S_2(\gamma) = \mathcal{H}(L_2)$. $S_1 = S_2$. □

(38) Suppose $x \in (\operatorname{unique}_{\mathbf{No}}\operatorname{op}(\alpha))(\beta)$. Then

(i) $\mathfrak{born}_{\approx} x = \mathfrak{born}\, x \subseteq \beta$, and

(ii) $x \in (\operatorname{unique}_{\mathbf{No}}\operatorname{op}(\alpha))(\mathfrak{born}\, x)$, and

(iii) $x \notin \bigcup \operatorname{rng}(\operatorname{unique}_{\mathbf{No}}\operatorname{op}(\alpha)\restriction \mathfrak{born}\, x)$.

PROOF: Set $M = \operatorname{unique}_{\mathbf{No}}\operatorname{op}(\alpha)$. Define $\mathcal{M}$[ordinal number] $\equiv x \in M(\$_1)$ and $\$_1 \in \operatorname{succ} \alpha$. Consider δ being an ordinal number such that $\mathcal{M}[\delta]$ and for every ordinal number E such that $\mathcal{M}[E]$ holds $\delta \subseteq E$. $x \notin \bigcup \operatorname{rng}(M\restriction\delta)$. Consider Y being a non empty, surreal-membered set such that $Y = \mathfrak{Born}_{\approx} x \cap$ made of $\bigcup \operatorname{rng}(M\restriction\delta)$ and $x =$ the Y-smallest surreal number. □

(39) If $\theta \subseteq \alpha \subseteq \beta$, then $(\operatorname{unique}_{\mathbf{No}}\operatorname{op}(\alpha))(\theta) = (\operatorname{unique}_{\mathbf{No}}\operatorname{op}(\beta))(\theta)$. The theorem is a consequence of (37).

(40) Suppose $\alpha \subseteq \beta$ and $\beta \in \operatorname{succ} \gamma$. Then $(\operatorname{unique}_{\mathbf{No}}\operatorname{op}(\gamma))(\alpha) \subseteq (\operatorname{unique}_{\mathbf{No}}\operatorname{op}(\gamma))(\beta)$.

Let x be a surreal number. The functor $\operatorname{Unique}_{\mathbf{No}}(x)$ yielding a surreal number is defined by

(Def. 10) $it \approx x$ and $it \in (\operatorname{unique}_{\mathbf{No}}\operatorname{op}(\mathfrak{born}_{\approx} x))(\mathfrak{born}_{\approx} x)$.

Now we state the propositions:

(41) If $x \approx y$, then $\operatorname{Unique}_{\mathbf{No}}(x) = \operatorname{Unique}_{\mathbf{No}}(y)$. The theorem is a consequence of (33) and (4).

(42) $\mathbf{0_{No}} = \operatorname{Unique}_{\mathbf{No}}(\mathbf{0_{No}})$. The theorem is a consequence of (38).

Let x be a surreal number. We say that x is unique surreal if and only if

(Def. 11) $x = \operatorname{Unique}_{\mathbf{No}}(x)$.

One can verify that $\mathbf{0_{No}}$ is unique surreal and there exists a surreal number which is unique surreal. Now we state the propositions:

(43) If x is an unique surreal number and $o \in \mathrm{L}_x \cup \mathrm{R}_x$, then o is an unique surreal number. The theorem is a consequence of (38), (1), and (39).

(44) If L_x is non empty and finite and x is an unique surreal number, then $\overline{\overline{\mathrm{L}_x}} = 1$. The theorem is a consequence of (12), (38), and (23).

(45) If R_x is non empty and finite and x is an unique surreal number, then $\overline{\overline{\mathrm{R}_x}} = 1$. The theorem is a consequence of (12), (38), and (24).

(46) $\overline{\overline{\mathrm{L}_x}} \oplus \overline{\overline{\mathrm{R}_x}} = 0$ if and only if $x = \mathbf{0_{No}}$.

(47) $\overline{\overline{\mathrm{L}_x}} \oplus \overline{\overline{\mathrm{R}_x}} = 1$ if and only if there exists a surreal number y such that $x = \langle \emptyset, \{y\} \rangle$ or $x = \langle \{y\}, \emptyset \rangle$.

PROOF: If $\overline{\overline{\mathrm{L}_x}} \oplus \overline{\overline{\mathrm{R}_x}} = 1$, then there exists a surreal number y such that $x = \langle \emptyset, \{y\} \rangle$ or $x = \langle \{y\}, \emptyset \rangle$ by [7, (86),(76)]. □

Let X be a set. We say that X is unique surreal-membered if and only if

(Def. 12) if $o \in X$, then o is an unique surreal number.

Note that every set which is empty is also unique surreal-membered. Let x be an unique surreal number. One can verify that $\mathrm{L}_x \cup \mathrm{R}_x$ is unique surreal-membered and $\{x\}$ is unique surreal-membered. Let X, Y be unique surreal-membered sets. One can check that $X \cup Y$ is unique surreal-membered. Let x be a surreal number. One can check that $\mathrm{Unique}_{\mathbf{No}}(x)$ is unique surreal. Now we state the propositions:

(48) If x is an unique surreal number, then $\mathfrak{born}\, x = \mathfrak{born}_{\approx} x$. The theorem is a consequence of (38).

(49) Suppose for every z such that $z \in \mathfrak{Born}_{\approx} x$ and $\mathrm{L}_z \cup \mathrm{R}_z$ is unique surreal-membered and $x \neq z$ holds $\overline{\overline{\mathrm{L}_x}} \oplus \overline{\overline{\mathrm{R}_x}} \in \overline{\overline{\mathrm{L}_z}} \oplus \overline{\overline{\mathrm{R}_z}}$ and $x \in \mathfrak{Born}_{\approx} x$ and $\mathrm{L}_x \cup \mathrm{R}_x$ is unique surreal-membered. Then x is an unique surreal number.

PROOF: Set $c = \mathrm{Unique}_{\mathbf{No}}(x)$. Set $\beta = \mathfrak{born}_{\approx} x$. $\mathfrak{born}_{\approx} c = \beta$ and $\mathfrak{Born}_{\approx} c = \mathfrak{Born}_{\approx} x$. $\mathfrak{born}_{\approx} c = \mathfrak{born}\, c$. $c \notin \bigcup \mathrm{rng}(\mathrm{unique}_{\mathbf{No}} \mathrm{op}(\beta) \restriction \beta)$. Consider Y being a non empty, surreal-membered set such that $Y = \mathfrak{Born}_{\approx} c \cap$ made of $\bigcup \mathrm{rng}(\mathrm{unique}_{\mathbf{No}} \mathrm{op}(\beta) \restriction \beta)$ and $c =$ the Y-smallest surreal number. $x \in \mathfrak{Born}_{\approx} c$. $\mathrm{L}_x \cup \mathrm{R}_x \subseteq \bigcup \mathrm{rng}(\mathrm{unique}_{\mathbf{No}} \mathrm{op}(\beta) \restriction \beta)$. □

(50) If x is an unique surreal number and y is an unique surreal number and $x \approx y$, then $x = y$. The theorem is a consequence of (41).

(51) Let us consider a surreal number c. Suppose $\mathfrak{born}\, c = \mathfrak{born}_{\approx} c$ and $\mathrm{L}_c \ll \{x\} \ll \mathrm{R}_c$. Then $\mathfrak{born}\, c \subseteq \mathfrak{born}\, x$.

PROOF: Define $\mathcal{P}[\text{ordinal number}] \equiv$ there exists y such that $\mathrm{L}_c \ll \{y\} \ll \mathrm{R}_c$ and $\mathfrak{born}\, y = \$_1$. Consider α such that $\mathcal{P}[\alpha]$ and for every β such that $\mathcal{P}[\beta]$ holds $\alpha \subseteq \beta$. Consider y such that $\mathrm{L}_c \ll \{y\} \ll \mathrm{R}_c$ and $\mathfrak{born}\, y = \alpha$. $\mathfrak{born}_{\approx} c = \mathfrak{born}_{\approx} y$. □

(52) Let us consider unique surreal numbers c, x. Suppose $\mathrm{L}_c \ll \{x\} \ll \mathrm{R}_c$ and $x \neq c$. Then $\mathfrak{born}\, c \in \mathfrak{born}\, x$. The theorem is a consequence of (48), (51), (50), (13), (1), (11), (17), (18), and (3).

(53) Suppose $\mathfrak{born}\, x = \mathfrak{born}_{\approx} x$ and $\mathfrak{born}\, x$ is not limit ordinal. Then there exist surreal numbers y, z such that

(i) $x \approx z$, and

(ii) $z = \langle \mathrm{L}_y \cup \{y\}, \mathrm{R}_y \rangle$ or $z = \langle \mathrm{L}_y, \mathrm{R}_y \cup \{y\} \rangle$.

Proof: Consider β being an ordinal number such that $\mathfrak{born}\, x = \operatorname{succ} \beta$. Define $\mathcal{L}$[object] $\equiv$ for every z such that $z = \$_1$ holds $\mathfrak{born}\, z \in \beta$ and $z < x$. Consider L being a set such that $o \in L$ iff $o \in \mathrm{Day}\beta$ and $\mathcal{L}[o]$. Define $\mathcal{R}$[object] $\equiv$ for every z such that $z = \$_1$ holds $\mathfrak{born}\, z \in \beta$ and $x < z$. Consider R being a set such that $o \in R$ iff $o \in \mathrm{Day}\beta$ and $\mathcal{R}[o]$. $L \ll R$. For every object o such that $o \in L \cup R$ there exists θ such that $\theta \in \beta$ and $o \in \mathrm{Day}\theta$. Reconsider $L_3 = \langle L, R \rangle$ as a surreal number. $L_3 \not\approx x$. $\square$

References

[1] Maan T. Alabdullah, Essam El-Seidy, and Neveen S. Morcos. On numbers and games. *International Journal of Scientific and Engineering Research*, 11:510–517, February 2020.

[2] Norman L. Alling. *Foundations of Analysis Over Surreal Number Fields*. Number 141 in Annals of Discrete Mathematics. North-Holland, 1987. ISBN 9780444702265.

[3] John Horton Conway. *On Numbers and Games*. A K Peters Ltd., Natick, MA, second edition, 2001. ISBN 1-56881-127-6.

[4] Philip Ehrlich. Conway names, the simplicity hierarchy and the surreal number tree. *Journal of Logic and Analysis*, 3(1):1–26, 2011. doi:10.4115/jla.2011.3.1.

[5] Philip Ehrlich. The absolute arithmetic continuum and the unification of all numbers great and small. *The Bulletin of Symbolic Logic*, 18(1):1–45, 2012. doi:10.2178/bsl/1327328438.

[6] Philp Ehrlich. Number systems with simplicity hierarchies: A generalization of Conway's theory of surreal numbers. *Journal of Symbolic Logic*, 66(3):1231–1258, 2001. doi:10.2307/2695104.

[7] Sebastian Koch. Natural addition of ordinals. *Formalized Mathematics*, 27(**2**):139–152, 2019. doi:10.2478/forma-2019-0015.

[8] Karol Pąk. Stirling numbers of the second kind. *Formalized Mathematics*, 13(**2**):337–345, 2005.

[9] Karol Pąk. Conway numbers – formal introduction. *Formalized Mathematics*, 31(1): 193–203, 2023. doi:10.2478/forma-2023-0018.

[10] Dierk Schleicher and Michael Stoll. An introduction to Conway's games and numbers. *Moscow Mathematical Journal*, 6:359–388, 2006. doi:10.17323/1609-4514-2006-6-2-359-388.

Accepted December 12, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 215–228, 2023
DOI: 10.2478/forma-2023-0020
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

The Ring of Conway Numbers in Mizar

Karol Pąk
Faculty of Computer Science
University of Białystok
Poland

Summary. Conway's introduction to algebraic operations on surreal numbers with a rather simple definition. However, he combines recursion with Conway's induction on surreal numbers, more formally he combines transfinite induction-recursion with the properties of proper classes, which is difficult to introduce formally.

This article represents a further step in our ongoing efforts to investigate the possibilities offered by Mizar with Tarski-Grothendieck set theory [4] to introduce the algebraic structure of Conway numbers and to prove their ring character.

MSC: 03H05 12J15 68V20

Keywords: surreal numbers; Conway's game

MML identifier: SURREALR, version: 8.1.14 5.76.1456

Introduction

We present a formal analysis of the contents of Chapter 1, *The Class* **No** *is a Field* of John Conway's seminal book [5]. We formalised four sections, namely *Properties of Addition*, *Properties of Negation*, *Properties of Addition and Order* and *Properties of Multiplication*. We begin our exploration by formulating and proving two schemes (i.e., second-order theorems) for defining arithmetic operations on surreal numbers using a technique that mimics induction-infinite recursion. Then, we examine the applicability of this solution by defining the opposite surreal number but also the sum and product of surreal numbers. We prove for each such operator simultaneously its correctness and crucial properties, in particular the preservation of pre-order under the operator. For this

purpose, we use transfinite induction with respect to successive generations of surreal numbers. Notice that we express the Conway induction using the transfinite induction with the Heisenberg sum of two ordinals [3, 6], formalised in [7].

The most important result is the formalisation of the following properties of the surreal numbers

$$x + 0_{\mathbf{No}} = x \quad (38), \qquad -(x+y) = -x + -y \quad (40), \qquad x \cdot 0_{\mathbf{No}} \approx 0_{\mathbf{No}} \quad (56),$$
$$x + y = y + x \quad (29), \qquad --x = x \quad (9), \qquad x \cdot 1_{\mathbf{No}} \approx x \quad (57),$$
$$(x + y) + z = x + (y + z) \quad (37), \qquad x + -x \approx 0_{\mathbf{No}} \quad (39), \qquad x \cdot y \approx y \cdot x \quad (51),$$

$$(-x) \cdot y = -x \cdot y = x \cdot (-y) \quad (58) \qquad (-x) \cdot (-y) = x \cdot y \quad (58),$$
$$x \cdot (y+z) \approx x \cdot y + x \cdot z \quad (67), \qquad (x \cdot y) \cdot z \approx x \cdot (y \cdot z) \quad (69),$$
$$0_{\mathbf{No}} < x \wedge 0_{\mathbf{No}} < y \Rightarrow 0_{\mathbf{No}} < x \cdot y \quad (72), \qquad y \leqslant z \Leftrightarrow x + y \leqslant x + z \quad (32).$$

The formalisation is mainly based on [1, 2, 5, 10].

1. Preliminaries

From now on α, β, γ denote ordinal numbers, o denotes an object, x, y, z, t, r, l denote surreal numbers, and X, Y denote sets.

Let f be a function. One can check that f is function yielding if and only if the condition (Def. 1) is satisfied.

(Def. 1) $\operatorname{rng} f$ is functional.

One can check that there exists a transfinite sequence which is $\subseteq$-monotone and function yielding. Let f be a $\subseteq$-monotone function and X be a set. Let us observe that $f \restriction X$ is $\subseteq$-monotone. Let f be a $\subseteq$-monotone, function yielding transfinite sequence. Let us note that $\bigcup \operatorname{rng} f$ is function-like and relation-like. Now we state the propositions:

(1) Let us consider a $\subseteq$-monotone, function yielding transfinite sequence f, and an object o. Suppose $o \in \operatorname{dom}(\bigcup \operatorname{rng} f)$. Then there exists α such that

(i) $\alpha \in \operatorname{dom} f$, and

(ii) $o \in \operatorname{dom}(f(\alpha))$.

(2) Let us consider a $\subseteq$-monotone, function yielding transfinite sequence f, and α. Suppose $\alpha \in \operatorname{dom} f$. Then

(i) $\operatorname{dom}(f(\alpha)) \subseteq \operatorname{dom}(\bigcup \operatorname{rng} f)$, and

(ii) for every o such that $o \in \operatorname{dom}(f(\alpha))$ holds $f(\alpha)(o) = (\bigcup \operatorname{rng} f)(o)$.

Proof: Set $U = \bigcup \operatorname{rng} f$. $\operatorname{dom}(f(\alpha)) \subseteq \operatorname{dom} U$. $\square$

(3) Let us consider a $\subseteq$-monotone, function yielding transfinite sequence f, an ordinal number α, and a set X. Suppose for every o such that $o \in X$ there exists an ordinal number β such that $o \in \operatorname{dom}(f(\beta))$ and $\beta \in \alpha$. Then $(\bigcup \operatorname{rng}(f\restriction\alpha))^\circ X = (\bigcup \operatorname{rng} f)^\circ X$. The theorem is a consequence of (2).

2. Surreal Number Operators – Schemes

The scheme *MonoFvSExists* deals with an ordinal number θ and a unary functor δ yielding a set and a binary functor $\mathcal{H}$ yielding an object and states that

(Sch. 1) There exists a $\subseteq$-monotone, function yielding transfinite sequence S such that $\operatorname{dom} S = \operatorname{succ}\theta$ and for every ordinal number α such that $\alpha \in \operatorname{succ}\theta$ there exists a many sorted set S_3 indexed by $\delta(\alpha)$ such that $S(\alpha) = S_3$ and for every o such that $o \in \delta(\alpha)$ holds $S_3(o) = \mathcal{H}(o, S\restriction\alpha)$

provided

- for every $\subseteq$-monotone, function yielding transfinite sequence S such that for every ordinal number α such that $\alpha \in \operatorname{dom} S$ holds $\operatorname{dom}(S(\alpha)) = \delta(\alpha)$ for every ordinal number α for every o such that $o \in \operatorname{dom}(S(\alpha))$ holds $\mathcal{H}(o, S\restriction\alpha) = \mathcal{H}(o, S)$ and
- for every ordinal numbers α, β such that $\alpha \subseteq \beta$ holds $\delta(\alpha) \subseteq \delta(\beta)$.

The scheme *MonoFvSUniq* deals with an ordinal number θ and a unary functor δ yielding a set and $\subseteq$-monotone, function yielding transfinite sequences S_1, S_2 and a binary functor $\mathcal{H}$ yielding an object and states that

(Sch. 2) $S_1\restriction\theta = S_2\restriction\theta$

provided

- $\theta \subseteq \operatorname{dom} S_1$ and $\theta \subseteq \operatorname{dom} S_2$ and
- for every ordinal number α such that $\alpha \in \theta$ there exists a many sorted set S_3 indexed by $\delta(\alpha)$ such that $S_1(\alpha) = S_3$ and for every o such that $o \in \delta(\alpha)$ holds $S_3(o) = \mathcal{H}(o, S_1\restriction\alpha)$ and
- for every ordinal number α such that $\alpha \in \theta$ there exists a many sorted set S_3 indexed by $\delta(\alpha)$ such that $S_2(\alpha) = S_3$ and for every o such that $o \in \delta(\alpha)$ holds $S_3(o) = \mathcal{H}(o, S_2\restriction\alpha)$.

3. The Opposite Surreal Number

Let us consider α. The functor $\mathrm{opposite}_{\mathbf{No}}(\alpha)$ yielding a many sorted set indexed by Dayα is defined by

(Def. 2) there exists a $\subseteq$-monotone, function yielding transfinite sequence S such that $\mathrm{dom}\, S = \mathrm{succ}\, \alpha$ and $it = S(\alpha)$ and for every β such that $\beta \in \mathrm{succ}\, \alpha$ there exists a many sorted set S_5 indexed by Dayβ such that $S(\beta) = S_5$ and for every o such that $o \in \mathrm{Day}\beta$ holds $S_5(o) = \langle (\bigcup \mathrm{rng}(S{\restriction}\beta))^\circ(\mathrm{R}_o), (\bigcup \mathrm{rng}(S{\restriction}\beta))^\circ(\mathrm{L}_o) \rangle$.

Now we state the propositions:

(4) Let us consider a $\subseteq$-monotone, function yielding transfinite sequence S. Suppose for every β such that $\beta \in \mathrm{dom}\, S$ there exists a many sorted set S_5 indexed by Dayβ such that $S(\beta) = S_5$ and for every o such that $o \in \mathrm{Day}\beta$ holds $S_5(o) = \langle (\bigcup \mathrm{rng}(S{\restriction}\beta))^\circ(\mathrm{R}_o), (\bigcup \mathrm{rng}(S{\restriction}\beta))^\circ(\mathrm{L}_o) \rangle$. If $\alpha \in \mathrm{dom}\, S$, then $\mathrm{opposite}_{\mathbf{No}}(\alpha) = S(\alpha)$.

Proof: Define $\delta(\text{ordinal number}) = \mathrm{Day}\$_1$. Define $\mathcal{H}(\text{object}, \subseteq\text{-monotone, function yielding transfinite sequence}) = \langle (\bigcup \mathrm{rng}\, \$_2)^\circ(\mathrm{R}_{\$_1}), (\bigcup \mathrm{rng}\, \$_2)^\circ(\mathrm{L}_{\$_1}) \rangle$. Consider S_2 being a $\subseteq$-monotone, function yielding transfinite sequence such that $\mathrm{dom}\, S_2 = \mathrm{succ}\, \alpha$ and $S_2(\alpha) = \mathrm{opposite}_{\mathbf{No}}(\alpha)$ and for every ordinal number β such that $\beta \in \mathrm{succ}\, \alpha$ there exists a many sorted set S_5 indexed by $\delta(\beta)$ such that $S_2(\beta) = S_5$ and for every object x such that $x \in \delta(\beta)$ holds $S_5(x) = \mathcal{H}(x, S_2{\restriction}\beta)$. $S_1{\restriction}\mathrm{succ}\, \alpha = S_2{\restriction}\mathrm{succ}\, \alpha$. $\square$

(5) Let us consider a $\subseteq$-monotone, function yielding transfinite sequence f. Suppose $o \in \mathrm{dom}(f(\beta))$ and $\beta \in \alpha$. Then

(i) $o \in \mathrm{dom}(\bigcup \mathrm{rng}(f{\restriction}\alpha))$, and

(ii) $(\bigcup \mathrm{rng}(f{\restriction}\alpha))(o) = (\bigcup \mathrm{rng}\, f)(o)$.

The theorem is a consequence of (2).

(6) Let us consider a $\subseteq$-monotone, function yielding transfinite sequence f, and ordinal numbers α, β. Suppose $o \in \mathrm{dom}(f(\beta))$ and $\beta \in \alpha$. Then $(\bigcup \mathrm{rng}(f{\restriction}\alpha))(o) = (\bigcup \mathrm{rng}\, f)(o)$. The theorem is a consequence of (2).

Let us consider x. The functor $-x$ yielding a set is defined by the term

(Def. 3) $(\mathrm{opposite}_{\mathbf{No}}(\mathfrak{born}\, x))(x)$.

Let X be a set. The functor $\ominus X$ yielding a set is defined by

(Def. 4) $o \in it$ iff there exists a surreal number x such that $x \in X$ and $o = -x$.

Now we state the proposition:

(7) $-x = \langle \ominus \mathrm{R}_x, \ominus \mathrm{L}_x \rangle$.

Proof: Set $\alpha = \mathfrak{born}\, x$. Consider S being a $\subseteq$-monotone, function yielding transfinite sequence such that $\mathrm{dom}\, S = \mathrm{succ}\, \alpha$ and $\mathrm{opposite}_{\mathbf{No}}(\alpha) = S(\alpha)$

and for every ordinal number β such that $\beta \in \operatorname{succ}\alpha$ there exists a many sorted set S_5 indexed by Dayβ such that $S(\beta) = S_5$ and for every object x such that $x \in \mathrm{Day}\beta$ holds $S_5(x) = \langle(\bigcup \operatorname{rng}(S\restriction\beta))^\circ(\mathrm{R}_x), (\bigcup \operatorname{rng}(S\restriction\beta))^\circ(\mathrm{L}_x)\rangle$. Consider S_3 being a many sorted set indexed by Dayα such that $S(\alpha) = S_3$ and for every object x such that $x \in \mathrm{Day}\alpha$ holds $S_3(x) = \langle(\bigcup \operatorname{rng}(S\restriction\alpha))^\circ(\mathrm{R}_x), (\bigcup \operatorname{rng}(S\restriction\alpha))^\circ(\mathrm{L}_x)\rangle$. Set $U = \bigcup \operatorname{rng}(S\restriction\alpha)$. $\ominus \mathrm{R}_x \subseteq U^\circ(\mathrm{R}_x)$. $U^\circ(\mathrm{R}_x) \subseteq \ominus \mathrm{R}_x$. $\ominus \mathrm{L}_x \subseteq U^\circ(\mathrm{L}_x)$. $U^\circ(\mathrm{L}_x) \subseteq \ominus \mathrm{L}_x$. $\square$

Let us consider x. One can check that $-x$ is surreal. Let X be a set. Let us note that $\ominus X$ is surreal-membered. Now we state the propositions:

(8) (i) $\mathrm{L}_{(-x)} = \ominus \mathrm{R}_x$, and

(ii) $\mathrm{R}_{(-x)} = \ominus \mathrm{L}_x$.

The theorem is a consequence of (7).

(9) CONWAY CH. 1 TH. 4(II):
$--x = x$.

Let us consider x. Let us observe that $--x$ reduces to x. Now we state the propositions:

(10) $x \leqslant y$ if and only if $-y \leqslant -x$.

(11) Let us consider a surreal number x, and an ordinal number δ. If $x \in \mathrm{Day}\delta$, then $-x \in \mathrm{Day}\delta$.

(12) $\mathfrak{born}\, x = \mathfrak{born}\,(-x)$.

(13) $\mathfrak{born}_{\approx} x = \mathfrak{born}_{\approx}(-x)$. The theorem is a consequence of (10) and (12).

(14) If $x \in \mathfrak{Born}_{\approx} y$, then $-x \in \mathfrak{Born}_{\approx}(-y)$. The theorem is a consequence of (10), (13), and (12).

(15) Let us consider a surreal-membered set X. Then $\ominus \ominus X = X$.

(16) $\overline{\overline{\ominus X}} \subseteq \overline{\overline{X}}$.

PROOF: Define $\mathcal{P}[\mathrm{object}, \mathrm{object}] \equiv$ for every x such that $x = \$_1$ holds $\$_2 = -x$. If $o \in \ominus X$, then there exists an object u such that $\mathcal{P}[o, u]$. Consider f being a function such that $\operatorname{dom} f = \ominus X$ and for every object o such that $o \in \ominus X$ holds $\mathcal{P}[o, f(o)]$. $\operatorname{rng} f \subseteq X$. f is one-to-one. $\square$

(17) Let us consider a surreal-membered set X. Then $\overline{\overline{X}} = \overline{\overline{\ominus X}}$. The theorem is a consequence of (15) and (16).

Let us consider surreal-membered sets X, Y. Now we state the propositions:

(18) $X \preceq Y$ if and only if $\ominus Y \preceq \ominus X$. The theorem is a consequence of (15).

(19) $X \ll Y$ if and only if $\ominus Y \ll \ominus X$. The theorem is a consequence of (15).

Now we state the propositions:

(20) Let us consider sets X_1, X_2. Then $\ominus(X_1 \cup X_2) = \ominus X_1 \cup \ominus X_2$.

(21) $\{-x\} = \ominus\{x\}$.

(22) $\ominus\emptyset = \emptyset$.

(23) $-\mathbf{0_{No}} = \mathbf{0_{No}}$. The theorem is a consequence of (7) and (22).

One can verify that $-\mathbf{0_{No}}$ reduces to $\mathbf{0_{No}}$. Now we state the proposition:

(24) $x \approx \mathbf{0_{No}}$ if and only if $-x \approx \mathbf{0_{No}}$.

Let α be an ordinal number. The functor Triangle α yielding a subset of Day$\alpha \times$ Dayα is defined by

(Def. 5) for every surreal numbers x, y, $\langle x, y\rangle \in it$ iff $\mathfrak{born}\, x \oplus \mathfrak{born}\, y \subseteq \alpha$.

Observe that Triangle α is non empty. Now we state the proposition:

(25) Let us consider ordinal numbers α, β. Suppose $\alpha \subseteq \beta$. Then Triangle $\alpha \subseteq$ Triangle β.

4. The Sum of Surreal Numbers

Let α be an ordinal number. The functor $\mathrm{sum}_{\mathbf{No}}(\alpha)$ yielding a many sorted set indexed by Triangle α is defined by

(Def. 6) there exists a $\subseteq$-monotone, function yielding transfinite sequence S such that $\mathrm{dom}\, S = \mathrm{succ}\, \alpha$ and $it = S(\alpha)$ and for every ordinal number β such that $\beta \in \mathrm{succ}\, \alpha$ there exists a many sorted set S_5 indexed by Triangle β such that $S(\beta) = S_5$ and for every object x such that $x \in$ Triangle β holds $S_5(x) = \langle (\bigcup \mathrm{rng}(S\restriction\beta))^\circ(\mathrm{L}_{\mathrm{L}_x} \times \{\mathrm{R}_x\} \cup \{\mathrm{L}_x\} \times \mathrm{L}_{\mathrm{R}_x}), (\bigcup \mathrm{rng}(S\restriction\beta))^\circ(\mathrm{R}_{\mathrm{L}_x} \times \{\mathrm{R}_x\} \cup \{\mathrm{L}_x\} \times \mathrm{R}_{\mathrm{R}_x})\rangle$.

Now we state the proposition:

(26) Let us consider a $\subseteq$-monotone, function yielding transfinite sequence S. Suppose for every ordinal number β such that $\beta \in \mathrm{dom}\, S$ there exists a many sorted set S_5 indexed by Triangle β such that $S(\beta) = S_5$ and for every object x such that $x \in$ Triangle β holds $S_5(x) = \langle (\bigcup \mathrm{rng}(S\restriction\beta))^\circ(\mathrm{L}_{\mathrm{L}_x} \times \{\mathrm{R}_x\} \cup \{\mathrm{L}_x\} \times \mathrm{L}_{\mathrm{R}_x}), (\bigcup \mathrm{rng}(S\restriction\beta))^\circ(\mathrm{R}_{\mathrm{L}_x} \times \{\mathrm{R}_x\} \cup \{\mathrm{L}_x\} \times \mathrm{R}_{\mathrm{R}_x})\rangle$. Let us consider an ordinal number α. If $\alpha \in \mathrm{dom}\, S$, then $\mathrm{sum}_{\mathbf{No}}(\alpha) = S(\alpha)$.
PROOF: Define $\delta(\text{ordinal number}) =$ Triangle $\$_1$. Define $\mathcal{H}(\text{object}, \subseteq\text{-monotone, function yielding transfinite sequence}) = \langle (\bigcup \mathrm{rng}\, \$_2)^\circ(\mathrm{L}_{\mathrm{L}_{\$_1}} \times \{\mathrm{R}_{\$_1}\} \cup \{\mathrm{L}_{\$_1}\} \times \mathrm{L}_{\mathrm{R}_{\$_1}}), (\bigcup \mathrm{rng}\, \$_2)^\circ(\mathrm{R}_{\mathrm{L}_{\$_1}} \times \{\mathrm{R}_{\$_1}\} \cup \{\mathrm{L}_{\$_1}\} \times \mathrm{R}_{\mathrm{R}_{\$_1}})\rangle$. Consider S_1 being a $\subseteq$-monotone, function yielding transfinite sequence such that $\mathrm{dom}\, S_1 = \mathrm{succ}\, \alpha$ and $\mathrm{sum}_{\mathbf{No}}(\alpha) = S_1(\alpha)$ and for every ordinal number β such that $\beta \in \mathrm{succ}\, \alpha$ there exists a many sorted set S_5 indexed by $\delta(\beta)$ such that $S_1(\beta) = S_5$ and for every object x such that $x \in \delta(\beta)$ holds $S_5(x) = \mathcal{H}(x, S_1\restriction\beta)$. $S\restriction \mathrm{succ}\, \alpha = S_1\restriction \mathrm{succ}\, \alpha$. $\square$

Let x, y be surreal numbers. The functor $x + y$ yielding a set is defined by the term

(Def. 7) $(\mathrm{sum}_{\mathbf{No}}(\mathfrak{born}\, x \oplus \mathfrak{born}\, y))(\langle x, y\rangle)$.

Let X, Y be sets. The functor $X \oplus Y$ yielding a set is defined by

(Def. 8) $o \in it$ iff there exist surreal numbers x, y such that $x \in X$ and $y \in Y$ and $o = x + y$.

Now we state the propositions:

(27) Let us consider a set X. Then $X \oplus \emptyset = \emptyset$.

(28) Let us consider surreal numbers x, y. Then $x + y = \langle (\mathrm{L}_x \oplus \{y\}) \cup (\{x\} \oplus \mathrm{L}_y), (\mathrm{R}_x \oplus \{y\}) \cup (\{x\} \oplus \mathrm{R}_y)\rangle$.

PROOF: Set $B_3 = \mathfrak{born}\, x$. Set $B_5 = \mathfrak{born}\, y$. Set $\alpha = B_3 \oplus B_5$. Consider S being a $\subseteq$-monotone, function yielding transfinite sequence such that $\mathrm{dom}\, S = \mathrm{succ}\, \alpha$ and $\mathrm{sum}_{\mathbf{No}}(\alpha) = S(\alpha)$ and for every ordinal number β such that $\beta \in \mathrm{succ}\, \alpha$ there exists a many sorted set S_5 indexed by $\mathrm{Triangle}\, \beta$ such that $S(\beta) = S_5$ and for every object x such that $x \in \mathrm{Triangle}\, \beta$ holds $S_5(x) = \langle (\bigcup \mathrm{rng}(S{\restriction}\beta))^\circ(\mathrm{L}_{\mathrm{L}_x} \times \{\mathrm{R}_x\} \cup \{\mathrm{L}_x\} \times \mathrm{L}_{\mathrm{R}_x}), (\bigcup \mathrm{rng}(S{\restriction}\beta))^\circ(\mathrm{R}_{\mathrm{L}_x} \times \{\mathrm{R}_x\} \cup \{\mathrm{L}_x\} \times \mathrm{R}_{\mathrm{R}_x})\rangle$. Consider S_3 being a many sorted set indexed by $\mathrm{Triangle}\, \alpha$ such that $S(\alpha) = S_3$ and for every object x such that $x \in \mathrm{Triangle}\, \alpha$ holds $S_3(x) = \langle (\bigcup \mathrm{rng}(S{\restriction}\alpha))^\circ(\mathrm{L}_{(x)_\mathbf{1}} \times \{\mathrm{R}_x\} \cup \{\mathrm{L}_x\} \times \mathrm{L}_{\mathrm{R}_x}), (\bigcup \mathrm{rng}(S{\restriction}\alpha))^\circ(\mathrm{R}_{\mathrm{L}_x} \times \{\mathrm{R}_x\} \cup \{\mathrm{L}_x\} \times \mathrm{R}_{\mathrm{R}_x})\rangle$. Set $U = \bigcup \mathrm{rng}(S{\restriction}\alpha)$. $U^\circ(\mathrm{L}_x \times \{y\}) \subseteq \mathrm{L}_x \oplus \{y\}$. $\mathrm{L}_x \oplus \{y\} \subseteq U^\circ(\mathrm{L}_x \times \{y\})$. $U^\circ(\mathrm{R}_x \times \{y\}) \subseteq \mathrm{R}_x \oplus \{y\}$. $\mathrm{R}_x \oplus \{y\} \subseteq U^\circ(\mathrm{R}_x \times \{y\})$. $U^\circ(\{x\} \times \mathrm{L}_y) \subseteq \{x\} \oplus \mathrm{L}_y$. $\{x\} \oplus \mathrm{L}_y \subseteq U^\circ(\{x\} \times \mathrm{L}_y)$. $U^\circ(\{x\} \times \mathrm{R}_y) \subseteq \{x\} \oplus \mathrm{R}_y$. $\{x\} \oplus \mathrm{R}_y \subseteq U^\circ(\{x\} \times \mathrm{R}_y)$. $\square$

(29) COMMUTATIVITY OF ADDITION FOR SURREAL NUMBER, CONWAY CH. 1 TH. 3(II):
$x + y = y + x$.

PROOF: Define $\mathcal{P}$[ordinal number] $\equiv$ for every surreal numbers x, y such that $\mathfrak{born}\, x \oplus \mathfrak{born}\, y \subseteq \$_1$ holds $x + y = y + x$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. $\square$

Let x, y be surreal numbers. Let us note that the functor $x + y$ is commutative. Now we state the proposition:

(30) Let us consider sets X, Y. Then $X \oplus Y = Y \oplus X$.

Let X, Y be sets. One can verify that the functor $X \oplus Y$ is commutative.

Let us consider x and y. Let us note that $x + y$ is surreal. Let x, y be surreal numbers. The functor $x - y$ yielding a surreal number is defined by the term

(Def. 9) $x + -y$.

Now we state the proposition:

(31) $\mathfrak{born}\, (x + y) \subseteq \mathfrak{born}\, x \oplus \mathfrak{born}\, y$.

Let X, Y be sets. Let us note that $X \oplus Y$ is surreal-membered. Now we state the propositions:

(32) Transitive Law of Addition for Surreal Number, Conway Ch. 1 Th. 5:
$x \leqslant y$ if and only if $x + z \leqslant y + z$.

(33) Let us consider sets X_1, X_2, Y. Then $(X_1 \cup X_2) \oplus Y = (X_1 \oplus Y) \cup (X_2 \oplus Y)$.

(34) Let us consider sets X, Y_1, Y_2. Then $X \oplus (Y_1 \cup Y_2) = (X \oplus Y_1) \cup (X \oplus Y_2)$.

(35) Let us consider sets X_1, X_2, Y_1, Y_2. Suppose $X_1 \lessdot X_2$ and $Y_1 \lessdot Y_2$. Then $X_1 \oplus Y_1 \lessdot X_2 \oplus Y_2$. The theorem is a consequence of (32).

(36) $\{x\} \oplus \{y\} = \{x + y\}$.

(37) Associativity of Addition for Surreal Number, Conway Ch. 1 Th. 3(iii):
$(x + y) + z = x + (y + z)$.
Proof: Define $\mathcal{P}$[ordinal number] $\equiv$ for every surreal numbers x, y, z such that $(\mathfrak{born}\, x \oplus \mathfrak{born}\, y) \oplus \mathfrak{born}\, z \subseteq \$_1$ holds $(x + y) + z = x + (y + z)$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. □

(38) Additive Identity for Surreal Number, Conway Ch. 1 Th. 3(i):
$x + \mathbf{0_{No}} = x$.
Proof: Set $y = \mathbf{0_{No}}$. Define $\mathcal{P}$[ordinal number] $\equiv$ for every surreal number x such that $\mathfrak{born}\, x = \$_1$ holds $x + y = x$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. □

Let us consider x. Let us note that $x + \mathbf{0_{No}}$ reduces to x. Now we state the proposition:

(39) Property of The Aditive Inverse for Surreal Number, Conway Ch. 1 Th. 4(iii):
$x - x \approx \mathbf{0_{No}}$.
Proof: Set $y = \mathbf{0_{No}}$. Define $\mathcal{P}$[ordinal number] $\equiv$ for every surreal number x such that $\mathfrak{born}\, x = \$_1$ holds $x + -x \approx y$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$ by (7), (28), [8, (43)], [9, (1)]. For every ordinal number δ, $\mathcal{P}[\delta]$. □

(40) Conway Ch. 1 Th. 4(i):
$-(x + y) = -x + -y$.
Proof: Define $\mathcal{P}$[ordinal number] $\equiv$ for every surreal numbers x, y such that $\mathfrak{born}\, x \oplus \mathfrak{born}\, y \subseteq \$_1$ holds $-(x + y) = -x + -y$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. □

(41) $x + y \leqslant z$ if and only if $x \leqslant z - y$.
PROOF: If $x+y \leqslant z$, then $x \leqslant z-y$. $x+y \leqslant z+-y+y$. $x+y \leqslant z+(-y+y)$. $y - y \approx \mathbf{0_{No}}$. $z + (-y + y) \leqslant z + \mathbf{0_{No}} = z$. □

(42) $x + y < z$ if and only if $x < z - y$.
PROOF: If $x + y < z$, then $x < z - y$. $z + -y \leqslant x + y + -y$. $z + -y \leqslant x + (y + -y)$. $y - y \approx \mathbf{0_{No}}$. $x + (y + -y) \leqslant x + \mathbf{0_{No}} = x$. □

(43) If $x \leqslant y$ and $z \leqslant t$, then $x + z \leqslant y + t$. The theorem is a consequence of (32).

(44) If $x \leqslant y$ and $z < t$, then $x + z < y + t$. The theorem is a consequence of (42), (39), (32), and (37).

(45) $x < y$ if and only if $\mathbf{0_{No}} < y - x$. The theorem is a consequence of (42).

(46) $x < y$ if and only if $x - y < \mathbf{0_{No}}$. The theorem is a consequence of (41).

(47) If $x - y \approx \mathbf{0_{No}}$, then $x \approx y$. The theorem is a consequence of (39), (37), and (43).

Let x be an object. Assume x is surreal. The functor $-'x$ yielding a surreal number is defined by

(Def. 10) for every surreal number x_1 such that $x_1 = x$ holds $it = -x_1$.

Let a be a surreal number. We identify $-'x$ with $-a$. Let x, y be objects. Assume x is surreal and y is surreal. The functor $x +' y$ yielding a surreal number is defined by

(Def. 11) for every surreal numbers x_1, y_1 such that $x_1 = x$ and $y_1 = y$ holds $it = x_1 + y_1$.

Let a, b be surreal numbers. We identify $x +' y$ with $a + b$.

5. THE PRODUCT OF SUPERREAL NUMBERS

Let α be an ordinal number. The functor $\mathrm{mult}_{\mathbf{No}}(\alpha)$ yielding a many sorted set indexed by Triangle α is defined by

(Def. 12) there exists a $\subseteq$-monotone, function yielding transfinite sequence S such that $\operatorname{dom} S = \operatorname{succ} \alpha$ and $it = S(\alpha)$ and for every ordinal number β such that $\beta \in \operatorname{succ} \alpha$ there exists a many sorted set S_5 indexed by Triangle β such that $S(\beta) = S_5$ and for every object x such that $x \in$ Triangle β holds $S_5(x) = \langle\{(((\bigcup \operatorname{rng}(S\restriction\beta))(\langle x_6, \mathrm{R}_x\rangle) +' (\bigcup \operatorname{rng}(S\restriction\beta))(\langle \mathrm{L}_x, y_4\rangle)) +' -'(\bigcup \operatorname{rng}(S\restriction\beta))(\langle x_6, y_4\rangle)$, where x_6 is an element of $\mathrm{L}_{\mathrm{L}_x}$, y_4 is an element of $\mathrm{L}_{\mathrm{R}_x} : x_6 \in \mathrm{L}_{\mathrm{L}_x}$ and $y_4 \in \mathrm{L}_{\mathrm{R}_x}\} \cup \{(((\bigcup \operatorname{rng}(S\restriction\beta))(\langle x_7, \mathrm{R}_x\rangle) +' (\bigcup \operatorname{rng}(S\restriction\beta))(\langle \mathrm{L}_x, y_5\rangle)) +' -'(\bigcup \operatorname{rng}(S\restriction\beta))(\langle x_7, y_5\rangle)$,where x_7 is an element of $\mathrm{R}_{\mathrm{L}_x}$, y_5 is an element of $\mathrm{R}_{\mathrm{R}_x} : x_7 \in \mathrm{R}_{\mathrm{L}_x}$ and $y_5 \in \mathrm{R}_{\mathrm{R}_x}\}$, $\{(((\bigcup \operatorname{rng}(S\restriction\beta))(\langle x_6, \mathrm{R}_x\rangle) +' (\bigcup \operatorname{rng}(S\restriction\beta))(\langle \mathrm{L}_x, y_5\rangle)) +' -'(\bigcup \operatorname{rng}(S\restriction\beta))(\langle x_6, y_5\rangle)$, where x_6 is

an element of $\mathrm{L}_{\mathrm{L}_x}, y_5$ is an element of $\mathrm{R}_{\mathrm{R}_x} : x_6 \in \mathrm{L}_{\mathrm{L}_x}$ and $y_5 \in \mathrm{R}_{\mathrm{R}_x}\} \cup \{((\bigcup \mathrm{rng}(S\restriction\beta))(\langle x_7, \mathrm{R}_x\rangle) +' (\bigcup \mathrm{rng}(S\restriction\beta))(\langle \mathrm{L}_x, y_4\rangle)) +' -' (\bigcup \mathrm{rng}(S\restriction\beta))(\langle x_7, y_4\rangle)$, where x_7 is an element of $\mathrm{R}_{\mathrm{L}_x}, y_4$ is an element of $\mathrm{L}_{\mathrm{R}_x} : x_7 \in \mathrm{R}_{\mathrm{L}_x}$ and $y_4 \in \mathrm{L}_{\mathrm{R}_x}\}\rangle$.

Let x, y be surreal numbers. The functor $x \cdot y$ yielding a set is defined by the term

(Def. 13) $(\mathrm{mult}_{\mathbf{No}}(\mathfrak{born}\, x \oplus \mathfrak{born}\, y))(\langle x, y\rangle)$.

Now we state the proposition:

(48) Let us consider a $\subseteq$-monotone, function yielding transfinite sequence S. Suppose for every ordinal number β such that $\beta \in \mathrm{dom}\, S$ there exists a many sorted set S_5 indexed by $\mathrm{Triangle}\,\beta$ such that $S(\beta) = S_5$ and for every object x such that $x \in \mathrm{Triangle}\,\beta$ holds $S_5(x) = \langle\{((\bigcup \mathrm{rng}(S\restriction\beta))(\langle x_6, \mathrm{R}_x\rangle) +' (\bigcup \mathrm{rng}(S\restriction\beta))(\langle \mathrm{L}_x, y_4\rangle)) +' -' (\bigcup \mathrm{rng}(S\restriction\beta))(\langle x_6, y_4\rangle)$, where x_6 is an element of $\mathrm{L}_{\mathrm{L}_x}, y_4$ is an element of $\mathrm{L}_{\mathrm{R}_x} : x_6 \in \mathrm{L}_{\mathrm{L}_x}$ and $y_4 \in \mathrm{L}_{\mathrm{R}_x}\} \cup \{((\bigcup \mathrm{rng}(S\restriction\beta))(\langle x_7, \mathrm{R}_x\rangle) +' (\bigcup \mathrm{rng}(S\restriction\beta))(\langle \mathrm{L}_x, y_5\rangle)) +' -' (\bigcup \mathrm{rng}(S\restriction\beta))(\langle x_7, y_5\rangle)$, where x_7 is an element of $\mathrm{R}_{\mathrm{L}_x}, y_5$ is an element of $\mathrm{R}_{\mathrm{R}_x} : x_7 \in \mathrm{R}_{\mathrm{L}_x}$ and $y_5 \in \mathrm{R}_{\mathrm{R}_x}\}, \{((\bigcup \mathrm{rng}(S\restriction\beta))(\langle x_6, \mathrm{R}_x\rangle) +' (\bigcup \mathrm{rng}(S\restriction\beta))(\langle \mathrm{L}_x, y_5\rangle)) +' -' (\bigcup \mathrm{rng}(S\restriction\beta))(\langle x_6, y_5\rangle)$, where x_6 is an element of $\mathrm{L}_{\mathrm{L}_x}, y_5$ is an element of $\mathrm{R}_{\mathrm{R}_x} : x_6 \in \mathrm{L}_{\mathrm{L}_x}$ and $y_5 \in \mathrm{R}_{\mathrm{R}_x}\} \cup \{((\bigcup \mathrm{rng}(S\restriction\beta))(\langle x_7, \mathrm{R}_x\rangle) +' (\bigcup \mathrm{rng}(S\restriction\beta))(\langle \mathrm{L}_x, y_4\rangle)) +' -' (\bigcup \mathrm{rng}(S\restriction\beta))(\langle x_7, y_4\rangle)$, where x_7 is an element of $\mathrm{R}_{\mathrm{L}_x}, y_4$ is an element of $\mathrm{L}_{\mathrm{R}_x} : x_7 \in \mathrm{R}_{\mathrm{L}_x}$ and $y_4 \in \mathrm{L}_{\mathrm{R}_x}\}\rangle$. Let us consider an ordinal number α. If $\alpha \in \mathrm{dom}\, S$, then $\mathrm{mult}_{\mathbf{No}}(\alpha) = S(\alpha)$.

PROOF: Define $\delta(\text{ordinal number}) = \mathrm{Triangle}\,\$_1$. Define $\mathcal{H}(\text{object}, \subseteq\text{-monotone, function yielding transfinite sequence}) = \langle\{((\bigcup \mathrm{rng}\,\$_2)(\langle x_6, \mathrm{R}_{\$_1}\rangle) +' (\bigcup \mathrm{rng}\,\$_2)(\langle \mathrm{L}_{\$_1}, y_4\rangle)) +' -' (\bigcup \mathrm{rng}\,\$_2)(\langle x_6, y_4\rangle)$, where x_6 is an element of $\mathrm{L}_{\mathrm{L}_{\$_1}}, y_4$ is an element of $\mathrm{L}_{\mathrm{R}_{\$_1}} : x_6 \in \mathrm{L}_{\mathrm{L}_{\$_1}}$ and $y_4 \in \mathrm{L}_{\mathrm{R}_{\$_1}}\} \cup \{((\bigcup \mathrm{rng}\,\$_2)(\langle x_7, \mathrm{R}_{\$_1}\rangle) +' (\bigcup \mathrm{rng}\,\$_2)(\langle \mathrm{L}_{\$_1}, y_5\rangle)) +' -' (\bigcup \mathrm{rng}\,\$_2)(\langle x_7, y_5\rangle)$, where x_7 is an element of $\mathrm{R}_{\mathrm{L}_{\$_1}}, y_5$ is an element of $\mathrm{R}_{\mathrm{R}_{\$_1}} : x_7 \in \mathrm{R}_{\mathrm{L}_{\$_1}}$ and $y_5 \in \mathrm{R}_{\mathrm{R}_{\$_1}}\}, \{((\bigcup \mathrm{rng}\,\$_2)(\langle x_6, \mathrm{R}_{\$_1}\rangle) +' (\bigcup \mathrm{rng}\,\$_2)(\langle \mathrm{L}_{\$_1}, y_5\rangle)) +' -' (\bigcup \mathrm{rng}\,\$_2)(\langle x_6, y_5\rangle)$, where x_6 is an element of $\mathrm{L}_{\mathrm{L}_{\$_1}}, y_5$ is an element of $\mathrm{R}_{\mathrm{R}_{\$_1}} : x_6 \in \mathrm{L}_{\mathrm{L}_{\$_1}}$ and $y_5 \in \mathrm{R}_{\mathrm{R}_{\$_1}}\} \cup \{((\bigcup \mathrm{rng}\,\$_2)(\langle x_7, \mathrm{R}_{\$_1}\rangle) +' (\bigcup \mathrm{rng}\,\$_2)(\langle \mathrm{L}_{\$_1}, y_4\rangle)) +' -' (\bigcup \mathrm{rng}\,\$_2)(\langle x_7, y_4\rangle)$, where x_7 is an element of $\mathrm{R}_{\mathrm{L}_{\$_1}}, y_4$ is an element of $\mathrm{L}_{\mathrm{R}_{\$_1}} : x_7 \in \mathrm{R}_{\mathrm{L}_{\$_1}}$ and $y_4 \in \mathrm{L}_{\mathrm{R}_{\$_1}}\}\rangle$. Consider S_1 being a $\subseteq$-monotone, function yielding transfinite sequence such that $\mathrm{dom}\, S_1 = \mathrm{succ}\,\alpha$ and $\mathrm{mult}_{\mathbf{No}}(\alpha) = S_1(\alpha)$ and for every ordinal number β such that $\beta \in \mathrm{succ}\,\alpha$ there exists a many sorted set S_5 indexed by $\delta(\beta)$ such that $S_1(\beta) = S_5$ and for every object x such that $x \in \delta(\beta)$ holds $S_5(x) = \mathcal{H}(x, S_1\restriction\beta)$. $S\restriction\mathrm{succ}\,\alpha = S_1\restriction\mathrm{succ}\,\alpha$. □

Let x, y be surreal numbers and X, Y be sets. The functor $\mathrm{comp}(X, x, y, Y)$ yielding a set is defined by

(Def. 14) $o \in it$ iff there exist surreal numbers x_1, y_1 such that $o = (x_1 \cdot y +' x \cdot y_1) +' -' x_1 \cdot y_1$ and $x_1 \in X$ and $y_1 \in Y$.

Now we state the propositions:

(49) Let us consider a set X. Then $\mathrm{comp}(X, x, y, \emptyset) = \emptyset$.

