Contents

Formaliz. Math. 25 (**4**)

FORMALIZED MATHEMATICS
Vol. 25, No. 4, Pages 249–259, 2017
DOI: 10.1515/forma-2017-0024

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

Formally Real Fields

Christoph Schwarzweller
Institute of Informatics
Faculty of Mathematics, Physics and Informatics
University of Gdańsk
Wita Stwosza 57, 80-308 Gdańsk, Poland

Summary. We extend the algebraic theory of ordered fields [7, 6] in Mizar [1, 2, 3]: we show that every preordering can be extended into an ordering, i.e. that formally real and ordered fields coincide. We further prove some characterizations of formally real fields, in particular the one by Artin and Schreier using sums of squares [4]. In the second part of the article we define absolute values and the square root function [5].

MSC: 12J15 03B35

Keywords: formally real fields; ordered fields; abstract value; square roots

MML identifier: `REALALG2`, version: `8.1.06 5.45.1311`

1. Preliminaries

Let X, Y be non empty sets. Let us observe that there exists a function which is non empty, X-defined, and Y-valued and the carrier of $\mathbb{F}_{\mathbb{Q}}$ is rational-membered.

Now we state the propositions:

(1) Let us consider a right zeroed, non empty additive loop structure L, and subsets S, T of L. If $0_L \in T$, then $S \subseteq S + T$.

(2) Let us consider a right unital, non empty multiplicative loop structure L, and subsets S, T of L. If $1_L \in T$, then $S \subseteq S \cdot T$.

(3) Let us consider an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure L, and a subset S of L. If $0_L \in S$, then for every element a of L, $S \subseteq S + a \cdot S$. The theorem is a consequence of (1).

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

(4) Let us consider an add-associative, right zeroed, right complementable, right unital, right distributive, non empty double loop structure L, and a subset S of L. If 0_L, $1_L \in S$, then for every element a of L, $a \in S + a \cdot S$.

(5) Let us consider an add-associative, right zeroed, right complementable, Abelian, left distributive, non empty double loop structure R, elements a, b of R, and an integer i. Then $i \star (a \cdot b) = (i \star a) \cdot b$.
PROOF: Define $\mathcal{P}[\text{integer}] \equiv \$_1 \star (a \cdot b) = (\$_1 \star a) \cdot b$. $\mathcal{P}[0]$ by [11, (59)]. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$. For every integer i, $\mathcal{P}[i]$. □

(6) Let us consider an add-associative, right zeroed, right complementable, Abelian, left distributive, non empty double loop structure R, an element a of R, and an integer i. Then $i \star (-a) = -i \star a$.
PROOF: Define $\mathcal{P}[\text{integer}] \equiv \$_1 \star (-a) = -\$_1 \star a$. $\mathcal{P}[0]$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$. For every integer i, $\mathcal{P}[i]$. □

Let R be a ring and a be an element of R. Let us consider a commutative ring R and elements a, b of R. Now we state the propositions:

(7) $(a+b)^{\mathbf{2}} = a^{\mathbf{2}} + 2 \star a \cdot b + b^{\mathbf{2}}$. The theorem is a consequence of (43).

(8) $(a-b)^{\mathbf{2}} = a^{\mathbf{2}} - 2 \star a \cdot b + b^{\mathbf{2}}$. The theorem is a consequence of (7), (43), and (6).

(9) $(a+b) \cdot (a-b) = a^{\mathbf{2}} - b^{\mathbf{2}}$.

(10) Let us consider an integral domain R, and elements a, b of R. Then $a^{\mathbf{2}} = b^{\mathbf{2}}$ if and only if $a = b$ or $a = -b$. The theorem is a consequence of (9).

Let us consider a field F and a non zero element a of F. Now we state the propositions:

(11) $(-a)^{-1} = -a^{-1}$.

(12) $(-a^{-1})^{-1} = -a$.

(13) $-(-a)^{-1} = a^{-1}$. The theorem is a consequence of (11).

(14) Let us consider a field F, an element a of F, and a non zero element b of F. Then $(\frac{a}{b})^{\mathbf{2}} = \frac{a^{\mathbf{2}}}{b^{\mathbf{2}}}$.