(50) Let us consider surreal numbers x, y. Then $x \cdot y = \langle\, \mathrm{comp}(\mathrm{L}_x, x, y, \mathrm{L}_y) \cup \mathrm{comp}(\mathrm{R}_x, x, y, \mathrm{R}_y),\ \mathrm{comp}(\mathrm{L}_x, x, y, \mathrm{R}_y) \cup \mathrm{comp}(\mathrm{R}_x, x, y, \mathrm{L}_y) \rangle$.

PROOF: Set $B_3 = \mathfrak{b}\mathrm{orn}\, x$. Set $B_5 = \mathfrak{b}\mathrm{orn}\, y$. Set $\alpha = B_3 \oplus B_5$. Define $\mathcal{H}$(object, $\subseteq$-monotone, function yielding transfinite sequence) = $\langle \{(((\bigcup \mathrm{rng}\, \$_2)(\langle x_6,\ \mathrm{R}_{\$_1} \rangle) +' (\bigcup \mathrm{rng}\, \$_2)(\langle \mathrm{L}_{\$_1},\ y_4 \rangle)) +' -' (\bigcup \mathrm{rng}\, \$_2)(\langle x_6,\ y_4 \rangle),$ where x_6 is an element of $\mathrm{L}_{\mathrm{L}_{\$_1}}, y_4$ is an element of $\mathrm{L}_{\mathrm{R}_{\$_1}} : x_6 \in \mathrm{L}_{\mathrm{L}_{\$_1}}$ and $y_4 \in \mathrm{L}_{\mathrm{R}_{\$_1}} \} \cup \{(((\bigcup \mathrm{rng}\, \$_2)(\langle x_7,\ \mathrm{R}_{\$_1} \rangle) +' (\bigcup \mathrm{rng}\, \$_2)(\langle \mathrm{L}_{\$_1},\ y_5 \rangle)) +' -' (\bigcup \mathrm{rng}\, \$_2)(\langle x_7,\ y_5 \rangle),$ where x_7 is an element of $\mathrm{R}_{\mathrm{L}_{\$_1}}, y_5$ is an element of $\mathrm{R}_{\mathrm{R}_{\$_1}} : x_7 \in \mathrm{R}_{\mathrm{L}_{\$_1}}$ and $y_5 \in \mathrm{R}_{\mathrm{R}_{\$_1}} \}, \{((\bigcup \mathrm{rng}\, \$_2)(\langle x_6,\ \mathrm{R}_{\$_1} \rangle) +' (\bigcup \mathrm{rng}\, \$_2)(\langle \mathrm{L}_{\$_1},\ y_5 \rangle)) +' -' (\bigcup \mathrm{rng}\, \$_2)(\langle x_6,\ y_5 \rangle),$ where x_6 is an element of $\mathrm{L}_{\mathrm{L}_{\$_1}}, y_5$ is an element of $\mathrm{R}_{\mathrm{R}_{\$_1}} : x_6 \in \mathrm{L}_{\mathrm{L}_{\$_1}}$ and $y_5 \in \mathrm{R}_{\mathrm{R}_{\$_1}} \} \cup \{(((\bigcup \mathrm{rng}\, \$_2)(\langle x_7,\ \mathrm{R}_{\$_1} \rangle) +' (\bigcup \mathrm{rng}\, \$_2)(\langle \mathrm{L}_{\$_1},\ y_4 \rangle)) +' -' (\bigcup \mathrm{rng}\, \$_2)(\langle x_7,\ y_4 \rangle),$ where x_7 is an element of $\mathrm{R}_{\mathrm{L}_{\$_1}}, y_4$ is an element of $\mathrm{L}_{\mathrm{R}_{\$_1}} : x_7 \in \mathrm{R}_{\mathrm{L}_{\$_1}}$ and $y_4 \in \mathrm{L}_{\mathrm{R}_{\$_1}} \} \rangle$. Consider S being a $\subseteq$-monotone, function yielding transfinite sequence such that $\mathrm{dom}\, S = \mathrm{succ}\, \alpha$ and $\mathrm{mult}_{\mathbf{No}}(\alpha) = S(\alpha)$ and for every ordinal number β such that $\beta \in \mathrm{succ}\, \alpha$ there exists a many sorted set S_5 indexed by $\mathrm{Triangle}\, \beta$ such that $S(\beta) = S_5$ and for every object x such that $x \in \mathrm{Triangle}\, \beta$ holds $S_5(x) = \mathcal{H}(x, S{\restriction}\beta)$. Consider S_3 being a many sorted set indexed by $\mathrm{Triangle}\, \alpha$ such that $S(\alpha) = S_3$ and for every object x such that $x \in \mathrm{Triangle}\, \alpha$ holds $S_3(x) = \mathcal{H}(x, S{\restriction}\alpha)$. Set $U = \bigcup \mathrm{rng}(S{\restriction}\alpha)$. For every surreal-membered sets X, Y such that $X \subseteq \mathrm{L}_x \cup \mathrm{R}_x$ and $Y \subseteq \mathrm{L}_y \cup \mathrm{R}_y$ holds $\{(U(\langle x_6,\ y \rangle) +' U(\langle x,\ y_4 \rangle)) +' -' U(\langle x_6,\ y_4 \rangle),$ where x_6 is an element of X, y_4 is an element of $Y : x_6 \in X$ and $y_4 \in Y\} = \mathrm{comp}(X, x, y, Y)$. $\square$

(51) (i) for every x and y, $x \cdot y$ is a surreal number, and

(ii) for every x and y, $x \cdot y = y \cdot x$, and

(iii) for every surreal numbers x_1, x_2, y, x_4, x_5 such that $x_1 \approx x_2$ and $x_4 = x_1 \cdot y$ and $x_5 = x_2 \cdot y$ holds $x_4 \approx x_5$, and

(iv) for every surreal numbers x_1, x_2, y_1, y_2, x_{12}, x_{21}, x_{11}, x_{22} such that $x_{11} = x_1 \cdot y_1$ and $x_{12} = x_1 \cdot y_2$ and $x_{21} = x_2 \cdot y_1$ and $x_{22} = x_2 \cdot y_2$ and $x_1 < x_2$ and $y_1 < y_2$ holds $x_{12} + x_{21} < x_{11} + x_{22}$.

PROOF: Define $\mathcal{P}$[ordinal number, surreal number, surreal number] $\equiv$ if $\mathfrak{b}\mathrm{orn}\, \$_2 \oplus \mathfrak{b}\mathrm{orn}\, \$_3 \subseteq \$_1$, then $\$_2 \cdot \$_3 = \$_3 \cdot \$_2$. Define $\mathcal{S}$[ordinal number, surreal number, surreal number] $\equiv$ if $\mathfrak{b}\mathrm{orn}\, \$_2 \oplus \mathfrak{b}\mathrm{orn}\, \$_3 \subseteq \$_1$, then $\$_2 \cdot \$_3$ is a surreal number. Define $\mathcal{T}$[ordinal number, surreal number, surreal number, surreal number] $\equiv$ for every surreal numbers x_4, x_5 such that $\mathfrak{b}\mathrm{orn}\, \$_2 \oplus \mathfrak{b}\mathrm{orn}\, \$_4 \subseteq \$_1$

and $\mathfrak{born}\,\$_3 \oplus \mathfrak{born}\,\$_4 \subseteq \$_1$ and $\$_2 \approx \$_3$ and $x_4 = \$_2 \cdot \$_4$ and $x_5 = \$_3 \cdot \$_4$ holds $x_4 \approx x_5$. Define $\mathcal{V}$[ordinal number, surreal number, surreal number, surreal number, surreal number] $\equiv$ for every surreal numbers x_{12}, x_{21}, x_{11}, x_{22} such that $\mathfrak{born}\,\$_2 \oplus \mathfrak{born}\,\$_4 \subseteq \$_1$ and $\mathfrak{born}\,\$_3 \oplus \mathfrak{born}\,\$_4 \subseteq \$_1$ and $\mathfrak{born}\,\$_2 \oplus \mathfrak{born}\,\$_5 \subseteq \$_1$ and $\mathfrak{born}\,\$_3 \oplus \mathfrak{born}\,\$_5 \subseteq \$_1$ and $x_{11} = \$_2 \cdot \$_4$ and $x_{12} = \$_2 \cdot \$_5$ and $x_{21} = \$_3 \cdot \$_4$ and $x_{22} = \$_3 \cdot \$_5$ and $\$_2 < \$_3 < \$_5$ holds $x_{12} + x_{21} < x_{11} + x_{22}$. Define $\mathcal{F}$[ordinal number] $\equiv$ for every x and y, $\mathcal{P}[\$_1, x, y]$. Define $\mathcal{G}$[ordinal number] $\equiv$ for every x and y, $\mathcal{S}[\$_1, x, y]$. Define $\mathcal{H}$[ordinal number] $\equiv$ for every surreal numbers x_1, x_2, y, $\mathcal{T}[\$_1, x_1, x_2, y]$. Define $\mathcal{I}$[ordinal number] $\equiv$ for every surreal numbers x_1, x_2, y_1, y_2, $\mathcal{V}[\$_1, x_1, x_2, y_1, y_2]$. Define θ[ordinal number] $\equiv \mathcal{F}[\$_1]$ and $\mathcal{G}[\$_1]$ and $\mathcal{H}[\$_1]$ and $\mathcal{I}[\$_1]$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\theta[\gamma]$ holds $\theta[\delta]$. For every ordinal number E, $\theta[E]$. For every surreal numbers x_1, x_2, y, x_4, x_5 such that $x_1 \approx x_2$ and $x_4 = x_1 \cdot y$ and $x_5 = x_2 \cdot y$ holds $x_4 \approx x_5$. □

Let a, b be surreal numbers. Observe that $a \cdot b$ is surreal. Let a, b be surreal numbers. One can check that the functor $a \cdot b$ is commutative. Let x, y be surreal numbers and X, Y be sets. Observe that $\mathrm{comp}(X, x, y, Y)$ is surreal-membered. Let us observe that the functor $\mathrm{comp}(X, x, y, Y)$ is defined by

(Def. 15) $o \in it$ iff there exist surreal numbers x_1, y_1 such that $o = x_1 \cdot y + x \cdot y_1 - x_1 \cdot y_1$ and $x_1 \in X$ and $y_1 \in Y$.

Now we state the propositions:

(52) $\mathrm{comp}(\{z\}, x, y, \{t\}) = \{z \cdot y + x \cdot t - z \cdot t\}$.

(53) Let us consider sets X, Y. Then $\mathrm{comp}(X, x, y, Y) = \mathrm{comp}(Y, y, x, X)$.

(54) Conway Ch. 1 Th. 8(i):
Let us consider surreal numbers x_1, x_2, y. If $x_1 \approx x_2$, then $x_1 \cdot y \approx x_2 \cdot y$.

(55) Conway Ch. 1 Th. 8(iii):
Let us consider surreal numbers x_1, x_2, y_1, y_2. Suppose $x_1 < x_2$ and $y_1 < y_2$. Then $x_1 \cdot y_2 + x_2 \cdot y_1 < x_1 \cdot y_1 + x_2 \cdot y_2$.

(56) Conway Ch. 1 Th. 7(i):
$x \cdot (\mathbf{0_{No}}) = \mathbf{0_{No}}$. The theorem is a consequence of (49) and (50).

(57) Multiplicative Identity for Surreal Number, Conway Ch. 1 Th. 7(ii):
$x \cdot (\mathbf{1_{No}}) = x$.
Proof: Define $\mathcal{P}$[ordinal number] $\equiv$ for every x such that $\mathfrak{born}\,x \subseteq \$_1$ holds $x \cdot (\mathbf{1_{No}}) = x$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. □

Let us consider x. Observe that $x\cdot(\mathbf{0_{No}})$ reduces to $\mathbf{0_{No}}$ and $x\cdot(\mathbf{1_{No}})$ reduces to x. Now we state the proposition:

(58) CONWAY CH. 1 TH. 7(IV):

(i) $x \cdot (-y) = -x \cdot y$, and

(ii) $(-x) \cdot y = -x \cdot y$, and

(iii) $(-x) \cdot (-y) = x \cdot y$.

Let us consider sets X, Y_1, Y_2. Now we state the propositions:

(59) If $Y_1 \subseteq Y_2$, then $\operatorname{comp}(X, x, y, Y_1) \subseteq \operatorname{comp}(X, x, y, Y_2)$.

(60) $\operatorname{comp}(X, x, y, Y_1 \cup Y_2) = \operatorname{comp}(X, x, y, Y_1) \cup \operatorname{comp}(X, x, y, Y_2)$. The theorem is a consequence of (59).

(61) Let us consider sets X, Y. Suppose for every x such that $x \in X$ there exists y such that $y \in Y$ and $x \approx y$. Then $X \lessdot Y$.

Let us consider sets X_1, X_2. Now we state the propositions:

(62) If $X_1 \lessdot X_2$, then $\ominus X_1 \lessdot \ominus X_2$. The theorem is a consequence of (10).

(63) $\ominus(X_1 \oplus X_2) = \ominus X_1 \oplus \ominus X_2$. The theorem is a consequence of (40).

(64) Let us consider a surreal-membered set X. Then $X \oplus \{\mathbf{0_{No}}\} = X$.

(65) If $x \approx y$, then $-x \approx -y$.

(66) Let us consider surreal numbers x_1, x_2, y_1, y_2. If $x_1 \approx x_2$ and $y_1 \approx y_2$, then $x_1 + y_1 \approx x_2 + y_2$.

(67) DISTRIBUTIVITY OF MULTIPLICATION OVER ADDITION FOR SURREAL NUMBERS, CONWAY CH. 1 TH. 7(V):
$x \cdot (y + z) \approx x \cdot y + x \cdot z$.
PROOF: Define $\mathcal{P}$[ordinal number] $\equiv$ for every surreal numbers x, y, z such that $(\operatorname{\mathfrak{born}} x \oplus \operatorname{\mathfrak{born}} y) \oplus \operatorname{\mathfrak{born}} z \subseteq \$_1$ holds $x \cdot (y + z) \approx x \cdot y + x \cdot z$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. $\square$

(68) Let us consider sets X_1, X_2, Y. Then $\operatorname{comp}(X_1 \cup X_2, x, y, Y) = \operatorname{comp}(X_1, x, y, Y) \cup \operatorname{comp}(X_2, x, y, Y)$. The theorem is a consequence of (53) and (60).

(69) ASSOCIATIVITY OF MULTIPLICATION FOR SURREAL NUMBERS, CONWAY CH. 1 TH. 7(VI):
$(x \cdot y) \cdot z \approx x \cdot (y \cdot z)$.
PROOF: Define $\mathcal{P}$[ordinal number] $\equiv$ for every surreal numbers x, y, z such that $(\operatorname{\mathfrak{born}} x \oplus \operatorname{\mathfrak{born}} y) \oplus \operatorname{\mathfrak{born}} z \subseteq \$_1$ holds $(x \cdot y) \cdot z \approx x \cdot (y \cdot z)$. For every ordinal number δ such that for every ordinal number γ such that $\gamma \in \delta$ holds $\mathcal{P}[\gamma]$ holds $\mathcal{P}[\delta]$. For every ordinal number δ, $\mathcal{P}[\delta]$. $\square$

(70) If $\mathbf{0_{No}} < x$ and $y < z$, then $y \cdot x < z \cdot x$. The theorem is a consequence of (51).

(71) If $x < \mathbf{0_{No}}$ and $y < z$, then $z \cdot x < y \cdot x$. The theorem is a consequence of (51).

(72) Conway Ch. 1 Th. 9:
$\mathbf{0_{No}} < x \cdot y$ if and only if $x < \mathbf{0_{No}}$ and $y < \mathbf{0_{No}}$ or $\mathbf{0_{No}} < x$ and $\mathbf{0_{No}} < y$. The theorem is a consequence of (51), (10), (58), and (23).

(73) If $\mathbf{0_{No}} < z$ and $x \cdot z < y \cdot z$, then $x < y$. The theorem is a consequence of (51) and (70).

(74) $x \cdot y < \mathbf{0_{No}}$ if and only if $x < \mathbf{0_{No}} < y$ or $\mathbf{0_{No}} < x$ and $y < \mathbf{0_{No}}$. The theorem is a consequence of (23), (10), (58), and (72).

(75) If $\mathbf{0_{No}} \leqslant x$ and $y \leqslant z$, then $y \cdot x \leqslant z \cdot x$. The theorem is a consequence of (51) and (70).

(76) $(x+y)\cdot(x+y) \approx x\cdot x+y\cdot y+(x\cdot y+y\cdot x)$. The theorem is a consequence of (67), (43), and (37).

(77) $x \cdot y \approx \mathbf{0_{No}}$ if and only if $x \approx \mathbf{0_{No}}$ or $y \approx \mathbf{0_{No}}$.

References

[1] Maan T. Alabdullah, Essam El-Seidy, and Neveen S. Morcos. On numbers and games. *International Journal of Scientific and Engineering Research*, 11:510–517, February 2020.

[2] Norman L. Alling. *Foundations of Analysis Over Surreal Number Fields*. Number 141 in Annals of Discrete Mathematics. North-Holland, 1987. ISBN 9780444702265.

[3] Heinz Bachmann. *Transfinite Zahlen*. Ergebnisse der Mathematik und ihrer Grenzgebiete, (1). Springer, Berlin, 2., neubearb. aufl. edition, 1967.

[4] Chad E. Brown and Karol Pąk. A tale of two set theories. In Cezary Kaliszyk, Edwin Brady, Andrea Kohlhase, and Claudio Sacerdoti Coen, editors, *Intelligent Computer Mathematics – 12th International Conference, CICM 2019, CIIRC, Prague, Czech Republic, July 8-12, 2019, Proceedings*, volume 11617 of *Lecture Notes in Computer Science*, pages 44–60. Springer, 2019. doi:10.1007/978-3-030-23250-4_4.

[5] John Horton Conway. *On Numbers and Games*. A K Peters Ltd., Natick, MA, second edition, 2001. ISBN 1-56881-127-6.

[6] Oliver Deiser. *Einführung in die Mengenlehre: die Mengenlehre Georg Cantors und ihre Axiomatisierung durch Ernst Zermelo*. Springer, Berlin, 2., verb. und erw. aufl. edition, 2004. ISBN 3-540-20401-6.

[7] Sebastian Koch. Natural addition of ordinals. *Formalized Mathematics*, 27(**2**):139–152, 2019. doi:10.2478/forma-2019-0015.

[8] Karol Pąk. Conway numbers – formal introduction. *Formalized Mathematics*, 31(1): 193–203, 2023. doi:10.2478/forma-2023-0018.

[9] Karol Pąk. Integration of game theoretic and tree theoretic approaches to Conway numbers. *Formalized Mathematics*, 31(1):205–213, 2023. doi:10.2478/forma-2023-0019.

[10] Dierk Schleicher and Michael Stoll. An introduction to Conway's games and numbers. *Moscow Mathematical Journal*, 6:359–388, 2006. doi:10.17323/1609-4514-2006-6-2-359-388.

Accepted December 12, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 229–275, 2023
DOI: 10.2478/forma-2023-0021
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part XI[1]

Adam Naumowicz
Faculty of Computer Science
University of Białystok
Poland

Summary. In this paper we present the Mizar formalization of the 36th problem from W. Sierpiński's book "250 Problems in Elementary Number Theory" [10].

MSC: 11A99 97F30 68V20

Keywords: number theory; base 10 representations; sums of digits; divisibility

MML identifier: NUMBER11, version: 8.1.14 5.76.1456

Introduction

This article demonstrates the solution to the 36th problem from W. Sierpiński's book "250 Problems in Elementary Number Theory" [10, 3]. To that end, for every positive integer $s \leqslant 25$ and for $s = 100$ we provide the least positive integer with the sum of its digits (in decimal system) equal to s, which is divisible by s. We make an extensive use of the general notion of natural number representations previously developed in [8] according to [9].

The preliminary part of this article contains a few auxiliary lemmas relating numbers and sequences of digits in a given numeric system. Most notably, we prove here the basic property that allows to determine the order between two numbers based on the digits representing them.

[1]The Mizar processing has been performed using the infrastructure of the University of Bialystok High Performance Computing Center.

The formalization of the main problem, using the Mizar system [1], [2], is split into theorems corresponding to every positive integer $s \leqslant 25$ and a specific one for $s = 100$. The first ten cases for $s < 10$ are obviously justified by taking the numbers s themselves. Other cases require studying successive multiples of s and the sums of digits of their decimal representations. The last case calls for a number with decimal digits composed of a leading 1, followed by a sequence of eleven 9s, and two trailing 0s. With such a large number evaluating all successive multiples of 100 would be impractical. Therefore, the final proof is of a general nature taking into account the properties of sequences of digits.

The work presented in this article is intended to extend the original dataset of Mizar elementary number theory formalizations presented in [6] and based on the Mizar article [7]. Other similar elementary facts concerning number divisibility can also be found, e.g., in articles [5, 4].

1. Preliminaries

Let n be a natural number. One can check that $\langle n \rangle$ is $\mathbb{N}$-valued. Let n_1, n_2 be natural numbers. One can verify that $\langle n_1, n_2 \rangle$ is $\mathbb{N}$-valued. Let n_1, n_2, n_3 be natural numbers. Note that $\langle n_1, n_2, n_3 \rangle$ is $\mathbb{N}$-valued. Let n_1, n_2, n_3, n_4 be natural numbers. One can check that $\langle n_1, n_2, n_3, n_4 \rangle$ is $\mathbb{N}$-valued. Now we state the proposition:

(1) Let us consider a natural number b, and a finite 0-sequence E of $\mathbb{N}$. If $E = \emptyset$, then $\operatorname{value}(E, b) = 0$.

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

(2) $\operatorname{value}(\langle n \rangle, b) = n$.

(3) If $n < b > 1$, then $\operatorname{digits}(n, b) = \langle n \rangle$. The theorem is a consequence of (2).

(4) Let us consider a natural number b. If $b > 1$, then $\operatorname{digits}(\operatorname{value}(\langle 0 \rangle, b), b) = \langle 0 \rangle$. The theorem is a consequence of (2).

(5) Let us consider a natural number b. Suppose $b > 1$. Let us consider a $\mathbb{N}$-valued finite 0-sequence s. Suppose $\operatorname{len} s > 0$ and $s(\operatorname{len} s - 1) \neq 0$ and for every natural number i such that $i \in \operatorname{dom} s$ holds $s(i) < b$. Then $\operatorname{digits}(\operatorname{value}(s, b), b) = s$.

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

(6) If $n < b > 1$, then $\sum \operatorname{digits}(n, b) = n$. The theorem is a consequence of (3).

(7) If $b > 1$, then $\operatorname{value}(n \longmapsto b -' 1, b) = b^n - 1$.

PROOF: Set $d = n \longmapsto b -' 1$. Set $g = (b -' 1) \cdot (b^{\kappa})_{\kappa \in \mathbb{N}}$. Set $d' = g \restriction n$. For every natural number i such that $i \in \operatorname{dom} d'$ holds $d'(i) = d(i) \cdot b^i$. $\operatorname{rng} d' \subseteq \mathbb{N}$. $\square$

(8) Let us consider a natural number b. Suppose $b > 1$. Let us consider a $\mathbb{N}$-valued finite 0-sequence s. Suppose $\operatorname{len} s > 0$ and for every natural number i such that $i \in \operatorname{dom} s$ holds $s(i) < b$. Then $s(\operatorname{len} s - 1) \cdot b^{\operatorname{len} s -' 1} \leqslant \operatorname{value}(s, b) < b^{\operatorname{len} s}$. The theorem is a consequence of (7).

(9) Let us consider natural numbers n, b. If $b > 1$, then $n < b^{\operatorname{len} \operatorname{digits}(n,b)}$. The theorem is a consequence of (8).

(10) Let us consider natural numbers n, m, b. If $n \neq 0$ and $b > 1$ and $m < \operatorname{len} \operatorname{digits}(n, b)$, then $n \geqslant b^m$. The theorem is a consequence of (8).

(11) Let us consider finite 0-sequences d_1, d_2 of $\mathbb{N}$, and a natural number b. Suppose $b > 1$ and $\operatorname{dom} d_1 = \operatorname{dom} d_2$ and for every natural number n such that $n \in \operatorname{dom} d_1$ holds $d_1(n) \leqslant d_2(n)$. Then $\operatorname{value}(d_1, b) \leqslant \operatorname{value}(d_2, b)$.

(12) Let us consider natural numbers m, n, b. Suppose $b > 1$. Then $m < n$ if and only if $\operatorname{len} \operatorname{digits}(m, b) < \operatorname{len} \operatorname{digits}(n, b)$ or $\operatorname{len} \operatorname{digits}(m, b) = \operatorname{len} \operatorname{digits}(n, b)$ and there exists a natural number i such that $i < \operatorname{len} \operatorname{digits}(m, b)$ and $(\operatorname{digits}(m, b))(i) < (\operatorname{digits}(n, b))(i)$ and for every natural number j such that $j < \operatorname{len} \operatorname{digits}(m, b)$ and $(\operatorname{digits}(m, b))(j) \neq (\operatorname{digits}(n, b))(j)$ holds $i \geqslant j$.

PROOF: Set $d_3 = \operatorname{digits}(m, b)$. Set $d_4 = \operatorname{digits}(n, b)$. Consider v_1 being a finite 0-sequence of $\mathbb{N}$ such that $\operatorname{dom} v_1 = \operatorname{dom} d_3$ and for every natural number i such that $i \in \operatorname{dom} v_1$ holds $v_1(i) = d_3(i) \cdot b^i$ and $\operatorname{value}(\operatorname{digits}(m, b), b) = \sum v_1$. Consider v_0 being a finite 0-sequence of $\mathbb{N}$ such that $\operatorname{dom} v_0 = \operatorname{dom} d_4$ and for every natural number i such that $i \in \operatorname{dom} v_0$ holds $v_0(i) = d_4(i) \cdot b^i$ and $\operatorname{value}(\operatorname{digits}(n, b), b) = \sum v_0$.

If $m < n$, then $\operatorname{len} d_3 < \operatorname{len} d_4$ or $\operatorname{len} d_3 = \operatorname{len} d_4$ and there exists a natural number i such that $i < \operatorname{len} d_3$ and $d_3(i) < d_4(i)$ and for every natural number j such that $j < \operatorname{len} d_3$ and $d_3(j) \neq d_4(j)$ holds $i \geqslant j$. If $\operatorname{len} d_3 < \operatorname{len} d_4$ or $\operatorname{len} d_3 = \operatorname{len} d_4$ and there exists a natural number i such that $i < \operatorname{len} d_3$ and $d_3(i) < d_4(i)$ and for every natural number j such that $j < \operatorname{len} d_3$ and $d_3(j) \neq d_4(j)$ holds $i \geqslant j$, then $m < n$. $\square$

(13) Let us consider a natural number n.
Then $100 \mid n$ if and only if $(\operatorname{digits}(n, 10))(0) = 0$ and $(\operatorname{digits}(n, 10))(1) = 0$.
PROOF: If $100 \mid n$, then $(\operatorname{digits}(n, 10))(0) = 0$ and $(\operatorname{digits}(n, 10))(1) = 0$. Consider d' being a finite 0-sequence of $\mathbb{N}$ such that $\operatorname{dom} d' = \operatorname{dom}(\operatorname{digits}(n, 10))$ and for every natural number i such that $i \in \operatorname{dom} d'$ holds $d'(i) = (\operatorname{digits}(n, 10))(i) \cdot 10^i$ and $\operatorname{value}(\operatorname{digits}(n, 10), 10) = \sum d'$. $\square$

(14) Let us consider a finite 0-sequence f. If $\operatorname{len} f \geqslant 2$, then $f \restriction 2 = \langle f(0), f(1) \rangle$.

2. Problem 36 for $s < 10$

Let n, s be natural numbers. We say that n is the solution to Sierpiński's problem 36 for s if and only if

(Def. 1) $\sum \mathrm{digits}(n, 10) = s$ and $s \mid n$ and for every natural number m such that $\sum \mathrm{digits}(m, 10) = s$ and $s \mid m$ holds $n \leqslant m$.

Now we state the proposition:

(15) Let us consider a natural number n. If $n < 10$, then n is the solution to Sierpiński's problem 36 for n. The theorem is a consequence of (3).

3. Problem 36 for $s = 10$

Now we state the propositions:

(16) $\mathrm{digits}(10, 10) = \langle 0, 1 \rangle$.

(17) $\sum \mathrm{digits}(10, 10) = 1$. The theorem is a consequence of (16).

(18) $\mathrm{digits}(20, 10) = \langle 0, 2 \rangle$.

(19) $\sum \mathrm{digits}(20, 10) = 2$. The theorem is a consequence of (18).

(20) $\mathrm{digits}(30, 10) = \langle 0, 3 \rangle$.

(21) $\sum \mathrm{digits}(30, 10) = 3$. The theorem is a consequence of (20).

(22) $\mathrm{digits}(40, 10) = \langle 0, 4 \rangle$.

(23) $\sum \mathrm{digits}(40, 10) = 4$. The theorem is a consequence of (22).

(24) $\mathrm{digits}(50, 10) = \langle 0, 5 \rangle$.

(25) $\sum \mathrm{digits}(50, 10) = 5$. The theorem is a consequence of (24).

(26) $\mathrm{digits}(60, 10) = \langle 0, 6 \rangle$.

(27) $\sum \mathrm{digits}(60, 10) = 6$. The theorem is a consequence of (26).

(28) $\mathrm{digits}(70, 10) = \langle 0, 7 \rangle$.

(29) $\sum \mathrm{digits}(70, 10) = 7$. The theorem is a consequence of (28).

(30) $\mathrm{digits}(80, 10) = \langle 0, 8 \rangle$.

(31) $\sum \mathrm{digits}(80, 10) = 8$. The theorem is a consequence of (30).

(32) $\mathrm{digits}(90, 10) = \langle 0, 9 \rangle$.

(33) $\sum \mathrm{digits}(90, 10) = 9$. The theorem is a consequence of (32).

(34) $\mathrm{digits}(100, 10) = \langle 0, 0, 1 \rangle$.

(35) $\sum \mathrm{digits}(100, 10) = 1$. The theorem is a consequence of (34).

(36) $\mathrm{digits}(110, 10) = \langle 0, 1, 1 \rangle$.

(37) $\sum \mathrm{digits}(110, 10) = 2$. The theorem is a consequence of (36).

(38) $\mathrm{digits}(120, 10) = \langle 0, 2, 1 \rangle$.

(39) $\sum \mathrm{digits}(120, 10) = 3$. The theorem is a consequence of (38).
(40) $\mathrm{digits}(130, 10) = \langle 0, 3, 1 \rangle$.
(41) $\sum \mathrm{digits}(130, 10) = 4$. The theorem is a consequence of (40).
(42) $\mathrm{digits}(140, 10) = \langle 0, 4, 1 \rangle$.
(43) $\sum \mathrm{digits}(140, 10) = 5$. The theorem is a consequence of (42).
(44) $\mathrm{digits}(150, 10) = \langle 0, 5, 1 \rangle$.
(45) $\sum \mathrm{digits}(150, 10) = 6$. The theorem is a consequence of (44).
(46) $\mathrm{digits}(160, 10) = \langle 0, 6, 1 \rangle$.
(47) $\sum \mathrm{digits}(160, 10) = 7$. The theorem is a consequence of (46).
(48) $\mathrm{digits}(170, 10) = \langle 0, 7, 1 \rangle$.
(49) $\sum \mathrm{digits}(170, 10) = 8$. The theorem is a consequence of (48).
(50) $\mathrm{digits}(180, 10) = \langle 0, 8, 1 \rangle$.
(51) $\sum \mathrm{digits}(180, 10) = 9$. The theorem is a consequence of (50).
(52) $\mathrm{digits}(190, 10) = \langle 0, 9, 1 \rangle$.
(53) $\sum \mathrm{digits}(190, 10) = 10$. The theorem is a consequence of (52).
(54) 190 is the solution to Sierpiński's problem 36 for 10. The theorem is a consequence of (53), (6), (17), (19), (21), (23), (25), (27), (29), (31), (33), (35), (37), (39), (41), (43), (45), (47), (49), and (51).

4. Problem 36 for $s = 11$

Now we state the propositions:
(55) $\mathrm{digits}(11, 10) = \langle 1, 1 \rangle$.
(56) $\sum \mathrm{digits}(11, 10) = 2$. The theorem is a consequence of (55).
(57) $\mathrm{digits}(22, 10) = \langle 2, 2 \rangle$.
(58) $\sum \mathrm{digits}(22, 10) = 4$. The theorem is a consequence of (57).
(59) $\mathrm{digits}(33, 10) = \langle 3, 3 \rangle$.
(60) $\sum \mathrm{digits}(33, 10) = 6$. The theorem is a consequence of (59).
(61) $\mathrm{digits}(44, 10) = \langle 4, 4 \rangle$.
(62) $\sum \mathrm{digits}(44, 10) = 8$. The theorem is a consequence of (61).
(63) $\mathrm{digits}(55, 10) = \langle 5, 5 \rangle$.
(64) $\sum \mathrm{digits}(55, 10) = 10$. The theorem is a consequence of (63).
(65) $\mathrm{digits}(66, 10) = \langle 6, 6 \rangle$.
(66) $\sum \mathrm{digits}(66, 10) = 12$. The theorem is a consequence of (65).
(67) $\mathrm{digits}(77, 10) = \langle 7, 7 \rangle$.

(68) $\sum \mathrm{digits}(77, 10) = 14$. The theorem is a consequence of (67).

(69) $\mathrm{digits}(88, 10) = \langle 8, 8 \rangle$.

(70) $\sum \mathrm{digits}(88, 10) = 16$. The theorem is a consequence of (69).

(71) $\mathrm{digits}(99, 10) = \langle 9, 9 \rangle$.

(72) $\sum \mathrm{digits}(99, 10) = 18$. The theorem is a consequence of (71).

(73) $\mathrm{digits}(121, 10) = \langle 1, 2, 1 \rangle$.

(74) $\sum \mathrm{digits}(121, 10) = 4$. The theorem is a consequence of (73).

(75) $\mathrm{digits}(132, 10) = \langle 2, 3, 1 \rangle$.

(76) $\sum \mathrm{digits}(132, 10) = 6$. The theorem is a consequence of (75).

(77) $\mathrm{digits}(143, 10) = \langle 3, 4, 1 \rangle$.

(78) $\sum \mathrm{digits}(143, 10) = 8$. The theorem is a consequence of (77).

(79) $\mathrm{digits}(154, 10) = \langle 4, 5, 1 \rangle$.

(80) $\sum \mathrm{digits}(154, 10) = 10$. The theorem is a consequence of (79).

(81) $\mathrm{digits}(165, 10) = \langle 5, 6, 1 \rangle$.

(82) $\sum \mathrm{digits}(165, 10) = 12$. The theorem is a consequence of (81).

(83) $\mathrm{digits}(176, 10) = \langle 6, 7, 1 \rangle$.

(84) $\sum \mathrm{digits}(176, 10) = 14$. The theorem is a consequence of (83).

(85) $\mathrm{digits}(187, 10) = \langle 7, 8, 1 \rangle$.

(86) $\sum \mathrm{digits}(187, 10) = 16$. The theorem is a consequence of (85).

(87) $\mathrm{digits}(198, 10) = \langle 8, 9, 1 \rangle$.

(88) $\sum \mathrm{digits}(198, 10) = 18$. The theorem is a consequence of (87).

(89) $\mathrm{digits}(209, 10) = \langle 9, 0, 2 \rangle$.

(90) $\sum \mathrm{digits}(209, 10) = 11$. The theorem is a consequence of (89).

(91) 209 is the solution to Sierpiński's problem 36 for 11. The theorem is a consequence of (90), (6), (56), (58), (60), (62), (64), (66), (68), (70), (72), (37), (74), (76), (78), (80), (82), (84), (86), and (88).

5. Problem 36 for $s = 12$

Now we state the propositions:

(92) $\mathrm{digits}(12, 10) = \langle 2, 1 \rangle$.

(93) $\sum \mathrm{digits}(12, 10) = 3$. The theorem is a consequence of (92).

(94) $\mathrm{digits}(24, 10) = \langle 4, 2 \rangle$.

(95) $\sum \mathrm{digits}(24, 10) = 6$. The theorem is a consequence of (94).

(96) $\mathrm{digits}(36, 10) = \langle 6, 3 \rangle$.

(97) $\sum \mathrm{digits}(36, 10) = 9$. The theorem is a consequence of (96).

(98) $\mathrm{digits}(48, 10) = \langle 8, 4 \rangle$.

(99) $\sum \mathrm{digits}(48, 10) = 12$. The theorem is a consequence of (98).

(100) 48 is the solution to Sierpiński's problem 36 for 12. The theorem is a consequence of (99), (6), (93), (95), and (97).

6. Problem 36 for $s = 13$

Now we state the propositions:

(101) $\mathrm{digits}(13, 10) = \langle 3, 1 \rangle$.

(102) $\sum \mathrm{digits}(13, 10) = 4$. The theorem is a consequence of (101).

(103) $\mathrm{digits}(26, 10) = \langle 6, 2 \rangle$.

(104) $\sum \mathrm{digits}(26, 10) = 8$. The theorem is a consequence of (103).

(105) $\mathrm{digits}(39, 10) = \langle 9, 3 \rangle$.

(106) $\sum \mathrm{digits}(39, 10) = 12$. The theorem is a consequence of (105).

(107) $\mathrm{digits}(52, 10) = \langle 2, 5 \rangle$.

(108) $\sum \mathrm{digits}(52, 10) = 7$. The theorem is a consequence of (107).

(109) $\mathrm{digits}(65, 10) = \langle 5, 6 \rangle$.

(110) $\sum \mathrm{digits}(65, 10) = 11$. The theorem is a consequence of (109).

(111) $\mathrm{digits}(78, 10) = \langle 8, 7 \rangle$.

(112) $\sum \mathrm{digits}(78, 10) = 15$. The theorem is a consequence of (111).

(113) $\mathrm{digits}(91, 10) = \langle 1, 9 \rangle$.

(114) $\sum \mathrm{digits}(91, 10) = 10$. The theorem is a consequence of (113).

(115) $\mathrm{digits}(104, 10) = \langle 4, 0, 1 \rangle$.

(116) $\sum \mathrm{digits}(104, 10) = 5$. The theorem is a consequence of (115).

(117) $\mathrm{digits}(117, 10) = \langle 7, 1, 1 \rangle$.

(118) $\sum \mathrm{digits}(117, 10) = 9$. The theorem is a consequence of (117).

(119) $\mathrm{digits}(156, 10) = \langle 6, 5, 1 \rangle$.

(120) $\sum \mathrm{digits}(156, 10) = 12$. The theorem is a consequence of (119).

(121) $\mathrm{digits}(169, 10) = \langle 9, 6, 1 \rangle$.

(122) $\sum \mathrm{digits}(169, 10) = 16$. The theorem is a consequence of (121).

(123) $\mathrm{digits}(182, 10) = \langle 2, 8, 1 \rangle$.

(124) $\sum \mathrm{digits}(182, 10) = 11$. The theorem is a consequence of (123).

(125) $\mathrm{digits}(195, 10) = \langle 5, 9, 1 \rangle$.

(126) $\sum \mathrm{digits}(195, 10) = 15$. The theorem is a consequence of (125).

(127) $\mathrm{digits}(208, 10) = \langle 8, 0, 2\rangle$.

(128) $\sum \mathrm{digits}(208, 10) = 10$. The theorem is a consequence of (127).

(129) $\mathrm{digits}(221, 10) = \langle 1, 2, 2\rangle$.

(130) $\sum \mathrm{digits}(221, 10) = 5$. The theorem is a consequence of (129).

(131) $\mathrm{digits}(234, 10) = \langle 4, 3, 2\rangle$.

(132) $\sum \mathrm{digits}(234, 10) = 9$. The theorem is a consequence of (131).

(133) $\mathrm{digits}(247, 10) = \langle 7, 4, 2\rangle$.

(134) $\sum \mathrm{digits}(247, 10) = 13$. The theorem is a consequence of (133).

(135) 247 is the solution to Sierpiński's problem 36 for 13. The theorem is a consequence of (134), (6), (102), (104), (106), (108), (110), (112), (114), (116), (118), (41), (78), (120), (122), (124), (126), (128), (130), and (132).

7. Problem 36 for $s = 14$

Now we state the propositions:

(136) $\mathrm{digits}(14, 10) = \langle 4, 1\rangle$.

(137) $\sum \mathrm{digits}(14, 10) = 5$. The theorem is a consequence of (136).

(138) $\mathrm{digits}(28, 10) = \langle 8, 2\rangle$.

(139) $\sum \mathrm{digits}(28, 10) = 10$. The theorem is a consequence of (138).

(140) $\mathrm{digits}(42, 10) = \langle 2, 4\rangle$.

(141) $\sum \mathrm{digits}(42, 10) = 6$. The theorem is a consequence of (140).

(142) $\mathrm{digits}(56, 10) = \langle 6, 5\rangle$.

(143) $\sum \mathrm{digits}(56, 10) = 11$. The theorem is a consequence of (142).

(144) $\mathrm{digits}(84, 10) = \langle 4, 8\rangle$.

(145) $\sum \mathrm{digits}(84, 10) = 12$. The theorem is a consequence of (144).

(146) $\mathrm{digits}(98, 10) = \langle 8, 9\rangle$.

(147) $\sum \mathrm{digits}(98, 10) = 17$. The theorem is a consequence of (146).

(148) $\mathrm{digits}(112, 10) = \langle 2, 1, 1\rangle$.

(149) $\sum \mathrm{digits}(112, 10) = 4$. The theorem is a consequence of (148).

(150) $\mathrm{digits}(126, 10) = \langle 6, 2, 1\rangle$.

(151) $\sum \mathrm{digits}(126, 10) = 9$. The theorem is a consequence of (150).

(152) $\mathrm{digits}(168, 10) = \langle 8, 6, 1\rangle$.

(153) $\sum \mathrm{digits}(168, 10) = 15$. The theorem is a consequence of (152).

(154) $\mathrm{digits}(196, 10) = \langle 6, 9, 1\rangle$.

(155) $\sum \mathrm{digits}(196, 10) = 16$. The theorem is a consequence of (154).

(156) $\mathrm{digits}(210, 10) = \langle 0, 1, 2\rangle$.

(157) $\sum \mathrm{digits}(210, 10) = 3$. The theorem is a consequence of (156).

(158) $\mathrm{digits}(224, 10) = \langle 4, 2, 2 \rangle$.

(159) $\sum \mathrm{digits}(224, 10) = 8$. The theorem is a consequence of (158).

(160) $\mathrm{digits}(238, 10) = \langle 8, 3, 2 \rangle$.

(161) $\sum \mathrm{digits}(238, 10) = 13$. The theorem is a consequence of (160).

(162) $\mathrm{digits}(252, 10) = \langle 2, 5, 2 \rangle$.

(163) $\sum \mathrm{digits}(252, 10) = 9$. The theorem is a consequence of (162).

(164) $\mathrm{digits}(266, 10) = \langle 6, 6, 2 \rangle$.

(165) $\sum \mathrm{digits}(266, 10) = 14$. The theorem is a consequence of (164).

(166) 266 is the solution to Sierpiński's problem 36 for 14. The theorem is a consequence of (165), (6), (137), (139), (141), (143), (29), (145), (147), (149), (151), (43), (80), (153), (124), (155), (157), (159), (161), and (163).

8. Problem 36 for $s = 15$

Now we state the propositions:

(167) $\mathrm{digits}(15, 10) = \langle 5, 1 \rangle$.

(168) $\sum \mathrm{digits}(15, 10) = 6$. The theorem is a consequence of (167).

(169) $\mathrm{digits}(45, 10) = \langle 5, 4 \rangle$.

(170) $\sum \mathrm{digits}(45, 10) = 9$. The theorem is a consequence of (169).

(171) $\mathrm{digits}(75, 10) = \langle 5, 7 \rangle$.

(172) $\sum \mathrm{digits}(75, 10) = 12$. The theorem is a consequence of (171).

(173) $\mathrm{digits}(105, 10) = \langle 5, 0, 1 \rangle$.

(174) $\sum \mathrm{digits}(105, 10) = 6$. The theorem is a consequence of (173).

(175) $\mathrm{digits}(135, 10) = \langle 5, 3, 1 \rangle$.

(176) $\sum \mathrm{digits}(135, 10) = 9$. The theorem is a consequence of (175).

(177) 195 is the solution to Sierpiński's problem 36 for 15. The theorem is a consequence of (126), (6), (168), (21), (170), (27), (172), (33), (174), (39), (176), (45), (82), and (51).

9. Problem 36 for $s = 16$

Now we state the propositions:

(178) $\mathrm{digits}(16, 10) = \langle 6, 1 \rangle$.

(179) $\sum \mathrm{digits}(16, 10) = 7$. The theorem is a consequence of (178).

(180) $\mathrm{digits}(32, 10) = \langle 2, 3 \rangle$.

(181) $\sum \mathrm{digits}(32, 10) = 5$. The theorem is a consequence of (180).

(182) $\mathrm{digits}(64, 10) = \langle 4, 6\rangle$.

(183) $\sum \mathrm{digits}(64, 10) = 10$. The theorem is a consequence of (182).

(184) $\mathrm{digits}(96, 10) = \langle 6, 9\rangle$.

(185) $\sum \mathrm{digits}(96, 10) = 15$. The theorem is a consequence of (184).

(186) $\mathrm{digits}(128, 10) = \langle 8, 2, 1\rangle$.

(187) $\sum \mathrm{digits}(128, 10) = 11$. The theorem is a consequence of (186).

(188) $\mathrm{digits}(144, 10) = \langle 4, 4, 1\rangle$.

(189) $\sum \mathrm{digits}(144, 10) = 9$. The theorem is a consequence of (188).

(190) $\mathrm{digits}(192, 10) = \langle 2, 9, 1\rangle$.

(191) $\sum \mathrm{digits}(192, 10) = 12$. The theorem is a consequence of (190).

(192) $\mathrm{digits}(240, 10) = \langle 0, 4, 2\rangle$.

(193) $\sum \mathrm{digits}(240, 10) = 6$. The theorem is a consequence of (192).

(194) $\mathrm{digits}(256, 10) = \langle 6, 5, 2\rangle$.

(195) $\sum \mathrm{digits}(256, 10) = 13$. The theorem is a consequence of (194).

(196) $\mathrm{digits}(272, 10) = \langle 2, 7, 2\rangle$.

(197) $\sum \mathrm{digits}(272, 10) = 11$. The theorem is a consequence of (196).

(198) $\mathrm{digits}(288, 10) = \langle 8, 8, 2\rangle$.

(199) $\sum \mathrm{digits}(288, 10) = 18$. The theorem is a consequence of (198).

(200) $\mathrm{digits}(304, 10) = \langle 4, 0, 3\rangle$.

(201) $\sum \mathrm{digits}(304, 10) = 7$. The theorem is a consequence of (200).

(202) $\mathrm{digits}(320, 10) = \langle 0, 2, 3\rangle$.

(203) $\sum \mathrm{digits}(320, 10) = 5$. The theorem is a consequence of (202).

(204) $\mathrm{digits}(336, 10) = \langle 6, 3, 3\rangle$.

(205) $\sum \mathrm{digits}(336, 10) = 12$. The theorem is a consequence of (204).

(206) $\mathrm{digits}(352, 10) = \langle 2, 5, 3\rangle$.

(207) $\sum \mathrm{digits}(352, 10) = 10$. The theorem is a consequence of (206).

(208) $\mathrm{digits}(368, 10) = \langle 8, 6, 3\rangle$.

(209) $\sum \mathrm{digits}(368, 10) = 17$. The theorem is a consequence of (208).

(210) $\mathrm{digits}(384, 10) = \langle 4, 8, 3\rangle$.

(211) $\sum \mathrm{digits}(384, 10) = 15$. The theorem is a consequence of (210).

(212) $\mathrm{digits}(400, 10) = \langle 0, 0, 4\rangle$.

(213) $\sum \mathrm{digits}(400, 10) = 4$. The theorem is a consequence of (212).

(214) $\mathrm{digits}(416, 10) = \langle 6, 1, 4\rangle$.

(215) $\sum \mathrm{digits}(416, 10) = 11$. The theorem is a consequence of (214).

(216) $\mathrm{digits}(432, 10) = \langle 2, 3, 4\rangle$.

(217) $\sum \mathrm{digits}(432, 10) = 9$. The theorem is a consequence of (216).

(218) $\mathrm{digits}(448, 10) = \langle 8, 4, 4 \rangle$.

(219) $\sum \mathrm{digits}(448, 10) = 16$. The theorem is a consequence of (218).

(220) 448 is the solution to Sierpiński's problem 36 for 16. The theorem is a consequence of (219), (6), (179), (181), (99), (183), (31), (185), (149), (187), (189), (47), (84), (191), (128), (159), (193), (195), (197), (199), (201), (203), (205), (207), (209), (211), (213), (215), and (217).

10. Problem 36 for $s = 17$

Now we state the propositions:

(221) $\mathrm{digits}(17, 10) = \langle 7, 1 \rangle$.

(222) $\sum \mathrm{digits}(17, 10) = 8$. The theorem is a consequence of (221).

(223) $\mathrm{digits}(34, 10) = \langle 4, 3 \rangle$.

(224) $\sum \mathrm{digits}(34, 10) = 7$. The theorem is a consequence of (223).

(225) $\mathrm{digits}(51, 10) = \langle 1, 5 \rangle$.

(226) $\sum \mathrm{digits}(51, 10) = 6$. The theorem is a consequence of (225).

(227) $\mathrm{digits}(68, 10) = \langle 8, 6 \rangle$.

(228) $\sum \mathrm{digits}(68, 10) = 14$. The theorem is a consequence of (227).

(229) $\mathrm{digits}(85, 10) = \langle 5, 8 \rangle$.

(230) $\sum \mathrm{digits}(85, 10) = 13$. The theorem is a consequence of (229).

(231) $\mathrm{digits}(102, 10) = \langle 2, 0, 1 \rangle$.

(232) $\sum \mathrm{digits}(102, 10) = 3$. The theorem is a consequence of (231).

(233) $\mathrm{digits}(119, 10) = \langle 9, 1, 1 \rangle$.

(234) $\sum \mathrm{digits}(119, 10) = 11$. The theorem is a consequence of (233).

(235) $\mathrm{digits}(136, 10) = \langle 6, 3, 1 \rangle$.

(236) $\sum \mathrm{digits}(136, 10) = 10$. The theorem is a consequence of (235).

(237) $\mathrm{digits}(153, 10) = \langle 3, 5, 1 \rangle$.

(238) $\sum \mathrm{digits}(153, 10) = 9$. The theorem is a consequence of (237).

(239) $\mathrm{digits}(204, 10) = \langle 4, 0, 2 \rangle$.

(240) $\sum \mathrm{digits}(204, 10) = 6$. The theorem is a consequence of (239).

(241) $\mathrm{digits}(255, 10) = \langle 5, 5, 2 \rangle$.

(242) $\sum \mathrm{digits}(255, 10) = 12$. The theorem is a consequence of (241).

(243) $\mathrm{digits}(289, 10) = \langle 9, 8, 2 \rangle$.

(244) $\sum \mathrm{digits}(289, 10) = 19$. The theorem is a consequence of (243).

(245) $\mathrm{digits}(306, 10) = \langle 6, 0, 3 \rangle$.

(246) $\sum \mathrm{digits}(306, 10) = 9$. The theorem is a consequence of (245).

(247) $\mathrm{digits}(323, 10) = \langle 3, 2, 3\rangle$.

(248) $\sum \mathrm{digits}(323, 10) = 8$. The theorem is a consequence of (247).

(249) $\mathrm{digits}(340, 10) = \langle 0, 4, 3\rangle$.

(250) $\sum \mathrm{digits}(340, 10) = 7$. The theorem is a consequence of (249).

(251) $\mathrm{digits}(357, 10) = \langle 7, 5, 3\rangle$.

(252) $\sum \mathrm{digits}(357, 10) = 15$. The theorem is a consequence of (251).

(253) $\mathrm{digits}(374, 10) = \langle 4, 7, 3\rangle$.

(254) $\sum \mathrm{digits}(374, 10) = 14$. The theorem is a consequence of (253).

(255) $\mathrm{digits}(391, 10) = \langle 1, 9, 3\rangle$.

(256) $\sum \mathrm{digits}(391, 10) = 13$. The theorem is a consequence of (255).

(257) $\mathrm{digits}(408, 10) = \langle 8, 0, 4\rangle$.

(258) $\sum \mathrm{digits}(408, 10) = 12$. The theorem is a consequence of (257).

(259) $\mathrm{digits}(425, 10) = \langle 5, 2, 4\rangle$.

(260) $\sum \mathrm{digits}(425, 10) = 11$. The theorem is a consequence of (259).

(261) $\mathrm{digits}(442, 10) = \langle 2, 4, 4\rangle$.

(262) $\sum \mathrm{digits}(442, 10) = 10$. The theorem is a consequence of (261).

(263) $\mathrm{digits}(459, 10) = \langle 9, 5, 4\rangle$.

(264) $\sum \mathrm{digits}(459, 10) = 18$. The theorem is a consequence of (263).

(265) $\mathrm{digits}(476, 10) = \langle 6, 7, 4\rangle$.

(266) $\sum \mathrm{digits}(476, 10) = 17$. The theorem is a consequence of (265).

(267) 476 is the solution to Sierpiński's problem 36 for 17. The theorem is a consequence of (266), (6), (222), (224), (226), (228), (230), (232), (234), (236), (238), (49), (86), (240), (130), (161), (242), (197), (244), (246), (248), (250), (252), (254), (256), (258), (260), (262), and (264).

11. Problem 36 for $s = 18$

Now we state the propositions:

(268) $\mathrm{digits}(18, 10) = \langle 8, 1\rangle$.

(269) $\sum \mathrm{digits}(18, 10) = 9$. The theorem is a consequence of (268).

(270) $\mathrm{digits}(54, 10) = \langle 4, 5\rangle$.

(271) $\sum \mathrm{digits}(54, 10) = 9$. The theorem is a consequence of (270).

(272) $\mathrm{digits}(72, 10) = \langle 2, 7\rangle$.

(273) $\sum \mathrm{digits}(72, 10) = 9$. The theorem is a consequence of (272).

(274) $\mathrm{digits}(108, 10) = \langle 8, 0, 1\rangle$.

(275) $\sum \mathrm{digits}(108, 10) = 9$. The theorem is a consequence of (274).

(276) $\mathrm{digits}(162, 10) = \langle 2, 6, 1\rangle$.

(277) $\sum \mathrm{digits}(162, 10) = 9$. The theorem is a consequence of (276).

(278) 198 is the solution to Sierpiński's problem 36 for 18. The theorem is a consequence of (88), (6), (269), (97), (271), (273), (33), (275), (151), (189), (277), and (51).

12. Problem 36 for $s = 19$

Now we state the propositions:

(279) $\mathrm{digits}(19, 10) = \langle 9, 1\rangle$.

(280) $\sum \mathrm{digits}(19, 10) = 10$. The theorem is a consequence of (279).

(281) $\mathrm{digits}(38, 10) = \langle 8, 3\rangle$.

(282) $\sum \mathrm{digits}(38, 10) = 11$. The theorem is a consequence of (281).

(283) $\mathrm{digits}(57, 10) = \langle 7, 5\rangle$.

(284) $\sum \mathrm{digits}(57, 10) = 12$. The theorem is a consequence of (283).

(285) $\mathrm{digits}(76, 10) = \langle 6, 7\rangle$.

(286) $\sum \mathrm{digits}(76, 10) = 13$. The theorem is a consequence of (285).

(287) $\mathrm{digits}(95, 10) = \langle 5, 9\rangle$.

(288) $\sum \mathrm{digits}(95, 10) = 14$. The theorem is a consequence of (287).

(289) $\mathrm{digits}(114, 10) = \langle 4, 1, 1\rangle$.

(290) $\sum \mathrm{digits}(114, 10) = 6$. The theorem is a consequence of (289).

(291) $\mathrm{digits}(133, 10) = \langle 3, 3, 1\rangle$.

(292) $\sum \mathrm{digits}(133, 10) = 7$. The theorem is a consequence of (291).

(293) $\mathrm{digits}(152, 10) = \langle 2, 5, 1\rangle$.

(294) $\sum \mathrm{digits}(152, 10) = 8$. The theorem is a consequence of (293).

(295) $\mathrm{digits}(171, 10) = \langle 1, 7, 1\rangle$.

(296) $\sum \mathrm{digits}(171, 10) = 9$. The theorem is a consequence of (295).

(297) $\mathrm{digits}(228, 10) = \langle 8, 2, 2\rangle$.

(298) $\sum \mathrm{digits}(228, 10) = 12$. The theorem is a consequence of (297).

(299) $\mathrm{digits}(285, 10) = \langle 5, 8, 2\rangle$.

(300) $\sum \mathrm{digits}(285, 10) = 15$. The theorem is a consequence of (299).

(301) $\mathrm{digits}(342, 10) = \langle 2, 4, 3\rangle$.

(302) $\sum \mathrm{digits}(342, 10) = 9$. The theorem is a consequence of (301).

(303) $\mathrm{digits}(361, 10) = \langle 1, 6, 3\rangle$.

(304) $\sum \mathrm{digits}(361, 10) = 10$. The theorem is a consequence of (303).

(305) $\mathrm{digits}(380, 10) = \langle 0, 8, 3\rangle$.

(306) $\sum \mathrm{digits}(380, 10) = 11$. The theorem is a consequence of (305).

(307) $\mathrm{digits}(399, 10) = \langle 9, 9, 3\rangle$.

(308) $\sum \mathrm{digits}(399, 10) = 21$. The theorem is a consequence of (307).

(309) $\mathrm{digits}(418, 10) = \langle 8, 1, 4\rangle$.

(310) $\sum \mathrm{digits}(418, 10) = 13$. The theorem is a consequence of (309).

(311) $\mathrm{digits}(437, 10) = \langle 7, 3, 4\rangle$.

(312) $\sum \mathrm{digits}(437, 10) = 14$. The theorem is a consequence of (311).

(313) $\mathrm{digits}(456, 10) = \langle 6, 5, 4\rangle$.

(314) $\sum \mathrm{digits}(456, 10) = 15$. The theorem is a consequence of (313).

(315) $\mathrm{digits}(475, 10) = \langle 5, 7, 4\rangle$.

(316) $\sum \mathrm{digits}(475, 10) = 16$. The theorem is a consequence of (315).

(317) $\mathrm{digits}(494, 10) = \langle 4, 9, 4\rangle$.

(318) $\sum \mathrm{digits}(494, 10) = 17$. The theorem is a consequence of (317).

(319) $\mathrm{digits}(513, 10) = \langle 3, 1, 5\rangle$.

(320) $\sum \mathrm{digits}(513, 10) = 9$. The theorem is a consequence of (319).

(321) $\mathrm{digits}(532, 10) = \langle 2, 3, 5\rangle$.

(322) $\sum \mathrm{digits}(532, 10) = 10$. The theorem is a consequence of (321).

(323) $\mathrm{digits}(551, 10) = \langle 1, 5, 5\rangle$.

(324) $\sum \mathrm{digits}(551, 10) = 11$. The theorem is a consequence of (323).

(325) $\mathrm{digits}(570, 10) = \langle 0, 7, 5\rangle$.

(326) $\sum \mathrm{digits}(570, 10) = 12$. The theorem is a consequence of (325).

(327) $\mathrm{digits}(589, 10) = \langle 9, 8, 5\rangle$.

(328) $\sum \mathrm{digits}(589, 10) = 22$. The theorem is a consequence of (327).

(329) $\mathrm{digits}(608, 10) = \langle 8, 0, 6\rangle$.

(330) $\sum \mathrm{digits}(608, 10) = 14$. The theorem is a consequence of (329).

(331) $\mathrm{digits}(627, 10) = \langle 7, 2, 6\rangle$.

(332) $\sum \mathrm{digits}(627, 10) = 15$. The theorem is a consequence of (331).

(333) $\mathrm{digits}(646, 10) = \langle 6, 4, 6\rangle$.

(334) $\sum \mathrm{digits}(646, 10) = 16$. The theorem is a consequence of (333).

(335) $\mathrm{digits}(665, 10) = \langle 5, 6, 6\rangle$.

(336) $\sum \mathrm{digits}(665, 10) = 17$. The theorem is a consequence of (335).

(337) $\mathrm{digits}(684, 10) = \langle 4, 8, 6\rangle$.

(338) $\sum \mathrm{digits}(684, 10) = 18$. The theorem is a consequence of (337).

(339) $\mathrm{digits}(703, 10) = \langle 3, 0, 7\rangle$.

(340) $\sum \text{digits}(703, 10) = 10$. The theorem is a consequence of (339).
(341) $\text{digits}(722, 10) = \langle 2, 2, 7 \rangle$.
(342) $\sum \text{digits}(722, 10) = 11$. The theorem is a consequence of (341).
(343) $\text{digits}(741, 10) = \langle 1, 4, 7 \rangle$.
(344) $\sum \text{digits}(741, 10) = 12$. The theorem is a consequence of (343).
(345) $\text{digits}(760, 10) = \langle 0, 6, 7 \rangle$.
(346) $\sum \text{digits}(760, 10) = 13$. The theorem is a consequence of (345).
(347) $\text{digits}(779, 10) = \langle 9, 7, 7 \rangle$.
(348) $\sum \text{digits}(779, 10) = 23$. The theorem is a consequence of (347).
(349) $\text{digits}(798, 10) = \langle 8, 9, 7 \rangle$.
(350) $\sum \text{digits}(798, 10) = 24$. The theorem is a consequence of (349).
(351) $\text{digits}(817, 10) = \langle 7, 1, 8 \rangle$.
(352) $\sum \text{digits}(817, 10) = 16$. The theorem is a consequence of (351).
(353) $\text{digits}(836, 10) = \langle 6, 3, 8 \rangle$.
(354) $\sum \text{digits}(836, 10) = 17$. The theorem is a consequence of (353).
(355) $\text{digits}(855, 10) = \langle 5, 5, 8 \rangle$.
(356) $\sum \text{digits}(855, 10) = 18$. The theorem is a consequence of (355).
(357) $\text{digits}(874, 10) = \langle 4, 7, 8 \rangle$.
(358) $\sum \text{digits}(874, 10) = 19$. The theorem is a consequence of (357).
(359) 874 is the solution to Sierpiński's problem 36 for 19. The theorem is a consequence of (358), (6), (280), (282), (284), (286), (288), (290), (292), (294), (296), (53), (90), (298), (134), (165), (300), (201), (248), (302), (304), (306), (308), (310), (312), (314), (316), (318), (320), (322), (324), (326), (328), (330), (332), (334), (336), (338), (340), (342), (344), (346), (348), (350), (352), (354), and (356).

13. Problem 36 for $s = 20$

Now we state the propositions:

(360) $\text{digits}(200, 10) = \langle 0, 0, 2 \rangle$.
(361) $\sum \text{digits}(200, 10) = 2$. The theorem is a consequence of (360).
(362) $\text{digits}(220, 10) = \langle 0, 2, 2 \rangle$.
(363) $\sum \text{digits}(220, 10) = 4$. The theorem is a consequence of (362).
(364) $\text{digits}(260, 10) = \langle 0, 6, 2 \rangle$.
(365) $\sum \text{digits}(260, 10) = 8$. The theorem is a consequence of (364).
(366) $\text{digits}(280, 10) = \langle 0, 8, 2 \rangle$.

(367) $\sum \mathrm{digits}(280, 10) = 10$. The theorem is a consequence of (366).
(368) $\mathrm{digits}(300, 10) = \langle 0, 0, 3 \rangle$.
(369) $\sum \mathrm{digits}(300, 10) = 3$. The theorem is a consequence of (368).
(370) $\mathrm{digits}(360, 10) = \langle 0, 6, 3 \rangle$.
(371) $\sum \mathrm{digits}(360, 10) = 9$. The theorem is a consequence of (370).
(372) $\mathrm{digits}(420, 10) = \langle 0, 2, 4 \rangle$.
(373) $\sum \mathrm{digits}(420, 10) = 6$. The theorem is a consequence of (372).
(374) $\mathrm{digits}(440, 10) = \langle 0, 4, 4 \rangle$.
(375) $\sum \mathrm{digits}(440, 10) = 8$. The theorem is a consequence of (374).
(376) $\mathrm{digits}(460, 10) = \langle 0, 6, 4 \rangle$.
(377) $\sum \mathrm{digits}(460, 10) = 10$. The theorem is a consequence of (376).
(378) $\mathrm{digits}(480, 10) = \langle 0, 8, 4 \rangle$.
(379) $\sum \mathrm{digits}(480, 10) = 12$. The theorem is a consequence of (378).
(380) $\mathrm{digits}(500, 10) = \langle 0, 0, 5 \rangle$.
(381) $\sum \mathrm{digits}(500, 10) = 5$. The theorem is a consequence of (380).
(382) $\mathrm{digits}(520, 10) = \langle 0, 2, 5 \rangle$.
(383) $\sum \mathrm{digits}(520, 10) = 7$. The theorem is a consequence of (382).
(384) $\mathrm{digits}(540, 10) = \langle 0, 4, 5 \rangle$.
(385) $\sum \mathrm{digits}(540, 10) = 9$. The theorem is a consequence of (384).
(386) $\mathrm{digits}(560, 10) = \langle 0, 6, 5 \rangle$.
(387) $\sum \mathrm{digits}(560, 10) = 11$. The theorem is a consequence of (386).
(388) $\mathrm{digits}(580, 10) = \langle 0, 8, 5 \rangle$.
(389) $\sum \mathrm{digits}(580, 10) = 13$. The theorem is a consequence of (388).
(390) $\mathrm{digits}(600, 10) = \langle 0, 0, 6 \rangle$.
(391) $\sum \mathrm{digits}(600, 10) = 6$. The theorem is a consequence of (390).
(392) $\mathrm{digits}(620, 10) = \langle 0, 2, 6 \rangle$.
(393) $\sum \mathrm{digits}(620, 10) = 8$. The theorem is a consequence of (392).
(394) $\mathrm{digits}(640, 10) = \langle 0, 4, 6 \rangle$.
(395) $\sum \mathrm{digits}(640, 10) = 10$. The theorem is a consequence of (394).
(396) $\mathrm{digits}(660, 10) = \langle 0, 6, 6 \rangle$.
(397) $\sum \mathrm{digits}(660, 10) = 12$. The theorem is a consequence of (396).
(398) $\mathrm{digits}(680, 10) = \langle 0, 8, 6 \rangle$.
(399) $\sum \mathrm{digits}(680, 10) = 14$. The theorem is a consequence of (398).
(400) $\mathrm{digits}(700, 10) = \langle 0, 0, 7 \rangle$.
(401) $\sum \mathrm{digits}(700, 10) = 7$. The theorem is a consequence of (400).

(402) $\mathrm{digits}(720, 10) = \langle 0, 2, 7\rangle$.
(403) $\sum \mathrm{digits}(720, 10) = 9$. The theorem is a consequence of (402).
(404) $\mathrm{digits}(740, 10) = \langle 0, 4, 7\rangle$.
(405) $\sum \mathrm{digits}(740, 10) = 11$. The theorem is a consequence of (404).
(406) $\mathrm{digits}(780, 10) = \langle 0, 8, 7\rangle$.
(407) $\sum \mathrm{digits}(780, 10) = 15$. The theorem is a consequence of (406).
(408) $\mathrm{digits}(800, 10) = \langle 0, 0, 8\rangle$.
(409) $\sum \mathrm{digits}(800, 10) = 8$. The theorem is a consequence of (408).
(410) $\mathrm{digits}(820, 10) = \langle 0, 2, 8\rangle$.
(411) $\sum \mathrm{digits}(820, 10) = 10$. The theorem is a consequence of (410).
(412) $\mathrm{digits}(840, 10) = \langle 0, 4, 8\rangle$.
(413) $\sum \mathrm{digits}(840, 10) = 12$. The theorem is a consequence of (412).
(414) $\mathrm{digits}(860, 10) = \langle 0, 6, 8\rangle$.
(415) $\sum \mathrm{digits}(860, 10) = 14$. The theorem is a consequence of (414).
(416) $\mathrm{digits}(880, 10) = \langle 0, 8, 8\rangle$.
(417) $\sum \mathrm{digits}(880, 10) = 16$. The theorem is a consequence of (416).
(418) $\mathrm{digits}(900, 10) = \langle 0, 0, 9\rangle$.
(419) $\sum \mathrm{digits}(900, 10) = 9$. The theorem is a consequence of (418).
(420) $\mathrm{digits}(920, 10) = \langle 0, 2, 9\rangle$.
(421) $\sum \mathrm{digits}(920, 10) = 11$. The theorem is a consequence of (420).
(422) $\mathrm{digits}(940, 10) = \langle 0, 4, 9\rangle$.
(423) $\sum \mathrm{digits}(940, 10) = 13$. The theorem is a consequence of (422).
(424) $\mathrm{digits}(960, 10) = \langle 0, 6, 9\rangle$.
(425) $\sum \mathrm{digits}(960, 10) = 15$. The theorem is a consequence of (424).
(426) $\mathrm{digits}(980, 10) = \langle 0, 8, 9\rangle$.
(427) $\sum \mathrm{digits}(980, 10) = 17$. The theorem is a consequence of (426).
(428) $\mathrm{digits}(1000, 10) = \langle 0, 0, 0, 1\rangle$.
(429) $\sum \mathrm{digits}(1000, 10) = 1$. The theorem is a consequence of (428).
(430) $\mathrm{digits}(1020, 10) = \langle 0, 2, 0, 1\rangle$.
(431) $\sum \mathrm{digits}(1020, 10) = 3$. The theorem is a consequence of (430).
(432) $\mathrm{digits}(1040, 10) = \langle 0, 4, 0, 1\rangle$.
(433) $\sum \mathrm{digits}(1040, 10) = 5$. The theorem is a consequence of (432).
(434) $\mathrm{digits}(1060, 10) = \langle 0, 6, 0, 1\rangle$.
(435) $\sum \mathrm{digits}(1060, 10) = 7$. The theorem is a consequence of (434).
(436) $\mathrm{digits}(1080, 10) = \langle 0, 8, 0, 1\rangle$.

(437) $\sum \mathrm{digits}(1080, 10) = 9$. The theorem is a consequence of (436).
(438) $\mathrm{digits}(1100, 10) = \langle 0, 0, 1, 1\rangle$.
(439) $\sum \mathrm{digits}(1100, 10) = 2$. The theorem is a consequence of (438).
(440) $\mathrm{digits}(1120, 10) = \langle 0, 2, 1, 1\rangle$.
(441) $\sum \mathrm{digits}(1120, 10) = 4$. The theorem is a consequence of (440).
(442) $\mathrm{digits}(1140, 10) = \langle 0, 4, 1, 1\rangle$.
(443) $\sum \mathrm{digits}(1140, 10) = 6$. The theorem is a consequence of (442).
(444) $\mathrm{digits}(1160, 10) = \langle 0, 6, 1, 1\rangle$.
(445) $\sum \mathrm{digits}(1160, 10) = 8$. The theorem is a consequence of (444).
(446) $\mathrm{digits}(1180, 10) = \langle 0, 8, 1, 1\rangle$.
(447) $\sum \mathrm{digits}(1180, 10) = 10$. The theorem is a consequence of (446).
(448) $\mathrm{digits}(1200, 10) = \langle 0, 0, 2, 1\rangle$.
(449) $\sum \mathrm{digits}(1200, 10) = 3$. The theorem is a consequence of (448).
(450) $\mathrm{digits}(1220, 10) = \langle 0, 2, 2, 1\rangle$.
(451) $\sum \mathrm{digits}(1220, 10) = 5$. The theorem is a consequence of (450).
(452) $\mathrm{digits}(1240, 10) = \langle 0, 4, 2, 1\rangle$.
(453) $\sum \mathrm{digits}(1240, 10) = 7$. The theorem is a consequence of (452).
(454) $\mathrm{digits}(1260, 10) = \langle 0, 6, 2, 1\rangle$.
(455) $\sum \mathrm{digits}(1260, 10) = 9$. The theorem is a consequence of (454).
(456) $\mathrm{digits}(1280, 10) = \langle 0, 8, 2, 1\rangle$.
(457) $\sum \mathrm{digits}(1280, 10) = 11$. The theorem is a consequence of (456).
(458) $\mathrm{digits}(1300, 10) = \langle 0, 0, 3, 1\rangle$.
(459) $\sum \mathrm{digits}(1300, 10) = 4$. The theorem is a consequence of (458).
(460) $\mathrm{digits}(1320, 10) = \langle 0, 2, 3, 1\rangle$.
(461) $\sum \mathrm{digits}(1320, 10) = 6$. The theorem is a consequence of (460).
(462) $\mathrm{digits}(1340, 10) = \langle 0, 4, 3, 1\rangle$.
(463) $\sum \mathrm{digits}(1340, 10) = 8$. The theorem is a consequence of (462).
(464) $\mathrm{digits}(1360, 10) = \langle 0, 6, 3, 1\rangle$.
(465) $\sum \mathrm{digits}(1360, 10) = 10$. The theorem is a consequence of (464).
(466) $\mathrm{digits}(1380, 10) = \langle 0, 8, 3, 1\rangle$.
(467) $\sum \mathrm{digits}(1380, 10) = 12$. The theorem is a consequence of (466).
(468) $\mathrm{digits}(1400, 10) = \langle 0, 0, 4, 1\rangle$.
(469) $\sum \mathrm{digits}(1400, 10) = 5$. The theorem is a consequence of (468).
(470) $\mathrm{digits}(1420, 10) = \langle 0, 2, 4, 1\rangle$.
(471) $\sum \mathrm{digits}(1420, 10) = 7$. The theorem is a consequence of (470).

(472) $\text{digits}(1440, 10) = \langle 0, 4, 4, 1\rangle$.
(473) $\sum \text{digits}(1440, 10) = 9$. The theorem is a consequence of (472).
(474) $\text{digits}(1460, 10) = \langle 0, 6, 4, 1\rangle$.
(475) $\sum \text{digits}(1460, 10) = 11$. The theorem is a consequence of (474).
(476) $\text{digits}(1480, 10) = \langle 0, 8, 4, 1\rangle$.
(477) $\sum \text{digits}(1480, 10) = 13$. The theorem is a consequence of (476).
(478) $\text{digits}(1500, 10) = \langle 0, 0, 5, 1\rangle$.
(479) $\sum \text{digits}(1500, 10) = 6$. The theorem is a consequence of (478).
(480) $\text{digits}(1520, 10) = \langle 0, 2, 5, 1\rangle$.
(481) $\sum \text{digits}(1520, 10) = 8$. The theorem is a consequence of (480).
(482) $\text{digits}(1540, 10) = \langle 0, 4, 5, 1\rangle$.
(483) $\sum \text{digits}(1540, 10) = 10$. The theorem is a consequence of (482).
(484) $\text{digits}(1560, 10) = \langle 0, 6, 5, 1\rangle$.
(485) $\sum \text{digits}(1560, 10) = 12$. The theorem is a consequence of (484).
(486) $\text{digits}(1580, 10) = \langle 0, 8, 5, 1\rangle$.
(487) $\sum \text{digits}(1580, 10) = 14$. The theorem is a consequence of (486).
(488) $\text{digits}(1600, 10) = \langle 0, 0, 6, 1\rangle$.
(489) $\sum \text{digits}(1600, 10) = 7$. The theorem is a consequence of (488).
(490) $\text{digits}(1620, 10) = \langle 0, 2, 6, 1\rangle$.
(491) $\sum \text{digits}(1620, 10) = 9$. The theorem is a consequence of (490).
(492) $\text{digits}(1640, 10) = \langle 0, 4, 6, 1\rangle$.
(493) $\sum \text{digits}(1640, 10) = 11$. The theorem is a consequence of (492).
(494) $\text{digits}(1660, 10) = \langle 0, 6, 6, 1\rangle$.
(495) $\sum \text{digits}(1660, 10) = 13$. The theorem is a consequence of (494).
(496) $\text{digits}(1680, 10) = \langle 0, 8, 6, 1\rangle$.
(497) $\sum \text{digits}(1680, 10) = 15$. The theorem is a consequence of (496).
(498) $\text{digits}(1700, 10) = \langle 0, 0, 7, 1\rangle$.
(499) $\sum \text{digits}(1700, 10) = 8$. The theorem is a consequence of (498).
(500) $\text{digits}(1720, 10) = \langle 0, 2, 7, 1\rangle$.
(501) $\sum \text{digits}(1720, 10) = 10$. The theorem is a consequence of (500).
(502) $\text{digits}(1740, 10) = \langle 0, 4, 7, 1\rangle$.
(503) $\sum \text{digits}(1740, 10) = 12$. The theorem is a consequence of (502).
(504) $\text{digits}(1760, 10) = \langle 0, 6, 7, 1\rangle$.
(505) $\sum \text{digits}(1760, 10) = 14$. The theorem is a consequence of (504).
(506) $\text{digits}(1780, 10) = \langle 0, 8, 7, 1\rangle$.

(507) $\sum \mathrm{digits}(1780, 10) = 16$. The theorem is a consequence of (506).
(508) $\mathrm{digits}(1800, 10) = \langle 0, 0, 8, 1\rangle$.
(509) $\sum \mathrm{digits}(1800, 10) = 9$. The theorem is a consequence of (508).
(510) $\mathrm{digits}(1820, 10) = \langle 0, 2, 8, 1\rangle$.
(511) $\sum \mathrm{digits}(1820, 10) = 11$. The theorem is a consequence of (510).
(512) $\mathrm{digits}(1840, 10) = \langle 0, 4, 8, 1\rangle$.
(513) $\sum \mathrm{digits}(1840, 10) = 13$. The theorem is a consequence of (512).
(514) $\mathrm{digits}(1860, 10) = \langle 0, 6, 8, 1\rangle$.
(515) $\sum \mathrm{digits}(1860, 10) = 15$. The theorem is a consequence of (514).
(516) $\mathrm{digits}(1880, 10) = \langle 0, 8, 8, 1\rangle$.
(517) $\sum \mathrm{digits}(1880, 10) = 17$. The theorem is a consequence of (516).
(518) $\mathrm{digits}(1900, 10) = \langle 0, 0, 9, 1\rangle$.
(519) $\sum \mathrm{digits}(1900, 10) = 10$. The theorem is a consequence of (518).
(520) $\mathrm{digits}(1920, 10) = \langle 0, 2, 9, 1\rangle$.
(521) $\sum \mathrm{digits}(1920, 10) = 12$. The theorem is a consequence of (520).
(522) $\mathrm{digits}(1940, 10) = \langle 0, 4, 9, 1\rangle$.
(523) $\sum \mathrm{digits}(1940, 10) = 14$. The theorem is a consequence of (522).
(524) $\mathrm{digits}(1960, 10) = \langle 0, 6, 9, 1\rangle$.
(525) $\sum \mathrm{digits}(1960, 10) = 16$. The theorem is a consequence of (524).
(526) $\mathrm{digits}(1980, 10) = \langle 0, 8, 9, 1\rangle$.
(527) $\sum \mathrm{digits}(1980, 10) = 18$. The theorem is a consequence of (526).
(528) $\mathrm{digits}(2000, 10) = \langle 0, 0, 0, 2\rangle$.
(529) $\sum \mathrm{digits}(2000, 10) = 2$. The theorem is a consequence of (528).
(530) $\mathrm{digits}(2020, 10) = \langle 0, 2, 0, 2\rangle$.
(531) $\sum \mathrm{digits}(2020, 10) = 4$. The theorem is a consequence of (530).
(532) $\mathrm{digits}(2040, 10) = \langle 0, 4, 0, 2\rangle$.
(533) $\sum \mathrm{digits}(2040, 10) = 6$. The theorem is a consequence of (532).
(534) $\mathrm{digits}(2060, 10) = \langle 0, 6, 0, 2\rangle$.
(535) $\sum \mathrm{digits}(2060, 10) = 8$. The theorem is a consequence of (534).
(536) $\mathrm{digits}(2080, 10) = \langle 0, 8, 0, 2\rangle$.
(537) $\sum \mathrm{digits}(2080, 10) = 10$. The theorem is a consequence of (536).
(538) $\mathrm{digits}(2100, 10) = \langle 0, 0, 1, 2\rangle$.
(539) $\sum \mathrm{digits}(2100, 10) = 3$. The theorem is a consequence of (538).
(540) $\mathrm{digits}(2120, 10) = \langle 0, 2, 1, 2\rangle$.
(541) $\sum \mathrm{digits}(2120, 10) = 5$. The theorem is a consequence of (540).

(542) $\text{digits}(2140, 10) = \langle 0, 4, 1, 2\rangle$.
(543) $\sum \text{digits}(2140, 10) = 7$. The theorem is a consequence of (542).
(544) $\text{digits}(2160, 10) = \langle 0, 6, 1, 2\rangle$.
(545) $\sum \text{digits}(2160, 10) = 9$. The theorem is a consequence of (544).
(546) $\text{digits}(2180, 10) = \langle 0, 8, 1, 2\rangle$.
(547) $\sum \text{digits}(2180, 10) = 11$. The theorem is a consequence of (546).
(548) $\text{digits}(2200, 10) = \langle 0, 0, 2, 2\rangle$.
(549) $\sum \text{digits}(2200, 10) = 4$. The theorem is a consequence of (548).
(550) $\text{digits}(2220, 10) = \langle 0, 2, 2, 2\rangle$.
(551) $\sum \text{digits}(2220, 10) = 6$. The theorem is a consequence of (550).
(552) $\text{digits}(2240, 10) = \langle 0, 4, 2, 2\rangle$.
(553) $\sum \text{digits}(2240, 10) = 8$. The theorem is a consequence of (552).
(554) $\text{digits}(2260, 10) = \langle 0, 6, 2, 2\rangle$.
(555) $\sum \text{digits}(2260, 10) = 10$. The theorem is a consequence of (554).
(556) $\text{digits}(2280, 10) = \langle 0, 8, 2, 2\rangle$.
(557) $\sum \text{digits}(2280, 10) = 12$. The theorem is a consequence of (556).
(558) $\text{digits}(2300, 10) = \langle 0, 0, 3, 2\rangle$.
(559) $\sum \text{digits}(2300, 10) = 5$. The theorem is a consequence of (558).
(560) $\text{digits}(2320, 10) = \langle 0, 2, 3, 2\rangle$.
(561) $\sum \text{digits}(2320, 10) = 7$. The theorem is a consequence of (560).
(562) $\text{digits}(2340, 10) = \langle 0, 4, 3, 2\rangle$.
(563) $\sum \text{digits}(2340, 10) = 9$. The theorem is a consequence of (562).
(564) $\text{digits}(2360, 10) = \langle 0, 6, 3, 2\rangle$.
(565) $\sum \text{digits}(2360, 10) = 11$. The theorem is a consequence of (564).
(566) $\text{digits}(2380, 10) = \langle 0, 8, 3, 2\rangle$.
(567) $\sum \text{digits}(2380, 10) = 13$. The theorem is a consequence of (566).
(568) $\text{digits}(2400, 10) = \langle 0, 0, 4, 2\rangle$.
(569) $\sum \text{digits}(2400, 10) = 6$. The theorem is a consequence of (568).
(570) $\text{digits}(2420, 10) = \langle 0, 2, 4, 2\rangle$.
(571) $\sum \text{digits}(2420, 10) = 8$. The theorem is a consequence of (570).
(572) $\text{digits}(2440, 10) = \langle 0, 4, 4, 2\rangle$.
(573) $\sum \text{digits}(2440, 10) = 10$. The theorem is a consequence of (572).
(574) $\text{digits}(2460, 10) = \langle 0, 6, 4, 2\rangle$.
(575) $\sum \text{digits}(2460, 10) = 12$. The theorem is a consequence of (574).
(576) $\text{digits}(2480, 10) = \langle 0, 8, 4, 2\rangle$.

(577) $\sum \mathrm{digits}(2480, 10) = 14$. The theorem is a consequence of (576).
(578) $\mathrm{digits}(2500, 10) = \langle 0, 0, 5, 2\rangle$.
(579) $\sum \mathrm{digits}(2500, 10) = 7$. The theorem is a consequence of (578).
(580) $\mathrm{digits}(2520, 10) = \langle 0, 2, 5, 2\rangle$.
(581) $\sum \mathrm{digits}(2520, 10) = 9$. The theorem is a consequence of (580).
(582) $\mathrm{digits}(2540, 10) = \langle 0, 4, 5, 2\rangle$.
(583) $\sum \mathrm{digits}(2540, 10) = 11$. The theorem is a consequence of (582).
(584) $\mathrm{digits}(2560, 10) = \langle 0, 6, 5, 2\rangle$.
(585) $\sum \mathrm{digits}(2560, 10) = 13$. The theorem is a consequence of (584).
(586) $\mathrm{digits}(2580, 10) = \langle 0, 8, 5, 2\rangle$.
(587) $\sum \mathrm{digits}(2580, 10) = 15$. The theorem is a consequence of (586).
(588) $\mathrm{digits}(2600, 10) = \langle 0, 0, 6, 2\rangle$.
(589) $\sum \mathrm{digits}(2600, 10) = 8$. The theorem is a consequence of (588).
(590) $\mathrm{digits}(2620, 10) = \langle 0, 2, 6, 2\rangle$.
(591) $\sum \mathrm{digits}(2620, 10) = 10$. The theorem is a consequence of (590).
(592) $\mathrm{digits}(2640, 10) = \langle 0, 4, 6, 2\rangle$.
(593) $\sum \mathrm{digits}(2640, 10) = 12$. The theorem is a consequence of (592).
(594) $\mathrm{digits}(2660, 10) = \langle 0, 6, 6, 2\rangle$.
(595) $\sum \mathrm{digits}(2660, 10) = 14$. The theorem is a consequence of (594).
(596) $\mathrm{digits}(2680, 10) = \langle 0, 8, 6, 2\rangle$.
(597) $\sum \mathrm{digits}(2680, 10) = 16$. The theorem is a consequence of (596).
(598) $\mathrm{digits}(2700, 10) = \langle 0, 0, 7, 2\rangle$.
(599) $\sum \mathrm{digits}(2700, 10) = 9$. The theorem is a consequence of (598).
(600) $\mathrm{digits}(2720, 10) = \langle 0, 2, 7, 2\rangle$.
(601) $\sum \mathrm{digits}(2720, 10) = 11$. The theorem is a consequence of (600).
(602) $\mathrm{digits}(2740, 10) = \langle 0, 4, 7, 2\rangle$.
(603) $\sum \mathrm{digits}(2740, 10) = 13$. The theorem is a consequence of (602).
(604) $\mathrm{digits}(2760, 10) = \langle 0, 6, 7, 2\rangle$.
(605) $\sum \mathrm{digits}(2760, 10) = 15$. The theorem is a consequence of (604).
(606) $\mathrm{digits}(2780, 10) = \langle 0, 8, 7, 2\rangle$.
(607) $\sum \mathrm{digits}(2780, 10) = 17$. The theorem is a consequence of (606).
(608) $\mathrm{digits}(2800, 10) = \langle 0, 0, 8, 2\rangle$.
(609) $\sum \mathrm{digits}(2800, 10) = 10$. The theorem is a consequence of (608).
(610) $\mathrm{digits}(2820, 10) = \langle 0, 2, 8, 2\rangle$.
(611) $\sum \mathrm{digits}(2820, 10) = 12$. The theorem is a consequence of (610).

(612) $\text{digits}(2840, 10) = \langle 0, 4, 8, 2\rangle$.
(613) $\sum \text{digits}(2840, 10) = 14$. The theorem is a consequence of (612).
(614) $\text{digits}(2860, 10) = \langle 0, 6, 8, 2\rangle$.
(615) $\sum \text{digits}(2860, 10) = 16$. The theorem is a consequence of (614).
(616) $\text{digits}(2880, 10) = \langle 0, 8, 8, 2\rangle$.
(617) $\sum \text{digits}(2880, 10) = 18$. The theorem is a consequence of (616).
(618) $\text{digits}(2900, 10) = \langle 0, 0, 9, 2\rangle$.
(619) $\sum \text{digits}(2900, 10) = 11$. The theorem is a consequence of (618).
(620) $\text{digits}(2920, 10) = \langle 0, 2, 9, 2\rangle$.
(621) $\sum \text{digits}(2920, 10) = 13$. The theorem is a consequence of (620).
(622) $\text{digits}(2940, 10) = \langle 0, 4, 9, 2\rangle$.
(623) $\sum \text{digits}(2940, 10) = 15$. The theorem is a consequence of (622).
(624) $\text{digits}(2960, 10) = \langle 0, 6, 9, 2\rangle$.
(625) $\sum \text{digits}(2960, 10) = 17$. The theorem is a consequence of (624).
(626) $\text{digits}(2980, 10) = \langle 0, 8, 9, 2\rangle$.
(627) $\sum \text{digits}(2980, 10) = 19$. The theorem is a consequence of (626).
(628) $\text{digits}(3000, 10) = \langle 0, 0, 0, 3\rangle$.
(629) $\sum \text{digits}(3000, 10) = 3$. The theorem is a consequence of (628).
(630) $\text{digits}(3020, 10) = \langle 0, 2, 0, 3\rangle$.
(631) $\sum \text{digits}(3020, 10) = 5$. The theorem is a consequence of (630).
(632) $\text{digits}(3040, 10) = \langle 0, 4, 0, 3\rangle$.
(633) $\sum \text{digits}(3040, 10) = 7$. The theorem is a consequence of (632).
(634) $\text{digits}(3060, 10) = \langle 0, 6, 0, 3\rangle$.
(635) $\sum \text{digits}(3060, 10) = 9$. The theorem is a consequence of (634).
(636) $\text{digits}(3080, 10) = \langle 0, 8, 0, 3\rangle$.
(637) $\sum \text{digits}(3080, 10) = 11$. The theorem is a consequence of (636).
(638) $\text{digits}(3100, 10) = \langle 0, 0, 1, 3\rangle$.
(639) $\sum \text{digits}(3100, 10) = 4$. The theorem is a consequence of (638).
(640) $\text{digits}(3120, 10) = \langle 0, 2, 1, 3\rangle$.
(641) $\sum \text{digits}(3120, 10) = 6$. The theorem is a consequence of (640).
(642) $\text{digits}(3140, 10) = \langle 0, 4, 1, 3\rangle$.
(643) $\sum \text{digits}(3140, 10) = 8$. The theorem is a consequence of (642).
(644) $\text{digits}(3160, 10) = \langle 0, 6, 1, 3\rangle$.
(645) $\sum \text{digits}(3160, 10) = 10$. The theorem is a consequence of (644).
(646) $\text{digits}(3180, 10) = \langle 0, 8, 1, 3\rangle$.

(647) $\sum \mathrm{digits}(3180, 10) = 12$. The theorem is a consequence of (646).
(648) $\mathrm{digits}(3200, 10) = \langle 0, 0, 2, 3\rangle$.
(649) $\sum \mathrm{digits}(3200, 10) = 5$. The theorem is a consequence of (648).
(650) $\mathrm{digits}(3220, 10) = \langle 0, 2, 2, 3\rangle$.
(651) $\sum \mathrm{digits}(3220, 10) = 7$. The theorem is a consequence of (650).
(652) $\mathrm{digits}(3240, 10) = \langle 0, 4, 2, 3\rangle$.
(653) $\sum \mathrm{digits}(3240, 10) = 9$. The theorem is a consequence of (652).
(654) $\mathrm{digits}(3260, 10) = \langle 0, 6, 2, 3\rangle$.
(655) $\sum \mathrm{digits}(3260, 10) = 11$. The theorem is a consequence of (654).
(656) $\mathrm{digits}(3280, 10) = \langle 0, 8, 2, 3\rangle$.
(657) $\sum \mathrm{digits}(3280, 10) = 13$. The theorem is a consequence of (656).
(658) $\mathrm{digits}(3300, 10) = \langle 0, 0, 3, 3\rangle$.
(659) $\sum \mathrm{digits}(3300, 10) = 6$. The theorem is a consequence of (658).
(660) $\mathrm{digits}(3320, 10) = \langle 0, 2, 3, 3\rangle$.
(661) $\sum \mathrm{digits}(3320, 10) = 8$. The theorem is a consequence of (660).
(662) $\mathrm{digits}(3340, 10) = \langle 0, 4, 3, 3\rangle$.
(663) $\sum \mathrm{digits}(3340, 10) = 10$. The theorem is a consequence of (662).
(664) $\mathrm{digits}(3360, 10) = \langle 0, 6, 3, 3\rangle$.
(665) $\sum \mathrm{digits}(3360, 10) = 12$. The theorem is a consequence of (664).
(666) $\mathrm{digits}(3380, 10) = \langle 0, 8, 3, 3\rangle$.
(667) $\sum \mathrm{digits}(3380, 10) = 14$. The theorem is a consequence of (666).
(668) $\mathrm{digits}(3400, 10) = \langle 0, 0, 4, 3\rangle$.
(669) $\sum \mathrm{digits}(3400, 10) = 7$. The theorem is a consequence of (668).
(670) $\mathrm{digits}(3420, 10) = \langle 0, 2, 4, 3\rangle$.
(671) $\sum \mathrm{digits}(3420, 10) = 9$. The theorem is a consequence of (670).
(672) $\mathrm{digits}(3440, 10) = \langle 0, 4, 4, 3\rangle$.
(673) $\sum \mathrm{digits}(3440, 10) = 11$. The theorem is a consequence of (672).
(674) $\mathrm{digits}(3460, 10) = \langle 0, 6, 4, 3\rangle$.
(675) $\sum \mathrm{digits}(3460, 10) = 13$. The theorem is a consequence of (674).
(676) $\mathrm{digits}(3480, 10) = \langle 0, 8, 4, 3\rangle$.
(677) $\sum \mathrm{digits}(3480, 10) = 15$. The theorem is a consequence of (676).
(678) $\mathrm{digits}(3500, 10) = \langle 0, 0, 5, 3\rangle$.
(679) $\sum \mathrm{digits}(3500, 10) = 8$. The theorem is a consequence of (678).
(680) $\mathrm{digits}(3520, 10) = \langle 0, 2, 5, 3\rangle$.
(681) $\sum \mathrm{digits}(3520, 10) = 10$. The theorem is a consequence of (680).

(682) $\text{digits}(3540, 10) = \langle 0, 4, 5, 3\rangle$.
(683) $\sum \text{digits}(3540, 10) = 12$. The theorem is a consequence of (682).
(684) $\text{digits}(3560, 10) = \langle 0, 6, 5, 3\rangle$.
(685) $\sum \text{digits}(3560, 10) = 14$. The theorem is a consequence of (684).
(686) $\text{digits}(3580, 10) = \langle 0, 8, 5, 3\rangle$.
(687) $\sum \text{digits}(3580, 10) = 16$. The theorem is a consequence of (686).
(688) $\text{digits}(3600, 10) = \langle 0, 0, 6, 3\rangle$.
(689) $\sum \text{digits}(3600, 10) = 9$. The theorem is a consequence of (688).
(690) $\text{digits}(3620, 10) = \langle 0, 2, 6, 3\rangle$.
(691) $\sum \text{digits}(3620, 10) = 11$. The theorem is a consequence of (690).
(692) $\text{digits}(3640, 10) = \langle 0, 4, 6, 3\rangle$.
(693) $\sum \text{digits}(3640, 10) = 13$. The theorem is a consequence of (692).
(694) $\text{digits}(3660, 10) = \langle 0, 6, 6, 3\rangle$.
(695) $\sum \text{digits}(3660, 10) = 15$. The theorem is a consequence of (694).
(696) $\text{digits}(3680, 10) = \langle 0, 8, 6, 3\rangle$.
(697) $\sum \text{digits}(3680, 10) = 17$. The theorem is a consequence of (696).
(698) $\text{digits}(3700, 10) = \langle 0, 0, 7, 3\rangle$.
(699) $\sum \text{digits}(3700, 10) = 10$. The theorem is a consequence of (698).
(700) $\text{digits}(3720, 10) = \langle 0, 2, 7, 3\rangle$.
(701) $\sum \text{digits}(3720, 10) = 12$. The theorem is a consequence of (700).
(702) $\text{digits}(3740, 10) = \langle 0, 4, 7, 3\rangle$.
(703) $\sum \text{digits}(3740, 10) = 14$. The theorem is a consequence of (702).
(704) $\text{digits}(3760, 10) = \langle 0, 6, 7, 3\rangle$.
(705) $\sum \text{digits}(3760, 10) = 16$. The theorem is a consequence of (704).
(706) $\text{digits}(3780, 10) = \langle 0, 8, 7, 3\rangle$.
(707) $\sum \text{digits}(3780, 10) = 18$. The theorem is a consequence of (706).
(708) $\text{digits}(3800, 10) = \langle 0, 0, 8, 3\rangle$.
(709) $\sum \text{digits}(3800, 10) = 11$. The theorem is a consequence of (708).
(710) $\text{digits}(3820, 10) = \langle 0, 2, 8, 3\rangle$.
(711) $\sum \text{digits}(3820, 10) = 13$. The theorem is a consequence of (710).
(712) $\text{digits}(3840, 10) = \langle 0, 4, 8, 3\rangle$.
(713) $\sum \text{digits}(3840, 10) = 15$. The theorem is a consequence of (712).
(714) $\text{digits}(3860, 10) = \langle 0, 6, 8, 3\rangle$.
(715) $\sum \text{digits}(3860, 10) = 17$. The theorem is a consequence of (714).
(716) $\text{digits}(3880, 10) = \langle 0, 8, 8, 3\rangle$.

(717) $\sum \mathrm{digits}(3880, 10) = 19$. The theorem is a consequence of (716).

(718) $\mathrm{digits}(3900, 10) = \langle 0, 0, 9, 3 \rangle$.

(719) $\sum \mathrm{digits}(3900, 10) = 12$. The theorem is a consequence of (718).

(720) $\mathrm{digits}(3920, 10) = \langle 0, 2, 9, 3 \rangle$.

(721) $\sum \mathrm{digits}(3920, 10) = 14$. The theorem is a consequence of (720).

(722) $\mathrm{digits}(3940, 10) = \langle 0, 4, 9, 3 \rangle$.

(723) $\sum \mathrm{digits}(3940, 10) = 16$. The theorem is a consequence of (722).

(724) $\mathrm{digits}(3960, 10) = \langle 0, 6, 9, 3 \rangle$.

(725) $\sum \mathrm{digits}(3960, 10) = 18$. The theorem is a consequence of (724).

(726) $\mathrm{digits}(3980, 10) = \langle 0, 8, 9, 3 \rangle$.

(727) $\sum \mathrm{digits}(3980, 10) = 20$. The theorem is a consequence of (726).

(728) 3980 is the solution to Sierpiński's problem 36 for 20. The theorem is a consequence of (727), (6), (19), (23), (27), (31), (35), (39), (43), (47), (51), (361), (363), (193), (365), (367), (369), (203), (250), (371), (306), (213), (373), (375), (377), (379), (381), (383), (385), (387), (389), (391), (393), (395), (397), (399), (401), (403), (405), (346), (407), (409), (411), (413), (415), (417), (419), (421), (423), (425), (427), (429), (431), (433), (435), (437), (439), (441), (443), (445), (447), (449), (451), (453), (455), (457), (459), (461), (463), (465), (467), (469), (471), (473), (475), (477), (479), (481), (483), (485), (487), (489), (491), (493), (495), (497), (499), (501), (503), (505), (507), (509), (511), (513), (515), (517), (519), (521), (523), (525), (527), (529), (531), (533), (535), (537), (539), (541), (543), (545), (547), (549), (551), (553), (555), (557), (559), (561), (563), (565), (567), (569), (571), (573), (575), (577), (579), (581), (583), (585), (587), (589), (591), (593), (595), (597), (599), (601), (603), (605), (607), (609), (611), (613), (615), (617), (619), (621), (623), (625), (627), (629), (631), (633), (635), (637), (639), (641), (643), (645), (647), (649), (651), (653), (655), (657), (659), (661), (663), (665), (667), (669), (671), (673), (675), (677), (679), (681), (683), (685), (687), (689), (691), (693), (695), (697), (699), (701), (703), (705), (707), (709), (711), (713), (715), (717), (719), (721), (723), and (725).

14. PROBLEM 36 FOR $s = 21$

Now we state the propositions:

(729) $\mathrm{digits}(21, 10) = \langle 1, 2\rangle$.

(730) $\sum \mathrm{digits}(21, 10) = 3$. The theorem is a consequence of (729).

(731) $\mathrm{digits}(63, 10) = \langle 3, 6\rangle$.

(732) $\sum \mathrm{digits}(63, 10) = 9$. The theorem is a consequence of (731).

(733) $\mathrm{digits}(147, 10) = \langle 7, 4, 1\rangle$.

(734) $\sum \mathrm{digits}(147, 10) = 12$. The theorem is a consequence of (733).

(735) $\mathrm{digits}(189, 10) = \langle 9, 8, 1\rangle$.

(736) $\sum \mathrm{digits}(189, 10) = 18$. The theorem is a consequence of (735).

(737) $\mathrm{digits}(231, 10) = \langle 1, 3, 2\rangle$.

(738) $\sum \mathrm{digits}(231, 10) = 6$. The theorem is a consequence of (737).

(739) $\mathrm{digits}(273, 10) = \langle 3, 7, 2\rangle$.

(740) $\sum \mathrm{digits}(273, 10) = 12$. The theorem is a consequence of (739).

(741) $\mathrm{digits}(294, 10) = \langle 4, 9, 2\rangle$.

(742) $\sum \mathrm{digits}(294, 10) = 15$. The theorem is a consequence of (741).

(743) $\mathrm{digits}(315, 10) = \langle 5, 1, 3\rangle$.

(744) $\sum \mathrm{digits}(315, 10) = 9$. The theorem is a consequence of (743).

(745) $\mathrm{digits}(378, 10) = \langle 8, 7, 3\rangle$.

(746) $\sum \mathrm{digits}(378, 10) = 18$. The theorem is a consequence of (745).

(747) 399 is the solution to Sierpiński's problem 36 for 21. The theorem is a consequence of (308), (6), (730), (141), (732), (145), (174), (151), (734), (153), (736), (157), (738), (163), (740), (742), (744), (205), (252), and (746).

15. PROBLEM 36 FOR $s = 22$

Now we state the propositions:

(748) $\mathrm{digits}(242, 10) = \langle 2, 4, 2\rangle$.

(749) $\sum \mathrm{digits}(242, 10) = 8$. The theorem is a consequence of (748).

(750) $\mathrm{digits}(264, 10) = \langle 4, 6, 2\rangle$.

(751) $\sum \mathrm{digits}(264, 10) = 12$. The theorem is a consequence of (750).

(752) $\mathrm{digits}(286, 10) = \langle 6, 8, 2\rangle$.

(753) $\sum \mathrm{digits}(286, 10) = 16$. The theorem is a consequence of (752).

(754) $\mathrm{digits}(308, 10) = \langle 8, 0, 3\rangle$.

(755) $\sum \mathrm{digits}(308, 10) = 11$. The theorem is a consequence of (754).
(756) $\mathrm{digits}(330, 10) = \langle 0, 3, 3\rangle$.
(757) $\sum \mathrm{digits}(330, 10) = 6$. The theorem is a consequence of (756).
(758) $\mathrm{digits}(396, 10) = \langle 6, 9, 3\rangle$.
(759) $\sum \mathrm{digits}(396, 10) = 18$. The theorem is a consequence of (758).
(760) $\mathrm{digits}(462, 10) = \langle 2, 6, 4\rangle$.
(761) $\sum \mathrm{digits}(462, 10) = 12$. The theorem is a consequence of (760).
(762) $\mathrm{digits}(484, 10) = \langle 4, 8, 4\rangle$.
(763) $\sum \mathrm{digits}(484, 10) = 16$. The theorem is a consequence of (762).
(764) $\mathrm{digits}(506, 10) = \langle 6, 0, 5\rangle$.
(765) $\sum \mathrm{digits}(506, 10) = 11$. The theorem is a consequence of (764).
(766) $\mathrm{digits}(528, 10) = \langle 8, 2, 5\rangle$.
(767) $\sum \mathrm{digits}(528, 10) = 15$. The theorem is a consequence of (766).
(768) $\mathrm{digits}(550, 10) = \langle 0, 5, 5\rangle$.
(769) $\sum \mathrm{digits}(550, 10) = 10$. The theorem is a consequence of (768).
(770) $\mathrm{digits}(572, 10) = \langle 2, 7, 5\rangle$.
(771) $\sum \mathrm{digits}(572, 10) = 14$. The theorem is a consequence of (770).
(772) $\mathrm{digits}(594, 10) = \langle 4, 9, 5\rangle$.
(773) $\sum \mathrm{digits}(594, 10) = 18$. The theorem is a consequence of (772).
(774) $\mathrm{digits}(616, 10) = \langle 6, 1, 6\rangle$.
(775) $\sum \mathrm{digits}(616, 10) = 13$. The theorem is a consequence of (774).
(776) $\mathrm{digits}(638, 10) = \langle 8, 3, 6\rangle$.
(777) $\sum \mathrm{digits}(638, 10) = 17$. The theorem is a consequence of (776).
(778) $\mathrm{digits}(682, 10) = \langle 2, 8, 6\rangle$.
(779) $\sum \mathrm{digits}(682, 10) = 16$. The theorem is a consequence of (778).
(780) $\mathrm{digits}(704, 10) = \langle 4, 0, 7\rangle$.
(781) $\sum \mathrm{digits}(704, 10) = 11$. The theorem is a consequence of (780).
(782) $\mathrm{digits}(726, 10) = \langle 6, 2, 7\rangle$.
(783) $\sum \mathrm{digits}(726, 10) = 15$. The theorem is a consequence of (782).
(784) $\mathrm{digits}(748, 10) = \langle 8, 4, 7\rangle$.
(785) $\sum \mathrm{digits}(748, 10) = 19$. The theorem is a consequence of (784).
(786) $\mathrm{digits}(770, 10) = \langle 0, 7, 7\rangle$.
(787) $\sum \mathrm{digits}(770, 10) = 14$. The theorem is a consequence of (786).
(788) $\mathrm{digits}(792, 10) = \langle 2, 9, 7\rangle$.
(789) $\sum \mathrm{digits}(792, 10) = 18$. The theorem is a consequence of (788).

(790) $\text{digits}(814, 10) = \langle 4, 1, 8\rangle$.

(791) $\sum \text{digits}(814, 10) = 13$. The theorem is a consequence of (790).

(792) $\text{digits}(858, 10) = \langle 8, 5, 8\rangle$.

(793) $\sum \text{digits}(858, 10) = 21$. The theorem is a consequence of (792).

(794) $\text{digits}(902, 10) = \langle 2, 0, 9\rangle$.

(795) $\sum \text{digits}(902, 10) = 11$. The theorem is a consequence of (794).

(796) $\text{digits}(924, 10) = \langle 4, 2, 9\rangle$.

(797) $\sum \text{digits}(924, 10) = 15$. The theorem is a consequence of (796).

(798) $\text{digits}(946, 10) = \langle 6, 4, 9\rangle$.

(799) $\sum \text{digits}(946, 10) = 19$. The theorem is a consequence of (798).

(800) $\text{digits}(968, 10) = \langle 8, 6, 9\rangle$.

(801) $\sum \text{digits}(968, 10) = 23$. The theorem is a consequence of (800).

(802) $\text{digits}(990, 10) = \langle 0, 9, 9\rangle$.

(803) $\sum \text{digits}(990, 10) = 18$. The theorem is a consequence of (802).

(804) $\text{digits}(1012, 10) = \langle 2, 1, 0, 1\rangle$.

(805) $\sum \text{digits}(1012, 10) = 4$. The theorem is a consequence of (804).

(806) $\text{digits}(1034, 10) = \langle 4, 3, 0, 1\rangle$.

(807) $\sum \text{digits}(1034, 10) = 8$. The theorem is a consequence of (806).

(808) $\text{digits}(1056, 10) = \langle 6, 5, 0, 1\rangle$.

(809) $\sum \text{digits}(1056, 10) = 12$. The theorem is a consequence of (808).

(810) $\text{digits}(1078, 10) = \langle 8, 7, 0, 1\rangle$.

(811) $\sum \text{digits}(1078, 10) = 16$. The theorem is a consequence of (810).

(812) $\text{digits}(1122, 10) = \langle 2, 2, 1, 1\rangle$.

(813) $\sum \text{digits}(1122, 10) = 6$. The theorem is a consequence of (812).

(814) $\text{digits}(1144, 10) = \langle 4, 4, 1, 1\rangle$.

(815) $\sum \text{digits}(1144, 10) = 10$. The theorem is a consequence of (814).

(816) $\text{digits}(1166, 10) = \langle 6, 6, 1, 1\rangle$.

(817) $\sum \text{digits}(1166, 10) = 14$. The theorem is a consequence of (816).

(818) $\text{digits}(1188, 10) = \langle 8, 8, 1, 1\rangle$.

(819) $\sum \text{digits}(1188, 10) = 18$. The theorem is a consequence of (818).

(820) $\text{digits}(1210, 10) = \langle 0, 1, 2, 1\rangle$.

(821) $\sum \text{digits}(1210, 10) = 4$. The theorem is a consequence of (820).

(822) $\text{digits}(1232, 10) = \langle 2, 3, 2, 1\rangle$.

(823) $\sum \text{digits}(1232, 10) = 8$. The theorem is a consequence of (822).

(824) $\text{digits}(1254, 10) = \langle 4, 5, 2, 1\rangle$.

(825) $\sum \mathrm{digits}(1254, 10) = 12$. The theorem is a consequence of (824).
(826) $\mathrm{digits}(1276, 10) = \langle 6, 7, 2, 1\rangle$.
(827) $\sum \mathrm{digits}(1276, 10) = 16$. The theorem is a consequence of (826).
(828) $\mathrm{digits}(1298, 10) = \langle 8, 9, 2, 1\rangle$.
(829) $\sum \mathrm{digits}(1298, 10) = 20$. The theorem is a consequence of (828).
(830) $\mathrm{digits}(1342, 10) = \langle 2, 4, 3, 1\rangle$.
(831) $\sum \mathrm{digits}(1342, 10) = 10$. The theorem is a consequence of (830).
(832) $\mathrm{digits}(1364, 10) = \langle 4, 6, 3, 1\rangle$.
(833) $\sum \mathrm{digits}(1364, 10) = 14$. The theorem is a consequence of (832).
(834) $\mathrm{digits}(1386, 10) = \langle 6, 8, 3, 1\rangle$.
(835) $\sum \mathrm{digits}(1386, 10) = 18$. The theorem is a consequence of (834).
(836) $\mathrm{digits}(1408, 10) = \langle 8, 0, 4, 1\rangle$.
(837) $\sum \mathrm{digits}(1408, 10) = 13$. The theorem is a consequence of (836).
(838) $\mathrm{digits}(1430, 10) = \langle 0, 3, 4, 1\rangle$.
(839) $\sum \mathrm{digits}(1430, 10) = 8$. The theorem is a consequence of (838).
(840) $\mathrm{digits}(1452, 10) = \langle 2, 5, 4, 1\rangle$.
(841) $\sum \mathrm{digits}(1452, 10) = 12$. The theorem is a consequence of (840).
(842) $\mathrm{digits}(1474, 10) = \langle 4, 7, 4, 1\rangle$.
(843) $\sum \mathrm{digits}(1474, 10) = 16$. The theorem is a consequence of (842).
(844) $\mathrm{digits}(1496, 10) = \langle 6, 9, 4, 1\rangle$.
(845) $\sum \mathrm{digits}(1496, 10) = 20$. The theorem is a consequence of (844).
(846) $\mathrm{digits}(1518, 10) = \langle 8, 1, 5, 1\rangle$.
(847) $\sum \mathrm{digits}(1518, 10) = 15$. The theorem is a consequence of (846).
(848) $\mathrm{digits}(1562, 10) = \langle 2, 6, 5, 1\rangle$.
(849) $\sum \mathrm{digits}(1562, 10) = 14$. The theorem is a consequence of (848).
(850) $\mathrm{digits}(1584, 10) = \langle 4, 8, 5, 1\rangle$.
(851) $\sum \mathrm{digits}(1584, 10) = 18$. The theorem is a consequence of (850).
(852) $\mathrm{digits}(1606, 10) = \langle 6, 0, 6, 1\rangle$.
(853) $\sum \mathrm{digits}(1606, 10) = 13$. The theorem is a consequence of (852).
(854) $\mathrm{digits}(1628, 10) = \langle 8, 2, 6, 1\rangle$.
(855) $\sum \mathrm{digits}(1628, 10) = 17$. The theorem is a consequence of (854).
(856) $\mathrm{digits}(1650, 10) = \langle 0, 5, 6, 1\rangle$.
(857) $\sum \mathrm{digits}(1650, 10) = 12$. The theorem is a consequence of (856).
(858) $\mathrm{digits}(1672, 10) = \langle 2, 7, 6, 1\rangle$.
(859) $\sum \mathrm{digits}(1672, 10) = 16$. The theorem is a consequence of (858).

(860) $\text{digits}(1694, 10) = \langle 4, 9, 6, 1\rangle$.
(861) $\sum \text{digits}(1694, 10) = 20$. The theorem is a consequence of (860).
(862) $\text{digits}(1716, 10) = \langle 6, 1, 7, 1\rangle$.
(863) $\sum \text{digits}(1716, 10) = 15$. The theorem is a consequence of (862).
(864) $\text{digits}(1738, 10) = \langle 8, 3, 7, 1\rangle$.
(865) $\sum \text{digits}(1738, 10) = 19$. The theorem is a consequence of (864).
(866) $\text{digits}(1782, 10) = \langle 2, 8, 7, 1\rangle$.
(867) $\sum \text{digits}(1782, 10) = 18$. The theorem is a consequence of (866).
(868) $\text{digits}(1804, 10) = \langle 4, 0, 8, 1\rangle$.
(869) $\sum \text{digits}(1804, 10) = 13$. The theorem is a consequence of (868).
(870) $\text{digits}(1826, 10) = \langle 6, 2, 8, 1\rangle$.
(871) $\sum \text{digits}(1826, 10) = 17$. The theorem is a consequence of (870).
(872) $\text{digits}(1848, 10) = \langle 8, 4, 8, 1\rangle$.
(873) $\sum \text{digits}(1848, 10) = 21$. The theorem is a consequence of (872).
(874) $\text{digits}(1870, 10) = \langle 0, 7, 8, 1\rangle$.
(875) $\sum \text{digits}(1870, 10) = 16$. The theorem is a consequence of (874).
(876) $\text{digits}(1892, 10) = \langle 2, 9, 8, 1\rangle$.
(877) $\sum \text{digits}(1892, 10) = 20$. The theorem is a consequence of (876).
(878) $\text{digits}(1914, 10) = \langle 4, 1, 9, 1\rangle$.
(879) $\sum \text{digits}(1914, 10) = 15$. The theorem is a consequence of (878).
(880) $\text{digits}(1936, 10) = \langle 6, 3, 9, 1\rangle$.
(881) $\sum \text{digits}(1936, 10) = 19$. The theorem is a consequence of (880).
(882) $\text{digits}(1958, 10) = \langle 8, 5, 9, 1\rangle$.
(883) $\sum \text{digits}(1958, 10) = 23$. The theorem is a consequence of (882).
(884) $\text{digits}(2002, 10) = \langle 2, 0, 0, 2\rangle$.
(885) $\sum \text{digits}(2002, 10) = 4$. The theorem is a consequence of (884).
(886) $\text{digits}(2024, 10) = \langle 4, 2, 0, 2\rangle$.
(887) $\sum \text{digits}(2024, 10) = 8$. The theorem is a consequence of (886).
(888) $\text{digits}(2046, 10) = \langle 6, 4, 0, 2\rangle$.
(889) $\sum \text{digits}(2046, 10) = 12$. The theorem is a consequence of (888).
(890) $\text{digits}(2068, 10) = \langle 8, 6, 0, 2\rangle$.
(891) $\sum \text{digits}(2068, 10) = 16$. The theorem is a consequence of (890).
(892) $\text{digits}(2090, 10) = \langle 0, 9, 0, 2\rangle$.
(893) $\sum \text{digits}(2090, 10) = 11$. The theorem is a consequence of (892).
(894) $\text{digits}(2112, 10) = \langle 2, 1, 1, 2\rangle$.

(895) $\sum \mathrm{digits}(2112, 10) = 6$. The theorem is a consequence of (894).

(896) $\mathrm{digits}(2134, 10) = \langle 4, 3, 1, 2 \rangle$.

(897) $\sum \mathrm{digits}(2134, 10) = 10$. The theorem is a consequence of (896).

(898) $\mathrm{digits}(2156, 10) = \langle 6, 5, 1, 2 \rangle$.

(899) $\sum \mathrm{digits}(2156, 10) = 14$. The theorem is a consequence of (898).

(900) $\mathrm{digits}(2178, 10) = \langle 8, 7, 1, 2 \rangle$.

(901) $\sum \mathrm{digits}(2178, 10) = 18$. The theorem is a consequence of (900).

(902) $\mathrm{digits}(2222, 10) = \langle 2, 2, 2, 2 \rangle$.

(903) $\sum \mathrm{digits}(2222, 10) = 8$. The theorem is a consequence of (902).

(904) $\mathrm{digits}(2244, 10) = \langle 4, 4, 2, 2 \rangle$.

(905) $\sum \mathrm{digits}(2244, 10) = 12$. The theorem is a consequence of (904).

(906) $\mathrm{digits}(2266, 10) = \langle 6, 6, 2, 2 \rangle$.

(907) $\sum \mathrm{digits}(2266, 10) = 16$. The theorem is a consequence of (906).

(908) $\mathrm{digits}(2288, 10) = \langle 8, 8, 2, 2 \rangle$.

(909) $\sum \mathrm{digits}(2288, 10) = 20$. The theorem is a consequence of (908).

(910) $\mathrm{digits}(2310, 10) = \langle 0, 1, 3, 2 \rangle$.

(911) $\sum \mathrm{digits}(2310, 10) = 6$. The theorem is a consequence of (910).

(912) $\mathrm{digits}(2332, 10) = \langle 2, 3, 3, 2 \rangle$.

(913) $\sum \mathrm{digits}(2332, 10) = 10$. The theorem is a consequence of (912).

(914) $\mathrm{digits}(2354, 10) = \langle 4, 5, 3, 2 \rangle$.

(915) $\sum \mathrm{digits}(2354, 10) = 14$. The theorem is a consequence of (914).

(916) $\mathrm{digits}(2376, 10) = \langle 6, 7, 3, 2 \rangle$.

(917) $\sum \mathrm{digits}(2376, 10) = 18$. The theorem is a consequence of (916).

(918) $\mathrm{digits}(2398, 10) = \langle 8, 9, 3, 2 \rangle$.

(919) $\sum \mathrm{digits}(2398, 10) = 22$. The theorem is a consequence of (918).

(920) 2398 is the solution to Sierpiński's problem 36 for 22. The theorem is a consequence of (919), (6), (58), (62), (66), (70), (37), (76), (80), (84), (88), (363), (749), (751), (753), (755), (757), (207), (254), (759), (310), (375), (761), (763), (765), (767), (769), (771), (773), (775), (777), (397), (779), (781), (783), (785), (787), (789), (791), (354), (793), (417), (795), (797), (799), (801), (803), (805), (807), (809), (811), (439), (813), (815), (817), (819), (821), (823), (825), (827), (829), (461), (831), (833), (835), (837), (839), (841), (843), (845), (847), (483), (849), (851), (853), (855), (857), (859), (861), (863), (865), (505), (867), (869), (871), (873), (875), (877), (879), (881), (883), (527), (885), (887), (889), (891), (893), (895),

(897), (899), (901), (549), (903), (905), (907), (909), (911), (913), (915), and (917).

16. PROBLEM 36 FOR $s = 23$

Now we state the propositions:

(921) $\text{digits}(23, 10) = \langle 3, 2\rangle$.

(922) $\sum \text{digits}(23, 10) = 5$. The theorem is a consequence of (921).

(923) $\text{digits}(46, 10) = \langle 6, 4\rangle$.

(924) $\sum \text{digits}(46, 10) = 10$. The theorem is a consequence of (923).

(925) $\text{digits}(69, 10) = \langle 9, 6\rangle$.

(926) $\sum \text{digits}(69, 10) = 15$. The theorem is a consequence of (925).

(927) $\text{digits}(92, 10) = \langle 2, 9\rangle$.

(928) $\sum \text{digits}(92, 10) = 11$. The theorem is a consequence of (927).

(929) $\text{digits}(115, 10) = \langle 5, 1, 1\rangle$.

(930) $\sum \text{digits}(115, 10) = 7$. The theorem is a consequence of (929).

(931) $\text{digits}(138, 10) = \langle 8, 3, 1\rangle$.

(932) $\sum \text{digits}(138, 10) = 12$. The theorem is a consequence of (931).

(933) $\text{digits}(161, 10) = \langle 1, 6, 1\rangle$.

(934) $\sum \text{digits}(161, 10) = 8$. The theorem is a consequence of (933).

(935) $\text{digits}(184, 10) = \langle 4, 8, 1\rangle$.

(936) $\sum \text{digits}(184, 10) = 13$. The theorem is a consequence of (935).

(937) $\text{digits}(207, 10) = \langle 7, 0, 2\rangle$.

(938) $\sum \text{digits}(207, 10) = 9$. The theorem is a consequence of (937).

(939) $\text{digits}(230, 10) = \langle 0, 3, 2\rangle$.

(940) $\sum \text{digits}(230, 10) = 5$. The theorem is a consequence of (939).

(941) $\text{digits}(253, 10) = \langle 3, 5, 2\rangle$.

(942) $\sum \text{digits}(253, 10) = 10$. The theorem is a consequence of (941).

(943) $\text{digits}(276, 10) = \langle 6, 7, 2\rangle$.

(944) $\sum \text{digits}(276, 10) = 15$. The theorem is a consequence of (943).

(945) $\text{digits}(299, 10) = \langle 9, 9, 2\rangle$.

(946) $\sum \text{digits}(299, 10) = 20$. The theorem is a consequence of (945).

(947) $\text{digits}(322, 10) = \langle 2, 2, 3\rangle$.

(948) $\sum \text{digits}(322, 10) = 7$. The theorem is a consequence of (947).

(949) $\text{digits}(345, 10) = \langle 5, 4, 3\rangle$.

(950) $\sum \mathrm{digits}(345, 10) = 12$. The theorem is a consequence of (949).
(951) $\mathrm{digits}(414, 10) = \langle 4, 1, 4 \rangle$.
(952) $\sum \mathrm{digits}(414, 10) = 9$. The theorem is a consequence of (951).
(953) $\mathrm{digits}(483, 10) = \langle 3, 8, 4 \rangle$.
(954) $\sum \mathrm{digits}(483, 10) = 15$. The theorem is a consequence of (953).
(955) $\mathrm{digits}(529, 10) = \langle 9, 2, 5 \rangle$.
(956) $\sum \mathrm{digits}(529, 10) = 16$. The theorem is a consequence of (955).
(957) $\mathrm{digits}(552, 10) = \langle 2, 5, 5 \rangle$.
(958) $\sum \mathrm{digits}(552, 10) = 12$. The theorem is a consequence of (957).
(959) $\mathrm{digits}(575, 10) = \langle 5, 7, 5 \rangle$.
(960) $\sum \mathrm{digits}(575, 10) = 17$. The theorem is a consequence of (959).
(961) $\mathrm{digits}(598, 10) = \langle 8, 9, 5 \rangle$.
(962) $\sum \mathrm{digits}(598, 10) = 22$. The theorem is a consequence of (961).
(963) $\mathrm{digits}(621, 10) = \langle 1, 2, 6 \rangle$.
(964) $\sum \mathrm{digits}(621, 10) = 9$. The theorem is a consequence of (963).
(965) $\mathrm{digits}(644, 10) = \langle 4, 4, 6 \rangle$.
(966) $\sum \mathrm{digits}(644, 10) = 14$. The theorem is a consequence of (965).
(967) $\mathrm{digits}(667, 10) = \langle 7, 6, 6 \rangle$.
(968) $\sum \mathrm{digits}(667, 10) = 19$. The theorem is a consequence of (967).
(969) $\mathrm{digits}(690, 10) = \langle 0, 9, 6 \rangle$.
(970) $\sum \mathrm{digits}(690, 10) = 15$. The theorem is a consequence of (969).
(971) $\mathrm{digits}(713, 10) = \langle 3, 1, 7 \rangle$.
(972) $\sum \mathrm{digits}(713, 10) = 11$. The theorem is a consequence of (971).
(973) $\mathrm{digits}(736, 10) = \langle 6, 3, 7 \rangle$.
(974) $\sum \mathrm{digits}(736, 10) = 16$. The theorem is a consequence of (973).
(975) $\mathrm{digits}(759, 10) = \langle 9, 5, 7 \rangle$.
(976) $\sum \mathrm{digits}(759, 10) = 21$. The theorem is a consequence of (975).
(977) $\mathrm{digits}(782, 10) = \langle 2, 8, 7 \rangle$.
(978) $\sum \mathrm{digits}(782, 10) = 17$. The theorem is a consequence of (977).
(979) $\mathrm{digits}(805, 10) = \langle 5, 0, 8 \rangle$.
(980) $\sum \mathrm{digits}(805, 10) = 13$. The theorem is a consequence of (979).
(981) $\mathrm{digits}(828, 10) = \langle 8, 2, 8 \rangle$.
(982) $\sum \mathrm{digits}(828, 10) = 18$. The theorem is a consequence of (981).
(983) $\mathrm{digits}(851, 10) = \langle 1, 5, 8 \rangle$.
(984) $\sum \mathrm{digits}(851, 10) = 14$. The theorem is a consequence of (983).

(985) $\text{digits}(897, 10) = \langle 7, 9, 8\rangle$.
(986) $\sum \text{digits}(897, 10) = 24$. The theorem is a consequence of (985).
(987) $\text{digits}(943, 10) = \langle 3, 4, 9\rangle$.
(988) $\sum \text{digits}(943, 10) = 16$. The theorem is a consequence of (987).
(989) $\text{digits}(966, 10) = \langle 6, 6, 9\rangle$.
(990) $\sum \text{digits}(966, 10) = 21$. The theorem is a consequence of (989).
(991) $\text{digits}(989, 10) = \langle 9, 8, 9\rangle$.
(992) $\sum \text{digits}(989, 10) = 26$. The theorem is a consequence of (991).
(993) $\text{digits}(1035, 10) = \langle 5, 3, 0, 1\rangle$.
(994) $\sum \text{digits}(1035, 10) = 9$. The theorem is a consequence of (993).
(995) $\text{digits}(1058, 10) = \langle 8, 5, 0, 1\rangle$.
(996) $\sum \text{digits}(1058, 10) = 14$. The theorem is a consequence of (995).
(997) $\text{digits}(1081, 10) = \langle 1, 8, 0, 1\rangle$.
(998) $\sum \text{digits}(1081, 10) = 10$. The theorem is a consequence of (997).
(999) $\text{digits}(1104, 10) = \langle 4, 0, 1, 1\rangle$.
(1000) $\sum \text{digits}(1104, 10) = 6$. The theorem is a consequence of (999).
(1001) $\text{digits}(1127, 10) = \langle 7, 2, 1, 1\rangle$.
(1002) $\sum \text{digits}(1127, 10) = 11$. The theorem is a consequence of (1001).
(1003) $\text{digits}(1150, 10) = \langle 0, 5, 1, 1\rangle$.
(1004) $\sum \text{digits}(1150, 10) = 7$. The theorem is a consequence of (1003).
(1005) $\text{digits}(1173, 10) = \langle 3, 7, 1, 1\rangle$.
(1006) $\sum \text{digits}(1173, 10) = 12$. The theorem is a consequence of (1005).
(1007) $\text{digits}(1196, 10) = \langle 6, 9, 1, 1\rangle$.
(1008) $\sum \text{digits}(1196, 10) = 17$. The theorem is a consequence of (1007).
(1009) $\text{digits}(1219, 10) = \langle 9, 1, 2, 1\rangle$.
(1010) $\sum \text{digits}(1219, 10) = 13$. The theorem is a consequence of (1009).
(1011) $\text{digits}(1242, 10) = \langle 2, 4, 2, 1\rangle$.
(1012) $\sum \text{digits}(1242, 10) = 9$. The theorem is a consequence of (1011).
(1013) $\text{digits}(1265, 10) = \langle 5, 6, 2, 1\rangle$.
(1014) $\sum \text{digits}(1265, 10) = 14$. The theorem is a consequence of (1013).
(1015) $\text{digits}(1288, 10) = \langle 8, 8, 2, 1\rangle$.
(1016) $\sum \text{digits}(1288, 10) = 19$. The theorem is a consequence of (1015).
(1017) $\text{digits}(1311, 10) = \langle 1, 1, 3, 1\rangle$.
(1018) $\sum \text{digits}(1311, 10) = 6$. The theorem is a consequence of (1017).
(1019) $\text{digits}(1334, 10) = \langle 4, 3, 3, 1\rangle$.

(1020) $\sum \mathrm{digits}(1334, 10) = 11$. The theorem is a consequence of (1019).

(1021) $\mathrm{digits}(1357, 10) = \langle 7, 5, 3, 1\rangle$.

(1022) $\sum \mathrm{digits}(1357, 10) = 16$. The theorem is a consequence of (1021).

(1023) $\mathrm{digits}(1403, 10) = \langle 3, 0, 4, 1\rangle$.

(1024) $\sum \mathrm{digits}(1403, 10) = 8$. The theorem is a consequence of (1023).

(1025) $\mathrm{digits}(1426, 10) = \langle 6, 2, 4, 1\rangle$.

(1026) $\sum \mathrm{digits}(1426, 10) = 13$. The theorem is a consequence of (1025).

(1027) $\mathrm{digits}(1449, 10) = \langle 9, 4, 4, 1\rangle$.

(1028) $\sum \mathrm{digits}(1449, 10) = 18$. The theorem is a consequence of (1027).

(1029) $\mathrm{digits}(1472, 10) = \langle 2, 7, 4, 1\rangle$.

(1030) $\sum \mathrm{digits}(1472, 10) = 14$. The theorem is a consequence of (1029).

(1031) $\mathrm{digits}(1495, 10) = \langle 5, 9, 4, 1\rangle$.

(1032) $\sum \mathrm{digits}(1495, 10) = 19$. The theorem is a consequence of (1031).

(1033) $\mathrm{digits}(1541, 10) = \langle 1, 4, 5, 1\rangle$.

(1034) $\sum \mathrm{digits}(1541, 10) = 11$. The theorem is a consequence of (1033).

(1035) $\mathrm{digits}(1564, 10) = \langle 4, 6, 5, 1\rangle$.

(1036) $\sum \mathrm{digits}(1564, 10) = 16$. The theorem is a consequence of (1035).

(1037) $\mathrm{digits}(1587, 10) = \langle 7, 8, 5, 1\rangle$.

(1038) $\sum \mathrm{digits}(1587, 10) = 21$. The theorem is a consequence of (1037).

(1039) $\mathrm{digits}(1610, 10) = \langle 0, 1, 6, 1\rangle$.

(1040) $\sum \mathrm{digits}(1610, 10) = 8$. The theorem is a consequence of (1039).

(1041) $\mathrm{digits}(1633, 10) = \langle 3, 3, 6, 1\rangle$.

(1042) $\sum \mathrm{digits}(1633, 10) = 13$. The theorem is a consequence of (1041).

(1043) $\mathrm{digits}(1656, 10) = \langle 6, 5, 6, 1\rangle$.

(1044) $\sum \mathrm{digits}(1656, 10) = 18$. The theorem is a consequence of (1043).

(1045) $\mathrm{digits}(1679, 10) = \langle 9, 7, 6, 1\rangle$.

(1046) $\sum \mathrm{digits}(1679, 10) = 23$. The theorem is a consequence of (1045).

(1047) 1679 is the solution to Sierpiński's problem 36 for 23. The theorem is a consequence of (1046), (6), (922), (924), (926), (928), (930), (932), (934), (936), (938), (940), (942), (944), (946), (948), (950), (209), (256), (952), (312), (377), (954), (765), (956), (958), (960), (962), (964), (966), (968), (970), (972), (974), (976), (978), (980), (982), (984), (358), (986), (421), (988), (990), (992), (805), (994), (996), (998), (1000), (1002), (1004), (1006), (1008), (1010), (1012), (1014), (1016), (1018), (1020), (1022), (467), (1024), (1026), (1028), (1030), (1032), (847), (1034), (1036), (1038), (1040), (1042), and (1044).

17. PROBLEM 36 FOR $s = 24$

Now we state the propositions:

(1048) $\text{digits}(216, 10) = \langle 6, 1, 2\rangle$.

(1049) $\sum \text{digits}(216, 10) = 9$. The theorem is a consequence of (1048).

(1050) $\text{digits}(312, 10) = \langle 2, 1, 3\rangle$.

(1051) $\sum \text{digits}(312, 10) = 6$. The theorem is a consequence of (1050).

(1052) $\text{digits}(504, 10) = \langle 4, 0, 5\rangle$.

(1053) $\sum \text{digits}(504, 10) = 9$. The theorem is a consequence of (1052).

(1054) $\text{digits}(576, 10) = \langle 6, 7, 5\rangle$.

(1055) $\sum \text{digits}(576, 10) = 18$. The theorem is a consequence of (1054).

(1056) $\text{digits}(624, 10) = \langle 4, 2, 6\rangle$.

(1057) $\sum \text{digits}(624, 10) = 12$. The theorem is a consequence of (1056).

(1058) $\text{digits}(648, 10) = \langle 8, 4, 6\rangle$.

(1059) $\sum \text{digits}(648, 10) = 18$. The theorem is a consequence of (1058).

(1060) $\text{digits}(672, 10) = \langle 2, 7, 6\rangle$.

(1061) $\sum \text{digits}(672, 10) = 15$. The theorem is a consequence of (1060).

(1062) $\text{digits}(696, 10) = \langle 6, 9, 6\rangle$.

(1063) $\sum \text{digits}(696, 10) = 21$. The theorem is a consequence of (1062).

(1064) $\text{digits}(744, 10) = \langle 4, 4, 7\rangle$.

(1065) $\sum \text{digits}(744, 10) = 15$. The theorem is a consequence of (1064).

(1066) $\text{digits}(768, 10) = \langle 8, 6, 7\rangle$.

(1067) $\sum \text{digits}(768, 10) = 21$. The theorem is a consequence of (1066).

(1068) $\text{digits}(816, 10) = \langle 6, 1, 8\rangle$.

(1069) $\sum \text{digits}(816, 10) = 15$. The theorem is a consequence of (1068).

(1070) $\text{digits}(864, 10) = \langle 4, 6, 8\rangle$.

(1071) $\sum \text{digits}(864, 10) = 18$. The theorem is a consequence of (1070).

(1072) $\text{digits}(888, 10) = \langle 8, 8, 8\rangle$.

(1073) $\sum \text{digits}(888, 10) = 24$. The theorem is a consequence of (1072).

(1074) 888 is the solution to Sierpiński's problem 36 for 24. The theorem is a consequence of (1073), (6), (95), (99), (273), (185), (39), (189), (153), (191), (1049), (193), (751), (199), (1051), (205), (371), (211), (258), (217), (314), (379), (1053), (767), (958), (1055), (391), (1057), (1059), (1061), (1063), (403), (1065), (1067), (789), (1069), (413), and (1071).

18. Problem 36 for $s = 25$

Now we state the propositions:

(1075) $\mathrm{digits}(25, 10) = \langle 5, 2 \rangle$.

(1076) $\sum \mathrm{digits}(25, 10) = 7$. The theorem is a consequence of (1075).

(1077) $\mathrm{digits}(125, 10) = \langle 5, 2, 1 \rangle$.

(1078) $\sum \mathrm{digits}(125, 10) = 8$. The theorem is a consequence of (1077).

(1079) $\mathrm{digits}(175, 10) = \langle 5, 7, 1 \rangle$.

(1080) $\sum \mathrm{digits}(175, 10) = 13$. The theorem is a consequence of (1079).

(1081) $\mathrm{digits}(225, 10) = \langle 5, 2, 2 \rangle$.

(1082) $\sum \mathrm{digits}(225, 10) = 9$. The theorem is a consequence of (1081).

(1083) $\mathrm{digits}(250, 10) = \langle 0, 5, 2 \rangle$.

(1084) $\sum \mathrm{digits}(250, 10) = 7$. The theorem is a consequence of (1083).

(1085) $\mathrm{digits}(275, 10) = \langle 5, 7, 2 \rangle$.

(1086) $\sum \mathrm{digits}(275, 10) = 14$. The theorem is a consequence of (1085).

(1087) $\mathrm{digits}(325, 10) = \langle 5, 2, 3 \rangle$.

(1088) $\sum \mathrm{digits}(325, 10) = 10$. The theorem is a consequence of (1087).

(1089) $\mathrm{digits}(350, 10) = \langle 0, 5, 3 \rangle$.

(1090) $\sum \mathrm{digits}(350, 10) = 8$. The theorem is a consequence of (1089).

(1091) $\mathrm{digits}(375, 10) = \langle 5, 7, 3 \rangle$.

(1092) $\sum \mathrm{digits}(375, 10) = 15$. The theorem is a consequence of (1091).

(1093) $\mathrm{digits}(450, 10) = \langle 0, 5, 4 \rangle$.

(1094) $\sum \mathrm{digits}(450, 10) = 9$. The theorem is a consequence of (1093).

(1095) $\mathrm{digits}(525, 10) = \langle 5, 2, 5 \rangle$.

(1096) $\sum \mathrm{digits}(525, 10) = 12$. The theorem is a consequence of (1095).

(1097) $\mathrm{digits}(625, 10) = \langle 5, 2, 6 \rangle$.

(1098) $\sum \mathrm{digits}(625, 10) = 13$. The theorem is a consequence of (1097).

(1099) $\mathrm{digits}(650, 10) = \langle 0, 5, 6 \rangle$.

(1100) $\sum \mathrm{digits}(650, 10) = 11$. The theorem is a consequence of (1099).

(1101) $\mathrm{digits}(675, 10) = \langle 5, 7, 6 \rangle$.

(1102) $\sum \mathrm{digits}(675, 10) = 18$. The theorem is a consequence of (1101).

(1103) $\mathrm{digits}(725, 10) = \langle 5, 2, 7 \rangle$.

(1104) $\sum \mathrm{digits}(725, 10) = 14$. The theorem is a consequence of (1103).

(1105) $\mathrm{digits}(750, 10) = \langle 0, 5, 7 \rangle$.

(1106) $\sum \mathrm{digits}(750, 10) = 12$. The theorem is a consequence of (1105).

(1107) $\mathrm{digits}(775, 10) = \langle 5, 7, 7 \rangle$.

(1108) $\sum \text{digits}(775, 10) = 19$. The theorem is a consequence of (1107).
(1109) $\text{digits}(825, 10) = \langle 5, 2, 8 \rangle$.
(1110) $\sum \text{digits}(825, 10) = 15$. The theorem is a consequence of (1109).
(1111) $\text{digits}(850, 10) = \langle 0, 5, 8 \rangle$.
(1112) $\sum \text{digits}(850, 10) = 13$. The theorem is a consequence of (1111).
(1113) $\text{digits}(875, 10) = \langle 5, 7, 8 \rangle$.
(1114) $\sum \text{digits}(875, 10) = 20$. The theorem is a consequence of (1113).
(1115) $\text{digits}(925, 10) = \langle 5, 2, 9 \rangle$.
(1116) $\sum \text{digits}(925, 10) = 16$. The theorem is a consequence of (1115).
(1117) $\text{digits}(950, 10) = \langle 0, 5, 9 \rangle$.
(1118) $\sum \text{digits}(950, 10) = 14$. The theorem is a consequence of (1117).
(1119) $\text{digits}(975, 10) = \langle 5, 7, 9 \rangle$.
(1120) $\sum \text{digits}(975, 10) = 21$. The theorem is a consequence of (1119).
(1121) $\text{digits}(1025, 10) = \langle 5, 2, 0, 1 \rangle$.
(1122) $\sum \text{digits}(1025, 10) = 8$. The theorem is a consequence of (1121).
(1123) $\text{digits}(1050, 10) = \langle 0, 5, 0, 1 \rangle$.
(1124) $\sum \text{digits}(1050, 10) = 6$. The theorem is a consequence of (1123).
(1125) $\text{digits}(1075, 10) = \langle 5, 7, 0, 1 \rangle$.
(1126) $\sum \text{digits}(1075, 10) = 13$. The theorem is a consequence of (1125).
(1127) $\text{digits}(1125, 10) = \langle 5, 2, 1, 1 \rangle$.
(1128) $\sum \text{digits}(1125, 10) = 9$. The theorem is a consequence of (1127).
(1129) $\text{digits}(1175, 10) = \langle 5, 7, 1, 1 \rangle$.
(1130) $\sum \text{digits}(1175, 10) = 14$. The theorem is a consequence of (1129).
(1131) $\text{digits}(1225, 10) = \langle 5, 2, 2, 1 \rangle$.
(1132) $\sum \text{digits}(1225, 10) = 10$. The theorem is a consequence of (1131).
(1133) $\text{digits}(1250, 10) = \langle 0, 5, 2, 1 \rangle$.
(1134) $\sum \text{digits}(1250, 10) = 8$. The theorem is a consequence of (1133).
(1135) $\text{digits}(1275, 10) = \langle 5, 7, 2, 1 \rangle$.
(1136) $\sum \text{digits}(1275, 10) = 15$. The theorem is a consequence of (1135).
(1137) $\text{digits}(1325, 10) = \langle 5, 2, 3, 1 \rangle$.
(1138) $\sum \text{digits}(1325, 10) = 11$. The theorem is a consequence of (1137).
(1139) $\text{digits}(1350, 10) = \langle 0, 5, 3, 1 \rangle$.
(1140) $\sum \text{digits}(1350, 10) = 9$. The theorem is a consequence of (1139).
(1141) $\text{digits}(1375, 10) = \langle 5, 7, 3, 1 \rangle$.
(1142) $\sum \text{digits}(1375, 10) = 16$. The theorem is a consequence of (1141).

(1143) $\mathrm{digits}(1425, 10) = \langle 5, 2, 4, 1\rangle$.

(1144) $\sum \mathrm{digits}(1425, 10) = 12$. The theorem is a consequence of (1143).

(1145) $\mathrm{digits}(1450, 10) = \langle 0, 5, 4, 1\rangle$.

(1146) $\sum \mathrm{digits}(1450, 10) = 10$. The theorem is a consequence of (1145).

(1147) $\mathrm{digits}(1475, 10) = \langle 5, 7, 4, 1\rangle$.

(1148) $\sum \mathrm{digits}(1475, 10) = 17$. The theorem is a consequence of (1147).

(1149) $\mathrm{digits}(1525, 10) = \langle 5, 2, 5, 1\rangle$.

(1150) $\sum \mathrm{digits}(1525, 10) = 13$. The theorem is a consequence of (1149).

(1151) $\mathrm{digits}(1550, 10) = \langle 0, 5, 5, 1\rangle$.

(1152) $\sum \mathrm{digits}(1550, 10) = 11$. The theorem is a consequence of (1151).

(1153) $\mathrm{digits}(1575, 10) = \langle 5, 7, 5, 1\rangle$.

(1154) $\sum \mathrm{digits}(1575, 10) = 18$. The theorem is a consequence of (1153).

(1155) $\mathrm{digits}(1625, 10) = \langle 5, 2, 6, 1\rangle$.

(1156) $\sum \mathrm{digits}(1625, 10) = 14$. The theorem is a consequence of (1155).

(1157) $\mathrm{digits}(1675, 10) = \langle 5, 7, 6, 1\rangle$.

(1158) $\sum \mathrm{digits}(1675, 10) = 19$. The theorem is a consequence of (1157).

(1159) $\mathrm{digits}(1725, 10) = \langle 5, 2, 7, 1\rangle$.

(1160) $\sum \mathrm{digits}(1725, 10) = 15$. The theorem is a consequence of (1159).

(1161) $\mathrm{digits}(1750, 10) = \langle 0, 5, 7, 1\rangle$.

(1162) $\sum \mathrm{digits}(1750, 10) = 13$. The theorem is a consequence of (1161).

(1163) $\mathrm{digits}(1775, 10) = \langle 5, 7, 7, 1\rangle$.

(1164) $\sum \mathrm{digits}(1775, 10) = 20$. The theorem is a consequence of (1163).

(1165) $\mathrm{digits}(1825, 10) = \langle 5, 2, 8, 1\rangle$.

(1166) $\sum \mathrm{digits}(1825, 10) = 16$. The theorem is a consequence of (1165).

(1167) $\mathrm{digits}(1850, 10) = \langle 0, 5, 8, 1\rangle$.

(1168) $\sum \mathrm{digits}(1850, 10) = 14$. The theorem is a consequence of (1167).

(1169) $\mathrm{digits}(1875, 10) = \langle 5, 7, 8, 1\rangle$.

(1170) $\sum \mathrm{digits}(1875, 10) = 21$. The theorem is a consequence of (1169).

(1171) $\mathrm{digits}(1925, 10) = \langle 5, 2, 9, 1\rangle$.

(1172) $\sum \mathrm{digits}(1925, 10) = 17$. The theorem is a consequence of (1171).

(1173) $\mathrm{digits}(1950, 10) = \langle 0, 5, 9, 1\rangle$.

(1174) $\sum \mathrm{digits}(1950, 10) = 15$. The theorem is a consequence of (1173).

(1175) $\mathrm{digits}(1975, 10) = \langle 5, 7, 9, 1\rangle$.

(1176) $\sum \mathrm{digits}(1975, 10) = 22$. The theorem is a consequence of (1175).

(1177) $\mathrm{digits}(2025, 10) = \langle 5, 2, 0, 2\rangle$.

(1178) $\sum \text{digits}(2025, 10) = 9$. The theorem is a consequence of (1177).
(1179) $\text{digits}(2050, 10) = \langle 0, 5, 0, 2 \rangle$.
(1180) $\sum \text{digits}(2050, 10) = 7$. The theorem is a consequence of (1179).
(1181) $\text{digits}(2075, 10) = \langle 5, 7, 0, 2 \rangle$.
(1182) $\sum \text{digits}(2075, 10) = 14$. The theorem is a consequence of (1181).
(1183) $\text{digits}(2125, 10) = \langle 5, 2, 1, 2 \rangle$.
(1184) $\sum \text{digits}(2125, 10) = 10$. The theorem is a consequence of (1183).
(1185) $\text{digits}(2150, 10) = \langle 0, 5, 1, 2 \rangle$.
(1186) $\sum \text{digits}(2150, 10) = 8$. The theorem is a consequence of (1185).
(1187) $\text{digits}(2175, 10) = \langle 5, 7, 1, 2 \rangle$.
(1188) $\sum \text{digits}(2175, 10) = 15$. The theorem is a consequence of (1187).
(1189) $\text{digits}(2225, 10) = \langle 5, 2, 2, 2 \rangle$.
(1190) $\sum \text{digits}(2225, 10) = 11$. The theorem is a consequence of (1189).
(1191) $\text{digits}(2250, 10) = \langle 0, 5, 2, 2 \rangle$.
(1192) $\sum \text{digits}(2250, 10) = 9$. The theorem is a consequence of (1191).
(1193) $\text{digits}(2275, 10) = \langle 5, 7, 2, 2 \rangle$.
(1194) $\sum \text{digits}(2275, 10) = 16$. The theorem is a consequence of (1193).
(1195) $\text{digits}(2325, 10) = \langle 5, 2, 3, 2 \rangle$.
(1196) $\sum \text{digits}(2325, 10) = 12$. The theorem is a consequence of (1195).
(1197) $\text{digits}(2350, 10) = \langle 0, 5, 3, 2 \rangle$.
(1198) $\sum \text{digits}(2350, 10) = 10$. The theorem is a consequence of (1197).
(1199) $\text{digits}(2375, 10) = \langle 5, 7, 3, 2 \rangle$.
(1200) $\sum \text{digits}(2375, 10) = 17$. The theorem is a consequence of (1199).
(1201) $\text{digits}(2425, 10) = \langle 5, 2, 4, 2 \rangle$.
(1202) $\sum \text{digits}(2425, 10) = 13$. The theorem is a consequence of (1201).
(1203) $\text{digits}(2450, 10) = \langle 0, 5, 4, 2 \rangle$.
(1204) $\sum \text{digits}(2450, 10) = 11$. The theorem is a consequence of (1203).
(1205) $\text{digits}(2475, 10) = \langle 5, 7, 4, 2 \rangle$.
(1206) $\sum \text{digits}(2475, 10) = 18$. The theorem is a consequence of (1205).
(1207) $\text{digits}(2525, 10) = \langle 5, 2, 5, 2 \rangle$.
(1208) $\sum \text{digits}(2525, 10) = 14$. The theorem is a consequence of (1207).
(1209) $\text{digits}(2550, 10) = \langle 0, 5, 5, 2 \rangle$.
(1210) $\sum \text{digits}(2550, 10) = 12$. The theorem is a consequence of (1209).
(1211) $\text{digits}(2575, 10) = \langle 5, 7, 5, 2 \rangle$.
(1212) $\sum \text{digits}(2575, 10) = 19$. The theorem is a consequence of (1211).

(1213) $\mathrm{digits}(2625, 10) = \langle 5, 2, 6, 2\rangle$.
(1214) $\sum \mathrm{digits}(2625, 10) = 15$. The theorem is a consequence of (1213).
(1215) $\mathrm{digits}(2650, 10) = \langle 0, 5, 6, 2\rangle$.
(1216) $\sum \mathrm{digits}(2650, 10) = 13$. The theorem is a consequence of (1215).
(1217) $\mathrm{digits}(2675, 10) = \langle 5, 7, 6, 2\rangle$.
(1218) $\sum \mathrm{digits}(2675, 10) = 20$. The theorem is a consequence of (1217).
(1219) $\mathrm{digits}(2725, 10) = \langle 5, 2, 7, 2\rangle$.
(1220) $\sum \mathrm{digits}(2725, 10) = 16$. The theorem is a consequence of (1219).
(1221) $\mathrm{digits}(2750, 10) = \langle 0, 5, 7, 2\rangle$.
(1222) $\sum \mathrm{digits}(2750, 10) = 14$. The theorem is a consequence of (1221).
(1223) $\mathrm{digits}(2775, 10) = \langle 5, 7, 7, 2\rangle$.
(1224) $\sum \mathrm{digits}(2775, 10) = 21$. The theorem is a consequence of (1223).
(1225) $\mathrm{digits}(2825, 10) = \langle 5, 2, 8, 2\rangle$.
(1226) $\sum \mathrm{digits}(2825, 10) = 17$. The theorem is a consequence of (1225).
(1227) $\mathrm{digits}(2850, 10) = \langle 0, 5, 8, 2\rangle$.
(1228) $\sum \mathrm{digits}(2850, 10) = 15$. The theorem is a consequence of (1227).
(1229) $\mathrm{digits}(2875, 10) = \langle 5, 7, 8, 2\rangle$.
(1230) $\sum \mathrm{digits}(2875, 10) = 22$. The theorem is a consequence of (1229).
(1231) $\mathrm{digits}(2925, 10) = \langle 5, 2, 9, 2\rangle$.
(1232) $\sum \mathrm{digits}(2925, 10) = 18$. The theorem is a consequence of (1231).
(1233) $\mathrm{digits}(2950, 10) = \langle 0, 5, 9, 2\rangle$.
(1234) $\sum \mathrm{digits}(2950, 10) = 16$. The theorem is a consequence of (1233).
(1235) $\mathrm{digits}(2975, 10) = \langle 5, 7, 9, 2\rangle$.
(1236) $\sum \mathrm{digits}(2975, 10) = 23$. The theorem is a consequence of (1235).
(1237) $\mathrm{digits}(3025, 10) = \langle 5, 2, 0, 3\rangle$.
(1238) $\sum \mathrm{digits}(3025, 10) = 10$. The theorem is a consequence of (1237).
(1239) $\mathrm{digits}(3050, 10) = \langle 0, 5, 0, 3\rangle$.
(1240) $\sum \mathrm{digits}(3050, 10) = 8$. The theorem is a consequence of (1239).
(1241) $\mathrm{digits}(3075, 10) = \langle 5, 7, 0, 3\rangle$.
(1242) $\sum \mathrm{digits}(3075, 10) = 15$. The theorem is a consequence of (1241).
(1243) $\mathrm{digits}(3125, 10) = \langle 5, 2, 1, 3\rangle$.
(1244) $\sum \mathrm{digits}(3125, 10) = 11$. The theorem is a consequence of (1243).
(1245) $\mathrm{digits}(3150, 10) = \langle 0, 5, 1, 3\rangle$.
(1246) $\sum \mathrm{digits}(3150, 10) = 9$. The theorem is a consequence of (1245).
(1247) $\mathrm{digits}(3175, 10) = \langle 5, 7, 1, 3\rangle$.

(1248) $\sum \text{digits}(3175, 10) = 16$. The theorem is a consequence of (1247).
(1249) $\text{digits}(3225, 10) = \langle 5, 2, 2, 3 \rangle$.
(1250) $\sum \text{digits}(3225, 10) = 12$. The theorem is a consequence of (1249).
(1251) $\text{digits}(3250, 10) = \langle 0, 5, 2, 3 \rangle$.
(1252) $\sum \text{digits}(3250, 10) = 10$. The theorem is a consequence of (1251).
(1253) $\text{digits}(3275, 10) = \langle 5, 7, 2, 3 \rangle$.
(1254) $\sum \text{digits}(3275, 10) = 17$. The theorem is a consequence of (1253).
(1255) $\text{digits}(3325, 10) = \langle 5, 2, 3, 3 \rangle$.
(1256) $\sum \text{digits}(3325, 10) = 13$. The theorem is a consequence of (1255).
(1257) $\text{digits}(3350, 10) = \langle 0, 5, 3, 3 \rangle$.
(1258) $\sum \text{digits}(3350, 10) = 11$. The theorem is a consequence of (1257).
(1259) $\text{digits}(3375, 10) = \langle 5, 7, 3, 3 \rangle$.
(1260) $\sum \text{digits}(3375, 10) = 18$. The theorem is a consequence of (1259).
(1261) $\text{digits}(3425, 10) = \langle 5, 2, 4, 3 \rangle$.
(1262) $\sum \text{digits}(3425, 10) = 14$. The theorem is a consequence of (1261).
(1263) $\text{digits}(3450, 10) = \langle 0, 5, 4, 3 \rangle$.
(1264) $\sum \text{digits}(3450, 10) = 12$. The theorem is a consequence of (1263).
(1265) $\text{digits}(3475, 10) = \langle 5, 7, 4, 3 \rangle$.
(1266) $\sum \text{digits}(3475, 10) = 19$. The theorem is a consequence of (1265).
(1267) $\text{digits}(3525, 10) = \langle 5, 2, 5, 3 \rangle$.
(1268) $\sum \text{digits}(3525, 10) = 15$. The theorem is a consequence of (1267).
(1269) $\text{digits}(3550, 10) = \langle 0, 5, 5, 3 \rangle$.
(1270) $\sum \text{digits}(3550, 10) = 13$. The theorem is a consequence of (1269).
(1271) $\text{digits}(3575, 10) = \langle 5, 7, 5, 3 \rangle$.
(1272) $\sum \text{digits}(3575, 10) = 20$. The theorem is a consequence of (1271).
(1273) $\text{digits}(3625, 10) = \langle 5, 2, 6, 3 \rangle$.
(1274) $\sum \text{digits}(3625, 10) = 16$. The theorem is a consequence of (1273).
(1275) $\text{digits}(3650, 10) = \langle 0, 5, 6, 3 \rangle$.
(1276) $\sum \text{digits}(3650, 10) = 14$. The theorem is a consequence of (1275).
(1277) $\text{digits}(3675, 10) = \langle 5, 7, 6, 3 \rangle$.
(1278) $\sum \text{digits}(3675, 10) = 21$. The theorem is a consequence of (1277).
(1279) $\text{digits}(3725, 10) = \langle 5, 2, 7, 3 \rangle$.
(1280) $\sum \text{digits}(3725, 10) = 17$. The theorem is a consequence of (1279).
(1281) $\text{digits}(3750, 10) = \langle 0, 5, 7, 3 \rangle$.
(1282) $\sum \text{digits}(3750, 10) = 15$. The theorem is a consequence of (1281).

(1283) $\mathrm{digits}(3775, 10) = \langle 5, 7, 7, 3\rangle$.

(1284) $\sum \mathrm{digits}(3775, 10) = 22$. The theorem is a consequence of (1283).

(1285) $\mathrm{digits}(3825, 10) = \langle 5, 2, 8, 3\rangle$.

(1286) $\sum \mathrm{digits}(3825, 10) = 18$. The theorem is a consequence of (1285).

(1287) $\mathrm{digits}(3850, 10) = \langle 0, 5, 8, 3\rangle$.

(1288) $\sum \mathrm{digits}(3850, 10) = 16$. The theorem is a consequence of (1287).

(1289) $\mathrm{digits}(3875, 10) = \langle 5, 7, 8, 3\rangle$.

(1290) $\sum \mathrm{digits}(3875, 10) = 23$. The theorem is a consequence of (1289).

(1291) $\mathrm{digits}(3925, 10) = \langle 5, 2, 9, 3\rangle$.

(1292) $\sum \mathrm{digits}(3925, 10) = 19$. The theorem is a consequence of (1291).

(1293) $\mathrm{digits}(3950, 10) = \langle 0, 5, 9, 3\rangle$.

(1294) $\sum \mathrm{digits}(3950, 10) = 17$. The theorem is a consequence of (1293).

(1295) $\mathrm{digits}(3975, 10) = \langle 5, 7, 9, 3\rangle$.

(1296) $\sum \mathrm{digits}(3975, 10) = 24$. The theorem is a consequence of (1295).

(1297) $\mathrm{digits}(4000, 10) = \langle 0, 0, 0, 4\rangle$.

(1298) $\sum \mathrm{digits}(4000, 10) = 4$. The theorem is a consequence of (1297).

(1299) $\mathrm{digits}(4025, 10) = \langle 5, 2, 0, 4\rangle$.

(1300) $\sum \mathrm{digits}(4025, 10) = 11$. The theorem is a consequence of (1299).

(1301) $\mathrm{digits}(4050, 10) = \langle 0, 5, 0, 4\rangle$.

(1302) $\sum \mathrm{digits}(4050, 10) = 9$. The theorem is a consequence of (1301).

(1303) $\mathrm{digits}(4075, 10) = \langle 5, 7, 0, 4\rangle$.

(1304) $\sum \mathrm{digits}(4075, 10) = 16$. The theorem is a consequence of (1303).

(1305) $\mathrm{digits}(4100, 10) = \langle 0, 0, 1, 4\rangle$.

(1306) $\sum \mathrm{digits}(4100, 10) = 5$. The theorem is a consequence of (1305).

(1307) $\mathrm{digits}(4125, 10) = \langle 5, 2, 1, 4\rangle$.

(1308) $\sum \mathrm{digits}(4125, 10) = 12$. The theorem is a consequence of (1307).

(1309) $\mathrm{digits}(4150, 10) = \langle 0, 5, 1, 4\rangle$.

(1310) $\sum \mathrm{digits}(4150, 10) = 10$. The theorem is a consequence of (1309).

(1311) $\mathrm{digits}(4175, 10) = \langle 5, 7, 1, 4\rangle$.

(1312) $\sum \mathrm{digits}(4175, 10) = 17$. The theorem is a consequence of (1311).

(1313) $\mathrm{digits}(4200, 10) = \langle 0, 0, 2, 4\rangle$.

(1314) $\sum \mathrm{digits}(4200, 10) = 6$. The theorem is a consequence of (1313).

(1315) $\mathrm{digits}(4225, 10) = \langle 5, 2, 2, 4\rangle$.

(1316) $\sum \mathrm{digits}(4225, 10) = 13$. The theorem is a consequence of (1315).

(1317) $\mathrm{digits}(4250, 10) = \langle 0, 5, 2, 4\rangle$.

(1318) $\sum \text{digits}(4250, 10) = 11$. The theorem is a consequence of (1317).
(1319) $\text{digits}(4275, 10) = \langle 5, 7, 2, 4 \rangle$.
(1320) $\sum \text{digits}(4275, 10) = 18$. The theorem is a consequence of (1319).
(1321) $\text{digits}(4300, 10) = \langle 0, 0, 3, 4 \rangle$.
(1322) $\sum \text{digits}(4300, 10) = 7$. The theorem is a consequence of (1321).
(1323) $\text{digits}(4325, 10) = \langle 5, 2, 3, 4 \rangle$.
(1324) $\sum \text{digits}(4325, 10) = 14$. The theorem is a consequence of (1323).
(1325) $\text{digits}(4350, 10) = \langle 0, 5, 3, 4 \rangle$.
(1326) $\sum \text{digits}(4350, 10) = 12$. The theorem is a consequence of (1325).
(1327) $\text{digits}(4375, 10) = \langle 5, 7, 3, 4 \rangle$.
(1328) $\sum \text{digits}(4375, 10) = 19$. The theorem is a consequence of (1327).
(1329) $\text{digits}(4400, 10) = \langle 0, 0, 4, 4 \rangle$.
(1330) $\sum \text{digits}(4400, 10) = 8$. The theorem is a consequence of (1329).
(1331) $\text{digits}(4425, 10) = \langle 5, 2, 4, 4 \rangle$.
(1332) $\sum \text{digits}(4425, 10) = 15$. The theorem is a consequence of (1331).
(1333) $\text{digits}(4450, 10) = \langle 0, 5, 4, 4 \rangle$.
(1334) $\sum \text{digits}(4450, 10) = 13$. The theorem is a consequence of (1333).
(1335) $\text{digits}(4475, 10) = \langle 5, 7, 4, 4 \rangle$.
(1336) $\sum \text{digits}(4475, 10) = 20$. The theorem is a consequence of (1335).
(1337) $\text{digits}(4500, 10) = \langle 0, 0, 5, 4 \rangle$.
(1338) $\sum \text{digits}(4500, 10) = 9$. The theorem is a consequence of (1337).
(1339) $\text{digits}(4525, 10) = \langle 5, 2, 5, 4 \rangle$.
(1340) $\sum \text{digits}(4525, 10) = 16$. The theorem is a consequence of (1339).
(1341) $\text{digits}(4550, 10) = \langle 0, 5, 5, 4 \rangle$.
(1342) $\sum \text{digits}(4550, 10) = 14$. The theorem is a consequence of (1341).
(1343) $\text{digits}(4575, 10) = \langle 5, 7, 5, 4 \rangle$.
(1344) $\sum \text{digits}(4575, 10) = 21$. The theorem is a consequence of (1343).
(1345) $\text{digits}(4600, 10) = \langle 0, 0, 6, 4 \rangle$.
(1346) $\sum \text{digits}(4600, 10) = 10$. The theorem is a consequence of (1345).
(1347) $\text{digits}(4625, 10) = \langle 5, 2, 6, 4 \rangle$.
(1348) $\sum \text{digits}(4625, 10) = 17$. The theorem is a consequence of (1347).
(1349) $\text{digits}(4650, 10) = \langle 0, 5, 6, 4 \rangle$.
(1350) $\sum \text{digits}(4650, 10) = 15$. The theorem is a consequence of (1349).
(1351) $\text{digits}(4675, 10) = \langle 5, 7, 6, 4 \rangle$.
(1352) $\sum \text{digits}(4675, 10) = 22$. The theorem is a consequence of (1351).

(1353) $\mathrm{digits}(4700, 10) = \langle 0, 0, 7, 4\rangle$.

(1354) $\sum \mathrm{digits}(4700, 10) = 11$. The theorem is a consequence of (1353).

(1355) $\mathrm{digits}(4725, 10) = \langle 5, 2, 7, 4\rangle$.

(1356) $\sum \mathrm{digits}(4725, 10) = 18$. The theorem is a consequence of (1355).

(1357) $\mathrm{digits}(4750, 10) = \langle 0, 5, 7, 4\rangle$.

(1358) $\sum \mathrm{digits}(4750, 10) = 16$. The theorem is a consequence of (1357).

(1359) $\mathrm{digits}(4775, 10) = \langle 5, 7, 7, 4\rangle$.

(1360) $\sum \mathrm{digits}(4775, 10) = 23$. The theorem is a consequence of (1359).

(1361) $\mathrm{digits}(4800, 10) = \langle 0, 0, 8, 4\rangle$.

(1362) $\sum \mathrm{digits}(4800, 10) = 12$. The theorem is a consequence of (1361).

(1363) $\mathrm{digits}(4825, 10) = \langle 5, 2, 8, 4\rangle$.

(1364) $\sum \mathrm{digits}(4825, 10) = 19$. The theorem is a consequence of (1363).

(1365) $\mathrm{digits}(4850, 10) = \langle 0, 5, 8, 4\rangle$.

(1366) $\sum \mathrm{digits}(4850, 10) = 17$. The theorem is a consequence of (1365).

(1367) $\mathrm{digits}(4875, 10) = \langle 5, 7, 8, 4\rangle$.

(1368) $\sum \mathrm{digits}(4875, 10) = 24$. The theorem is a consequence of (1367).

(1369) $\mathrm{digits}(4900, 10) = \langle 0, 0, 9, 4\rangle$.

(1370) $\sum \mathrm{digits}(4900, 10) = 13$. The theorem is a consequence of (1369).

(1371) $\mathrm{digits}(4925, 10) = \langle 5, 2, 9, 4\rangle$.

(1372) $\sum \mathrm{digits}(4925, 10) = 20$. The theorem is a consequence of (1371).

(1373) $\mathrm{digits}(4950, 10) = \langle 0, 5, 9, 4\rangle$.

(1374) $\sum \mathrm{digits}(4950, 10) = 18$. The theorem is a consequence of (1373).

(1375) $\mathrm{digits}(4975, 10) = \langle 5, 7, 9, 4\rangle$.

(1376) $\sum \mathrm{digits}(4975, 10) = 25$. The theorem is a consequence of (1375).

(1377) 4975 is the solution to Sierpiński's problem 36 for 25. The theorem is a consequence of (1376), (6), (1076), (25), (172), (35), (1078), (45), (1080), (361), (1082), (1084), (1086), (369), (1088), (1090), (1092), (213), (260), (1094), (316), (381), (1096), (769), (960), (391), (1098), (1100), (1102), (401), (1104), (1106), (1108), (409), (1110), (1112), (1114), (419), (1116), (1118), (1120), (429), (1122), (1124), (1126), (439), (1128), (1004), (1130), (449), (1132), (1134), (1136), (459), (1138), (1140), (1142), (469), (1144), (1146), (1148), (479), (1150), (1152), (1154), (489), (1156), (857), (1158), (499), (1160), (1162), (1164), (509), (1166), (1168), (1170), (519), (1172), (1174), (1176), (529), (1178), (1180), (1182), (539), (1184), (1186), (1188), (549), (1190), (1192), (1194), (559), (1196), (1198), (1200), (569), (1202), (1204), (1206), (579), (1208), (1210), (1212), (589), (1214), (1216), (1218), (599), (1220), (1222), (1224), (609), (1226), (1228), (1230), (619), (1232),

(1234), (1236), (629), (1238), (1240), (1242), (639), (1244), (1246), (1248), (649), (1250), (1252), (1254), (659), (1256), (1258), (1260), (669), (1262), (1264), (1266), (679), (1268), (1270), (1272), (689), (1274), (1276), (1278), (699), (1280), (1282), (1284), (709), (1286), (1288), (1290), (719), (1292), (1294), (1296), (1298), (1300), (1302), (1304), (1306), (1308), (1310), (1312), (1314), (1316), (1318), (1320), (1322), (1324), (1326), (1328), (1330), (1332), (1334), (1336), (1338), (1340), (1342), (1344), (1346), (1348), (1350), (1352), (1354), (1356), (1358), (1360), (1362), (1364), (1366), (1368), (1370), (1372), and (1374).

19. Problem 36 for $s = 100$

Now we state the proposition:

(1378) value$((\langle 0,0\rangle^\frown(11 \longmapsto 9))^\frown\langle 1\rangle, 10)$ is the solution to Sierpiński's problem 36 for 100. The theorem is a consequence of (5), (13), (12), and (14).

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] D. R. Kaprekar. Multidigital numbers. *Scripta Mathematica*, 21:27, 1955.

[4] Artur Korniłowicz. Elementary number theory problems. Part III. *Formalized Mathematics*, 30(**2**):135–158, 2022. doi:10.2478/forma-2022-0011.

[5] Artur Korniłowicz and Dariusz Surowik. Elementary number theory problems. Part II. *Formalized Mathematics*, 29(**1**):63–68, 2021. doi:10.2478/forma-2021-0006.

[6] Adam Naumowicz. Dataset description: Formalization of elementary number theory in Mizar. In Christoph Benzmüller and Bruce R. Miller, editors, *Intelligent Computer Mathematics – 13th International Conference, CICM 2020, Bertinoro, Italy, July 26–31, 2020, Proceedings*, volume 12236 of *Lecture Notes in Computer Science*, pages 303–308. Springer, 2020. doi:10.1007/978-3-030-53518-6_22.

[7] Adam Naumowicz. Elementary number theory problems. Part I. *Formalized Mathematics*, 28(**1**):115–120, 2020. doi:10.2478/forma-2020-0010.

[8] Adam Naumowicz. On the representation of natural numbers in positional numeral systems. *Formalized Mathematics*, 14(**4**):221–223, 2006. doi:10.2478/v10037-006-0025-9.

[9] Wacław Sierpiński. *Elementary Theory of Numbers*. PWN, Warsaw, 1964.

[10] Wacław Sierpiński. *250 Problems in Elementary Number Theory*. Elsevier, 1970.

Accepted December 12, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 277–286, 2023
DOI: 10.2478/forma-2023-0022
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part XII – Primes in Arithmetic Progression

Adam Grabowski
Faculty of Computer Science
University of Białystok
Poland

Summary. In this paper another twelve problems from W. Sierpiński's book "250 Problems in Elementary Number Theory" are formalized, using the Mizar formalism, namely: 42, 43, 51, 51a, 57, 59, 72, 135, 136, and 153–155. Significant amount of the work is devoted to arithmetic progressions.

MSC: 11A41 97F30 68V20

Keywords: number theory; primes; arithmetic progression

MML identifier: NUMBER12, version: 8.1.14 5.76.1462

Introduction

This article contains solutions of selected problems from W. Sierpiński's book "250 Problems in Elementary Number Theory" [12] – the work outlined in [8]. We make an extensive use of the general notion of arithmetic progression developed previously in [2] and results on prime and composite numbers [7].

The preliminary part of the article contains the proof of Theorem 5 from [11], p. 121 (credited to Cantor) stating that if n and r are natural numbers, $n > 1$ and if n terms of the arithmetical progression m, $m+r$, ..., $m+(n-1)r$ are odd prime numbers, then the difference r is divisible by every prime less than n (see [1], vol. I, p. 425). It is used to solve Problem 72, that an increasing arithmetic progression with ten terms, formed of primes, with the least possible last term is the one with the first term 199 and difference 210.

Problems 42, 43, 51, and 51a are taken from Section II ("Relatively prime numbers"), Problems 57, 59, and 72 are from Section III ("Arithmetic progressions"), the rest, i.e. Problems 135, 136 – from Section IV ("Prime and composite numbers").

Problem 42 is closely connected to polygonal numbers formalized in [3].

Problems 153–155, taken from Section V ("Diophantine equations") deal with the solution of the equation

$$\frac{x}{y}+\frac{y}{z}+\frac{z}{x}=k$$

in positive integers x, y, and z, where k is equal to one, two, and three, respectively. More general idea of the problem (open in [12]), about positive integer solution of this equation with arbitrary natural k is discussed quite recently in [13].

Proofs of other problems are straightforward formalizations of solutions given in the book, by means of available development of number theory in Mizar [4], [5], using ellipsis [6] extensively, looking forward for more advanced automatization of arithmetical calculations [9].

1. Preliminaries

Now we state the proposition:

(1) Let us consider objects x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}. Then $\{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}\} = \{x_1, x_2, x_3, x_4, x_5\} \cup \{x_6, x_7, x_8, x_9, x_{10}\}$.

Let m be a composite natural number and n be a non zero natural number. Let us observe that $m \cdot n$ is composite. Let m, n be non zero, non trivial natural numbers. Observe that $m \cdot n$ is composite. Let r be a real number. Let us observe that r^2 is non negative.

Let k be a natural number and n be a non zero, non trivial natural number. Let us observe that $k + n$ is non trivial and non zero and $k + 1$ is non zero and $k + 2$ is non trivial and non zero and $k + 3$ is non trivial and non zero. Now we state the propositions:

(2) Let us consider a natural number n. Suppose $n \bmod 11 = 1$ and $n \bmod 2 = 1$. Then $n \bmod 22 = 1$.

(3) Let us consider natural numbers m, n, r. Suppose $n > 1$ and for every natural number i such that $0 \leqslant i < n$ holds $(\mathrm{ArProg}(m, r))(i)$ is odd and prime. Let us consider a prime number p. If $p < n$, then $p \mid r$.

2. PROBLEM 42

Now we state the proposition:

(4) Let us consider natural numbers a, m, n. If a and m are relatively prime and $n \mid a$, then n and m are relatively prime.

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

(5) a and $2 \cdot a + 1$ are relatively prime.

(6) a and $6 \cdot a + 1$ are relatively prime.

(7) a and $3 \cdot a + 1$ are relatively prime.

(8) Let us consider an increasing finite sequence f of elements of $\mathbb{N}$, and a natural number x. Suppose for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) < x$. Then $f \frown \langle x \rangle$ is increasing.

PROOF: Consider k being a natural number such that $\operatorname{dom} f = \operatorname{Seg} k$. Set $f_4 = f \frown \langle x \rangle$. For every natural numbers m, n such that m, $n \in \operatorname{dom} f_4$ and $m < n$ holds $f_4(m) < f_4(n)$. □

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

(9) $\operatorname{Seg} 1 \longmapsto n$ is an increasing finite sequence of elements of $\mathbb{N}$.

PROOF: Set $f = \operatorname{Seg} 1 \longmapsto n$. For every natural numbers m, n such that m, $n \in \operatorname{dom} f$ and $m < n$ holds $f(m) < f(n)$. □

(10) There exists an increasing, non-empty finite sequence f of elements of $\mathbb{N}$ such that

(i) $\operatorname{dom} f = \operatorname{Seg}(n + 1)$, and

(ii) for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i)$ is triangular, and

(iii) f is with all coprime terms.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ there exists an increasing, non-empty finite sequence f of elements of $\mathbb{N}$ such that $\operatorname{dom} f = \operatorname{Seg}(\$_1 + 1)$ and for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i)$ is triangular and f is with all coprime terms. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k + 1]$. For every natural number n, $\mathcal{P}[n]$.

Consider f being an increasing, non-empty finite sequence of elements of $\mathbb{N}$ such that $\operatorname{dom} f = \operatorname{Seg}(n + 1)$ and for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i)$ is triangular and f is with all coprime terms. □

3. Problem 43

Let n be a natural number. The functor Tetrahedron(n) yielding a natural number is defined by the term

(Def. 1) $\frac{n\cdot(n+1)\cdot(n+2)}{6}$.

We say that n is tetrahedral if and only if

(Def. 2) there exists a natural number k such that $n = \mathrm{Tetrahedron}(k)$.

Now we state the proposition:

(11) Let us consider a natural number n. Then there exists an increasing, non-empty finite sequence f of elements of $\mathbb{N}$ such that

(i) $\mathrm{dom}\, f = \mathrm{Seg}(n+1)$, and

(ii) for every natural number i such that $i \in \mathrm{dom}\, f$ holds $f(i)$ is tetrahedral, and

(iii) f is with all coprime terms.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ there exists an increasing, non-empty finite sequence f of elements of $\mathbb{N}$ such that $\mathrm{dom}\, f = \mathrm{Seg}(\$_1 + 1)$ and for every natural number i such that $i \in \mathrm{dom}\, f$ holds $f(i)$ is tetrahedral and f is with all coprime terms. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number n, $\mathcal{P}[n]$.

Consider f being an increasing, non-empty finite sequence of elements of $\mathbb{N}$ such that $\mathrm{dom}\, f = \mathrm{Seg}(n+1)$ and for every natural number i such that $i \in \mathrm{dom}\, f$ holds $f(i)$ is tetrahedral and f is with all coprime terms. □

4. Problem 51

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

(12) $\gcd(n, \mathrm{Fermat}\, n) = 1$.

(13) n and Fermat n are relatively prime.

5. Problem 51a

Now we state the propositions:

(14) Let us consider natural numbers n, k, m. Suppose $n \mid k \cdot m$. Then there exist natural numbers a, b such that

(i) $a \mid k$, and

(ii) $b \mid m$, and

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

(15) Let us consider a set A. Suppose $A = \{n$, where n is a non zero natural number : $\gcd(n, 2^n - 1) > 1\}$. Then

(i) A is infinite, and

(ii) for every natural number k such that $k \in A$ holds $k \geqslant 6$.

PROOF: For every non zero natural number k, $\gcd(6 \cdot k, 2^{6 \cdot k} - 1) \geqslant 3$. For every non zero natural number k, $6 \cdot k \in A$. For every natural number m, there exists a natural number n such that $n \geqslant m$ and $n \in A$. For every natural number k such that $k \in A$ holds $k \geqslant 6$ by [14, (5)]. □

6. PROBLEM 57

Let us consider positive natural numbers a, b and natural numbers k, x, m. Now we state the propositions:

(16) If $(\mathrm{ArProg}(b, a))(k) = x^{\mathbf{2}}$, then $(\mathrm{ArProg}(b, a))(m^{\mathbf{2}} \cdot a + 2 \cdot m \cdot x + k) = (m \cdot a + x)^{\mathbf{2}}$.

(17) If $(\mathrm{ArProg}(b, a))(k) = x^{\mathbf{2}}$, then $(\mathrm{ArProg}(b, a))(m^{\mathbf{2}} \cdot a + 2 \cdot m \cdot x + k)$ is a square.

(18) Let us consider non zero natural numbers m, n. Suppose m is quadratic residue modulo n. Then there exists a natural number i such that $(\mathrm{ArProg}(m, n))(i)$ is a square.

(19) Let us consider non zero natural numbers m, n, and a set A. Suppose $A = \{i$, where i is a natural number : $(\mathrm{ArProg}(m, n))(i)$ is a square$\}$. Then A is infinite if and only if m is quadratic residue modulo n.

PROOF: Consider i being a natural number such that $(\mathrm{ArProg}(m, n))(i)$ is a square. Consider x being a natural number such that $(\mathrm{ArProg}(m, n))(i) = x^{\mathbf{2}}$. For every natural number j, there exists a natural number k such that $k \geqslant j$ and $k \in A$. □

7. PROBLEM 59

Now we state the proposition:

(20) Let us consider a natural number k. If $k > 1$, then $k \cdot k \nmid k$.

Observe that there exists an arithmetic progression which is non-empty, natural-valued, and increasing. Now we state the propositions:

(21) Let us consider a natural number n, and a prime number p. If n is perfect power and $p \mid n$, then $p^2 \mid n$.

(22) There exists no non-empty, natural-valued, increasing arithmetic progression f such that for every natural numbers i, $\mathcal{N}$ such that $\mathcal{N} = f(i)$ holds $\mathcal{N}$ is perfect power.

PROOF: Consider f being a non-empty, natural-valued, increasing arithmetic progression such that for every natural numbers i, $\mathcal{N}$ such that $\mathcal{N} = f(i)$ holds $\mathcal{N}$ is perfect power. Reconsider $b = f(0)$ as a natural number. Reconsider $a = \mathrm{difference}(f)$ as a natural number.

Consider p being a prime number such that $p > a + b$. Reconsider $p_2 = p^{\mathbf{2}}$ as a natural number. $\gcd(a, p) = 1$. Consider x, y being natural numbers such that $a \cdot x - p_2 \cdot y = 1$. Reconsider $k = (p - b) \cdot x$ as a natural number. Reconsider $a_1 = a \cdot k + b$ as a natural number. $p_2 \nmid a \cdot k + b$. a_1 is not perfect power. □

8. PROBLEM 72

Now we state the propositions:

(23) Let us consider an arithmetic progression f. Suppose for every natural number i, $f(i)$ is a prime number. Then $\mathrm{difference}(f)$ is an integer.

(24) Let us consider prime numbers p, q. If $p - q$ is odd, then $p = 2$ or $q = 2$.

Let p, q be prime numbers. One can check that $p - q$ is integer. Let p, q be greater than 2 prime numbers. Observe that $p - q$ is even. Let us consider an increasing arithmetic progression f. Now we state the propositions:

(25) If for every natural number i, $f(i)$ is a prime number, then $f(1) > 2$.

(26) If for every natural number i, $f(i)$ is a prime number, then $\mathrm{difference}(f)$ is an even natural number. The theorem is a consequence of (25).

(27) $(\mathrm{ArProg}(199, 210))(0) = 199$.

(28) $(\mathrm{ArProg}(199, 210))(1) = 409$. The theorem is a consequence of (27).

(29) $(\mathrm{ArProg}(199, 210))(2) = 619$. The theorem is a consequence of (28).

(30) $(\mathrm{ArProg}(199, 210))(3) = 829$. The theorem is a consequence of (29).

(31) $(\mathrm{ArProg}(199, 210))(4) = 1039$. The theorem is a consequence of (30).

(32) $(\mathrm{ArProg}(199, 210))(5) = 1249$. The theorem is a consequence of (31).

(33) $(\mathrm{ArProg}(199, 210))(6) = 1459$. The theorem is a consequence of (32).

(34) $(\mathrm{ArProg}(199, 210))(7) = 1669$. The theorem is a consequence of (33).

(35) $(\mathrm{ArProg}(199, 210))(8) = 1879$. The theorem is a consequence of (34).

(36) $(\mathrm{ArProg}(199, 210))(9) = 2089$. The theorem is a consequence of (35).

Let f be a natural-valued arithmetic progression. One can verify that $\mathrm{difference}(f)$ is integer. Let us consider an increasing, natural-valued arithmetic progression f. Now we state the propositions:

(37) If for every natural number i such that $0 \leqslant i < 10$ holds $f(i)$ is an odd prime number, then $210 \mid \text{difference}(f)$. The theorem is a consequence of (3).

(38) If for every natural number i such that $0 \leqslant i < 10$ holds $f(i)$ is an odd prime number, then $\text{difference}(f) \geqslant 210$.

(39) Let us consider an increasing, natural-valued arithmetic progression f. Suppose for every natural number i such that $0 \leqslant i < 10$ holds $f(i)$ is an odd prime number and $\text{difference}(f) = 210$. Let us consider a natural number f_0. If $f_0 = f(0)$, then $f_0 \bmod 11 = 1$.

PROOF: $f_0 \bmod 11 \neq 0$. $f_0 \bmod 11 \neq 10$. $f_0 \bmod 11 \neq 9$. $f_0 \bmod 11 \neq 8$. $f_0 \bmod 11 \neq 7$. $f_0 \bmod 11 \neq 6$. $f_0 \bmod 11 \neq 5$. $f_0 \bmod 11 \neq 4$. $f_0 \bmod 11 \neq 3$. $f_0 \bmod 11 \neq 2$. □

Let us consider an increasing, natural-valued arithmetic progression f. Now we state the propositions:

(40) If for every natural number i such that $0 \leqslant i < 10$ holds $f(i)$ is an odd prime number and $\text{difference}(f) = 210$, then $f(0) \geqslant 199$.

PROOF: $f(0) \bmod 11 = 1$. $f(0) \bmod 22 = 1$. If $f(0) \operatorname{div} 22 = 0$, then $f(0) = 1$. If $f(0) \operatorname{div} 22 = 1$, then $f(0) = 23$. If $f(0) \operatorname{div} 22 = 2$, then $f(0) = 45$. If $f(0) \operatorname{div} 22 = 3$, then $f(0) = 67$. If $f(0) \operatorname{div} 22 = 4$, then $f(0) = 89$. If $f(0) \operatorname{div} 22 = 5$, then $f(0) = 111$. If $f(0) \operatorname{div} 22 = 6$, then $f(0) = 133$. If $f(0) \operatorname{div} 22 = 7$, then $f(0) = 155$. If $f(0) \operatorname{div} 22 = 8$, then $f(0) = 177$. If $f(0) \operatorname{div} 22 > 4$, then $f(0) \geqslant 199$. $f(0) \neq 23$. $f(0) \neq 67$. $f(0) \neq 89$. □

(41) If for every natural number i such that $0 \leqslant i < 10$ holds $f(i)$ is an odd prime number, then $f(9) \geqslant 2089$. The theorem is a consequence of (37), (40), and (38).

(42) $\operatorname{rng}(\operatorname{ArProg}(199, 210) \restriction 10) = \{199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089\}$.

PROOF: Set $g = \operatorname{ArProg}(199, 210)$. $\operatorname{rng}(\operatorname{ArProg}(199, 210) \restriction 10) \subseteq \{199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089\}$. $x = g(0)$ or $x = g(1)$ or $x = g(2)$ or $x = g(3)$ or $x = g(4)$ or $x = g(5)$ or $x = g(6)$ or $x = g(7)$ or $x = g(8)$ or $x = g(9)$. $x \in \operatorname{rng}(\operatorname{ArProg}(199, 210) \restriction 10)$. □

(43) $\overline{\overline{\operatorname{rng}(\operatorname{ArProg}(199, 210) \restriction 10) \cap \mathbb{P}}} = 10$.

PROOF: Set $f = \operatorname{ArProg}(199, 210) \restriction 10$. $\{199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089\} \subseteq \operatorname{rng} f \cap \mathbb{P}$. $\{199, 409, 619, 829, 1039\}$ misses $\{1249, 1459, 1669, 1879, 2089\}$. $\operatorname{rng} f \cap \mathbb{P} \subseteq \{199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089\}$. □

9. Problem 135

Now we state the proposition:

(44) Let us consider a prime number p. Suppose $p+2$ is a prime number and $p+6$ is a prime number and $p+8$ is a prime number and $p+12$ is a prime number and $p+14$ is a prime number. Then $p=5$.

10. Problem 136

Let n be an integer. The functor PrimeDivisors(n) yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 3) $\{k$, where k is a prime number : $k \mid n\}$.

Now we state the propositions:

(45) Let us consider an integer i. Then PrimeDivisors(i) $\subseteq \mathbb{P}$.

(46) Let us consider a non zero natural number n. Then PrimeDivisors(n) $\subseteq$ Seg n.

(47) Let us consider a natural number n. Then PrimeDivisors(n) $\subseteq$ the set of positive divisors of n.

(48) Let us consider natural numbers a, b. Then PrimeDivisors($a \cdot b$) = PrimeDivisors(a) $\cup$ PrimeDivisors(b).
Proof: PrimeDivisors($a \cdot b$) $\subseteq$ PrimeDivisors(a) $\cup$ PrimeDivisors(b) by [10, (7)]. □

(49) Let us consider a natural number n, and a natural number a. If $n \geqslant 1$, then PrimeDivisors(a^n) = PrimeDivisors(a).
Proof: PrimeDivisors(a^n) $\subseteq$ PrimeDivisors(a). Consider k being a prime number such that $k = x$ and $k \mid a$. □

(50) Let us consider a natural number k, and a prime number p. If $k \geqslant 1$, then PrimeDivisors(p^k) = $\{p\}$.
Proof: Define $\mathcal{P}$[natural number] $\equiv$ PrimeDivisors($p^{\$_1+1}$) = $\{p\}$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number n, $\mathcal{P}[n]$. □

(51) PrimeDivisors(1) = $\emptyset$.

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

(52) If $k \geqslant 1$, then PrimeDivisors($2^k \cdot (2^k - 2)$) = $\{2\} \cup$ PrimeDivisors($2^{k-'1} - 1$). The theorem is a consequence of (48) and (50).

(53) If $k \geqslant 1$, then PrimeDivisors($2^k - 2$) = $\{2\} \cup$ PrimeDivisors($2^{k-'1} - 1$). The theorem is a consequence of (48).

(54) PrimeDivisors$(2^k \cdot (2^k - 2) + 1)$ = PrimeDivisors$(2^k - 1)$. The theorem is a consequence of (48).

(55) Let us consider a natural number a. Then PrimeDivisors$(a \cdot a)$ = PrimeDivisors(a). The theorem is a consequence of (48).

(56) Let us consider natural numbers k, m, n. Suppose $k \geqslant 1$ and $m = 2^k - 2$ and $n = 2^k \cdot (2^k - 2)$. Then

(i) PrimeDivisors(m) = PrimeDivisors(n), and

(ii) PrimeDivisors$(m + 1)$ = PrimeDivisors$(n + 1)$.

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

(57) (i) PrimeDivisors(75) = PrimeDivisors(1215), and

(ii) PrimeDivisors$(75 + 1)$ = PrimeDivisors$(1215 + 1)$.

The theorem is a consequence of (48) and (55).

11. PROBLEM 153

Now we state the propositions:

(58) Let us consider positive real numbers x, y, z. Then $\frac{x}{y} \cdot \frac{y}{z} \cdot \frac{z}{x} = 1$.

(59) There exist no positive natural numbers x, y, z such that $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 1$. The theorem is a consequence of (58).

12. PROBLEM 154

Now we state the propositions:

(60) Let us consider a positive real number a, and a positive natural number n. Then $\sqrt[n]{a}$ is positive.

(61) Let us consider positive real numbers a, b, c. If it is not true that $a = b$ and $b = c$, then $(\frac{a+b+c}{3})^3 > a \cdot b \cdot c$. The theorem is a consequence of (60).

(62) There exist no positive natural numbers x, y, z such that $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 2$. The theorem is a consequence of (58) and (61).

13. PROBLEM 155

Now we state the proposition:

(63) Let us consider positive natural numbers x, y, z. If $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 3$, then $x = y$ and $y = z$. The theorem is a consequence of (61) and (58).

References

[1] Leonard Eugene Dickson. *History of Theory of Numbers*. New York, 1952.

[2] Adam Grabowski. Elementary number theory problems. Part VI. *Formalized Mathematics*, 30(**3**):235–244, 2022. doi:10.2478/forma-2022-0019.

[3] Adam Grabowski. Polygonal numbers. *Formalized Mathematics*, 21(**2**):103–113, 2013. doi:10.2478/forma-2013-0012.

[4] Adam Grabowski and Christoph Schwarzweller. Translating mathematical vernacular into knowledge repositories. In Michael Kohlhase, editor, *Mathematical Knowledge Management*, volume 3863 of *Lecture Notes in Computer Science*, pages 49–64. Springer, 2006. doi:10.1007/11618027_4. 4th International Conference on Mathematical Knowledge Management, Bremen, Germany, MKM 2005, July 15–17, 2005, Revised Selected Papers.

[5] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Mizar in a nutshell. *Journal of Formalized Reasoning*, 3(2):153–245, 2010.

[6] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[7] Artur Korniłowicz and Adam Naumowicz. Elementary number theory problems. Part V. *Formalized Mathematics*, 30(**3**):229–234, 2022. doi:10.2478/forma-2022-0018.

[8] Adam Naumowicz. Dataset description: Formalization of elementary number theory in Mizar. In Christoph Benzmüller and Bruce R. Miller, editors, *Intelligent Computer Mathematics – 13th International Conference, CICM 2020, Bertinoro, Italy, July 26–31, 2020, Proceedings*, volume 12236 of *Lecture Notes in Computer Science*, pages 303–308. Springer, 2020. doi:10.1007/978-3-030-53518-6_22.

[9] Adam Naumowicz. Extending numeric automation for number theory formalizations in Mizar. In Catherine Dubois and Manfred Kerber, editors, *Intelligent Computer Mathematics – 16th International Conference, CICM 2023, Cambridge, UK, September 5–8, 2023, Proceedings*, volume 14101 of *Lecture Notes in Computer Science*, pages 309–314. Springer, 2023. doi:10.1007/978-3-031-42753-4_23.

[10] Christoph Schwarzweller. Proth numbers. *Formalized Mathematics*, 22(**2**):111–118, 2014. doi:10.2478/forma-2014-0013.

[11] Wacław Sierpiński. *Elementary Theory of Numbers*. PWN, Warsaw, 1964.

[12] Wacław Sierpiński. *250 Problems in Elementary Number Theory*. Elsevier, 1970.

[13] Nguyen Xuan Tho. On a remark of Sierpiński. *Rocky Mountain Journal of Mathematics*, 52(2):717–726, 2022. doi:10.1216/rmj.2022.52.717.

[14] Rafał Ziobro. Fermat's Little Theorem via divisibility of Newton's binomial. *Formalized Mathematics*, 23(**3**):215–229, 2015. doi:10.1515/forma-2015-0018.

Accepted December 18, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 287–298, 2023
DOI: 10.2478/forma-2023-0023
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Simple Extensions

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Agnieszka Rowińska-Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In this article we continue the formalization of field theory in Mizar. We introduce simple extensions: an extension E of F is simple if E is generated over F by a single element of E, that is $E = F(a)$ for some $a \in E$. First, we prove that a finite extension E of F is simple if and only if there are only finitely many intermediate fields between E and F [7]. Second, we show that finite extensions of a field F with characteristic 0 are always simple [1]. For this we had to prove, that irreducible polynomials over F have single roots only, which required extending results on divisibility and gcds of polynomials [14], [13] and formal derivation of polynomials [15].

MSC: 12F05 12F99 68V20

Keywords: field theory; intermediate field; simple extension; primitive element

MML identifier: `FIELD_14`, version: `8.1.14 5.76.1462`

Introduction

In this paper we formalize simple extensions [6] using the Mizar formalism [3, 2, 5, 4]. An extension E of F is simple, if E is generated by a single element, that is $E = F(a)$ for some $a \in E$. It is well known that both all finite extensions of fields with characteristic 0 and finite extensions of finite fields are simple, so that most common field extensions are simple. In this paper we deal with fields of characteristic 0 only.

In the preliminary section, we provide some technical lemmas about sums of finite sequences and field extensions. We also define the set of intermediate fields between E and F needed later to characterize simple extensions.

The next two sections provide a number of basic theorems about bags and polynomials necessary to prove our main theorems, for example, that if all roots a of a polynomial of $p * q$ have multiplicity 1, then p and q have no common roots.

The fourth section deals with divisibility of polynomials [8]. We among others show that the gcd of two polynomials is the same in F and an extension E of F and that for a polynomial p_1 of the form

$$(x - a_1) \cdot (x - a_2) \cdot \cdots \cdot (x - a_n)$$

$gcd(p_1, p_2)$ with a polynomial p_2 is again of the form

$$(x - b_1) \cdot (x - b_2) \cdot \cdots \cdot (x - b_k),$$

where the b_j are exactly the common roots of p_1 and p_2. We also show that the number of monic divisors of a polynomial is bounded by $2^{\deg\, p}$. This is crucial in the proof that a simple extension has only a finite number of intermediate fields.

To show that finite extensions of characteric 0 are simple, it is used that an irreducible polynomial has no multiple roots. This is shown in section five using derivatives [1]: for an irreducible polynomial we have $gcd(p, p') = 1$, so p is square free.

In the last section we finally define simple extensions and primitive elements, and show the main results. A finite extension E over an infinite field F is simple if and only if there are only finitely many intermediate fields between E and F: If $E = F(a)$ is simple, then each intermediate field K is uniquely determined by the roots of a's minimal polynomial over K. Because each such polynomial is a monic divisor of p's minimal polynomial over E, there are only finitely many intermediate fields. If the number of intermediate fields is finite, then – because F is infinite – for a and b there exist x and y with $x \neq y$, and $F(a + x * b) = F(a + y * b)$. Then both a and b are in $F(a + x * b)$ [1] from which follows that $F(a, b) = F(a + x * b)$, so that E is simple by induction. Because a field with characteristic 0 is infinite, this also shows our second main result: every finite extension E over a field F with characteristic 0 is simple.

1. Preliminaries

Let n be a non zero, natural number. Note that $n - 1$ is natural. Let n be an element of $\mathbb{N}$. Note that $n -' 1$ is natural. Let R be a ring and n be a natural number. Let us note that $n \cdot (0_R)$ reduces to 0_R. Observe that every finite sequence of elements of $\mathbb{N}$ is non-negative yielding. Now we state the proposition:

(1) Let us consider a finite sequence f of elements of $\mathbb{N}$, and natural numbers i, j. If i, $j \in \operatorname{dom} f$ and $i \neq j$, then $\sum f \geqslant f(i) + f(j)$.

Let F be a field, E be an extension of F, and a, b be F-algebraic elements of E. One can verify that the functor $\{a, b\}$ yields an F-algebraic subset of E. Let K be an extension of F and E be a K-extending extension of F. Note that every F-algebraic element of E is K-algebraic. Let E be an F-finite extension of F. One can verify that every subset of E is F-algebraic.

Let K be an F-finite extension of F. Note that there exists an extension of F which is K-extending and F-finite. Let E be an extension of F and K be an extension of E. Let us observe that there exists an extension of F which is K-extending and E-extending. Now we state the propositions:

(2) Let us consider a field F, an extension E of F, and subsets T_1, T_2, T_3 of E. Suppose $\operatorname{FAdj}(F, T_1) = \operatorname{FAdj}(F, T_2)$. Then $\operatorname{FAdj}(F, T_1 \cup T_3) = \operatorname{FAdj}(F, T_2 \cup T_3)$.

(3) Let us consider a ring R, a ring extension S of R, an element a of R, an element b of S, and an element n of $\mathbb{N}$. If $a = b$, then $n \cdot a = n \cdot b$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \$_1 \cdot a = \$_1 \cdot b$. For every natural number k, $\mathcal{P}[k]$. $\square$

Let F be a field and E be an extension of F.

The functor IntermediateFields(E, F) yielding a set is defined by

(Def. 1) for every object x, $x \in it$ iff there exists a strict field K such that $K = x$ and F is a subfield of K and K is a subfield of E.

One can check that IntermediateFields(E, F) is non empty and field-membered. Now we state the propositions:

(4) Let us consider a field F, an extension E of F, and a strict field K. Then $K \in \operatorname{IntermediateFields}(E, F)$ if and only if F is a subfield of K and K is a subfield of E.

(5) Let us consider a field F, an extension E of F, and an F-extending extension K of E. Then $\operatorname{IntermediateFields}(E, F) \subseteq \operatorname{IntermediateFields}(K, F)$.

2. MORE ON BAGS

Let Z be a non empty set and B be a bag of Z. One can verify that the functor $\overline{\overline{B}}$ yields an element of $\mathbb{N}$. Let us consider a non empty set Z and bags B_1, B_2 of Z. Now we state the propositions:

(6) $B_1 \mid B_2$ if and only if there exists a bag B_3 of Z such that $B_2 = B_1 + B_3$.

(7) If $B_1 \mid B_2$, then $\overline{\overline{B_1}} \leqslant \overline{\overline{B_2}}$. The theorem is a consequence of (6).

(8) Let us consider a non empty set Z, a bag B of Z, and an object o. Then $B(o) \leqslant \overline{\overline{B}}$.

(9) Let us consider a non empty set Z, a bag B of Z, and objects o_1, o_2. Suppose $B(o_1) = \overline{\overline{B}}$ and $o_2 \neq o_1$. Then $B(o_2) = 0$. The theorem is a consequence of (1).

(10) Let us consider an integral domain R, and a bag B_1 of the carrier of R. Then $\overline{\overline{B_1}} = 1$ if and only if there exists an element a of R such that $B_1 = \mathrm{Bag}(\{a\})$. The theorem is a consequence of (8) and (9).

(11) Let us consider a field F, and non zero bags B_1, B_2 of the carrier of F. If $B_2 \mid B_1$ and $\overline{\overline{B_1}} = 1$, then $B_2 = B_1$. The theorem is a consequence of (10) and (7).

(12) Let us consider a non empty set Z, and bags B_1, B_2 of Z. If $B_2 \mid B_1$ and $B_1 -' B_2$ is zero, then $B_2 = B_1$.

(13) Let us consider a field F, and non empty, finite subsets S_1, S_2 of F. Then $\mathrm{Bag}(S_1) \mid \mathrm{Bag}(S_2)$ if and only if $S_1 \subseteq S_2$.

(14) Let us consider a field F, a non zero bag B of the carrier of F, and a non empty, finite subset S_1 of F. Then $B \mid \mathrm{Bag}(S_1)$ if and only if there exists a non empty, finite subset S_2 of F such that $B = \mathrm{Bag}(S_2)$ and $S_2 \subseteq S_1$. The theorem is a consequence of (13).

3. More on Polynomials

Let R be an integral domain and p, q be non constant elements of the carrier of Polynom-Ring R. Let us note that $p \cdot q$ is non constant. Now we state the propositions:

(15) Let us consider a field F, a monic polynomial p over F, and a polynomial r over F. If $p * r$ is monic, then r is monic.

(16) Let us consider an integral domain R, and a polynomial p over R. Then p is monic and constant if and only if $p = \mathbf{1}.R$.

(17) Let us consider an integral domain R, an element a of R, and a non zero natural number m. Then $(\mathrm{rpoly}(1, a))^m$ is a product of linear polynomials of R.

(18) Let us consider a field F, a polynomial p over F, an extension E of F, a polynomial q over E, and an element n of $\mathbb{N}$. If $q = p$, then $q^n = p^n$.

(19) Let us consider a field F, a polynomial p over F, and elements i, j of $\mathbb{N}$. Then $p^{i+j} = p^i * p^j$.

(20) Let us consider a field F, an element a of F, and a product of linear polynomials p of F and $\{a\}$. Then $p = \mathrm{rpoly}(1, a)$.

(21) Let us consider a field F, non zero bags B_1, B_2 of the carrier of F, a product of linear polynomials p of F and B_1, and a product of linear polynomials q of F and B_2. If $B_1 = B_2$, then $p = q$.

(22) Let us consider a field F, an extension E of F, an element p of the carrier of Polynom-Ring F, and an element q of the carrier of Polynom-Ring E. If $q = p$, then $\mathrm{Coeff}(q) = \mathrm{Coeff}(p)$.

(23) Let us consider a field F, non zero polynomials p, q over F, and an element a of F. Then $\mathrm{multiplicity}(p, a) \leqslant \mathrm{multiplicity}(p * q, a)$.

(24) Let us consider a field F, an extension E of F, polynomials p, q over F, and polynomials p_1, q_1 over E. If $p_1 = p$ and $q_1 = q$, then $p_1[q_1] = p[q]$.

PROOF: Consider f being a finite sequence of elements of the carrier of Polynom-Ring F such that $p[q] = \sum f$ and $\operatorname{len} f = \operatorname{len} p$ and for every element n of $\mathbb{N}$ such that $n \in \operatorname{dom} f$ holds $f(n) = p(n -' 1) \cdot (q^{n-'1})$.

Consider g being a finite sequence of elements of the carrier of Polynom-Ring E such that $p_1[q_1] = \sum g$ and $\operatorname{len} g = \operatorname{len} p_1$ and for every element n of $\mathbb{N}$ such that $n \in \operatorname{dom} g$ holds $g(n) = p_1(n -' 1) \cdot ({q_1}^{n-'1})$. $f = g$ by (18), [11, (23)], [12, (2)]. □

(25) Let us consider a field F, polynomials p, q over F, an extension E of F, and an element a of E. Then $\mathrm{ExtEval}(p[q], a) = \mathrm{ExtEval}(p, \mathrm{ExtEval}(q, a))$. The theorem is a consequence of (24).

(26) Let us consider a field F, elements a, b of F, an extension E of F, and an element x of E. Then $\mathrm{ExtEval}(\langle a, b\rangle, x) = ({}^{@}(a, E)) + ({}^{@}(b, E)) \cdot x$.

(27) Let us consider a non degenerated commutative ring R, and polynomials p, q over R. Then $\mathrm{Roots}(p) \subseteq \mathrm{Roots}(p * q)$.

(28) Let us consider an integral domain R, non empty, finite subsets S_1, S_2 of R, a product of linear polynomials p of R and S_1, and a product of linear polynomials q of R and S_2. Suppose $S_1 \cap S_2 = \emptyset$. Then $p * q$ is a product of linear polynomials of R and $S_1 \cup S_2$.

(29) Let us consider a field F, and non zero polynomials p, q over F. Suppose for every element a of F such that a is a root of $p * q$ holds $\mathrm{multiplicity}(p * q, a) = 1$. Then $\mathrm{Roots}(p) \cap \mathrm{Roots}(q) = \emptyset$.

(30) Let us consider a field F, and a product of linear polynomials p of F. Then p is a product of linear polynomials of F and $\mathrm{Roots}(p)$ if and only if for every element a of F such that a is a root of p holds $\mathrm{multiplicity}(p, a) = 1$.

(31) Let us consider a field F, a non empty, finite subset S of F, a product of linear polynomials p of F and S, and a non zero polynomial q over F with roots. Suppose $p * q$ is a product of linear polynomials of F and

$S \cup \mathrm{Roots}(q)$. Then q is a product of linear polynomials of F and $\mathrm{Roots}(q)$. The theorem is a consequence of (15), (23), and (30).

(32) Let us consider a field F, a non empty, finite subset S of F, an element a of F, a product of linear polynomials p of F and $S \cup \{a\}$, and a non constant polynomial q over F. Suppose $p = \mathrm{rpoly}(1, a) * q$ and $a \notin S$. Then q is a product of linear polynomials of F and S.
PROOF: $\mathrm{rpoly}(1, a)$ is a product of linear polynomials of F and $\{a\}$. For every element b of F such that b is a root of $\mathrm{rpoly}(1, a) * q$ holds $\mathrm{multiplicity}(\mathrm{rpoly}(1, a) * q, b) = 1$. $S = \mathrm{Roots}(q)$. □

(33) Let us consider a field F, non empty, finite subsets S_1, S_2 of F, a product of linear polynomials p of F and S_1, an element a of F, and a non constant polynomial q over F. Suppose $p = \mathrm{rpoly}(1, a) * q$ and $S_2 = S_1 \setminus \{a\}$. Then q is a product of linear polynomials of F and S_2. The theorem is a consequence of (32).

4. On Divisibility and Polynomial GCDs

Let R, S be non degenerated commutative rings and p be a polynomial over R. We say that p is square-free over S if and only if

(Def. 2) there exists no non constant polynomial q_1 over S and there exists a polynomial q_2 over S such that $q_2 = p$ and ${q_1}^2 \mid q_2$.

Let R be a non degenerated commutative ring. We say that p is square-free if and only if

(Def. 3) p is square-free over R.

Let R be an integral domain. Let us note that there exists a non constant polynomial over R which is square-free and there exists a non constant polynomial over R which is non square-free. Now we state the propositions:

(34) Let us consider a non degenerated commutative ring R, and a polynomial p over R. Then p is square-free if and only if there exists no non constant polynomial q over R such that $q^2 \mid p$.

(35) Let us consider a field F, and a monic polynomial p over F. If $p \mid \mathbf{1}.F$, then $p = \mathbf{1}.F$.

(36) Let us consider a field F, and non zero polynomials p, q over F. Then $\mathrm{BRoots}(p) \mid \mathrm{BRoots}(p * q)$. The theorem is a consequence of (23).

(37) Let us consider an integral domain R, and polynomials p, q over R. If $q \mid p$, then $\mathrm{Roots}(q) \subseteq \mathrm{Roots}(p)$.

(38) Let us consider a field F, polynomials p, q over F, and a non zero polynomial r over F. If $r * q \mid r * p$, then $q \mid p$.

(39) Let us consider a field F, polynomials p, q over F, and a monic polynomial r over F. Then $\gcd(r * p, r * q) = r * (\gcd(p, q))$. The theorem is a consequence of (15), (38), and (35).

(40) Let us consider a field F, polynomials p, q over F, and elements n, k of $\mathbb{N}$. If $q^n \mid p$ and $k \leqslant n$, then $q^k \mid p$. The theorem is a consequence of (19).

(41) Let us consider a field F, an extension E of F, an element p of the carrier of Polynom-Ring F, and an element q of the carrier of Polynom-Ring E. If $q = p$, then if q is irreducible, then p is irreducible.

(42) Let us consider a GCD domain R. Then every element of R is a GCD of a and 0_R.

Let us consider an EuclideanRing R, elements a, b of R, and a GCD g of a and b. Now we state the propositions:

(43) There exist elements r, s of R such that $g = a \cdot r + b \cdot s$.

(44) $\{g\}$–ideal $= \{a, b\}$–ideal. The theorem is a consequence of (43).

(45) Let us consider a field F, an extension E of F, elements p, q of the carrier of Polynom-Ring F, and elements p_1, q_1 of the carrier of Polynom-Ring E. If $p_1 = p$ and $q_1 = q$, then $\gcd(p_1, q_1) = \gcd(p, q)$.

(46) Let us consider a field F, and an element p of the carrier of Polynom-Ring F. Then $\gcd(p, \mathbf{0}.F) = \operatorname{NormPoly} p$.

(47) Let us consider a field F, an element p of the carrier of Polynom-Ring F, and a non zero element q of the carrier of Polynom-Ring F. If $q \mid p$, then $\gcd(p, q) = \operatorname{NormPoly} q$.

(48) Let us consider a field F, an extension E of F, elements p, q of the carrier of Polynom-Ring F, and elements p_1, q_1 of the carrier of Polynom-Ring E. If $p_1 = p$ and $q_1 = q$, then $q_1 \mid p_1$ iff $q \mid p$. The theorem is a consequence of (45) and (47).

(49) Let us consider a field F, a non zero bag B_1 of the carrier of F, a product of linear polynomials p of F and B_1, and a non constant, monic polynomial q over F. Then $q \mid p$ if and only if there exists a non zero bag B_2 of the carrier of F such that q is a product of linear polynomials of F and B_2 and $B_2 \mid B_1$. The theorem is a consequence of (36), (12), and (21).

(50) Let us consider a field F, a non empty, finite subset S_1 of F, a product of linear polynomials p of F and S_1, and a non constant, monic polynomial q over F. Then $q \mid p$ if and only if there exists a non empty, finite subset S_2 of F such that q is a product of linear polynomials of F and S_2 and $S_2 \subseteq S_1$. The theorem is a consequence of (49), (14), and (13).

(51) Let us consider a field F, a product of linear polynomials p of F, a monic polynomial q over F, and an element a of F. Then $q \mid \operatorname{rpoly}(1, a) * p$ if

and only if $q \mid p$ or there exists a polynomial r over F such that $r \mid p$ and $q = \mathrm{rpoly}(1, a) * r$. The theorem is a consequence of (16), (49), and (38).

(52) Let us consider a field F, a product of linear polynomials p of F, and a polynomial q over F. Then $\mathrm{Roots}(p) \cap \mathrm{Roots}(q) = \emptyset$ if and only if $\gcd(p, q) = \mathbf{1}.F$.

(53) Let us consider a field F, non empty, finite subsets S_1, S_2 of F, a product of linear polynomials p_1 of F and S_1, and a polynomial p_2 over F. Suppose $S_2 = S_1 \cap \mathrm{Roots}(p_2)$. Then $\gcd(p_1, p_2)$ is a product of linear polynomials of F and S_2.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non empty, finite subsets S_1, S_2 of F for every product of linear polynomials p_1 of F and S_1 for every polynomial p_2 over F such that $\overline{\overline{S_2}} = \$_1$ and $S_2 = S_1 \cap \mathrm{Roots}(p_2)$ holds $\gcd(p_1, p_2)$ is a product of linear polynomials of F and S_2. $\mathcal{P}[1]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{S_2}} = n$. $\square$

Let R be an integral domain and p be a polynomial over R. The functors: Divisors(p) and MonicDivisors(p) yielding non empty subsets of the carrier of Polynom-Ring R are defined by terms

(Def. 4) $\{q$, where q is an element of the carrier of Polynom-Ring $R : q \mid p\}$,

(Def. 5) $\{q$, where q is a monic element of the carrier of Polynom-Ring $R : q \mid p\}$,

respectively. Now we state the propositions:

(54) Let us consider a field F, and an element a of F.
Then $\mathrm{MonicDivisors}(\mathrm{rpoly}(1, a)) = \{\mathbf{1}.F, \mathrm{rpoly}(1, a)\}$.

(55) Let us consider a field F, a non zero element p of the carrier of Polynom-Ring F, and a non zero element a of F.
Then $\mathrm{MonicDivisors}(p) = \mathrm{MonicDivisors}(a \cdot p)$.

(56) Let us consider a field F, an extension E of F, a polynomial p over F, and a polynomial q over E. If $q = p$, then $\mathrm{MonicDivisors}(p) \subseteq \mathrm{MonicDivisors}(q)$.

Let F be a field and p be a non zero polynomial over F. Let us note that MonicDivisors(p) is finite. Now we state the proposition:

(57) Let us consider a field F, and a non zero polynomial p over F. Then $\overline{\overline{\mathrm{MonicDivisors}(p)}} \leqslant 2^{\deg(p)}$. The theorem is a consequence of (55), (56), and (16).

5. Formal Derivative of Polynomials and Multiplicity of Roots

Let R be a ring. We introduce the notation $\mathrm{Deriv}(R)$ as a synonym of $\mathrm{Der1}(R)$. Let R be an integral domain. Observe that $\mathrm{Deriv}(R)$ is derivation. Now we state the propositions:

(58) Let us consider a non degenerated commutative ring R. Then

(i) $(\mathrm{Deriv}(R))(\mathbf{1}.R) = \mathbf{0}.R$, and

(ii) $(\mathrm{Deriv}(R))(\mathbf{0}.R) = \mathbf{0}.R$.

(59) Let us consider a ring R, an element p of the carrier of Polynom-Ring R, and an element a of R. Then $(\mathrm{Deriv}(R))(a \cdot p) = a \cdot (\mathrm{Deriv}(R))(p)$.

(60) Let us consider a non degenerated commutative ring R, and a constant element p of the carrier of Polynom-Ring R. Then $(\mathrm{Deriv}(R))(p) = \mathbf{0}.R$. The theorem is a consequence of (59) and (58).

(61) Let us consider a ring R, and an element a of R. Then $(\mathrm{Deriv}(R))(\mathrm{X} - a) = \mathbf{1}.R$.

(62) Let us consider a non degenerated commutative ring R, and an element p of the carrier of Polynom-Ring R. Then $(\mathrm{Deriv}(R))(p^0) = \mathbf{0}.R$. The theorem is a consequence of (58).

(63) Let us consider an integral domain R, an element p of the carrier of Polynom-Ring R, and a non zero element n of $\mathbb{N}$. Then $(\mathrm{Deriv}(R))(p^n) = n \cdot (p^{n-1} \cdot (\mathrm{Deriv}(R))(p))$.

(64) Let us consider a non degenerated commutative ring R, and a non zero element p of the carrier of Polynom-Ring R. Then $\deg((\mathrm{Deriv}(R))(p)) < \deg(p)$.

(65) Let us consider a field F, and a non zero element p of the carrier of Polynom-Ring F. Suppose $\gcd(p, (\mathrm{Deriv}(F))(p)) = \mathbf{1}.F$. Then p is square-free.

(66) Let us consider a non degenerated commutative ring R, an element p of the carrier of Polynom-Ring R, a commutative ring extension S of R, and an element q of the carrier of Polynom-Ring S. If $q = p$, then $(\mathrm{Deriv}(S))(q) = (\mathrm{Deriv}(R))(p)$. The theorem is a consequence of (3).

Let R be a non degenerated commutative ring, S be a commutative ring extension of R, p be a non zero polynomial over R, and a be an element of S. The functor multiplicity(p, a) yielding an element of $\mathbb{N}$ is defined by

(Def. 6) there exists a non zero polynomial q over S such that $q = p$ and $it = \mathrm{multiplicity}(q, a)$.

Now we state the propositions:

(67) Let us consider a field F, a non zero polynomial p over F, an element a of F, and an element n of $\mathbb{N}$. Then $n = \mathrm{multiplicity}(p, a)$ if and only if $(\mathrm{X} - a)^n \mid p$ and $(\mathrm{X} - a)^{n+1} \nmid p$.

(68) Let us consider a field F with characteristic 0, and a non zero element p of the carrier of Polynom-Ring F. Then $\deg((\mathrm{Deriv}(F))(p)) = \deg(p) - 1$. The theorem is a consequence of (60) and (64).

(69) Let us consider a field F with characteristic 0, and an element p of the carrier of Polynom-Ring F. Then $(\mathrm{Deriv}(F))(p) = \mathbf{0}.F$ if and only if p is constant. The theorem is a consequence of (68) and (60).

(70) Let us consider a field F with characteristic 0, and an irreducible element p of the carrier of Polynom-Ring F. Then $\gcd(p, (\mathrm{Deriv}(F))(p)) = \mathbf{1}.F$. The theorem is a consequence of (69) and (64).

(71) Let us consider a field F with characteristic 0, an irreducible element p of the carrier of Polynom-Ring F, an extension E of F, and an element a of E. If a is a root of p in E, then $\mathrm{multiplicity}(p, a) = 1$. The theorem is a consequence of (66), (70), (45), (65), (67), and (40).

6. Simple Extensions

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

(Def. 7) there exists an element a of E such that $E \approx \mathrm{FAdj}(F, \{a\})$.

Let a be an element of E. We say that a is F-primitive if and only if

(Def. 8) $E \approx \mathrm{FAdj}(F, \{a\})$.

Let us note that there exists an extension of F which is F-simple and F-finite. Let E be an F-simple extension of F. One can verify that there exists an element of E which is F-primitive.

Let E be an extension of F and a be an element of E. The functor $\deg(a, F)$ yielding an integer is defined by the term

(Def. 9) $\deg(\mathrm{FAdj}(F, \{a\}), F)$.

Now we state the propositions:

(72) Let us consider a field F, an F-finite extension E of F, and an element a of E. Then $\deg(a, F) \mid \deg(E, F)$.

(73) Let us consider a field F, and an F-finite extension E of F. Then E is F-simple if and only if there exists an element a of E such that $\deg(a, F) = \deg(E, F)$.

(74) Let us consider a field F, an F-finite extension E of F, and an element a of E. Then a is F-primitive if and only if $\deg(a, F) = \deg(E, F)$.

(75) Let us consider a field F, an F-finite extension K of F, an F-finite, F-extending extension E of K, and a K-algebraic element a of E. Suppose $E \approx \mathrm{FAdj}(F, \{a\})$. Then

(i) $E \approx \mathrm{FAdj}(K, \{a\})$, and

(ii) $K \approx \mathrm{FAdj}(F, \mathrm{Coeff}(\mathrm{MinPoly}(a, K)))$.

PROOF: $\mathrm{FAdj}(K, \{a\}) = \mathrm{FAdj}(F, \{a\})$ by [9, (11)]. Set $K_1 = \mathrm{FAdj}(F, \mathrm{Coeff}(\mathrm{MinPoly}(a, K)))$. Reconsider $E_1 = E$ as an F-extending extension of K_1. Reconsider $a_1 = a$ as a K_1-algebraic element of E_1. $\mathrm{FAdj}(F, \{a_1\}) = \mathrm{FAdj}(K_1, \{a_1\})$. Reconsider $p = \mathrm{MinPoly}(a, K)$ as a polynomial over K_1. p is irreducible. □

(76) Let us consider an infinite field F, and an F-finite extension E of F. Then E is F-simple if and only if $\mathrm{IntermediateFields}(E, F)$ is finite. The theorem is a consequence of (5), (2), (4), (75), and (22).

(77) Let us consider a field F with characteristic 0, an extension E of F, and F-algebraic elements a, b of E. Then there exists an element x of F such that $\mathrm{FAdj}(F, \{a, b\}) = \mathrm{FAdj}(F, \{a + ({}^{@}(x, E)) \cdot b\})$.

PROOF: Set $K = \mathrm{FAdj}(F, \{a, b\})$. Set $m_1 = \mathrm{MinPoly}(a, F)$. Set $m_3 = \mathrm{MinPoly}(b, F)$. Reconsider $a_3 = a$, $b_1 = b$ as an element of K. Consider Z being an extension of E such that Z is algebraic closed. Set $R_1 = \mathrm{Roots}(Z, m_1)$. Set $R_2 = (\mathrm{Roots}(Z, m_3)) \setminus \{b\}$. There exists an element x of F such that for every elements c, d of Z such that $c \in R_1$ and $d \in R_2$ holds $({}^{@}(a_3, Z)) + ({}^{@}(x, Z)) \cdot ({}^{@}(b_1, Z)) \neq c + ({}^{@}(x, Z)) \cdot d$.

Consider x being an element of F such that for every elements c, d of Z such that $c \in R_1$ and $d \in R_2$ holds $({}^{@}(a_3, Z)) + ({}^{@}(x, Z)) \cdot ({}^{@}(b_1, Z)) \neq c + ({}^{@}(x, Z)) \cdot d$. Set $l_1 = ({}^{@}(a_3, Z)) + ({}^{@}(x, Z)) \cdot ({}^{@}(b_1, Z))$. Set $G = \mathrm{FAdj}(F, \{l_1\})$. G is a subfield of K. Reconsider $m_2 = \mathrm{MinPoly}(a, F)$, $m_4 = \mathrm{MinPoly}(b, F)$ as a polynomial over G.

Reconsider $m_2 = \mathrm{MinPoly}(a, F)$, $m_4 = \mathrm{MinPoly}(b, F)$ as a non constant polynomial over G. Set $g = \langle {}^{@}(G, l_1), -({}^{@}(x, G)) \rangle$. Set $h = m_2[g]$. Reconsider $m_5 = m_4$, $h_1 = h$ as a polynomial over Z. $\gcd(h_1, m_5) = \mathrm{X} - ({}^{@}(b_1, Z))$. $b \in G$. $a \in G$. $a + ({}^{@}(x, E)) \cdot b = ({}^{@}(a_3, Z)) + ({}^{@}(x, Z)) \cdot ({}^{@}(b_1, Z))$ by [10, (12)]. □

Let F be a field with characteristic 0. One can verify that every F-finite extension of F is F-simple.

References

[1] Andreas Gathmann. *Einführung in die Algebra*. Lecture Notes, University of Kaiserslautern, Germany, 2011.

[2] Adam Grabowski and Christoph Schwarzweller. Translating mathematical vernacular into knowledge repositories. In Michael Kohlhase, editor, *Mathematical Knowledge Management*, volume 3863 of *Lecture Notes in Computer Science*, pages 49–64. Springer, 2006. doi:10.1007/11618027_4. 4th International Conference on Mathematical Knowledge Management, Bremen, Germany, MKM 2005, July 15–17, 2005, Revised Selected Papers.

[3] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Mizar in a nutshell. *Journal of Formalized Reasoning*, 3(2):153–245, 2010.

[4] 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.

[5] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[6] Serge Lang. *Algebra*. PWN, Warszawa, 1984.

[7] Serge Lang. *Algebra*. Springer Verlag, 2002 (Revised Third Edition).

[8] Heinz Lüneburg. *Gruppen, Ringe, Körper: Die grundlegenden Strukturen der Algebra*. Oldenbourg Verlag, 1999.

[9] Christoph Schwarzweller. Normal extensions. *Formalized Mathematics*, 31(1):121–130, 2023. doi:10.2478/forma-2023-0011.

[10] Christoph Schwarzweller. Renamings and a condition-free formalization of Kronecker's construction. *Formalized Mathematics*, 28(**2**):129–135, 2020. doi:10.2478/forma-2020-0012.

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

[12] Christoph Schwarzweller. Splitting fields. *Formalized Mathematics*, 29(**3**):129–139, 2021. doi:10.2478/forma-2021-0013.

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

[14] Christoph Schwarzweller, Artur Korniłowicz, and Agnieszka Rowińska-Schwarzweller. Some algebraic properties of polynomial rings. *Formalized Mathematics*, 24(**3**):227–237, 2016. doi:10.1515/forma-2016-0019.

[15] Yasushige Watase. Derivation of commutative rings and the Leibniz formula for power of derivation. *Formalized Mathematics*, 29(**1**):1–8, 2021. doi:10.2478/forma-2021-0001.

Accepted December 18, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 299–308, 2023
DOI: 10.2478/forma-2023-0024
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Symmetrical Piecewise Linear Functions Composed by Absolute Value Function

Takashi Mitsuishi
Faculty of Business and Informatics
Nagano University, Japan

Summary. We continue the formal development of the application of piecewise linear functions and centroids in the area of fuzzy set theory. The corresponding piecewise linear functions are symmetrical and composed by absolute function. In this paper we prove that the membership functions of isosceles triangle type and isosceles trapezoid type can be constructed by functions of this type.

MSC: 03E72 68V20

Keywords: fuzzy set; fuzzy number; centroid

MML identifier: FUZZY_8, version: 8.1.14 5.76.1462

Introduction

In this paper, some mathematical properties of piecewise linear functions are formalized in Mizar [11], [10] in order to use them in fuzzy set theory [2], [22]. The focused piecewise linear functions are symmetrical and composed by absolute function. L-R fuzzy number is applied for various fields [1], [3], [20], [12]. Since isosceles triangle type and isosceles trapezoid type membership functions are simple [4], they are applied for the membership functions of L-R fuzzy number in most cases [17]. It is formalized that the membership functions of isosceles triangle type [16] and isosceles trapezoid type (introduced formally in Mizar in [5]) can be constructed by absolute value functions. We wanted to avoid duplication [9] of some basic functional notions, so we use extensively Mizar functor "AffineMap" denoting just linear function with two parameters.

We prove that the centroids of the composite function of two continuous functions are the weighted averages of the areas and centroids of the functions

that compose them [21]. Moreover, some calculation and operation between membership functions for fuzzy approximate reasoning [19], e.g. Mamdani method [13] and the product-sum-gravity method [18] are formalized, extending also the development of both fuzzy numbers within the Mizar Mathematical Library [7] and fuzzy sets in general [14], [15], [8] (for another recent formal development in this area, see [6]).

1. Preliminaries

From now on A denotes a non empty, closed interval subset of $\mathbb{R}$. Now we state the proposition:

(1) Let us consider real numbers b, c, d. If $b > 0$ and $c > 0$ and $d > 0$, then $\frac{b-d}{\frac{b}{c}} < c$.

Let us consider real numbers a, x. Now we state the propositions:

(2) $a - |a \cdot x| \leqslant a$.

(3) $a - |x| \leqslant a$.

(4) Let us consider real numbers a, b, c, x. Then $|\frac{b\cdot(a-x-a)}{c}| = |\frac{b\cdot(a+x-a)}{c}|$.

Let us consider real numbers a, b, c. Now we state the propositions:

(5) $|\max(c, a) - \max(c, b)| \leqslant |a - b|$.

(6) $|\min(c, a) - \min(c, b)| \leqslant |a - b|$.

(7) Let us consider real numbers a, b, c, d. Then $|\min(c, \max(d, a)) - \min(c, \max(d, b))| \leqslant |a - b|$. The theorem is a consequence of (6) and (5).

2. Continuous Functions

Let us consider a real number c and partial functions f, g from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(8) Suppose $]-\infty, c] \subseteq \operatorname{dom} f$ and $[c, +\infty[\subseteq \operatorname{dom} g$.
Then $f\restriction]-\infty, c[+ \cdot g\restriction [c, +\infty[= f\restriction]-\infty, c] + \cdot g\restriction [c, +\infty[$.
Proof: Set $f_1 = f\restriction]-\infty, c[+ \cdot g\restriction [c, +\infty[$. Set $f_2 = f\restriction]-\infty, c] + \cdot g\restriction [c, +\infty[$. For every object x such that $x \in \operatorname{dom} f_1$ holds $f_1(x) = f_2(x)$. □

(9) Suppose f is continuous and g is continuous and $f(c) = g(c)$ and $]-\infty, c] \subseteq \operatorname{dom} f$ and $[c, +\infty[\subseteq \operatorname{dom} g$. Then $f\restriction]-\infty, c] + \cdot g\restriction [c, +\infty[$ is continuous.
Proof: Set $F = f\restriction]-\infty, c] + \cdot g\restriction [c, +\infty[$. For every real number x_0 such that $x_0 \in \operatorname{dom} F$ holds F is continuous in x_0. □

(10) Let us consider a real number c, and functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Suppose f is continuous and g is continuous and $f(c) = g(c)$. Then $f\restriction]-\infty, c] + \cdot g\restriction[c, +\infty[$ is a continuous function from $\mathbb{R}$ into $\mathbb{R}$. The theorem is a consequence of (9).

(11) Let us consider real numbers a, b, c, and functions f, g, h from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a \leqslant b \leqslant c$ and f is continuous and g is continuous and $h\restriction[a, c] = f\restriction[a, b] + \cdot g\restriction[b, c]$ and $f(b) = g(b)$. Then $\int\limits_{[a,c]} h(x)dx = \int\limits_{[a,b]} f(x)dx + \int\limits_{[b,c]} g(x)dx$.

(12) Let us consider a function f from $\mathbb{R}$ into $\mathbb{R}$, and real numbers a, b, c. Suppose $a \leqslant b \leqslant c$ and $[a, c] \subseteq \operatorname{dom} f$ and $f\restriction[a, b]$ is bounded and $f\restriction[b, c]$ is bounded and f is integrable on $[a, b]$ and f is integrable on $[b, c]$. Then

(i) f is integrable on $[a, c]$, and

(ii) $\int\limits_a^c f(x)dx = \int\limits_a^b f(x)dx + \int\limits_b^c f(x)dx$.

(13) Let us consider real numbers a, b, c, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a \leqslant c$ and f is integrable on $[a, c]$ and $f\restriction[a, c]$ is bounded and $[a, c] \subseteq \operatorname{dom} f$ and $b \in [a, c]$. Then

(i) f is integrable on $[a, b]$, and

(ii) f is integrable on $[b, c]$, and

(iii) $\int\limits_a^c f(x)dx = \int\limits_a^b f(x)dx + \int\limits_b^c f(x)dx$.

(14) Let us consider a real number a, and functions f, g, h from $\mathbb{R}$ into $\mathbb{R}$. Suppose $f\restriction A$ is bounded and f is integrable on A and $g\restriction A$ is bounded and g is integrable on A and $a \in A$ and $h = f\restriction]-\infty, a] + \cdot g\restriction[a, +\infty[$ and $f(a) = g(a)$. Then h is integrable on A.

PROOF: For every object x such that $x \in \operatorname{dom}(f\restriction[\inf A, a])$ holds $(f\restriction[\inf A, a])(x) = (h\restriction[\inf A, a])(x)$. For every object x such that $x \in \operatorname{dom}(g\restriction[a, \sup A])$ holds $(g\restriction[a, \sup A])(x) = (h\restriction[a, \sup A])(x)$. f is integrable on $[\inf A, a]$. g is integrable on $[a, \sup A]$. □

(15) Let us consider real numbers a, b, c, and functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a \leqslant b \leqslant c$. Then $(f\restriction]-\infty, b] + \cdot g\restriction[b, +\infty[)\restriction[a, c] = f\restriction[a, b] + \cdot g\restriction[b, c]$.

PROOF: For every object x such that $x \in \operatorname{dom}((f\restriction]-\infty, b] + \cdot g\restriction[b, +\infty[)\restriction[a, c])$ holds $((f\restriction]-\infty, b] + \cdot g\restriction[b, +\infty[)\restriction[a, c])(x) = (f\restriction[a, b] + \cdot g\restriction[b, c])(x)$. □

(16) Let us consider real numbers a, b, c, and functions f, g, h from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a \leqslant b \leqslant c$ and f is integrable on $[a, c]$ and $f\restriction[a, c]$ is bounded and g is integrable on $[a, c]$ and $g\restriction[a, c]$ is bounded and $h = f\restriction]-\infty, b] + \cdot g\restriction[b, +\infty[$ and $f(b) = g(b)$. Then $\int\limits_{[a,c]} h(x)dx = \int\limits_{[a,b]} f(x)dx + \int\limits_{[b,c]} g(x)dx$. The theorem is a consequence of (15) and (14).

3. Area and Centroid of Continuous Functions

Now we state the propositions:

(17) Let us consider functions f, g, h from $\mathbb{R}$ into $\mathbb{R}$, and real numbers a, b, c. Suppose $a \leqslant b \leqslant c$ and f is continuous and g is continuous and $h\restriction[a, c] = f\restriction[a, b] + \cdot g\restriction[b, c]$ and $\int\limits_{[a,b]} f(x)dx \neq 0$ and $\int\limits_{[b,c]} g(x)dx \neq 0$ and $f(b) = g(b)$. Then $\operatorname{centroid}(h, [a, c]) = \frac{1}{\int\limits_{[a,c]} h(x)dx} \cdot ((\operatorname{centroid}(f, [a, b])) \cdot (\int\limits_{[a,b]} f(x)dx) + (\operatorname{centroid}(g, [b, c])) \cdot (\int\limits_{[b,c]} g(x)dx))$.

(18) Let us consider a function f from $\mathbb{R}$ into $\mathbb{R}$, and real numbers a, b, c. Suppose for every real number x, $f(x) = b - |\frac{b\cdot(x-a)}{c}|$. Let us consider a real number y. Then $f(a - y) = f(a + y)$.

(19) Let us consider a function f from $\mathbb{R}$ into $\mathbb{R}$, and real numbers a, b, c, d, e. Suppose for every real number x, $f(x) = \min(d, \max(e, b - |\frac{b\cdot(x-a)}{c}|))$. Let us consider a real number y. Then $f(a - y) = f(a + y)$.

(20) Let us consider real numbers a, b, c, d. Suppose $b > 0$ and $c > 0$ and $d > 0$ and $d < b$. Let us consider a real number x. Then $(d \cdot \operatorname{TrapezoidalFS}((a - c), (a + \frac{d-b}{\frac{b}{c}}), (a + \frac{b-d}{\frac{b}{c}}), (a + c)))(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$.

Proof: For every real number x, $(d \cdot \operatorname{TrapezoidalFS}((a-c), (a+\frac{d-b}{\frac{b}{c}}), (a+\frac{b-d}{\frac{b}{c}}), (a + c)))(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. □

(21) Let us consider real numbers a, b, c, d. Suppose $b > 0$ and $c > 0$ and $d > 0$ and $d < b$. Then $\operatorname{centroid}(d \cdot \operatorname{TrapezoidalFS}((a - c), (a + \frac{d-b}{\frac{b}{c}}), (a + \frac{b-d}{\frac{b}{c}}), (a + c)), [a - c, a + c]) = a$.

Let us consider real numbers a, b, c, d and a function f from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(22) Suppose $b > 0$ and $c > 0$ and $d > 0$ and $d < b$ and for every real number x, $f(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. Then $f = d \cdot \text{TrapezoidalFS}((a - c), (a + \frac{d-b}{\frac{b}{c}}), (a + \frac{b-d}{\frac{b}{c}}), (a + c))$. The theorem is a consequence of (20).

(23) Suppose $b > 0$ and $c > 0$ and $d > 0$ and $d < b$ and for every real number x, $f(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. Then $\text{centroid}(f, [a - c, a + c]) = a$. The theorem is a consequence of (22) and (21).

Let us consider real numbers a, b, c, d, e and a function f from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(24) If $b \neq 0$ and $c \neq 0$ and for every real number x, $f(x) = \min(d, \max(e, b - |\frac{b\cdot(x-a)}{c}|))$, then f is Lipschitzian.

PROOF: There exists a real number r such that $0 < r$ and for every real numbers x_1, x_2 such that $x_1, x_2 \in \text{dom } f$ holds $|f(x_1) - f(x_2)| \leqslant r \cdot |x_1 - x_2|$. □

(25) If $c \neq 0$ and for every real number x, $f(x) = \min(d, \max(e, b - |\frac{b\cdot(x-a)}{c}|))$, then f is Lipschitzian. The theorem is a consequence of (24).

Let us consider real numbers a, b, c, d and a function f from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(26) Suppose $c > 0$ and for every real number x, $f(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. Then

(i) f is integrable on A, and

(ii) $f \restriction A$ is bounded.

The theorem is a consequence of (25).

(27) Suppose $b > 0$ and $c > 0$ and $d > 0$ and for every real number x, $f(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. Then

(i) $f(\inf[a - c, a + c]) = 0$, and

(ii) $f(\sup[a - c, a + c]) = 0$.

(28) Let us consider real numbers a, b, c. Suppose $b > 0$ and $c > 0$. Let us consider a real number x. If $x \notin [a - c, a + c]$, then $\max(0, b - |\frac{b\cdot(x-a)}{c}|) = 0$.

PROOF: Define $\mathcal{H}(\text{element of } \mathbb{R}) = (\max(0, b - |\frac{b\cdot(\$_1 - a)}{c}|))(\in \mathbb{R})$. Consider h being a function from $\mathbb{R}$ into $\mathbb{R}$ such that for every element x of $\mathbb{R}$, $h(x) = \mathcal{H}(x)$. For every real number x, $h(x) = \max(0, b - |\frac{b\cdot(x-a)}{c}|)$. □

(29) Let us consider real numbers a, b, c, d. Suppose $b > 0$ and $c > 0$ and $d > 0$. Let us consider a real number x. Suppose $x \notin [a - c, a + c]$. Then $\min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|)) = 0$. The theorem is a consequence of (28).

Let us consider real numbers a, b, c, d, a function f from $\mathbb{R}$ into $\mathbb{R}$, and a real number x. Now we state the propositions:

(30) Suppose $b > 0$ and $c > 0$ and $d > 0$ and for every real number x, $f(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. Then if $x \notin [a-c, a+c]$, then $f(x) = 0$. The theorem is a consequence of (29).

(31) Suppose $b > 0$ and $c > 0$ and $d > 0$ and for every real number x, $f(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. Then if $x \in A \setminus [a - c, a + c]$, then $f(x) = 0$. The theorem is a consequence of (30).

Let us consider real numbers a, b, c, d and a function f from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(32) Suppose $b > 0$ and $c > 0$ and $d > 0$ and $[a-c, a+c] \subseteq A$ and for every real number x, $f(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. Then $\operatorname{centroid}(f, A) = a$. The theorem is a consequence of (26), (31), (27), and (23).

(33) Suppose $b > 0$ and $c > 0$ and $d > 0$ and $[a - c, a + c] \subseteq A$ and $d < b$ and for every real number x, $f(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. Then $\operatorname{centroid}(f, A) = \operatorname{centroid}(f, [a - c, a + c])$. The theorem is a consequence of (32) and (23).

(34) Let us consider real numbers a, b, c, d, and functions f, F from $\mathbb{R}$ into $\mathbb{R}$. Suppose $b > 0$ and $c > 0$ and $d > 0$ and for every real number x, $f(x) = \max(0, b-|\frac{b\cdot(x-a)}{c}|)$ and for every real number x, $F(x) = \min(d, \max(0, b-|\frac{b\cdot(x-a)}{c}|))$. Then $\operatorname{centroid}(f, [a - c, a + c]) = \operatorname{centroid}(F, [a - c, a + c])$. The theorem is a consequence of (23) and (3).

(35) Let us consider real numbers a, b, c, d, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $b > 0$ and $c > 0$ and $d > 0$ and $d < b$ and for every real number x, $f(x) = \min(d, \max(0, b - |\frac{b\cdot(x-a)}{c}|))$. Then $f\restriction[a - c, a + c] = ((\operatorname{AffineMap}(\frac{b}{c}, b - \frac{a\cdot b}{c}))\restriction[a - c, a + \frac{d-b}{\frac{b}{c}}]+\cdot(\operatorname{AffineMap}(0, d))\restriction[a + \frac{d-b}{\frac{b}{c}}, a + \frac{b-d}{\frac{b}{c}}])+\cdot(\operatorname{AffineMap}(-\frac{b}{c}, b + \frac{a\cdot b}{c}))\restriction[a + \frac{b-d}{\frac{b}{c}}, a + c]$.

Proof: $-\frac{b-d}{\frac{b}{c}} > -c$. $\frac{b-d}{\frac{b}{c}} < c$. For every object x such that $x \in \operatorname{dom}(f\restriction[a-c, a + c])$ holds $(f\restriction[a - c, a + c])(x) = (((\operatorname{AffineMap}(\frac{b}{c}, b - \frac{a\cdot b}{c}))\restriction[a - c, a + \frac{d-b}{\frac{b}{c}}]+\cdot(\operatorname{AffineMap}(0, d))\restriction[a+\frac{d-b}{\frac{b}{c}}, a+\frac{b-d}{\frac{b}{c}}])+\cdot(\operatorname{AffineMap}(-\frac{b}{c}, b+\frac{a\cdot b}{c}))\restriction[a+\frac{b-d}{\frac{b}{c}}, a + c])(x)$. □

4. Some Special Examples

Now we state the proposition:

(36) Let us consider real numbers a, b, c, d, r, s. Suppose $a < b < c < d$. Then

(i) $(\operatorname{AffineMap}(\frac{r}{b-a}, -\frac{a\cdot r}{b-a}))(a) = 0$, and

(ii) $(\operatorname{AffineMap}(\frac{r}{b-a}, -\frac{a\cdot r}{b-a}))(b) = r$, and

(iii) $(\mathrm{AffineMap}(\frac{s-r}{c-b}, s - \frac{c\cdot(s-r)}{c-b}))(b) = r$, and

(iv) $(\mathrm{AffineMap}(\frac{s-r}{c-b}, s - \frac{c\cdot(s-r)}{c-b}))(c) = s$, and

(v) $(\mathrm{AffineMap}(\frac{-s}{d-c}, -\frac{d\cdot(-s)}{d-c}))(c) = s$, and

(vi) $(\mathrm{AffineMap}(\frac{-s}{d-c}, -\frac{d\cdot(-s)}{d-c}))(d) = 0$.

Let us consider real numbers a, b, c, d, r, s and a function f from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(37) Suppose $a < b < c < d$ and $f\restriction[a,d] = ((\mathrm{AffineMap}(\frac{r}{b-a}, -\frac{a\cdot r}{b-a}))\restriction[a,b] + \cdot (\mathrm{AffineMap}(\frac{s-r}{c-b}, s - \frac{c\cdot(s-r)}{c-b}))\restriction[b,c]) + \cdot (\mathrm{AffineMap}(\frac{-s}{d-c}, -\frac{d\cdot(-s)}{d-c}))\restriction[c,d]$. Then $\int_{[a,d]} (\mathrm{id}_{\mathbb{R}} \cdot f)(x)dx = \int_{[a,b]} (\mathrm{id}_{\mathbb{R}} \cdot (\mathrm{AffineMap}(\frac{r}{b-a}, -\frac{a\cdot r}{b-a})))(x)dx + \int_{[b,c]} (\mathrm{id}_{\mathbb{R}} \cdot (\mathrm{AffineMap}(\frac{s-r}{c-b}, s - \frac{c\cdot(s-r)}{c-b})))(x)dx + \int_{[c,d]} (\mathrm{id}_{\mathbb{R}} \cdot (\mathrm{AffineMap}(\frac{-s}{d-c}, -\frac{d\cdot(-s)}{d-c})))(x)dx$.

PROOF: Set $f_3 = \mathrm{AffineMap}(\frac{r}{b-a}, -\frac{a\cdot r}{b-a})$. Set $f_4 = \mathrm{AffineMap}(\frac{s-r}{c-b}, s - \frac{c\cdot(s-r)}{c-b})$. Reconsider $h = f_3\restriction]-\infty, b[+ \cdot f_4\restriction[b, +\infty[$ as a function from $\mathbb{R}$ into $\mathbb{R}$. $f_3(b) = r$. For every object x such that $x \in \mathrm{dom}(h\restriction[a,c])$ holds $(h\restriction[a,c])(x) = (f_3\restriction[a,b] + \cdot f_4\restriction[b,c])(x)$. □

(38) Suppose $a < b < c < d$ and $f\restriction[a,d] = ((\mathrm{AffineMap}(\frac{r}{b-a}, -\frac{a\cdot r}{b-a}))\restriction[a,b] + \cdot (\mathrm{AffineMap}(\frac{s-r}{c-b}, s - \frac{c\cdot(s-r)}{c-b}))\restriction[b,c]) + \cdot (\mathrm{AffineMap}(\frac{-s}{d-c}, -\frac{d\cdot(-s)}{d-c}))\restriction[c,d]$. Then $\int_{[a,d]} f(x)dx = \int_{[a,b]} (\mathrm{AffineMap}(\frac{r}{b-a}, -\frac{a\cdot r}{b-a}))(x)dx + \int_{[b,c]} (\mathrm{AffineMap}(\frac{s-r}{c-b}, s - \frac{c\cdot(s-r)}{c-b}))(x)dx + \int_{[c,d]} (\mathrm{AffineMap}(\frac{-s}{d-c}, -\frac{d\cdot(-s)}{d-c}))(x)dx$.

PROOF: Set $f_3 = \mathrm{AffineMap}(\frac{r}{b-a}, -\frac{a\cdot r}{b-a})$. Set $f_4 = \mathrm{AffineMap}(\frac{s-r}{c-b}, s - \frac{c\cdot(s-r)}{c-b})$. Reconsider $h = f_3\restriction]-\infty, b[+ \cdot f_4\restriction[b, +\infty[$ as a function from $\mathbb{R}$ into $\mathbb{R}$. $f_3(b) = r$. For every object x such that $x \in \mathrm{dom}(h\restriction[a,c])$ holds $(h\restriction[a,c])(x) = (f_3\restriction[a,b] + \cdot f_4\restriction[b,c])(x)$. $\int_{[a,c]} h(x)dx = \int_{[a,b]} f_3(x)dx + \int_{[b,c]} f_4(x)dx$.

□

Let us consider real numbers a, b, c, d, r, s, x. Now we state the propositions:

(39) Suppose $a < b < c < d$ and $r \geqslant 0$ and $s \geqslant 0$ and ($x < a$ or $d < x$). Then $(((\mathrm{AffineMap}(\frac{r}{b-a}, -\frac{a\cdot r}{b-a}))\restriction]-\infty, b] + \cdot (\mathrm{AffineMap}(\frac{s-r}{c-b}, s - \frac{c\cdot(s-r)}{c-b}))\restriction[b,c]) + \cdot (\mathrm{AffineMap}(\frac{-s}{d-c}, -\frac{d\cdot(-s)}{d-c}))\restriction[c, +\infty[)(x) \leqslant 0$.

(40) Suppose $a < b < c < d$ and $r \geqslant 0$ and $s \geqslant 0$ and $x \in [a, d]$. Then $(((\text{AffineMap}(\frac{r}{b-a}, -\frac{a \cdot r}{b-a}))\restriction]-\infty, b] + \cdot (\text{AffineMap}(\frac{s-r}{c-b}, s - \frac{c \cdot (s-r)}{c-b}))\restriction [b, c]) + \cdot (\text{AffineMap}(\frac{-s}{d-c}, -\frac{d \cdot (-s)}{d-c}))\restriction [c, +\infty[)(x) \geqslant 0$.

(41) Let us consider real numbers a, b, c, d, r, s. Suppose $a < b < c < d$ and $r \geqslant 0$ and $s \geqslant 0$ and $r = s$. Let us consider a real number x. Then $(r \cdot \text{TrapezoidalFS}(a, b, c, d))(x) = \max_+((((\text{AffineMap}(\frac{r}{b-a}, -\frac{a \cdot r}{b-a}))\restriction]-\infty, b] + \cdot (\text{AffineMap}(\frac{s-r}{c-b}, s - \frac{c \cdot (s-r)}{c-b}))\restriction [b, c]) + \cdot (\text{AffineMap}(\frac{-s}{d-c}, -\frac{d \cdot (-s)}{d-c}))\restriction [c, +\infty[)(x))$.

Proof: Set $T = \text{TrapezoidalFS}(a, b, c, d)$. For every real number x, $(r \cdot T)(x) = \max_+((((\text{AffineMap}(\frac{r}{b-a}, -\frac{a \cdot r}{b-a}))\restriction]-\infty, b] + \cdot (\text{AffineMap}(\frac{s-r}{c-b}, s - \frac{c \cdot (s-r)}{c-b}))\restriction [b, c]) + \cdot (\text{AffineMap}(\frac{-s}{d-c}, -\frac{d \cdot (-s)}{d-c}))\restriction [c, +\infty[)(x))$. $\square$

(42) Let us consider real numbers a, b, c, d. Suppose $c \leqslant d$. Then

(i) $\int\limits_{[c,d]} (\text{id}_{\mathbb{R}} \cdot (\text{AffineMap}(a, b)))(x)dx = (d-c) \cdot (\dfrac{a \cdot (d \cdot d + d \cdot c + c \cdot c)}{3} + \dfrac{b \cdot (d+c)}{2})$, and

(ii) $\int\limits_{[c,d]} (\text{AffineMap}(a, b))(x)dx = (d-c) \cdot (\dfrac{a \cdot (d+c)}{2} + b)$.

(43) Let us consider real numbers a, b, c, d, r, s, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a < b < c < d$ and $f\restriction [a, d] = ((\text{AffineMap}(\frac{r}{b-a}, -\frac{a \cdot r}{b-a}))\restriction [a, b] + \cdot (\text{AffineMap}(\frac{s-r}{c-b}, s - \frac{c \cdot (s-r)}{c-b}))\restriction [b, c]) + \cdot (\text{AffineMap}(\frac{-s}{d-c}, -\frac{d \cdot (-s)}{d-c}))\restriction [c, d]$. Then $\text{centroid}(f, [a, d]) = \Bigg((b-a) \cdot (\frac{\frac{r}{b-a} \cdot (b \cdot b + b \cdot a + a \cdot a)}{3} + \frac{(-\frac{a \cdot r}{b-a}) \cdot (b+a)}{2}) + (c-b) \cdot (\frac{\frac{s-r}{c-b} \cdot (c \cdot c + c \cdot b + b \cdot b)}{3} + \frac{(s - \frac{c \cdot (s-r)}{c-b}) \cdot (c+b)}{2}) + (d-c) \cdot (\frac{\frac{-s}{d-c} \cdot (d \cdot d + d \cdot c + c \cdot c)}{3} + \frac{(-\frac{d \cdot (-s)}{d-c}) \cdot (d+c)}{2})\Bigg) / \Bigg((b-a) \cdot (\frac{\frac{r}{b-a} \cdot (b+a)}{2} + -\frac{a \cdot r}{b-a}) + (c-b) \cdot (\frac{\frac{s-r}{c-b} \cdot (c+b)}{2} + (s - \frac{c \cdot (s-r)}{c-b})) + (d-c) \cdot (\frac{\frac{-s}{d-c} \cdot (d+c)}{2} + -\frac{d \cdot (-s)}{d-c})\Bigg)$. The theorem is a consequence of (37), (38), and (42).

(44) Let us consider real numbers b, c, d. Suppose $b < c$. Then $(\text{AffineMap}(d \cdot \frac{1}{c-b}, d \cdot (-\frac{b}{c-b}))) + (\text{AffineMap}(d \cdot (-\frac{1}{c-b}), d \cdot \frac{c}{c-b})) = \text{AffineMap}(0, d)$.

(45) Let us consider real numbers a, b, c, p, q. Suppose $a < b < c$. Then $(\text{AffineMap}(p, q))\restriction [a, b] + \cdot (\text{AffineMap}(p, q))\restriction [b, c] = (\text{AffineMap}(p, q))\restriction [a, c]$.

Proof: Set $f = \text{AffineMap}(p, q)$. For every object x such that $x \in \text{dom}(f\restriction [a, c])$ holds $(f\restriction [a, c])(x) = (f\restriction [a, b] + \cdot f\restriction [b, c])(x)$. $\square$

Let us consider real numbers a, b, c and a real number x. Now we state the propositions:

(46) If $a < b < c$, then if $x \in [a, b]$, then $(\text{TriangularFS}(a, b, c))(x) = (\text{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a}))(x)$.

PROOF: For every real number x such that $x \in [a, b]$ holds $(\text{TriangularFS}(a, b, c))(x) = (\text{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a}))(x)$. □

(47) If $a < b < c$, then if $x \in [b, c]$, then $(\text{TriangularFS}(a, b, c))(x) = (\text{AffineMap}(-\frac{1}{c-b}, \frac{c}{c-b}))(x)$.

(48) If $a < b < c$, then if $x \notin]a, c[$, then $(\text{TriangularFS}(a, b, c))(x) = (\text{AffineMap}(0, 0))(x)$.

PROOF: For every real number x such that $x \notin]a, c[$ holds $(\text{TriangularFS}(a, b, c))(x) = (\text{AffineMap}(0, 0))(x)$. □

REFERENCES

[1] Didier Dubois and Henri Prade. Operations on fuzzy numbers. *International Journal of Systems Science*, 9(6):613–626, 1978. doi:10.1080/00207727808941724.

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

[3] Ronald E. Giachetti and Robert E. Young. A parametric representation of fuzzy numbers and their arithmetic operators. *Fuzzy Sets and Systems*, 91(2):185–202, 1997. doi:10.1016/S0165-0114(97)00140-1.

[4] Eikou Gonda, Hitoshi Miyata, and Masaaki Ohkita. Self-turning of fuzzy rules with different types of MSFs (in Japanese). *Journal of Japan Society for Fuzzy Theory and Intelligent Informatics*, 16(6):540–550, 2004. doi:10.3156/jsoft.16.540.

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

[6] Adam Grabowski. Fuzzy implications in the Mizar system. In *30th IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 2021, Luxembourg, July 11–14, 2021*, pages 1–6. IEEE, 2021. doi:10.1109/FUZZ45933.2021.9494593.

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

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

[9] Adam Grabowski and Christoph Schwarzweller. On duplication in mathematical repositories. In Serge Autexier, Jacques Calmet, David Delahaye, Patrick D. F. Ion, Laurence Rideau, Renaud Rioboo, and Alan P. Sexton, editors, *Intelligent Computer Mathematics, 10th International Conference, AISC 2010, 17th Symposium, Calculemus 2010, and 9th International Conference, MKM 2010, Paris, France, July 5–10, 2010. Proceedings*, volume 6167 of *Lecture Notes in Computer Science*, pages 300–314. Springer, 2010. doi:10.1007/978-3-642-14128-7_26.

[10] Adam Grabowski and Christoph Schwarzweller. Translating mathematical vernacular into knowledge repositories. In Michael Kohlhase, editor, *Mathematical Knowledge Management*, volume 3863 of *Lecture Notes in Computer Science*, pages 49–64. Springer, 2006. doi:10.1007/11618027_4. 4th International Conference on Mathematical Knowledge Management, Bremen, Germany, MKM 2005, July 15–17, 2005, Revised Selected Papers.

[11] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Mizar in a nutshell. *Journal of Formalized Reasoning*, 3(2):153–245, 2010.

[12] Tetsuro Katafuchi, Kiyoji Asai, and Hiroshi Fujita. Investigation of deffuzification in fuzzy inference: Proposal of a new defuzzification method (in Japanese). *Medical Imaging and Information Sciences*, 18(1):19–30, 2001. doi:10.11318/mii1984.18.19.

[13] Ebrahim H. Mamdani. Application of fuzzy algorithms for control of simple dynamic plant. *IEE Proceedings*, 121:1585–1588, 1974.

[14] Takashi Mitsuishi. Some properties of membership functions composed of triangle functions and piecewise linear functions. *Formalized Mathematics*, 29(**2**):103–115, 2021. doi:10.2478/forma-2021-0011.

[15] Takashi Mitsuishi. Definition of centroid method as defuzzification. *Formalized Mathematics*, 30(**2**):125–134, 2022. doi:10.2478/forma-2022-0010.

[16] Takashi Mitsuishi. Isosceles triangular and isosceles trapezoidal membership functions using centroid method. *Formalized Mathematics*, 31(1):59–66, 2023. doi:10.2478/forma-2023-0006.

[17] Takashi Mitsuishi, Takanori Terashima, Nami Shimada, Toshimichi Homma, and Yasunari Shidama. Approximate reasoning using LR fuzzy number as input for sensorless fuzzy control. In *2016 IEEE Symposium on Sensorless Control for Electrical Drives (SLED)*, pages 1–5, 2016. doi:10.1109/SLED.2016.7518804.

[18] Masaharu Mizumoto. Improvement of fuzzy control (IV)-case by product-sum-gravity method. In *Proc. 6th Fuzzy System Symposium, 1990*, pages 9–13, 1990.

[19] Timothy J. Ross. *Fuzzy Logic with Engineering Applications*. John Wiley and Sons Ltd, 2010.

[20] Luciano Stefanini and Laerte Sorini. Fuzzy arithmetic with parametric LR fuzzy numbers. In *Proceedings of the Joint 2009 International Fuzzy Systems Association World Congress and 2009 European Society of Fuzzy Logic and Technology Conference*, pages 600–605, 2009.

[21] Werner Van Leekwijck and Etienne E. Kerre. Defuzzification: Criteria and classification. *Fuzzy Sets and Systems*, 108(2):159–178, 1999.

[22] Lotfi Zadeh. Fuzzy sets. *Information and Control*, 8(3):338–353, 1965. doi:10.1016/S0019-9958(65)90241-X.

Accepted December 18, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 309–324, 2023
DOI: 10.2478/forma-2023-0025
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Integral of Continuous Functions of Two Variables[1]

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

Yasunari Shidama
Karuizawa Hotch 244-1
Nagano, Japan

Summary. We extend the formalization of the integral theory of one-variable functions for Riemann and Lebesgue integrals, showing that the Lebesgue integral of a continuous function of two variables coincides with the Riemann iterated integral of a projective function.

MSC: 26B15 97I50 68V20

Keywords: double integral; repeated integral

MML identifier: `MESFUN16`, version: `8.1.14 5.76.1462`

Introduction

So far, the authors have proved in Mizar [2], [15] many theorems on the integral theory of one-variable functions for Riemann and Lebesgue integrals [9], [5], [11] (for interesting survey of formalizations of real analysis in another proof-assistants like ACL2 [13], Isabelle/HOL [12], Coq [3], see [4]). As a result, we have shown that if a function bounded on a closed interval (i.e., a continuous function) is Riemann integrable, then it is Lebesgue integrable, and both integrals coincide [10]. Furthermore, for the Lebesgue integral, there exist integral theorems on the product measure spaces [9]. From these results, this article

[1]This work was supported by JSPS KAKENHI 23K11242.

shows that the Lebesgue integral of a continuous function of two variables coincides with the Riemann iterated integral of a projective function [1]. In the first three sections of this article, we summarize the basic properties of the projection of functions of two variables. In the last section, we prove integrability and iterated integrals of continuous functions of two variables.

Note that the continuity of functions of many variables is not directly addressed in this article, since there are quite a few formal notions of continuity which can be applied in this case (although they are essentially the same; for the discussion on the pros and cons of duplications in the Mizar Mathematical Library, see [14]). The formalization follows [19] and [16].

1. Preliminaries

Now we state the propositions:

(1) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, and a partial function f from X to $\overline{\mathbb{R}}$. If $\operatorname{dom} f = \emptyset$, then $\int f \,\mathrm{d}M = 0$.

(2) Let us consider a non empty set X, a σ-field S of subsets of X, a σ-measure M on S, and a partial function f from X to $\mathbb{R}$. If $\operatorname{dom} f = \emptyset$, then $\int f \,\mathrm{d}M = 0$. The theorem is a consequence of (1).

(3) Let us consider a non empty set X, a σ-field S of subsets of X, and a σ-measure M on S. If M is σ-finite, then $\mathrm{COM}(M)$ is σ-finite.
Proof: Consider E being a set sequence of S such that for every natural number n, $M(E(n)) < +\infty$ and $\bigcup E = X$. For every natural number n, $E(n) \in \mathrm{COM}(S, M)$. Reconsider $E_1 = E$ as a set sequence of $\mathrm{COM}(S, M)$. For every natural number n, $(\mathrm{COM}(M))(E_1(n)) < +\infty$. □

(4) B-Meas is σ-finite.
Proof: Define $\mathcal{S}(\text{natural number}) = [-\$_1, \$_1] (\in 2^{\mathbb{R}})$. Consider E being a function from $\mathbb{N}$ into $2^{\mathbb{R}}$ such that for every element i of $\mathbb{N}$, $E(i) = \mathcal{S}(i)$. For every natural number n, $E(n) = [-n, n]$. For every natural number n, $E(n) \in$ the Borel sets by [7, (5)]. For every natural number n, $(\text{B-Meas})(E(n)) < +\infty$ by [8, (71)]. □

(5) L-Meas is σ-finite.

(6) ProdMeas(L-Meas, L-Meas) is σ-finite.

(7) Let us consider a closed interval subset I of $\mathbb{R}$, and a subset E of the real normed space of $\mathbb{R}$. If $I = E$, then E is compact.
Proof: For every sequence s_1 of the real normed space of $\mathbb{R}$ such that $\operatorname{rng} s_1 \subseteq E$ there exists a sequence s_2 of the real normed space of $\mathbb{R}$ such that s_2 is subsequence of s_1 and convergent and $\lim s_2 \in E$. □

Let S_1, S_2 be real normed spaces, D_1 be a subset of S_1, and D_2 be a subset of S_2. Let us note that the functor $D_1 \times D_2$ yields a subset of $S_1 \times S_2$. Now we state the propositions:

(8) Let us consider real normed spaces P, Q, a subset E of P, and a subset F of Q. Suppose E is compact and F is compact. Then $E \times F$ is subset of $P \times Q$ and compact.
PROOF: Set $S = P \times Q$. Set $X = E \times F$. For every sequence s_1 of S such that $\operatorname{rng} s_1 \subseteq X$ there exists a sequence s_2 of S such that s_2 is subsequence of s_1 and convergent and $\lim s_2 \in X$. □

(9) Let us consider closed interval subsets I, J of $\mathbb{R}$, and a subset E of (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$). If $E = I \times J$, then E is compact. The theorem is a consequence of (7) and (8).

(10) Let us consider a set E, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, and a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$. Suppose $f = g$ and $E \subseteq \operatorname{dom} f$. Then f is uniformly continuous on E if and only if for every real number e such that $0 < e$ there exists a real number r such that $0 < r$ and for every real numbers x_1, x_2, y_1, y_2 such that $\langle x_1, y_1 \rangle$, $\langle x_2, y_2 \rangle \in E$ and $|x_2 - x_1| < r$ and $|y_2 - y_1| < r$ holds $|g(\langle x_2, y_2 \rangle) - g(\langle x_1, y_1 \rangle)| < e$.
PROOF: For every real number e such that $0 < e$ there exists a real number r such that $0 < r$ and for every points z_1, z_2 of (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) such that z_1, $z_2 \in E$ and $\|z_1 - z_2\| < r$ holds $\|f_{/z_1} - f_{/z_2}\| < e$. □

(11) Let us consider intervals I, J. Then

(i) $I \times J$ is a subset of (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$), and

(ii) $I \times J \in \sigma(\text{MeasRect}(\text{L-Field}, \text{L-Field}))$.

(12) Let us consider a point z of the real normed space of $\mathbb{R}$, and real numbers x, r. If $x = z$, then $\text{Ball}(z, r) =]x - r, x + r[$.
PROOF: For every object p, $p \in \text{Ball}(z, r)$ iff $p \in]x - r, x + r[$. □

(13) Let us consider a point z of (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$), and a real number r. Suppose $0 < r$. Then there exists a real number s and there exist real numbers x, y such that $0 < s < r$ and $z = \langle x, y \rangle$ and $]x - s, x + s[\times]y - s, y + s[\subseteq \text{Ball}(z, r)$. The theorem is a consequence of (12).

Let us consider a subset A of (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$). Now we state the propositions:

(14) Suppose for every real numbers a, b such that $\langle a, b \rangle \in A$ there exists

a real-membered set R such that R is non empty and upper bounded and $R = \{r$,where r is a real number : $0 < r$ and $]a-r, a+r[\times]b-r, b+r[\subseteq A\}$. Then there exists a function F from A into $\mathbb{R}$ such that for every real numbers a, b such that $\langle a, b\rangle \in A$ there exists a real-membered set R such that R is non empty and upper bounded and $R = \{r$, where r is a real number : $0 < r$ and $]a-r, a+r[\times]b-r, b+r[\subseteq A\}$ and $F(\langle a, b\rangle) = \frac{\sup R}{2}$. PROOF: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exist real numbers a, b and there exists a real-membered set R such that $\$_1 = \langle a, b\rangle$ and R is non empty and upper bounded and $R = \{r$, where r is a real number : $0 < r$ and $]a-r, a+r[\times]b-r, b+r[\subseteq A\}$ and $\$_2 = \frac{\sup R}{2}$. For every object x such that $x \in A$ there exists an object y such that $y \in \mathbb{R}$ and $\mathcal{P}[x, y]$.

Consider F being a function from A into $\mathbb{R}$ such that for every object x such that $x \in A$ holds $\mathcal{P}[x, F(x)]$. For every real numbers a, b such that $\langle a, b\rangle \in A$ there exists a real-membered set R such that R is non empty and upper bounded and $R = \{r$, where r is a real number : $0 < r$ and $]a-r, a+r[\times]b-r, b+r[\subseteq A\}$ and $F(\langle a, b\rangle) = \frac{\sup R}{2}$. □

(15) If A is open, then $A \in \sigma(\text{MeasRect}(\text{L-Field}, \text{L-Field}))$. The theorem is a consequence of (13) and (14).

(16) Let us consider a subset H of the real normed space of $\mathbb{R}$, and an open interval subset I of $\mathbb{R}$. If $H = I$, then H is open.
PROOF: For every point x of the real normed space of $\mathbb{R}$ such that $x \in H$ there exists a neighbourhood N of x such that $N \subseteq H$ by [6, (18)], [18, (4)]. □

(17) Let us consider a real number r, a set X, and a partial function g from X to $\mathbb{R}$. Then $\text{LE-dom}(g, r) = g^{-1}(]-\infty, r[)$.

2. Continuity of Two-variable Functions

Now we state the propositions:

(18) Let us consider closed interval subsets I, J of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, and a partial function g from $\mathbb{R}\times\mathbb{R}$ to $\mathbb{R}$. Suppose f is continuous on $I \times J$ and $f = g$. Let us consider a real number e. Suppose $0 < e$. Then there exists a real number r such that

(i) $0 < r$, and

(ii) for every real numbers x_1, x_2, y_1, y_2 such that $\langle x_1, y_1\rangle$, $\langle x_2, y_2\rangle \in I \times J$ and $|x_2 - x_1| < r$ and $|y_2 - y_1| < r$ holds $|g(\langle x_2, y_2\rangle) - g(\langle x_1, y_1\rangle)| < e$.

The theorem is a consequence of (9) and (10).

(19) Let us consider a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, and a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$. If $f = g$, then $\|f\| = |g|$.

(20) Let us consider a non empty set X, a partial function g from X to $\mathbb{R}$, and a subset A of X. Then $|g{\restriction}A| = |g|{\restriction}A$.

PROOF: For every object x such that $x \in \operatorname{dom} |g{\restriction}A|$ holds $|g{\restriction}A|(x) = (|g|{\restriction}A)(x)$. □

(21) Let us consider a real normed space S, a point x_0 of S, and partial functions f, g from S to the real normed space of $\mathbb{R}$. Suppose f is continuous in x_0 and $g = \|f\|$. Then g is continuous in x_0.

PROOF: For every sequence s_1 of S such that $\operatorname{rng} s_1 \subseteq \operatorname{dom} g$ and s_1 is convergent and $\lim s_1 = x_0$ holds $g_* s_1$ is convergent and $g_{/x_0} = \lim(g_* s_1)$. □

(22) Let us consider a set X, a real normed space S, and partial functions f, g from S to the real normed space of $\mathbb{R}$. Suppose f is continuous on X and $g = \|f\|$. Then g is continuous on X. The theorem is a consequence of (21).

(23) Let us consider closed interval subsets I, J of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, and a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$. Suppose f is continuous on $I \times J$ and $f = g$. Let us consider a real number e. Suppose $0 < e$. Then there exists a real number r such that

(i) $0 < r$, and

(ii) for every real numbers x_1, x_2, y_1, y_2 such that $\langle x_1, y_1 \rangle$, $\langle x_2, y_2 \rangle \in I \times J$ and $|x_2 - x_1| < r$ and $|y_2 - y_1| < r$ holds $||g|(\langle x_2, y_2 \rangle) - |g|(\langle x_1, y_1 \rangle)| < e$.

The theorem is a consequence of (19), (22), and (18).

(24) Let us consider a real number r, a real normed space S, a subset E of S, and a partial function f from S to the real normed space of $\mathbb{R}$. Suppose f is continuous on E and $\operatorname{dom} f = E$. Then there exists a subset H of S such that

(i) $H \cap E = f^{-1}(]-\infty, r[)$, and

(ii) H is open.

PROOF: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a point t of S and there exists a real number s such that $t = \$_1$ and $s = \$_2$ and $0 < s$ and for every object t_1 such that $t_1 \in E \cap \{t_1$, where t_1 is a point of $S : \|t_1 - t\| < s\}$ holds $f(t_1) \in]-\infty, r[$.

For every object z such that $z \in f^{-1}(]-\infty, r[)$ there exists an object y such that $y \in \mathbb{R}$ and $\mathcal{P}[z, y]$. Consider R being a function from $f^{-1}(]-\infty, r[)$ into $\mathbb{R}$ such that for every object x such that $x \in f^{-1}(]-\infty, r[)$ holds $\mathcal{P}[x, R(x)]$. Define $\mathcal{Q}[\text{object}, \text{object}] \equiv$ there exists a point t of S such that $t = \$_1$ and $0 < R(\$_1)$ and $\$_2 = \{t_1$, where t_1 is a point of $S : \|t_1 - t\| < R(\$_1)\}$. For every object z such that $z \in f^{-1}(]-\infty, r[)$ there exists an object y such that $y \in 2^\alpha$ and $\mathcal{Q}[z, y]$, where α is the carrier of S.

Consider B being a function from $f^{-1}(]-\infty, r[)$ into $2^{(\text{the carrier of } S)}$ such that for every object x such that $x \in f^{-1}(]-\infty, r[)$ holds $\mathcal{Q}[x, B(x)]$. Set $H = \bigcup \operatorname{rng} B$. For every object z, $z \in H \cap E$ iff $z \in f^{-1}(]-\infty, r[)$. For every point z of S such that $z \in H$ there exists a neighbourhood N of z such that $N \subseteq H$. $\square$

3. Properties of Projective Functions

Now we state the propositions:

(25) Let us consider non empty sets X, Y, Z, a subset A of X, a subset B of Y, an element x of X, and a partial function f from $X \times Y$ to Z. Suppose $\operatorname{dom} f = A \times B$. Then

(i) if $x \in A$, then $\operatorname{dom}(\text{ProjPMap1}(f, x)) = B$, and

(ii) if $x \notin A$, then $\operatorname{dom}(\text{ProjPMap1}(f, x)) = \emptyset$.

(26) Let us consider non empty sets X, Y, Z, a subset A of X, a subset B of Y, an element y of Y, and a partial function f from $X \times Y$ to Z. Suppose $\operatorname{dom} f = A \times B$. Then

(i) if $y \in B$, then $\operatorname{dom}(\text{ProjPMap2}(f, y)) = A$, and

(ii) if $y \notin B$, then $\operatorname{dom}(\text{ProjPMap2}(f, y)) = \emptyset$.

(27) Let us consider non empty sets X, Y, a subset A of X, a subset B of Y, an element x of X, and a partial function f from $X \times Y$ to $\mathbb{R}$. Suppose $\operatorname{dom} f = A \times B$. Then

(i) if $x \in A$, then $\operatorname{dom}(\text{ProjPMap1}(\overline{\mathbb{R}}(f), x)) = B$ and $\operatorname{dom}(\text{ProjPMap1}(|\overline{\mathbb{R}}(f)|, x)) = B$, and

(ii) if $x \notin A$, then $\operatorname{dom}(\text{ProjPMap1}(\overline{\mathbb{R}}(f), x)) = \emptyset$ and $\operatorname{dom}(\text{ProjPMap1}(|\overline{\mathbb{R}}(f)|, x)) = \emptyset$.

The theorem is a consequence of (25).

(28) Let us consider non empty sets X, Y, a subset A of X, a subset B of Y, an element y of Y, and a partial function f from $X \times Y$ to $\mathbb{R}$. Suppose $\operatorname{dom} f = A \times B$. Then

(i) if $y \in B$, then $\operatorname{dom}(\operatorname{ProjPMap2}(\overline{\mathbb{R}}(f), y)) = A$ and $\operatorname{dom}(\operatorname{ProjPMap2}(|\overline{\mathbb{R}}(f)|, y)) = A$, and

(ii) if $y \notin B$, then $\operatorname{dom}(\operatorname{ProjPMap2}(\overline{\mathbb{R}}(f), y)) = \emptyset$ and $\operatorname{dom}(\operatorname{ProjPMap2}(|\overline{\mathbb{R}}(f)|, y)) = \emptyset$.

The theorem is a consequence of (26).

(29) Let us consider non empty sets X, Y, a set Z, a partial function f from $X \times Y$ to Z, an element x of X, and an element y of Y. Then

(i) $\operatorname{rng} \operatorname{ProjPMap1}(f, x) \subseteq \operatorname{rng} f$, and

(ii) $\operatorname{rng} \operatorname{ProjPMap2}(f, y) \subseteq \operatorname{rng} f$.

Let us consider non empty sets X, Y, a partial function f from $X \times Y$ to $\mathbb{R}$, an element x of X, and an element y of Y. Now we state the propositions:

(30) (i) $\operatorname{ProjPMap1}(\overline{\mathbb{R}}(f), x)$ is a partial function from Y to $\mathbb{R}$, and

(ii) $\operatorname{ProjPMap1}(|\overline{\mathbb{R}}(f)|, x)$ is a partial function from Y to $\mathbb{R}$, and

(iii) $\operatorname{ProjPMap2}(\overline{\mathbb{R}}(f), y)$ is a partial function from X to $\mathbb{R}$, and

(iv) $\operatorname{ProjPMap2}(|\overline{\mathbb{R}}(f)|, y)$ is a partial function from X to $\mathbb{R}$.

The theorem is a consequence of (29).

(31) (i) $\operatorname{ProjPMap1}(\overline{\mathbb{R}}(f), x) = \overline{\mathbb{R}}(\operatorname{ProjPMap1}(f, x))$, and

(ii) $\operatorname{ProjPMap1}(|\overline{\mathbb{R}}(f)|, x) = |\overline{\mathbb{R}}(\operatorname{ProjPMap1}(f, x))|$, and

(iii) $\operatorname{ProjPMap2}(\overline{\mathbb{R}}(f), y) = \overline{\mathbb{R}}(\operatorname{ProjPMap2}(f, y))$, and

(iv) $\operatorname{ProjPMap2}(|\overline{\mathbb{R}}(f)|, y) = |\overline{\mathbb{R}}(\operatorname{ProjPMap2}(f, y))|$.

(32) (i) $\operatorname{ProjPMap1}(|f|, x) = |\operatorname{ProjPMap1}(f, x)|$, and

(ii) $\operatorname{ProjPMap2}(|f|, y) = |\operatorname{ProjPMap2}(f, y)|$.

Let us consider a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and an element t of $\mathbb{R}$. Now we state the propositions:

(33) If f is continuous on $\operatorname{dom} f$ and $f = g$, then $\operatorname{ProjPMap1}(g, t)$ is continuous and $\operatorname{ProjPMap2}(g, t)$ is continuous.

PROOF: For every real number y_0 such that $y_0 \in \operatorname{dom}(\operatorname{ProjPMap1}(g, t))$ holds $\operatorname{ProjPMap1}(g, t)$ is continuous in y_0. For every real number x_0 such that $x_0 \in \operatorname{dom}(\operatorname{ProjPMap2}(g, t))$ holds $\operatorname{ProjPMap2}(g, t)$ is continuous in x_0. □

(34) Suppose f is continuous on $\operatorname{dom} f$ and $f = g$. Then

(i) $\operatorname{ProjPMap1}(|g|, t)$ is continuous, and

(ii) $\operatorname{ProjPMap2}(|g|, t)$ is continuous.

The theorem is a consequence of (33) and (32).

(35) Suppose f is uniformly continuous on $\operatorname{dom} f$ and $f = g$. Then

(i) ProjPMap1(g, t) is uniformly continuous, and

(ii) ProjPMap2(g, t) is uniformly continuous.

PROOF: For every real number r such that $0 < r$ there exists a real number s such that $0 < s$ and for every real numbers y_1, y_2 such that y_1, $y_2 \in \operatorname{dom}(\text{ProjPMap1}(g, t))$ and $|y_1 - y_2| < s$ holds $|(\text{ProjPMap1}(g, t))(y_1) - (\text{ProjPMap1}(g, t))(y_2)| < r$. For every real number r such that $0 < r$ there exists a real number s such that $0 < s$ and for every real numbers x_1, x_2 such that x_1, $x_2 \in \operatorname{dom}(\text{ProjPMap2}(g, t))$ and $|x_1 - x_2| < s$ holds $|(\text{ProjPMap2}(g, t))(x_1) - (\text{ProjPMap2}(g, t))(x_2)| < r$ by [17, (1)]. □

(36) Let us consider an element x of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function P_1 from $\mathbb{R}$ to $\mathbb{R}$. Suppose f is continuous on $\operatorname{dom} f$ and $f = g$ and $P_1 = \text{ProjPMap1}(\overline{\mathbb{R}}(g), x)$. Then P_1 is continuous. The theorem is a consequence of (31) and (33).

(37) Let us consider an element y of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function P_2 from $\mathbb{R}$ to $\mathbb{R}$. Suppose f is continuous on $\operatorname{dom} f$ and $f = g$ and $P_2 = \text{ProjPMap2}(\overline{\mathbb{R}}(g), y)$. Then P_2 is continuous. The theorem is a consequence of (31) and (33).

(38) Let us consider an element x of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function P_1 from $\mathbb{R}$ to $\mathbb{R}$. Suppose f is continuous on $\operatorname{dom} f$ and $f = g$ and $P_1 = \text{ProjPMap1}(|\overline{\mathbb{R}}(g)|, x)$. Then P_1 is continuous. The theorem is a consequence of (31), (32), and (34).

(39) Let us consider an element y of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function p_2 from $\mathbb{R}$ to $\mathbb{R}$. Suppose f is continuous on $\operatorname{dom} f$ and $f = g$ and $p_2 = \text{ProjPMap2}(|\overline{\mathbb{R}}(g)|, y)$. Then p_2 is continuous. The theorem is a consequence of (31), (32), and (34).

4. Integral of Continuous Functions of Two Variables

Let us consider a subset I of $\mathbb{R}$, a non empty, closed interval subset J of $\mathbb{R}$, an element x of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function P_1 from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(40) Suppose $x \in I$ and $\operatorname{dom} f = I \times J$ and f is continuous on $I \times J$ and $f = g$ and $P_1 = \operatorname{ProjPMap1}(\overline{\mathbb{R}}(g), x)$. Then

(i) $P_1 \restriction J$ is bounded, and

(ii) P_1 is integrable on J.

The theorem is a consequence of (31), (27), and (33).

(41) Suppose $x \in I$ and $\operatorname{dom} f = I \times J$ and f is continuous on $I \times J$ and $f = g$ and $P_1 = \operatorname{ProjPMap1}(\overline{\mathbb{R}}(g), x)$. Then

(i) P_1 is integrable on L-Meas, and

(ii) $\int_J P_1(x)dx = \int P_1 \,\mathrm{d}\, \text{L-Meas}$, and

(iii) $\int_J P_1(x)dx = \int \operatorname{ProjPMap1}(\overline{\mathbb{R}}(g), x) \,\mathrm{d}\, \text{L-Meas}$, and

(iv) $\int_J P_1(x)dx = (\operatorname{Integral2}(\text{L-Meas}, \overline{\mathbb{R}}(g)))(x)$.

The theorem is a consequence of (27) and (40).

Let us consider a non empty, closed interval subset I of $\mathbb{R}$, a subset J of $\mathbb{R}$, an element y of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function P_2 from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(42) Suppose $y \in J$ and $\operatorname{dom} f = I \times J$ and f is continuous on $I \times J$ and $f = g$ and $P_2 = \operatorname{ProjPMap2}(\overline{\mathbb{R}}(g), y)$. Then

(i) $P_2 \restriction I$ is bounded, and

(ii) P_2 is integrable on I.

The theorem is a consequence of (31), (28), and (33).

(43) Suppose $y \in J$ and $\operatorname{dom} f = I \times J$ and f is continuous on $I \times J$ and $f = g$ and $P_2 = \operatorname{ProjPMap2}(\overline{\mathbb{R}}(g), y)$. Then

(i) P_2 is integrable on L-Meas, and

(ii) $\int_I P_2(x)dx = \int P_2 \,\mathrm{d}\,\text{L-Meas}$, and

(iii) $\int_I P_2(x)dx = \int \text{ProjPMap2}(\overline{\mathbb{R}}(g), y) \,\mathrm{d}\,\text{L-Meas}$, and

(iv) $\int_I P_2(x)dx = (\text{Integral1}(\text{L-Meas}, \overline{\mathbb{R}}(g)))(y)$.

The theorem is a consequence of (28) and (42).

(44) Let us consider a subset I of $\mathbb{R}$, a non empty, closed interval subset J of $\mathbb{R}$, an element x of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function P_1 from $\mathbb{R}$ to $\mathbb{R}$. Suppose $x \in I$ and $\operatorname{dom} f = I \times J$ and f is continuous on $I \times J$ and $f = g$ and $P_1 = \text{ProjPMap1}(|\overline{\mathbb{R}}(g)|, x)$. Then

(i) $P_1 \restriction J$ is bounded, and

(ii) P_1 is integrable on J.

The theorem is a consequence of (27) and (38).

(45) Let us consider a subset I of $\mathbb{R}$, a non empty, closed interval subset J of $\mathbb{R}$, an element x of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, a partial function P_1 from $\mathbb{R}$ to $\mathbb{R}$, and an element E of L-Field. Suppose $x \in I$ and $\operatorname{dom} f = I \times J$ and f is continuous on $I \times J$ and $f = g$ and $P_1 = \text{ProjPMap1}(|\overline{\mathbb{R}}(g)|, x)$ and $E = J$. Then P_1 is E-measurable. The theorem is a consequence of (27) and (44).

(46) Let us consider a subset I of $\mathbb{R}$, a non empty, closed interval subset J of $\mathbb{R}$, an element x of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function P_1 from $\mathbb{R}$ to $\mathbb{R}$. Suppose $x \in I$ and $\operatorname{dom} f = I \times J$ and f is continuous on $I \times J$ and $f = g$ and $P_1 = \text{ProjPMap1}(|\overline{\mathbb{R}}(g)|, x)$. Then

(i) P_1 is integrable on L-Meas, and

(ii) $\int_J P_1(x)dx = \int P_1 \,\mathrm{d}\,\text{L-Meas}$, and

(iii) $\int_J P_1(x)dx = \int \text{ProjPMap1}(|\overline{\mathbb{R}}(g)|, x) \,\mathrm{d}\,\text{L-Meas}$, and

(iv) $\int_J P_1(x)dx = (\text{Integral2}(\text{L-Meas}, |\overline{\mathbb{R}}(g)|))(x)$.

The theorem is a consequence of (27) and (44).

(47) Let us consider a non empty, closed interval subset I of $\mathbb{R}$, a subset J of $\mathbb{R}$, an element y of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function P_2 from $\mathbb{R}$ to $\mathbb{R}$. Suppose $y \in J$ and $\operatorname{dom} f = I \times J$ and f is continuous on $I \times J$ and $f = g$ and $P_2 = \operatorname{ProjPMap2}(|\overline{\mathbb{R}}(g)|, y)$. Then

(i) $P_2 \restriction I$ is bounded, and

(ii) P_2 is integrable on I.

The theorem is a consequence of (28) and (39).

(48) Let us consider a non empty, closed interval subset I of $\mathbb{R}$, a subset J of $\mathbb{R}$, an element y of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, a partial function P_2 from $\mathbb{R}$ to $\mathbb{R}$, and an element E of L-Field. Suppose $y \in J$ and $\operatorname{dom} f = I \times J$ and f is continuous on $I \times J$ and $f = g$ and $P_2 = \operatorname{ProjPMap2}(|\overline{\mathbb{R}}(g)|, y)$ and $E = I$. Then P_2 is E-measurable. The theorem is a consequence of (28) and (47).

(49) Let us consider a non empty, closed interval subset I of $\mathbb{R}$, a subset J of $\mathbb{R}$, an element y of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function P_2 from $\mathbb{R}$ to $\mathbb{R}$. Suppose $y \in J$ and $\operatorname{dom} f = I \times J$ and f is continuous on $I \times J$ and $f = g$ and $P_2 = \operatorname{ProjPMap2}(|\overline{\mathbb{R}}(g)|, y)$. Then

(i) P_2 is integrable on L-Meas, and

(ii) $\int_I P_2(x)dx = \int P_2 \,\mathrm{d}\, \text{L-Meas}$, and

(iii) $\int_I P_2(x)dx = \int \operatorname{ProjPMap2}(|\overline{\mathbb{R}}(g)|, y) \,\mathrm{d}\, \text{L-Meas}$, and

(iv) $\int_I P_2(x)dx = (\operatorname{Integral1}(\text{L-Meas}, |\overline{\mathbb{R}}(g)|))(y)$.

The theorem is a consequence of (28) and (47).

(50) Let us consider non empty, closed interval subsets I, J of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and an element E of $\sigma(\operatorname{MeasRect}(\text{L-Field}, \text{L-Field}))$. Suppose $I \times$

$J = \operatorname{dom} f$ and f is continuous on $I \times J$ and $f = g$ and $E = I \times J$. Then g is E-measurable. The theorem is a consequence of (17), (24), and (15).

(51) Let us consider a subset I of $\mathbb{R}$, a non empty, closed interval subset J of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, and a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$. Suppose $I \times J = \operatorname{dom} f$ and f is continuous on $I \times J$ and $f = g$. Then

(i) Integral2(L-Meas, $|\overline{\mathbb{R}}(g)|)\restriction I$ is a partial function from $\mathbb{R}$ to $\mathbb{R}$, and

(ii) Integral2(L-Meas, $\overline{\mathbb{R}}(g))\restriction I$ is a partial function from $\mathbb{R}$ to $\mathbb{R}$.

The theorem is a consequence of (30), (46), and (41).

Let us consider non empty, closed interval subsets I, J of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) $\times$ (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function G_2 from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(52) Suppose $I \times J = \operatorname{dom} f$ and f is continuous on $I \times J$ and $f = g$ and $G_2 = \text{Integral2(L-Meas, } |\overline{\mathbb{R}}(g)|)\restriction I$. Then G_2 is continuous.

PROOF: Consider c, d being real numbers such that $J = [c, d]$. For every real number e such that $0 < e$ there exists a real number r such that $0 < r$ and for every real numbers x_1, x_2 such that $|x_2 - x_1| < r$ and x_1, $x_2 \in I$ for every real number y such that $y \in J$ holds $||g|(\langle x_2, y\rangle) - |g|(\langle x_1, y\rangle)| < e$. Set $R = \overline{\mathbb{R}}(g)$. For every elements x, y of $\mathbb{R}$ such that $x \in I$ and $y \in J$ holds $(\text{ProjPMap1}(|R|, x))(y) = |R|(x, y)$ and $|R|(x, y) = |g|(\langle x, y\rangle)$ and $|R|(x, y) = |g|(\langle x, y\rangle)$.

For every real number e such that $0 < e$ there exists a real number r such that $0 < r$ and for every elements x_1, x_2 of $\mathbb{R}$ such that $|x_2 - x_1| < r$ and x_1, $x_2 \in I$ for every element y of $\mathbb{R}$ such that $y \in J$ holds $|(\text{ProjPMap1}(|R|, x_2))(y) - (\text{ProjPMap1}(|R|, x_1))(y)| < e$. For every real numbers x_0, r such that $x_0 \in I$ and $0 < r$ there exists a real number s such that $0 < s$ and for every real number x_1 such that $x_1 \in I$ and $|x_1 - x_0| < s$ holds $|G_2(x_1) - G_2(x_0)| < r$. □

(53) Suppose $I \times J = \operatorname{dom} f$ and f is continuous on $I \times J$ and $f = g$ and $G_2 = \text{Integral2(L-Meas, } \overline{\mathbb{R}}(g))\restriction I$. Then G_2 is continuous.

PROOF: Consider c, d being real numbers such that $J = [c, d]$. For every real number e such that $0 < e$ there exists a real number r such that $0 < r$ and for every real numbers x_1, x_2 such that $|x_2 - x_1| < r$ and x_1, $x_2 \in I$ for every real number y such that $y \in J$ holds $|g(\langle x_2, y\rangle) - g(\langle x_1, y\rangle)| < e$. Set $R = \overline{\mathbb{R}}(g)$.

For every real number e such that $0 < e$ there exists a real number r such that $0 < r$ and for every elements x_1, x_2 of $\mathbb{R}$ such that

$|x_2 - x_1| < r$ and x_1, $x_2 \in I$ for every element y of $\mathbb{R}$ such that $y \in J$ holds $|(\mathrm{ProjPMap1}(R, x_2))(y) - (\mathrm{ProjPMap1}(R, x_1))(y)| < e$. For every real numbers x_0, r such that $x_0 \in I$ and $0 < r$ there exists a real number s such that $0 < s$ and for every real number x_1 such that $x_1 \in I$ and $|x_1 - x_0| < s$ holds $|G_2(x_1) - G_2(x_0)| < r$. □

(54) Let us consider non empty, closed interval subsets I, J of $\mathbb{R}$, a partial function g from (the real normed space of $\mathbb{R}$) × (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, and a partial function f from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$. Suppose $I \times J = \operatorname{dom} g$ and g is continuous on $I \times J$ and $g = f$. Then

(i) Integral1(L-Meas, $|\overline{\mathbb{R}}(f)|)\restriction J$ is a partial function from $\mathbb{R}$ to $\mathbb{R}$, and

(ii) Integral1(L-Meas, $\overline{\mathbb{R}}(f))\restriction J$ is a partial function from $\mathbb{R}$ to $\mathbb{R}$.

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

Let us consider non empty, closed interval subsets I, J of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) × (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function G_1 from $\mathbb{R}$ to $\mathbb{R}$. Now we state the propositions:

(55) Suppose $I \times J = \operatorname{dom} f$ and f is continuous on $I \times J$ and $f = g$ and $G_1 = \mathrm{Integral1}(\text{L-Meas}, |\overline{\mathbb{R}}(g)|)\restriction J$. Then G_1 is continuous.

PROOF: Consider a, b being real numbers such that $I = [a, b]$. For every real number e such that $0 < e$ there exists a real number r such that $0 < r$ and for every real numbers y_1, y_2 such that $|y_2 - y_1| < r$ and y_1, $y_2 \in J$ for every real number x such that $x \in I$ holds $||g|(\langle x, y_2\rangle) - |g|(\langle x, y_1\rangle)| < e$. Set $R = \overline{\mathbb{R}}(g)$. For every elements x, y of $\mathbb{R}$ such that $x \in I$ and $y \in J$ holds $(\mathrm{ProjPMap2}(|R|, y))(x) = |R|(x, y)$ and $|R|(x, y) = |g(\langle x, y\rangle)|$ and $|R|(x, y) = |g|(\langle x, y\rangle)$.

For every real number e such that $0 < e$ there exists a real number r such that $0 < r$ and for every elements y_1, y_2 of $\mathbb{R}$ such that $|y_2 - y_1| < r$ and y_1, $y_2 \in J$ for every element x of $\mathbb{R}$ such that $x \in I$ holds $|(\mathrm{ProjPMap2}(|R|, y_2))(x) - (\mathrm{ProjPMap2}(|R|, y_1))(x)| < e$. For every real numbers y_0, r such that $y_0 \in J$ and $0 < r$ there exists a real number s such that $0 < s$ and for every real number y_1 such that $y_1 \in J$ and $|y_1 - y_0| < s$ holds $|G_1(y_1) - G_1(y_0)| < r$. □

(56) Suppose $I \times J = \operatorname{dom} f$ and f is continuous on $I \times J$ and $f = g$ and $G_1 = \mathrm{Integral1}(\text{L-Meas}, \overline{\mathbb{R}}(g))\restriction J$. Then G_1 is continuous.

PROOF: Consider a, b being real numbers such that $I = [a, b]$. For every real number e such that $0 < e$ there exists a real number r such that $0 < r$ and for every real numbers y_1, y_2 such that $|y_2 - y_1| < r$ and y_1, $y_2 \in J$ for every real number x such that $x \in I$ holds $|g(\langle x, y_2\rangle) - g(\langle x, y_1\rangle)| < e$. Set $R = \overline{\mathbb{R}}(g)$.

For every real number e such that $0 < e$ there exists a real number r such that $0 < r$ and for every elements y_1, y_2 of $\mathbb{R}$ such that $|y_2 - y_1| < r$ and y_1, $y_2 \in J$ for every element x of $\mathbb{R}$ such that $x \in I$ holds $|(\mathrm{ProjPMap2}(R, y_2))(x) - (\mathrm{ProjPMap2}(R, y_1))(x)| < e$. For every real numbers y_0, r such that $y_0 \in J$ and $0 < r$ there exists a real number s such that $0 < s$ and for every real number y_1 such that $y_1 \in J$ and $|y_1 - y_0| < s$ holds $|G_1(y_1) - G_1(y_0)| < r$. □

(57) Let us consider non empty, closed interval subsets I, J of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) × (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, and a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$. Suppose $I \times J = \operatorname{dom} f$ and f is continuous on $I \times J$ and $f = g$. Then

(i) g is integrable on ProdMeas(L-Meas, L-Meas), and

(ii) for every element x of $\mathbb{R}$, $(\mathrm{Integral2}(\text{L-Meas}, |\overline{\mathbb{R}}(g)|))(x) < +\infty$, and

(iii) for every element y of $\mathbb{R}$, $(\mathrm{Integral1}(\text{L-Meas}, |\overline{\mathbb{R}}(g)|))(y) < +\infty$, and

(iv) for every element U of L-Field, Integral2(L-Meas, $\overline{\mathbb{R}}(g)$) is U-measurable, and

(v) for every element V of L-Field, Integral1(L-Meas, $\overline{\mathbb{R}}(g)$) is V-measurable, and

(vi) Integral2(L-Meas, $\overline{\mathbb{R}}(g)$) is integrable on L-Meas, and

(vii) Integral1(L-Meas, $\overline{\mathbb{R}}(g)$) is integrable on L-Meas, and

(viii) $\int g \,\mathrm{d}\, \mathrm{ProdMeas}(\text{L-Meas}, \text{L-Meas}) = \int \mathrm{Integral2}(\text{L-Meas}, \overline{\mathbb{R}}(g)) \,\mathrm{d}\, \text{L-Meas}$, and

(ix) $\int g \,\mathrm{d}\, \mathrm{ProdMeas}(\text{L-Meas}, \text{L-Meas}) = \int \mathrm{Integral1}(\text{L-Meas}, \overline{\mathbb{R}}(g)) \,\mathrm{d}\, \text{L-Meas}$.

(58) Let us consider non empty, closed interval subsets I, J of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) × (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, and a partial function G_2 from $\mathbb{R}$ to $\mathbb{R}$. Suppose $I \times J = \operatorname{dom} f$ and f is continuous on $I \times J$ and $f = g$ and $G_2 = \mathrm{Integral2}(\text{L-Meas}, \overline{\mathbb{R}}(g)) \restriction I$. Then $\int \overline{\mathbb{R}}(g) \,\mathrm{d}\, \mathrm{ProdMeas}(\text{L-Meas}, \text{L-Meas}) = \int_I G_2(x)dx$.

Proof: Set $R = \overline{\mathbb{R}}(g)$. Set $N_1 = \mathbb{R} \setminus I$. Set $R_2 = \mathrm{Integral2}(\text{L-Meas}, R)$. Set $F_1 = R_2 \restriction N_1$. G_2 is continuous. For every element x of $\mathbb{R}$ such that $x \in \operatorname{dom} F_1$ holds $F_1(x) = 0$. □

(59) Let us consider non empty, closed interval subsets I, J of $\mathbb{R}$, a partial function f from (the real normed space of $\mathbb{R}$) × (the real normed space of $\mathbb{R}$) to the real normed space of $\mathbb{R}$, a partial function g from $\mathbb{R} \times \mathbb{R}$ to

$\mathbb{R}$, and a partial function G_1 from $\mathbb{R}$ to $\mathbb{R}$. Suppose $I \times J = \operatorname{dom} f$ and f is continuous on $I \times J$ and $f = g$ and $G_1 = \text{Integral1}(\text{L-Meas}, \overline{\mathbb{R}}(g)) \restriction J$. Then $\int \overline{\mathbb{R}}(g) \,\mathrm{d}\, \text{ProdMeas}(\text{L-Meas}, \text{L-Meas}) = \int_J G_1(x)dx$.

PROOF: Set $R = \overline{\mathbb{R}}(g)$. Set $N_2 = \mathbb{R} \setminus J$. Set $R_1 = \text{Integral1}(\text{L-Meas}, R)$. Set $F_1 = R_1 \restriction N_2$. $G_1 \restriction J$ is bounded and G_1 is integrable on J. For every element y of $\mathbb{R}$ such that $y \in \operatorname{dom} F_1$ holds $F_1(y) = 0$. □

REFERENCES

[1] Tom M. Apostol. *Calculus*, volume II. Wiley, second edition, 1969.

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

[3] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Improving real analysis in Coq: A user-friendly approach to integrals and derivatives. In Chris Hawblitzel and Dale Miller, editors, *Certified Programs and Proofs – Second International Conference, CPP 2012, Kyoto, Japan, December 13–15, 2012. Proceedings*, volume 7679 of *Lecture Notes in Computer Science*, pages 289–304. Springer, 2012. doi:10.1007/978-3-642-35308-6_22.

[4] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Formalization of real analysis: A survey of proof assistants and libraries. *Mathematical Structures in Computer Science*, 26:1196–1233, 2015.

[5] Noboru Endou. Improper integral. Part II. *Formalized Mathematics*, 29(**4**):279–294, 2021. doi:10.2478/forma-2021-0024.

[6] Noboru Endou. Antiderivatives and integration. *Formalized Mathematics*, 31(1):131–141, 2023. doi:10.2478/forma-2023-0012.

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

[8] Noboru Endou. Reconstruction of the one-dimensional Lebesgue measure. *Formalized Mathematics*, 28(**1**):93–104, 2020. doi:10.2478/forma-2020-0008.

[9] Noboru Endou. Fubini's theorem. *Formalized Mathematics*, 27(**1**):67–74, 2019. doi:10.2478/forma-2019-0007.

[10] Noboru Endou. Relationship between the Riemann and Lebesgue integrals. *Formalized Mathematics*, 29(**4**):185–199, 2021. doi:10.2478/forma-2021-0018.

[11] Noboru Endou. Absolutely integrable functions. *Formalized Mathematics*, 30(**1**):31–51, 2022. doi:10.2478/forma-2022-0004.

[12] Jacques D. Fleuriot. On the mechanization of real analysis in Isabelle/HOL. In Mark Aagaard and John Harrison, editors, *Theorem Proving in Higher Order Logics*, pages 145–161. Springer Berlin Heidelberg, 2000. ISBN 978-3-540-44659-0.

[13] Ruben Gamboa. *Continuity and Differentiability*, pages 301–315. Springer US, 2000. ISBN 978-1-4757-3188-0. doi:10.1007/978-1-4757-3188-0_18.

[14] Adam Grabowski and Christoph Schwarzweller. On duplication in mathematical repositories. In Serge Autexier, Jacques Calmet, David Delahaye, Patrick D. F. Ion, Laurence Rideau, Renaud Rioboo, and Alan P. Sexton, editors, *Intelligent Computer Mathematics, 10th International Conference, AISC 2010, 17th Symposium, Calculemus 2010, and 9th International Conference, MKM 2010, Paris, France, July 5–10, 2010. Proceedings*, volume 6167 of *Lecture Notes in Computer Science*, pages 300–314. Springer, 2010. doi:10.1007/978-3-642-14128-7_26.

[15] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Mizar in a nutshell. *Journal of Formalized Reasoning*, 3(2):153–245, 2010.

[16] Serge Lang. *Calculus of Several Variables*. Springer, third edition, 2012.
[17] 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.
[18] Keiko Narita, Noboru Endou, and Yasunari Shidama. Weak convergence and weak* convergence. *Formalized Mathematics*, 23(**3**):231–241, 2015. doi:10.1515/forma-2015-0019.
[19] Edward S. Smith, Meyer Salkover, and Howard K. Justice. *Calculus*. John Wiley and Sons, second edition, 1958.

Accepted December 18, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 325–339, 2023
DOI: 10.2478/forma-2023-0026
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Tarski Geometry Axioms. Part V – Half-planes and Planes

Roland Coghetto
cafr-MSA2P asbl
Rue de la Brasserie 5
7100 La Louvière, Belgium

Adam Grabowski
Faculty of Computer Science
University of Białystok
Poland

Summary. In the article, we continue the formalization of the work devoted to Tarski's geometry – the book "Metamathematische Methoden in der Geometrie" by W. Schwabhäuser, W. Szmielew, and A. Tarski. We use the Mizar system to formalize Chapter 9 of this book. We deal with half-planes and planes proving their properties as well as the theory of intersecting lines.

MSC: 51A05 51M04 68V20

Keywords: Tarski geometry; half-plane; plane

MML identifier: GTARSKI5, version: 8.1.14 5.76.1462

Introduction

In the article, we continue [6], [7], and [8] – the formalization of the work devoted to Tarski's geometry – the book "Metamathematische Methoden in der Geometrie" (SST for short) by W. Schwabhäuser, W. Szmielew, and A. Tarski [18], [10], [11]. We use the Mizar system [1], [2] to formalize (parts of) Chapter 9 of the SST book developing also results of Gupta [12] included there.

The first Mizar article formalizing Tarski's axioms [17] was inspired by another formalizations of SST: within the classical two-valued logic with Isabelle/HOL by Makarios [13, 14, 15], Metamath or by means of Coq [16, 4]. Some of the results were obtained with the help of other automatic proof assistants, either partially [9], or completely [3]. Relatively recent achievement was the import of huge portions of code from GeoCoq into Isabelle [5].

Here we define the notion of half-planes and planes and prove some of their basic properties, a theory of intersecting lines (including orthogonality), notions of betweenness including lines and points, shifting this notion into planes and spaces of higher dimension.

1. Preliminaries

Now we state the proposition:

(1) Let us consider Tarski plane S satisfying the axiom of congruence identity and the axiom of betweenness identity, and points a, b, c of S. If $a, b \leqslant c, c$, then $a = b$.

2. Betweenness Relation Revisited

Let S be a non empty Tarski plane, a, b be points of S, and A be a subset of S. We say that A lies between a and b if and only if

(Def. 1) A is a line and $a \notin A$ and $b \notin A$ and there exists a point t of S such that $t \in A$ and t lies between a and b.

Now we state the proposition:

(2) Let us consider a non empty Tarski plane S satisfying the axiom of betweenness identity, a point a of S, and a subset A of S. Then A does not lie between a and a.

Let S be a non empty Tarski plane and a, b, p, q be points of S. We say that between(a, p, q, b) if and only if

(Def. 2) $p \neq q$ and Line(p, q) lies between a and b.

From now on S denotes a non empty Tarski plane satisfying the axiom of congruence identity, the axiom of segment construction, the axiom of betweenness identity, and the axiom of Pasch, a, b denote points of S, and A denotes a subset of S. Now we state the proposition:

(3) 9.2 Satz:

If A lies between a and b, then A lies between b and a.

In the sequel S denotes a non empty Tarski plane satisfying seven Tarski's geometry axioms, a, b, c, m, r, s denote points of S, and A denotes a subset of S. Now we state the propositions:

(4) If b lies between a and c and A is a line and a, $c \in A$, then $b \in A$.

(5) If b lies between a and c and $a \neq b$ and A is a line and a, $b \in A$, then $c \in A$.

(6) Suppose A lies between a and c and $m \in A$ and Middle(a, m, c) and $r \in A$. If $a \overset{\simeq}{r} b$ and b lies between r and a, then A lies between b and c. The theorem is a consequence of (4).

(7) 9.3 LEMMA:
If A lies between a and c and $m \in A$ and Middle(a, m, c) and $r \in A$, then for every b such that $a \overset{\simeq}{r} b$ holds A lies between b and c. The theorem is a consequence of (6), (4), and (5).

Let S be a non empty Tarski plane satisfying seven Tarski's geometry axioms, a, b be points of S, and A be a subset of S. We say that $A \perp_a b$ if and only if

(Def. 3) $\overline{A, a} \perp \overline{a, b}$.

3. HALF-LINES AND OUTER PASCH

Let S be a non empty Tarski plane and K be a subset of S. We say that K is a half-line if and only if

(Def. 4) there exist points p, a of S such that $p \neq a$ and $K = \mathrm{HalfLine}(p, a)$.

Now we state the proposition:

(8) Let us consider points a, b, c, d, e of S. Suppose $b \neq c$ and $c \neq d$ and c lies between b and d and (b lies between a and c or a lies between b and c) and (d lies between c and e or e lies between c and d). Then c lies between a and e.

From now on S denotes a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms, a, b, c, d, m, p, q, r, s, x denote points of S, and A, A', E denote subsets of S. Now we state the propositions:

(9) Suppose $r \neq s$ and $s, c \leqslant r, a$ and A lies between a and c and $r \in A$ and $A \perp_r a$ and $s \in A$ and $A \perp_s c$. Then

(i) if Middle(r, m, s), then for every point u of S, $u \overset{\simeq}{r} a$ iff $\mathrm{S}_m(u) \overset{\simeq}{s} c$, and

(ii) for every points u, v of S such that $u \overset{\simeq}{r} a$ and $v \overset{\simeq}{s} c$ holds A lies between u and v.

The theorem is a consequence of (1) and (7).

(10) 9.4 LEMMA:
Suppose A lies between a and c and $r \in A$ and $A \perp_r a$ and $s \in A$ and $A \perp_s c$. Then

(i) if Middle(r, m, s), then for every point u of S, $u \overset{\simeq}{r} a$ iff $\mathrm{S}_m(u) \overset{\simeq}{s} c$, and

(ii) for every points u, v of S such that $u \overset{\simeq}{r} a$ and $v \overset{\simeq}{s} c$ holds A lies between u and v.

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

(11) Let us consider points a, b of S. If $a \neq b$, then $b \overset{\simeq}{a} b$.

(12) Satz 9.5 (Gupta 1965):
If A lies between a and c and $r \in A$, then for every b such that $a \overset{\simeq}{r} b$ holds A lies between b and c.
Proof: Consider p, q being points of S such that $p \neq q$ and $A = \mathrm{Line}(p, q)$. Consider x being a point of S such that x is perpendicular foot of p, q, a. $b \notin A$ by [7, (87), (45)]. Consider y being a point of S such that y is perpendicular foot of p, q, b. Consider z being a point of S such that z is perpendicular foot of p, q, c. Consider m being a point of S such that $\mathrm{Middle}(x, m, z)$. Set $d = \mathrm{S}_m(a)$. $d \notin A$ by [7, (87)]. $z \neq d$ by [7, (45), (87)]. $d \overset{\simeq}{z} c$. A lies between a and d and $m \in A$ and $\mathrm{Middle}(a, m, d)$ and $r \in A$ and $a \overset{\simeq}{r} b$. A lies between b and d. □

(13) Satz 9.6 (Satz von Pasch, Exterior form – Gupta 1965):
If c lies between a and p and q lies between b and c, then there exists x such that x lies between a and b and q lies between p and x. The theorem is a consequence of (12).

4. Points on the Same Side of the Line

Let S be a non empty Tarski plane, A be a subset of S, and a, b be points of S. We say that $a \overset{\simeq}{A} b$ if and only if

(Def. 5) there exists a point c of S such that A lies between a and c and A lies between b and c.

Let a, b, p, q be points of S. We say that $a \overset{\simeq}{p,q} b$ if and only if

(Def. 6) $p \neq q$ and $a \underset{\mathrm{Line}(p,q)}{\simeq} b$.

Now we state the propositions:

(14) 9.8 Satz:
If A lies between a and c, then A lies between b and c iff $a \overset{\simeq}{A} b$. The theorem is a consequence of (12).

(15) 9.9 Satz:
If A lies between a and b, then $\neg a \overset{\simeq}{A} b$. The theorem is a consequence of (14).

(16) 9.10 Lemma:
If A is a line and $a \notin A$, then there exists c such that A lies between a and c.

PROOF: Consider p, q such that $p \neq q$ and $A = \mathrm{Line}(p, q)$.
Set $c = \mathrm{S}_p(a)$. $p \neq c$ by [7, (104)]. □

(17) 9.11 SATZ: REFLEXIVITY:
If A is a line and $a \notin A$, then $a \overline{\overline{\in}}_A a$. The theorem is a consequence of (16).

(18) 9.12 SATZ: SYMMETRY:
If $a \overline{\overline{\in}}_A b$, then $b \overline{\overline{\in}}_A a$.

(19) 9.13 SATZ: TRANSITIVITY:
If $a \overline{\overline{\in}}_A b$ and $b \overline{\overline{\in}}_A c$, then $a \overline{\overline{\in}}_A c$. The theorem is a consequence of (14).

5. HALF-PLANES

Let S be a non empty Tarski plane, A be a subset of S, and a be a point of S. The functor $\mathrm{HalfPlane}(A, a)$ yielding a subset of S is defined by the term

(Def. 7) $\{x$, where x is a point of $S : x \overline{\overline{\in}}_A a\}$.

Let S be a non empty Tarski plane and p, q, a be points of S. Assume p, q and a are not collinear. The functor $\mathrm{HalfPlane}(p, q, a)$ yielding a set is defined by the term

(Def. 8) $\mathrm{HalfPlane}(\mathrm{Line}(p, q), a)$.

Now we state the propositions:

(20) If A is a line and $a \notin A$, then $a \in \mathrm{HalfPlane}(A, a)$. The theorem is a consequence of (17).

(21) If A is a line and $a \notin A$ and $b \notin A$ and $b \in \mathrm{HalfPlane}(A, a)$, then $a \in \mathrm{HalfPlane}(A, b)$.

(22) If $b \in \mathrm{HalfPlane}(A, a)$, then $\mathrm{HalfPlane}(A, b) \subseteq \mathrm{HalfPlane}(A, a)$. The theorem is a consequence of (19).

(23) If A is a line and $a \notin A$ and $b \notin A$ and $b \in \mathrm{HalfPlane}(A, a)$, then $\mathrm{HalfPlane}(A, b) = \mathrm{HalfPlane}(A, a)$. The theorem is a consequence of (21) and (22).

Let S be a non empty Tarski plane, A be a subset of S, and a, b be points of S. We say that a and b are on the opposite sides of A if and only if

(Def. 9) A lies between a and b.

Now we state the propositions:

(24) If $a \overline{\overline{\in}}_A b$, then A is a line and $a \notin A$ and $b \notin A$.

(25) 9.17 SATZ:
If $a \overline{\overline{\in}}_A b$ and c lies between a and b, then $c \overline{\overline{\in}}_A a$.
PROOF: Consider d being a point of S such that A lies between a and d and A lies between b and d. Consider x being a point of S such that $x \in A$

and x lies between a and d. Consider y being a point of S such that $y \in A$ and y lies between b and d. Consider t being a point of S such that t lies between c and d and t lies between x and y. $c \notin A$. A lies between c and d by (24), [7, (87), (14)]. □

6. Half-planes and Collinearity

Now we state the propositions:

(26) 9.18 Satz:
If A is a line and $p \in A$ and a, b and p are collinear, then A lies between a and b iff p lies between a and b and $a \notin A$ and $b \notin A$.

(27) If A is a line and $p \in A$ and $a \cong_p b$ and $a \notin A$, then A lies between b and $\mathrm{S}_p(a)$.
Proof: Set $c = \mathrm{S}_p(a)$. p lies between a and c. $c \neq p$. $b \notin A$ by [7, (87), (73)]. $c \notin A$ by [7, (87)]. □

(28) If A is a line and $p \in A$ and $a \notin A$, then A lies between a and $\mathrm{S}_p(a)$.
Proof: Set $c = \mathrm{S}_p(a)$. p lies between a and c. $c \neq p$. $c \notin A$ by [7, (87)]. □

(29) 9.19 Satz:
If A is a line and $p \in A$ and a, b and p are collinear, then $a \cong_A b$ iff $a \cong_p b$ and $a \notin A$. The theorem is a consequence of (15), (28), and (27).

7. Planes

Let S be a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms, A be a subset of S, and r be a point of S. Assume A is a line and $r \notin A$. The functor $\mathrm{Plane}(A, r)$ yielding a subset of S is defined by

(Def. 10) there exists a point r' of S such that A lies between r and r' and $it = (\mathrm{HalfPlane}(A, r) \cup A) \cup \mathrm{HalfPlane}(A, r')$.

Now we state the propositions:

(30) If A is a line and $r \notin A$, then $\mathrm{HalfPlane}(A, r) \subseteq \mathrm{Plane}(A, r)$.

(31) If A is a line and $r \notin A$, then $A \subseteq \mathrm{Plane}(A, r)$ and $r \in \mathrm{Plane}(A, r)$. The theorem is a consequence of (20) and (30).

(32) Suppose A is a line and $r \notin A$. Then $\mathrm{Plane}(A, r) = \{x$, where x is a point of $S : x \cong_A r$ or $x \in A$ or A lies between r and $x\}$.
Proof: Consider r' being a point of S such that A lies between r and r' and $\mathrm{Plane}(A, r) = (\mathrm{HalfPlane}(A, r) \cup A) \cup \mathrm{HalfPlane}(A, r')$. Set $P =$

$\{x$, where x is a point of $S : x \overset{\sim}{_A} r$ or $x \in A$ or A lies between r and $x\}$. Plane$(A, r) \subseteq P$ by [7, (14)], (14). $P \subseteq$ Plane(A, r) by [7, (14)]. □

Let S be a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms and p, q, r be points of S. Assume p, q and r are not collinear. The functor Plane(p, q, r) yielding a subset of S is defined by the term

(Def. 11) Plane(Line$(p, q), r)$.

Let E be a subset of S. We say that E is a plane if and only if

(Def. 12) there exist points p, q, r of S such that p, q and r are not collinear and $E =$ Plane(p, q, r).

Now we state the propositions:

(33) If A lies between a and b, then $b \in$ Plane(A, a). The theorem is a consequence of (32).

(34) 9.21 SATZ:
If A is a line and $r \notin A$ and $s \in$ Plane(A, r) and $s \notin A$, then Plane$(A, r) =$ Plane(A, s). The theorem is a consequence of (14) and (23).

(35) If A, A' intersect at p and A, A' intersect at q, then $p = q$.

(36) If A is a line and a, $p \in A$, then $\mathrm{S}_p(a) \in A$.

(37) 9.22 LEMMA:
If A, A' intersect at p and $r \in A'$ and $r \neq p$, then $A' \subseteq$ Plane(A, r). The theorem is a consequence of (32), (31), and (36).

(38) If A is a line and A' is a line and $A \neq A'$, then there exists a point r of S such that $r \notin A$ and $r \in A'$.

Let S be a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms and A, A' be subsets of S. Assume A is a line and A' is a line and $A \neq A'$ and $A \cap A'$ is not empty. The functor Plane(A, A') yielding a subset of S is defined by

(Def. 13) there exists a point r of S such that $r \notin A$ and $r \in A'$ and $it =$ Plane(A, r).

Now we state the propositions:

(39) Let us consider a non empty Tarski plane S, subsets A, B of S, and a point x of S. If A, B intersect at x, then B, A intersect at x.

(40) If A, A' intersect at p, then $A \subseteq$ Plane(A', A) and $A' \subseteq$ Plane(A, A'). The theorem is a consequence of (37).

(41) Suppose A, A' intersect at p. Then there exists a point r of S such that

(i) $r \notin A$, and

(ii) $r \in A'$, and

(iii) $\mathrm{Plane}(A, A') = \mathrm{Plane}(A, r)$, and

(iv) $A' = \mathrm{Line}(r, p)$, and

(v) there exists a point r' of S such that p lies between r and r' and $p \neq r'$ and r, p and r' are collinear and $r' \notin A$ and $\mathrm{Plane}(A, r) = \mathrm{Plane}(A, r')$.

PROOF: Consider r being a point of S such that $r \notin A$ and $r \in A'$ and $\mathrm{Plane}(A, A') = \mathrm{Plane}(A, r)$. Consider r' being a point of S such that p lies between r and r' and $p \neq r'$. $r' \notin A$ by [7, (89)]. $r' \in A'$ and $A' \subseteq \mathrm{Plane}(A, r)$. $\mathrm{Plane}(A, r) = \mathrm{Plane}(A, r')$. □

(42) If A, A' intersect at p, then $\mathrm{Plane}(A, A') \subseteq \mathrm{Plane}(A', A)$. The theorem is a consequence of (41), (32), (31), (40), (14), (34), (29), and (37).

Now we state the propositions:

(43) 9.24 SATZ:
If A, A' intersect at p, then $A \subseteq \mathrm{Plane}(A, A')$ and $A' \subseteq \mathrm{Plane}(A, A')$ and $\mathrm{Plane}(A, A') = \mathrm{Plane}(A', A)$. The theorem is a consequence of (39), (40), and (42).

(44) Suppose a, $b \in E$ and $a \neq b$ and p, q and r are not collinear and $E = \mathrm{Plane}(p, q, r)$ and $c \in \mathrm{Line}(p, q)$ and $c \notin \mathrm{Line}(a, b)$ and $b \notin \mathrm{Line}(p, q)$. Then

(i) $\mathrm{Line}(a, b) \subseteq E$, and

(ii) there exists c such that a, b and c are not collinear and $E = \mathrm{Plane}(a, b, c)$.

The theorem is a consequence of (43), (34), and (31).

(45) Suppose a, $b \in E$ and $a \neq b$ and p, q and r are not collinear and $E = \mathrm{Plane}(p, q, r)$ and $b \notin \mathrm{Line}(p, q)$ and $\mathrm{Line}(p, q) \neq \mathrm{Line}(a, b)$. Then

(i) $\mathrm{Line}(a, b) \subseteq E$, and

(ii) there exists c such that a, b and c are not collinear and $E = \mathrm{Plane}(a, b, c)$.

PROOF: Set $A = \mathrm{Line}(p, q)$. Set $A' = \mathrm{Line}(a, b)$. There exists a point c of S such that $c \notin A'$ and $c \in A$ by [7, (46), (83), (87)]. □

(46) SATZ 9.25:
If E is a plane and a, $b \in E$ and $a \neq b$, then $\mathrm{Line}(a, b) \subseteq E$ and there exists c such that a, b and c are not collinear and $E = \mathrm{Plane}(a, b, c)$. The theorem is a consequence of (31) and (45).

(47) SATZ 9.26:
If a, b and c are not collinear and E is a plane and a, b, $c \in E$, then $E = \mathrm{Plane}(a, b, c)$. The theorem is a consequence of (46) and (34).

(48) If A is a line and $a \notin A$, then $a \in \mathrm{Plane}(A, a)$. The theorem is a consequence of (32) and (17).

(49) 9.27.(1) SATZ:
If a, b and c are not collinear, then there exists a subset E of S such that $\mathrm{Plane}(a, b, c) = E$ and E is a plane and a, b, $c \in E$. The theorem is a consequence of (31) and (48).

(50) 9.27.(2) SATZ:
If A is a line and $c \notin A$, then there exists a subset E of S such that E is a plane and $A \subseteq E$ and $c \in E$ and $\mathrm{Plane}(A, c) = E$. The theorem is a consequence of (31) and (48).

(51) 9.27.(3) SATZ:
If A, A' intersect at p, then there exists a subset E of S such that E is a plane and $A \subseteq E$ and $A' \subseteq E$ and $\mathrm{Plane}(A, A') = E$. The theorem is a consequence of (50) and (43).

(52) 9.28 FOLGERUNG:
Suppose a, b and c are not collinear. Let us consider subsets E_1, E_2 of S. Suppose E_1 is a plane and a, b, $c \in E_1$ and E_2 is a plane and a, b, $c \in E_2$. Then $E_1 = E_2$. The theorem is a consequence of (47).

(53) 9.29 FOLGERUNG:
Suppose a, b and c are not collinear. Then

(i) $\mathrm{Plane}(a, b, c) = \mathrm{Plane}(b, c, a)$, and

(ii) $\mathrm{Plane}(a, b, c) = \mathrm{Plane}(c, a, b)$, and

(iii) $\mathrm{Plane}(a, b, c) = \mathrm{Plane}(b, a, c)$, and

(iv) $\mathrm{Plane}(a, b, c) = \mathrm{Plane}(a, c, b)$, and

(v) $\mathrm{Plane}(a, b, c) = \mathrm{Plane}(c, b, a)$.

The theorem is a consequence of (49) and (52).

(54) 9.30 FOLGERUNG:
Suppose A is a line. Let us consider subsets E_1, E_2 of S. Suppose E_1 is a plane and E_2 is a plane and $A \subseteq E_1$ and $A \subseteq E_2$ and $E_1 \neq E_2$. Let us consider a point x of S. Then $x \in E_1$ and $x \in E_2$ if and only if $x \in A$. The theorem is a consequence of (52).

(55) If $s \overset{\simeq}{}_{p,q} r$, then $s \neq p$ and $s \neq q$ and $r \neq p$ and $r \neq q$ and $p \neq q$.

(56) $\mathrm{Line}(b, c)$ does not lie between a and a.

(57) If A lies between a and b, then $a \neq b$.

(58) Let us consider Tarski plane S satisfying the axiom of congruence identity, the axiom of segment construction, the axiom of betweenness identity,

the axiom of Pasch, and Lower Dimension Axiom. Then there exist points p, q of S such that $p \neq q$.

(59) 9.31 Satz:

If $s \underset{p,q}{\simeq} r$ and $s \underset{p,r}{\simeq} q$, then $\mathrm{Line}(p, s)$ lies between q and r. The theorem is a consequence of (14), (29), (19), and (12).

8. Coplanarity Relation

Let S be a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms and A be a subset of S. We say that A is a set of coplanar points if and only if

(Def. 14) there exists a subset E of S such that E is a plane and $A \subseteq E$.

Let S be a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms and a, b, c, d be points of S. We say that a, b, c, d are coplanar if and only if

(Def. 15) there exists a subset E of S such that E is a plane and a, b, c, $d \in E$.

Now we state the propositions:

(60) Suppose a, b, c, d are coplanar. Then

(i) a, b, d, c are coplanar, and

(ii) a, c, b, d are coplanar, and

(iii) a, c, d, b are coplanar, and

(iv) a, d, c, b are coplanar, and

(v) a, d, b, c are coplanar, and

(vi) b, a, c, d are coplanar, and

(vii) b, a, d, c are coplanar, and

(viii) b, c, a, d are coplanar, and

(ix) b, c, d, a are coplanar, and

(x) b, d, a, c are coplanar, and

(xi) b, d, c, a are coplanar, and

(xii) c, a, b, d are coplanar, and

(xiii) c, a, d, b are coplanar, and

(xiv) c, b, a, d are coplanar, and

(xv) c, b, d, a are coplanar, and

(xvi) d, a, b, c are coplanar, and

(xvii) d, a, c, b are coplanar, and

(xviii) d, b, a, c are coplanar, and

(xix) d, b, c, a are coplanar.

(61) a, a, a, a are coplanar. The theorem is a consequence of (49).

(62) a, a, a, b are coplanar. The theorem is a consequence of (61) and (49).

(63) a, a, b, c are coplanar. The theorem is a consequence of (49), (46), and (62).

(64) If a, b and x are collinear and c, d and x are collinear and $a \neq x$ and $c \neq x$, then a, b, c, d are coplanar. The theorem is a consequence of (49), (31), and (53).

(65) If b, a and x are collinear and c, d and x are collinear and $b \neq x$ and $c \neq x$, then a, b, c, d are coplanar. The theorem is a consequence of (64).

(66) If a, b and x are collinear and c, d and x are collinear and $b \neq x$ and $c \neq x$, then a, b, c, d are coplanar. The theorem is a consequence of (65).

(67) Suppose a, b and x are collinear and c, d and x are collinear and ($b \neq x$ and $c \neq x$ or $b \neq x$ and $d \neq x$ or $a \neq x$ and $c \neq x$ or $a \neq x$ and $d \neq x$). Then a, b, c, d are coplanar. The theorem is a consequence of (66), (64), and (65).

(68) 9.33 SATZ:
a, b, c, d are coplanar if and only if there exists x such that a, b and x are collinear and c, d and x are collinear or a, c and x are collinear and b, d and x are collinear or a, d and x are collinear and b, c and x are collinear. The theorem is a consequence of (63), (47), (53), (59), (32), and (67).

(69) Suppose a, b and c are not collinear. Then

(i) $\mathrm{Plane}(a, b, c)$ is a plane, and

(ii) a, b, $c \in \mathrm{Plane}(a, b, c)$, and

(iii) for every points u, v of S such that u, $v \in \mathrm{Plane}(a, b, c)$ and $u \neq v$ holds $\mathrm{Line}(u, v) \subseteq \mathrm{Plane}(a, b, c)$.

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

(70) 9.34 SATZ:
Suppose a, b and c are not collinear. Let us consider a subset E of S. Suppose a, b, $c \in E$ and for every points u, v of S such that u, $v \in E$ and $u \neq v$ holds $\mathrm{Line}(u, v) \subseteq E$. Then $\mathrm{Plane}(a, b, c) \subseteq E$.
PROOF: $\mathrm{Plane}(a, b, c)$ is a plane and a, b, $c \in \mathrm{Plane}(a, b, c)$ and for every points u, v of S such that u, $v \in \mathrm{Plane}(a, b, c)$ and $u \neq v$ holds $\mathrm{Line}(u, v) \subseteq \mathrm{Plane}(a, b, c)$. $a \neq c$ by [7, (46), (14)]. $b \neq c$ by [7, (46)]. $\mathrm{Plane}(a, b, c) \subseteq E$ by (68), [7, (14)]. □

9. Towards Higher Dimensions

Let S be a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms, a, b be points of S, and A be a subset of S. We say that between$^2(a, A, b)$ if and only if

(Def. 16) A is a plane and $a \notin A$ and $b \notin A$ and there exists a point t of S such that $t \in A$ and t lies between a and b.

Now we state the propositions:

(71) 9.38 Satz (n = 2):
If between$^2(a, A, b)$, then between$^2(b, A, a)$.

(72) If p lies between a and c and $a \overset{\approx}{p} b$, then p lies between b and c.

(73) 9.39 Satz (n = 2):
If between$^2(a, A, c)$ and $r \in A$, then for every b such that $a \overset{\approx}{r} b$ holds between$^2(b, A, c)$. The theorem is a consequence of (69) and (12).

Let S be a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms, a, b be points of S, and A be a subset of S. We say that $a \overset{2}{\underset{A}{\simeq}} b$ if and only if

(Def. 17) there exists a point c of S such that between$^2(a, A, c)$ and between$^2(b, A, c)$.

Now we state the propositions:

(74) 9.41 Satz (n = 2):
If between$^2(a, A, c)$, then between$^2(b, A, c)$ iff $a \overset{2}{\underset{A}{\simeq}} b$. The theorem is a consequence of (69) and (73).

(75) 9.9 Satz (Version n = 2):
If between$^2(a, A, b)$, then $\neg(a \overset{2}{\underset{A}{\simeq}} b)$. The theorem is a consequence of (74).

(76) 9.10 Lemma (Version n = 2):
If A is a plane and $a \notin A$, then there exists c such that between$^2(a, A, c)$. Proof: Consider p, q, r such that p, q and r are not collinear and $A = \mathrm{Plane}(p, q, r)$. $r \notin \mathrm{Line}(p, q)$. $\mathrm{Line}(p, q) \subseteq A$. p, q, $r \in A$. Set $c = \mathrm{S}_p(a)$. $p \neq c$ by [7, (104)]. $c \notin A$. □

(77) 9.11 Satz (Version n = 2):
If A is a plane and $a \notin A$, then $a \overset{2}{\underset{A}{\simeq}} a$. The theorem is a consequence of (76).

(78) 9.12 Satz (Version n = 2):
If $a \overset{2}{\underset{A}{\simeq}} b$, then $b \overset{2}{\underset{A}{\simeq}} a$.

(79) 9.13 SATZ (VERSION N = 2):

If $a \overset{2}{\underset{A}{\simeq}} b$ and $b \overset{2}{\underset{A}{\simeq}} c$, then $a \overset{2}{\underset{A}{\simeq}} c$. The theorem is a consequence of (74).

10. HALF-SPACES

Let S be a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms, A be a subset of S, and a be a point of S. Assume A is a plane and $a \notin A$. The functor $\mathrm{HalfSpace}^3(A, a)$ yielding a subset of S is defined by the term

(Def. 18) $\{x$, where x is a point of $S : x \overset{2}{\underset{A}{\simeq}} a\}$.

Let p, q, a be points of S. Assume p, q and a are not collinear. The functor $\mathrm{HalfSpace}^3(p, q, a)$ yielding a set is defined by the term

(Def. 19) $\mathrm{HalfSpace}^3(\mathrm{Line}(p, q), a)$.

Now we state the propositions:

(80) If A is a plane and $a \notin A$, then $a \in \mathrm{HalfSpace}^3(A, a)$. The theorem is a consequence of (77).

(81) If A is a plane and $a \notin A$ and $b \notin A$ and $b \in \mathrm{HalfSpace}^3(A, a)$, then $a \in \mathrm{HalfSpace}^3(A, b)$.

(82) If A is a plane and $a \notin A$ and $b \notin A$ and $b \in \mathrm{HalfSpace}^3(A, a)$, then $\mathrm{HalfSpace}^3(A, b) \subseteq \mathrm{HalfSpace}^3(A, a)$. The theorem is a consequence of (79).

(83) If A is a plane and $a \notin A$ and $b \notin A$ and $b \in \mathrm{HalfSpace}^3(A, a)$, then $\mathrm{HalfSpace}^3(A, b) = \mathrm{HalfSpace}^3(A, a)$. The theorem is a consequence of (81) and (82).

11. TOWARDS SPACES IN HIGHER DIMENSIONS

Let S be a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms, A be a subset of S, and r be a point of S. Assume A is a plane and $r \notin A$. The functor $\mathrm{Space}^3(A, r)$ yielding a subset of S is defined by

(Def. 20) there exists a point r' of S such that $\mathrm{between}^2(r, A, r')$ and $it = (\mathrm{HalfSpace}^3(A, r) \cup A) \cup \mathrm{HalfSpace}^3(A, r')$.

Now we state the propositions:

(84) If A is a plane and $r \notin A$, then $\mathrm{HalfSpace}^3(A, r) \subseteq \mathrm{Space}^3(A, r)$.

(85) If A is a plane and $r \notin A$, then $A \subseteq \mathrm{Space}^3(A, r)$ and $r \in \mathrm{Space}^3(A, r)$. The theorem is a consequence of (80) and (84).

(86) Suppose A is a plane and $r \notin A$. Then $\mathrm{Space}^3(A, r) = \{x$, where x is a point of $S : x \overset{2}{\underset{A}{\simeq}} r$ or $x \in A$ or $\mathrm{between}^2\,(r, A, x)\}$.

PROOF: Consider r' being a point of S such that $\mathrm{between}^2(r, A, r')$ and $\mathrm{Space}^3(A, r) = (\mathrm{HalfSpace}^3(A, r) \cup A) \cup \mathrm{HalfSpace}^3(A, r')$. Set $P = \{x$,where x is a point of $S : x \overset{2}{\underset{A}{\simeq}} r$ or $x \in A$ or $\mathrm{between}^2\,(r, A, x)\}$. $\mathrm{Space}^3(A, r) \subseteq P$ by [7, (14)], (74). $P \subseteq \mathrm{Space}^3(A, r)$ by [7, (14)]. □

Let S be a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms and p_0, p_1, p_2, r be points of S. Assume p_0, p_1, p_2, r are not coplanar. The functor $\mathrm{Space}^3(p_0, p_1, p_2, r)$ yielding a subset of S is defined by the term

(Def. 21) $\mathrm{Space}^3(\mathrm{Plane}(p_0, p_1, p_2), r)$.

Let E be a subset of S. We say that E is a space^3 if and only if

(Def. 22) there exists a point r of S and there exists a subset A of S such that A is a plane and $r \notin A$ and $E = \mathrm{Space}^3(A, r)$.

Now we state the propositions:

(87) If A is a plane and a, b and c are not collinear and a, b, $c \in A$ and $d \notin A$, then a, b, c, d are not coplanar.

(88) Suppose E is a space^3. Then there exists a and there exists b and there exists c and there exists d such that a, b, c, d are not coplanar and $E = \mathrm{Space}^3(a, b, c, d)$. The theorem is a consequence of (69) and (87).

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] Michael Beeson and Larry Wos. OTTER proofs in Tarskian geometry. In *International Joint Conference on Automated Reasoning*, volume 8562 of *Lecture Notes in Computer Science*, pages 495–510. Springer, 2014. doi:10.1007/978-3-319-08587-6_38.

[4] Gabriel Braun and Julien Narboux. A synthetic proof of Pappus' theorem in Tarski's geometry. *Journal of Automated Reasoning*, 58(2):23, 2017. doi:10.1007/s10817-016-9374-4.

[5] Roland Coghetto. Tarski's parallel postulate implies the 5th Postulate of Euclid, the Postulate of Playfair and the original Parallel Postulate of Euclid. *Archive of Formal Proofs*, January 2021. `https://isa-afp.org/entries/IsaGeoCoq.html`, Formal proof development.

[6] Roland Coghetto and Adam Grabowski. Tarski geometry axioms – Part II. *Formalized Mathematics*, 24(**2**):157–166, 2016. doi:10.1515/forma-2016-0012.

[7] Roland Coghetto and Adam Grabowski. Tarski geometry axioms. Part III. *Formalized Mathematics*, 25(**4**):289–313, 2017. doi:10.1515/forma-2017-0028.

[8] Roland Coghetto and Adam Grabowski. Tarski geometry axioms. Part IV – right angle. *Formalized Mathematics*, 27(**1**):75–85, 2019. doi:10.2478/forma-2019-0008.

[9] Sana Stojanovic Durdevic, Julien Narboux, and Predrag Janičić. Automated generation of machine verifiable and readable proofs: a case study of Tarski's geometry. *Annals of Mathematics and Artificial Intelligence*, 74(3-4):249–269, 2015.

[10] Adam Grabowski. Tarski's geometry modelled in Mizar computerized proof assistant. In Maria Ganzha, Leszek Maciaszek, and Marcin Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, volume 8 of *ACSIS – Annals of Computer Science and Information Systems*, pages 373–381, 2016. doi:10.15439/2016F290.

[11] Adam Grabowski and Roland Coghetto. Tarski's geometry and the Euclidean plane in Mizar. In *Joint Proceedings of the FM4M, MathUI, and ThEdu Workshops, Doctoral Program, and Work in Progress at the Conference on Intelligent Computer Mathematics 2016 co-located with the 9th Conference on Intelligent Computer Mathematics (CICM 2016), Białystok, Poland, July 25–29, 2016*, volume 1785 of *CEUR-WS*, pages 4–9. CEUR-WS.org, 2016.

[12] Haragauri Narayan Gupta. *Contributions to the Axiomatic Foundations of Geometry*. PhD thesis, University of California-Berkeley, 1965.

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

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

[15] Timothy James McKenzie Makarios. A further simplification of Tarski's axioms of geometry. *Note di Matematica*, 33(2):123–132, 2014.

[16] Julien Narboux. Mechanical theorem proving in Tarski's geometry. In F. Botana and T. Recio, editors, *Automated Deduction in Geometry*, volume 4869 of *Lecture Notes in Computer Science*, pages 139–156. Springer, 2007.

[17] William Richter, Adam Grabowski, and Jesse Alama. Tarski geometry axioms. *Formalized Mathematics*, 22(**2**):167–176, 2014. doi:10.2478/forma-2014-0017.

[18] Wolfram Schwabhäuser, Wanda Szmielew, and Alfred Tarski. *Metamathematische Methoden in der Geometrie*. Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1983.

Accepted December 18, 2023

FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 341–352, 2023
DOI: 10.2478/forma-2023-0027
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Extensions of Orderings

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In this article we extend the algebraic theory of ordered fields [6], [8] in Mizar. We introduce extensions of orderings: if E is a field extension of F, then an ordering P of F extends to E, if there exists an ordering O of E containing P. We first prove some necessary and sufficient conditions for P being extendable to E, in particular that P extends to E if and only if the set $QS\ E := \{\sum a * b^2 \mid a \in P,\ b \in E\}$ is a preordering of E – or equivalently if and only if $-1 \notin QS\ E$. Then we show for non-square $a \in F$ that P extends to $F(\sqrt{a})$ if and only if P and finally that every ordering P of F extends to E if the degree of E over F is odd.

MSC: 12J15 12F99 68V20

Keywords: ordered fields; quadratic extensions; extensions of odd degree

MML identifier: `REALALG3`, version: `8.1.14 5.76.1462`

Introduction

In this article we extend the algebraic theory of ordered fields [5] using the Mizar formalism [1, 4, 2]. We define extensions of orderings: if E is a field extension of F and P an ordering of F, then P extends to E, if there is an ordering of E containing P.

In the preliminary section, we provide a number of technical lemmas. Among others we define the sets P^+ and P^- of positive and negative elements, respectively, and show that the existence of a partition $\{P^+, \{0\}, P\}$ is equivalent to our definition of orderings, e.g. that $P^+ \cup \{0\}$ is a positive cone [5].

The next section is devoted to polynomials [9]. Here we prove some theorems necessary for our main results, for example, that every polynomial of odd degree has an irreducible factor of odd degree. We also show the – rather technical – fact that evaluating a sum of polynomials is the same as summing up evaluations of the addends, that is for $a \in E$ we have

$$(\sum_{i=1}^{n} p_i)(a) \;=\; \sum_{i=1}^{n} p_i(a).$$

The third section presents more properties of the fields $F(a)$ for an element a such that $a^2 \in F$, but $a \notin F$. In this case the degree of the extension is 2, so that the representation of elements of $F(a)$ by $x + \cdot a \cdot y$ with $x, y \in F$ is unique [7]. This follows from $\{1, a\}$ being a basis of $F(a)$'s corresponding vector space [3].

Then in Section 4 we define extensions (cf. [13, 10]) of orderings and introduce the set of P-quadratic sums of E

$$QS(E) \;:=\; \{\sum a \cdot b^2 \mid a \in P,\; b \in E\}.$$

We show that P extends to E if and only if $QS(E)$ is an ordering of P, which is the case if and only if $1 \notin QS(E)$. This allows to prove our main theorems [8]: Firstly, that for a non-square element $a \in F$ an ordering P of F extends to $F(a)$ if and only if $\sqrt{a} \in P$; because if

$$-1 \;=\; \sum a_i \cdot (x_i + \cdot a \cdot y_i)^2 \in QS(E),$$

then because $-1 = 1 + a * 0$ would follow

$$-1 \;=\; \sum a_i \cdot {x_i}^2 + \cdot a_i \cdot y_i^2 \cdot a^2,$$

and hence $-1 \in P$, because $a_i, a^2 \in F$.

Secondly, that every ordering P of F extends to a field extension E of odd degree. The proof is by induction and uses the fact that E is a simple extension of F, e.g. $E = F(a)$. Then, because $\{1, a, \ldots, a^{n-1}\}$ is a basis of E, from $-1 = \sum a_i \cdot (x_i + a \cdot y_i)^2$ would follow the existence of an irreducible polynomial h with odd degree $< n$, so that by induction hypothesis P extends to $F(b)$, where h is the minimal polynomial of b. Then, however, the equation can again be pushed down to F giving $-1 \in P$.

1. Preliminaries

The scheme *3SeqDEx* deals with a non empty set $\mathcal{D}$ and a natural number $\mathcal{A}$ and a binary predicate $\mathcal{P}$ and a binary predicate $\mathcal{Q}$ and a binary predicate $\mathcal{R}$ and states that

(Sch. 1) There exist finite sequences p, q, r of elements of $\mathcal{D}$ such that $\operatorname{dom} p = \operatorname{Seg} \mathcal{A}$ and $\operatorname{dom} q = \operatorname{Seg} \mathcal{A}$ and $\operatorname{dom} r = \operatorname{Seg} \mathcal{A}$ and for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ holds $\mathcal{P}[k, p(k)]$ and for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ holds $\mathcal{Q}[k, q(k)]$ and for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ holds $\mathcal{R}[k, r(k)]$

provided

- for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ there exists an element x of $\mathcal{D}$ such that $\mathcal{P}[k, x]$ and
- for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ there exists an element x of $\mathcal{D}$ such that $\mathcal{Q}[k, x]$ and
- for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ there exists an element x of $\mathcal{D}$ such that $\mathcal{R}[k, x]$.

Now we state the proposition:

(1) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L. Then $-\{0_L\} = \{0_L\}$.

Let R be a ring. The functor $2.(R)$ yielding an element of R is defined by the term

(Def. 1) $1_R + 1_R$.

Let us note that there exists a field which has characteristic 2. Let R be a ring with characteristic 2. One can verify that $2.(R)$ is zero.

Let R be a non degenerated ring without characteristic 2. One can verify that $2.(R)$ is non zero and $2.(\mathbb{F}_{\mathbb{Q}})$ is non square and $2.(\mathbb{R}_{\mathrm{F}})$ is a square and there exists a field which is preordered and polynomial-disjoint and every non degenerated ring which is preordered and has also not characteristic 2. Now we state the proposition:

(2) Let us consider a field F, an extension E of F, and a finite sequence f of elements of E. Suppose for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) \in F$. Then

(i) f is a finite sequence of elements of F, and

(ii) $\sum f \in F$.

Let F be a field, a be sum of squares element of F, and b be sum of squares, non zero element of F. Observe that $a \cdot (b^{-1})$ is a sum of squares. Let f be a quadratic, non empty finite sequence of elements of F. Let us note that $\sum f$ is a sum of squares. Let R be a zero structure. Let us observe that there exists a finite sequence of elements of R which is trivial and $\varepsilon_{(\text{the carrier of } R)}$ is trivial and every finite sequence of elements of R which is empty is also trivial.

Let f, g be trivial finite sequences of elements of R. Observe that $f \frown g$ is trivial. Let R be a non degenerated ring, f be a non trivial finite sequence of elements of R, and g be a finite sequence of elements of R. Observe that $f \frown g$ is non trivial and $g \frown f$ is non trivial. Let R be a ring and f be a trivial finite sequence of elements of R. One can check that $\sum f$ is zero. Let E be a field, F be a subfield of E, and a be an element of F. The functor $^{@}(a, E)$ yielding an element of E is defined by the term

(Def. 2) a.

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

(Def. 3) $a \in$ the carrier of F.

Let us observe that there exists an element of E which is F-membered. Let a be an element of E. Assume a is F-membered. The functor $^{@}(F, a)$ yielding an element of F is defined by the term

(Def. 4) a.

Let a be an F-membered element of E. Observe that $^{@}(F, a)$ reduces to a. Let R be a non degenerated ring. One can check that 1_R is non zero and -1_R is non zero. Let R be a preordered, non degenerated ring, P be a preordering of R, and a, b be P-positive elements of R. Let us observe that $a + b$ is P-positive.

Let R be a preordered integral domain. Let us note that $a \cdot b$ is P-positive. Let R be a ring and S be a subset of R. The functors: S^+ and S^- yielding subsets of R are defined by terms

(Def. 5) $S \setminus \{0_R\}$,

(Def. 6) $(-S) \setminus \{0_R\}$,

respectively. Let R be a preordered, non degenerated ring and P be a preordering of R. Let us note that P^+ is non empty and P^- is non empty and $P^+ \cap P^-$ is empty and P^+ is closed under addition. Let R be a preordered integral domain. Note that P^+ is closed under multiplication. Now we state the propositions:

(3) Let us consider a preordered, non degenerated ring R, and a preordering P of R. Then

(i) $P + P^+ \subseteq P^+$, and

(ii) $P^+ + P \subseteq P^+$.

(4) Let us consider a preordered integral domain R, and a preordering P of R. Then

(i) $(P^-) \cdot (P^-) \subseteq P^+$, and

(ii) $(P^+) \cdot (P^-) \subseteq P^-$, and

(iii) $(P^-) \cdot (P^+) \subseteq P^-$.

(5) Let us consider a non degenerated integral domain R, and a subset S of R. Suppose S is a positive cone. Then

(i) $\{S^+, \{0_R\}, S^-\}$ is a partition of the carrier of R, and

(ii) S^+ is closed under addition and closed under multiplication.

(6) Let us consider a non degenerated ring R, and a subset S of R. Suppose $\{S, \{0_R\}, -S\}$ is a partition of the carrier of R and S is closed under addition and closed under multiplication. Then $S \cup \{0_R\}$ is a positive cone. The theorem is a consequence of (1).

(7) Let us consider an ordered field F, an extension E of F, an ordering P of F, and a finite sequence f of elements of E. Suppose for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) \in P$. Then $\sum f \in P$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence f of elements of E such that $\operatorname{len} f = \$_1$ and for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) \in P$ holds $\sum f \in P$. $\mathcal{P}[0]$ by [11, (2)], [12, (25)]. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\operatorname{len} f = n$. □

(8) Let us consider an ordered field F, an ordering P of F, and a field E. Suppose $E \approx F$. Then

(i) E is ordered, and

(ii) there exists a subset Q of E such that $Q = P$ and Q is a positive cone.

Let F be an ordered field. Let us observe that there exists an extension of F which is ordered.

2. SOME PROPERTIES OF POLYNOMIALS

Let F be a field, g be a non empty finite sequence of elements of the carrier of Polynom-Ring F, and i be an element of $\operatorname{dom} g$. Let us observe that the functor $g(i)$ yields an element of the carrier of Polynom-Ring F. Let us consider a field F and polynomials p, q over F. Now we state the propositions:

(9) If $\operatorname{LC} p + \operatorname{LC} q \neq 0_F$, then $\deg((p+q)) = \max(\deg(p), \deg(q))$.

(10) (i) if $\deg(p) > \deg(q)$, then $\operatorname{LC}(p+q) = \operatorname{LC} p$, and

(ii) if $\deg(p) < \deg(q)$, then $\operatorname{LC}(p+q) = \operatorname{LC} q$, and

(iii) if $\deg(p) = \deg(q)$ and $\operatorname{LC} p + \operatorname{LC} q \neq 0_F$, then $\operatorname{LC}(p+q) = \operatorname{LC} p + \operatorname{LC} q$.

The theorem is a consequence of (9).

Now we state the propositions:

(11) Let us consider a field F, and an element p of the carrier of Polynom-Ring F. Then $\deg(\mathrm{NormPoly}\, p) = \deg(p)$.

(12) Let us consider a field F, and a non constant element p of the carrier of Polynom-Ring F. Then there exists a non constant, monic element q of the carrier of Polynom-Ring F such that

(i) $q \mid p$, and

(ii) q is irreducible.

Proof: Define $\mathcal{Q}$[natural number] $\equiv$ for every non constant element p of the carrier of Polynom-Ring F such that $\deg(p) = \$_1$ there exists a non constant, monic element q of the carrier of Polynom-Ring F such that $q \mid p$ and q is irreducible. For every natural number k, $\mathcal{Q}[k]$. $\square$

(13) Let us consider a field F, and an element p of the carrier of Polynom-Ring F. Suppose $\deg(p)$ is odd. Then there exists a non constant, monic element q of the carrier of Polynom-Ring F such that

(i) $q \mid p$, and

(ii) q is irreducible, and

(iii) $\deg(q)$ is odd.

The theorem is a consequence of (11) and (12).

(14) Let us consider a field F, a finite sequence f of elements of the carrier of Polynom-Ring F, and a non zero polynomial p over F. Suppose $p = \sum f$. Let us consider a finite sequence g of elements of F, and a natural number n. Suppose for every element i of $\mathrm{dom}\, f$ for every polynomial q over F such that $q = f(i)$ holds $\deg(q) \leqslant n$. Then $\deg(p) \leqslant n$.

(15) Let us consider an ordered field F, an ordering P of F, a finite sequence f of elements of the carrier of Polynom-Ring F, and a non zero polynomial p over F. Suppose $p = \sum f$ and for every element i of $\mathrm{dom}\, f$ and for every polynomial q over F such that $q = f(i)$ holds $\deg(q)$ is even and $\mathrm{LC}\, q \in P$. Then $\deg(p)$ is even.

(16) Let us consider a field F, an extension E of F, a polynomial p over F, an element a of F, and elements x, b of E. If $b = a$, then $\mathrm{ExtEval}(a \cdot p, x) = b \cdot (\mathrm{ExtEval}(p, x))$.

(17) Let us consider a field F, an extension E of F, a finite sequence f of elements of the carrier of Polynom-Ring F, and a polynomial p over F. Suppose $p = \sum f$. Let us consider an element a of E, and a finite sequence g of elements of E. Suppose $\mathrm{len}\, g = \mathrm{len}\, f$ and for every element i of $\mathrm{dom}\, f$ and for every polynomial q over F such that $q = f(i)$ holds $g(i) = \mathrm{ExtEval}(q, a)$. Then $\mathrm{ExtEval}(p, a) = \sum g$.

3. MORE ON THE FIELDS $F(a)$

Now we state the propositions:

(18) Let us consider a field F, an extension E of F, an element a of E, and an element b of F. If $b = a^{\mathbf{2}}$, then $\mathrm{ExtEval}(\mathrm{X}^2\text{-}\, b, a) = 0_E$.

(19) Let us consider a field F, an extension E of F, and an element a of E. If $a^{\mathbf{2}} \in F$, then a is F-algebraic. The theorem is a consequence of (18).

(20) Let us consider a field F, an extension E of F, and an F-algebraic element a of E. Then $a \notin F$ if and only if for every non zero polynomial p over F such that $\mathrm{ExtEval}(p, a) = 0_E$ holds $\deg(p) \geqslant 2$.

(21) Let us consider a field F, an extension E of F, and an F-algebraic element a of E. Suppose $a \notin F$. Let us consider an element b of F. If $b = a^{\mathbf{2}}$, then $\mathrm{MinPoly}(a, F) = \mathrm{X}^2\text{-}\, b$. The theorem is a consequence of (18) and (20).

(22) Let us consider a field F, an extension E of F, and an element a of E. Suppose $a \notin F$ and $a^{\mathbf{2}} \in F$. Then

(i) $\{1_E, a\}$ is a basis of $\mathrm{VecSp}(\mathrm{FAdj}(F, \{a\}), F)$, and

(ii) $\deg(\mathrm{FAdj}(F, \{a\}), F) = 2$.

PROOF: Reconsider $a_1 = a$ as an F-algebraic element of E. Reconsider $b = a^{\mathbf{2}}$ as an element of F. $\deg(\mathrm{MinPoly}(a_1, F)) = \deg(\mathrm{X}^2\text{-}\, b)$. $\mathrm{Base}(a_1) = \{1_E, a\}$. □

(23) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and an element b of E. Then $b \in$ the carrier of $\mathrm{FAdj}(F, \{a\})$ if and only if there exists a polynomial p over F such that $\deg(p) < \deg(\mathrm{MinPoly}(a, F))$ and $b = \mathrm{ExtEval}(p, a)$.

(24) Let us consider a field F, an extension E of F, and an element a of E. Suppose $a^{\mathbf{2}} \in F$. Let us consider an element b of $\mathrm{FAdj}(F, \{a\})$. Then there exist elements c_1, c_2 of $\mathrm{FAdj}(F, \{a\})$ such that

(i) c_1, $c_2 \in F$, and

(ii) $b = c_1 + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot c_2$.

The theorem is a consequence of (22).

(25) Let us consider a field F, an extension E of F, and an element a of E. Suppose $a \notin F$ and $a^{\mathbf{2}} \in F$. Let us consider elements c_1, c_2, d_1, d_2 of $\mathrm{FAdj}(F, \{a\})$. Suppose $c_1, c_2, d_1, d_2 \in F$ and $c_1 + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot c_2 = d_1 + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot d_2$. Then

(i) $c_1 = d_1$, and

(ii) $c_2 = d_2$.

PROOF: Set $K = \mathrm{FAdj}(F, \{a\})$. Set $V = \mathrm{VecSp}(K, F)$. Set $j = {}^{@}(K, a)$. Reconsider $1_V = 1_K$, $j_1 = j$ as an element of V. Define $\mathcal{P}[\mathrm{object}, \mathrm{object}] \equiv \$_1 = 1_K$ and $\$_2 = c_1 - d_1$ or $\$_1 = j$ and $\$_2 = c_2 - d_2$ or $\$_1 \neq 1_K$ and $\$_1 \neq j$ and $\$_2 = 0_F$. For every object x such that $x \in$ the carrier of V there exists an object y such that $y \in$ the carrier of F and $\mathcal{P}[x, y]$.

Consider l being a function from the carrier of V into the carrier of F such that for every object x such that $x \in$ the carrier of V holds $\mathcal{P}[x, l(x)]$. For every element v of V such that $v \notin \{1_V, j_1\}$ holds $l(v) = 0_F$. $\{1_V, j_1\}$ is linearly independent. □

Let us consider a field F, an extension E of F, an element a of E, an element b of F, and a quadratic, non empty finite sequence f of elements of $\mathrm{FAdj}(F, \{a\})$. Now we state the propositions:

(26) Suppose $a \notin F$ and $a^{\mathbf{2}} = b$. Then there exist quadratic, non empty finite sequences g_1, g_2 of elements of F and there exists a non empty finite sequence g_3 of elements of F such that $\sum f = ({}^{@}(\sum g_1 + b \cdot (\sum g_2), \mathrm{FAdj}(F, \{a\}))) + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot ({}^{@}(\sum g_3, \mathrm{FAdj}(F, \{a\})))$.

(27) Suppose $a \notin F$ and $a^{\mathbf{2}} = b$ and $\sum f \in F$. Then there exist quadratic, non empty finite sequences g_1, g_2 of elements of F such that $\sum f = \sum g_1 + b \cdot (\sum g_2)$. The theorem is a consequence of (26) and (25).

4. Extensions of Orderings

Let F be an ordered field, E be a field, and P be an ordering of F. We say that P extends to E if and only if

(Def. 7) there exists a subset O of E such that $P \subseteq O$ and O is a positive cone.

Let E be an ordered extension of F and O be an ordering of E. We say that O extends P if and only if

(Def. 8) $O \cap (\text{the carrier of } F) = P$.

Let us consider an ordered field F, an ordered extension E of F, an ordering P of F, and an ordering O of E. Now we state the propositions:

(28) O extends P if and only if for every element a of F, $a \in P$ iff $a \in O$.

(29) O extends P if and only if $P \subseteq O$.

Let R be an ordered ring, P be an ordering of R, and a be an element of R. The functor $\mathrm{signum}(P, a)$ yielding an integer is defined by the term

(Def. 9)
$$\begin{cases} 1, & \textbf{if } a \in P \setminus \{0_R\}, \\ 0, & \textbf{if } a = 0_R, \\ -1, & \textbf{otherwise}. \end{cases}$$

The functor signum(P) yielding a function from the carrier of R into $\mathbb{Z}$ is defined by

(Def. 10) for every element a of R, $it(a) = \mathrm{signum}(P, a)$.

Now we state the propositions:

(30) Let us consider an ordered integral domain R, an ordering P of R, and an element a of R. Then $a = \mathrm{signum}(P, a) \star |a|_P$.

(31) Let us consider an ordered field F, an ordered extension E of F, an ordering P of F, and an ordering O of E. Then O extends P if and only if $\mathrm{signum}(O)\restriction(\text{the carrier of } F) = \mathrm{signum}(P)$. The theorem is a consequence of (29).

Let F be an ordered field, E be an extension of F, P be an ordering of F, and f be a finite sequence of elements of E. We say that f is P-quadratic if and only if

(Def. 11) for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, f$ there exists a non zero element a of E and there exists an element b of E such that $a \in P$ and $f(i) = a \cdot b^{\mathbf{2}}$.

Observe that there exists a finite sequence of elements of E which is P-quadratic and non empty. Let f, g be P-quadratic finite sequences of elements of E. One can check that $f \frown g$ is P-quadratic as a finite sequence of elements of E. Now we state the proposition:

(32) Let us consider an ordered field F, an extension E of F, an ordering P of F, a P-quadratic finite sequence f of elements of E, and finite sequences g_1, g_2 of elements of E. Suppose $f = g_1 \frown g_2$. Then

(i) g_1 is P-quadratic, and

(ii) g_2 is P-quadratic.

Let F be an ordered field, E be an extension of F, and P be an ordering of F. The functor P-quadraticSums(E) yielding a non empty subset of E is defined by the term

(Def. 12) the set of all $\sum f$ where f is a P-quadratic finite sequence of elements of E.

We introduce the notation $\mathrm{QS}(E, P)$ as a synonym of P-quadraticSums(E). Let us observe that $\mathrm{QS}(E, P)$ is closed under addition and closed under multiplication and has all sums of squares. Now we state the propositions:

(33) Let us consider an ordered field F, an ordering P of F, an extension E of F, and a non zero element a of E. Then $a \in \mathrm{QS}(E, P)$ if and only if there exists a P-quadratic, non empty finite sequence f of elements of E such that $\sum f = a$ and for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, f$ holds $f(i) \neq 0_E$. The theorem is a consequence of (32).

(34) Let us consider an ordered field F, an extension E of F, and an ordering P of F. Then $P \subseteq \mathrm{QS}(E, P)$.

(35) Let us consider an ordered field F, an ordered extension E of F, an ordering P of F, and an ordering O of E. If O extends P, then $\mathrm{QS}(E, P) \subseteq O$. PROOF: $P \subseteq O$. Define $\mathcal{P}$[natural number] $\equiv$ for every P-quadratic finite sequence f of elements of E such that $\mathrm{len}\, f = \$_1$ holds $\sum f \in O$. For every natural number k, $\mathcal{P}[k]$. $\square$

Let us consider an ordered field F, an extension E of F, and an ordering P of F. Now we state the propositions:

(36) $\mathrm{QS}(E, P)$ is a prepositive cone if and only if $-1_E \notin \mathrm{QS}(E, P)$.

(37) P extends to E if and only if $\mathrm{QS}(E, P)$ is a prepositive cone. The theorem is a consequence of (29), (35), (36), and (34).

(38) P extends to E if and only if for every P-quadratic, non empty finite sequence f of elements of E such that $\sum f = 0_E$ holds f is trivial. The theorem is a consequence of (29), (36), and (37).

(39) Let us consider an ordered field F, an extension E of F, an ordering P of F, and an element a of E. Suppose $a^{\mathbf{2}} \in F$. Let us consider a P-quadratic, non empty finite sequence f of elements of $\mathrm{FAdj}(F, \{a\})$. Then there exist non empty finite sequences g_1, g_2 of elements of $\mathrm{FAdj}(F, \{a\})$ such that

(i) $\sum f = \sum g_1 + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot (2 \star \sum g_2)$, and

(ii) for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, g_1$ there exists a non zero element b of $\mathrm{FAdj}(F, \{a\})$ and there exist elements c_1, c_2 of $\mathrm{FAdj}(F, \{a\})$ such that $b \in P$ and c_1, $c_2 \in F$ and $g_1(i) = b \cdot ({c_1}^{\mathbf{2}} + {c_2}^{\mathbf{2}} \cdot ({}^{@}(\mathrm{FAdj}(F, \{a\}), a))^{\mathbf{2}})$, and

(iii) for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, g_2$ there exists a non zero element b of $\mathrm{FAdj}(F, \{a\})$ and there exist elements c_1, c_2 of $\mathrm{FAdj}(F, \{a\})$ such that $b \in P$ and c_1, $c_2 \in F$ and $g_2(i) = b \cdot c_1 \cdot c_2$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every P-quadratic, non empty finite sequence f of elements of $\mathrm{FAdj}(F, \{a\})$ such that $\mathrm{len}\, f = \$_1$ there exist non empty finite sequences g_1, g_2 of elements of $\mathrm{FAdj}(F, \{a\})$ such that $\sum f = \sum g_1 + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot (2 \star \sum g_2)$ and for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, g_1$ there exists a non zero element b of $\mathrm{FAdj}(F, \{a\})$.

There exist elements c_1, c_2 of $\mathrm{FAdj}(F, \{a\})$ such that $b \in P$ and c_1, $c_2 \in F$ and $g_1(i) = b \cdot ({c_1}^{\mathbf{2}} + {c_2}^{\mathbf{2}} \cdot ({}^{@}(\mathrm{FAdj}(F, \{a\}), a))^{\mathbf{2}})$ and for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, g_2$ there exists a non zero element b of $\mathrm{FAdj}(F, \{a\})$ and there exist elements c_1, c_2 of $\mathrm{FAdj}(F, \{a\})$ such that $b \in P$ and c_1, $c_2 \in F$ and $g_2(i) = b \cdot c_1 \cdot c_2$. For every non zero natural

number k, $\mathcal{P}[k]$. Consider n being a natural number such that $n = \operatorname{len} f$. $\square$

(40) Let us consider an ordered field F, an extension E of F, and an element a of E. Suppose $a^{\mathbf{2}} \in F$. Let us consider an ordering P of F. Then P extends to $\operatorname{FAdj}(F, \{a\})$ if and only if $a^{\mathbf{2}} \in P$. The theorem is a consequence of (29), (8), (39), (2), (25), (7), (36), and (37).

(41) Let us consider an ordered, polynomial-disjoint field F, an ordering P of F, and a non square element a of F. Then P extends to $\operatorname{FAdj}(F, \{\sqrt{a}\})$ if and only if $a \in P$. The theorem is a consequence of (40).

(42) $\operatorname{Positives}(\mathbb{F}_{\mathbb{Q}})$ extends to $\operatorname{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2.(\mathbb{F}_{\mathbb{Q}})}\})$. The theorem is a consequence of (41).

(43) $\operatorname{Positives}(\mathbb{F}_{\mathbb{Q}})$ does not extend to $\operatorname{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{-1_{\mathbb{F}_{\mathbb{Q}}}}\})$.

(44) Let us consider an ordered field F, an ordering P of F, an extension E of F, an element a of F, and elements b, c of E. Suppose $b^{\mathbf{2}} = a$ and $c^{\mathbf{2}} = -a$. Then

(i) P extends to $\operatorname{FAdj}(F, \{b\})$, or

(ii) P extends to $\operatorname{FAdj}(F, \{c\})$.

The theorem is a consequence of (40).

(45) Let us consider an ordered, polynomial-disjoint field F, an ordering P of F, and non square elements a, b of F. Suppose $b = -a$. Then

(i) P extends to $\operatorname{FAdj}(F, \{\sqrt{a}\})$, or

(ii) P extends to $\operatorname{FAdj}(F, \{\sqrt{b}\})$.

The theorem is a consequence of (41).

Let us consider a formally real field F, an extension E of F, an element a of F, and an element b of E. Now we state the propositions:

(46) If $b^{\mathbf{2}} = a$ and $a \in \operatorname{QS}(F)$, then $\operatorname{FAdj}(F, \{b\})$ is formally real. The theorem is a consequence of (40).

(47) If $b^{\mathbf{2}} = a$ and $\operatorname{FAdj}(F, \{b\})$ is not formally real, then $-a \in \operatorname{QS}(F)$. The theorem is a consequence of (8) and (27).

Let us consider an ordered, polynomial-disjoint field F and a non square element a of F. Now we state the propositions:

(48) If $a \in \operatorname{QS}(F)$, then $\operatorname{FAdj}(F, \{\sqrt{a}\})$ is formally real. The theorem is a consequence of (46).

(49) If $\operatorname{FAdj}(F, \{\sqrt{a}\})$ is not formally real, then $-a \in \operatorname{QS}(F)$. The theorem is a consequence of (47).

(50) Let us consider an ordered field F, an ordering P of F, and an extension E of F. If $\deg(E, F)$ is an odd natural number, then P extends to E.
PROOF: Define $\mathcal{Q}$[natural number] $\equiv$ for every extension E of F such that $\deg(E, F) = 2 \cdot \$_1 + 1$ holds P extends to E. For every natural number k, $\mathcal{Q}[k]$. Reconsider $n = \deg(E1, F)$ as an odd natural number. Consider k being an integer such that $n = 2 \cdot k + 1$. □

(51) Let us consider an ordered field F, an ordering P of F, an irreducible element p of the carrier of Polynom-Ring F, an extension E of F, and an element a of E. Suppose $\deg(p)$ is odd and a is a root of p in E. Then P extends to $\mathrm{FAdj}(F, \{a\})$. The theorem is a consequence of (11) and (50).

REFERENCES

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

[2] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. Equality in computer proof-assistants. In Ganzha, Maria and Maciaszek, Leszek and Paprzycki, Marcin, editor, *Proceedings of the 2015 Federated Conference on Computer Science and Information Systems*, volume 5 of *ACSIS-Annals of Computer Science and Information Systems*, pages 45–54. IEEE, 2015. doi:10.15439/2015F229.

[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] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[5] Serge Lang. *Algebra*. PWN, Warszawa, 1984.

[6] Alexander Prestel. *Lectures on Formally Real Fields*. Springer-Verlag, 1984.

[7] Knut Radbruch. *Algebra I*. Lecture Notes, University of Kaiserslautern, Germany, 1991.

[8] Knut Radbruch. *Geordnete Körper*. Lecture Notes, University of Kaiserslautern, Germany, 1991.

[9] Piotr Rudnicki, Christoph Schwarzweller, and Andrzej Trybulec. Commutative algebra in the Mizar system. *Journal of Symbolic Computation*, 32(1/2):143–169, 2001. doi:10.1006/jsco.2001.0456.

[10] Christoph Schwarzweller. Normal extensions. *Formalized Mathematics*, 31(1):121–130, 2023. doi:10.2478/forma-2023-0011.

[11] Christoph Schwarzweller. Field extensions and Kronecker's construction. *Formalized Mathematics*, 27(**3**):229–235, 2019. doi:10.2478/forma-2019-0022.

[12] Christoph Schwarzweller. Ordered rings and fields. *Formalized Mathematics*, 25(**1**):63–72, 2017. doi:10.1515/forma-2017-0006.

[13] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Quadratic extensions. *Formalized Mathematics*, 29(**4**):229–240, 2021. doi:10.2478/forma-2021-0021.

Accepted December 18, 2023