(15) Let us consider a field F. Suppose $\mathrm{char}(F) \neq 2$. Let us consider an element a of F. Then $(\frac{a+1_F}{2 \star 1_F})^{\mathbf{2}} - (\frac{a-1_F}{2 \star 1_F})^{\mathbf{2}} = a$. The theorem is a consequence of (14), (7), (8), and (43).

Let us note that every non degenerated ring which is preordered has also characteristic 0. Let us consider a preordered ring R and a preordering P of R. Now we state the propositions:

(16) $(-P) \cdot P = P \cdot (-P)$.

(17) (i) $-P + -P \subseteq -P$, and

(ii) $(-P) \cdot (-P) \subseteq P$.

(18) (i) $(-P) \cdot P \subseteq -P$, and

(ii) $P \cdot (-P) \subseteq -P$.

The theorem is a consequence of (17) and (16).

(19) Let us consider a preordered ring R, a preordering P of R, and a natural number n. Then $n \star 1_R \in P$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv \$_1 \star 1_R \in P$. For every natural number k, $\mathcal{P}[k]$. $\square$

One can verify that every preordering of $\mathbb{Z}^{\mathrm{R}}$ is spanning and every preordering of $\mathbb{F}_{\mathbb{Q}}$ is spanning and every preordering of $\mathbb{R}_{\mathrm{F}}$ is spanning.

(20) Let us consider a preordering P of $\mathbb{Z}^{\mathrm{R}}$. Then $P = \mathrm{Positives}(\mathbb{Z}^{\mathrm{R}})$.

(21) Let us consider a preordering P of $\mathbb{F}_{\mathbb{Q}}$. Then $P = \mathrm{Positives}(\mathbb{F}_{\mathbb{Q}})$.

(22) Let us consider a preordering P of $\mathbb{R}_{\mathrm{F}}$. Then $P = \mathrm{Positives}(\mathbb{R}_{\mathrm{F}})$.

2. More on Ring Characteristic

Now we state the propositions:

(23) Let us consider a ring R. Then $\mathrm{char}(R) = 1$ if and only if R is degenerated.

(24) Let us consider a non degenerated ring R. Then $\mathrm{char}(R) = 2$ if and only if $2 \star 1_R = 0_R$.

(25) Let us consider an integral domain R. Then $\mathrm{char}(R) = 0$ if and only if for every non zero element a of R and for every non zero natural number n, $n \star a \neq 0_R$. The theorem is a consequence of (43).

(26) Let us consider an integral domain R with characteristic 0, and an element a of R. Then $-a = a$ if and only if $a = 0_R$. The theorem is a consequence of (25).

3. Maximal Preorderings

Let R be a preordered ring and P be a preordering of R. We say that P is maximal if and only if

(Def. 1) for every preordering Q of R such that $P \subseteq Q$ holds $P = Q$.

Now we state the propositions:

(27) Let us consider a preordered field F, a preordering P of F, and an element a of F. If $-a \notin P$, then $P + (a \cdot P)$ is a preordering of F.

PROOF: Set $S = P + (a \cdot P)$. $S + S \subseteq S$. $S \cdot S \subseteq S$ by [8, (8), (10)], [10, (3)], [9, (23)]. $P \subseteq S$. $\square$

(28) Let us consider a preordered field F, and a preordering P of F. Then P is maximal if and only if P is a positive cone. The theorem is a consequence of (36), (3), and (4).

Let F be a preordered field. Note that every preordering of F which is spanning is also maximal and every preordering of F which is maximal is also spanning. Now we state the proposition:

(29) Let us consider a preordered field F, and a preordering P of F. Then there exists a preordering Q of F such that

(i) $P \subseteq Q$, and

(ii) Q is maximal.

Let us note that every preordered field is ordered. Let us consider a preordered field F and a preordering P of F. Now we state the propositions:

(30) P is maximal if and only if P is an ordering of F.

(31) There exists an ordering O of F such that $P \subseteq O$. The theorem is a consequence of (29).

Let R be an ordered ring and P be a preordering of R. The functor $\bigcap_R P$ yielding a subset of R is defined by the term

(Def. 2) $\{x$, where x is an element of R : for every ordering O of R such that $P \subseteq O$ holds $x \in O\}$.

One can verify that $\bigcap_R P$ is non empty and $\bigcap_R P$ is closed under addition and closed under multiplication and has all squares.

Let F be an ordered field and P be a preordering of F. One can verify that $\bigcap_F P$ is negative-disjoint. Let us consider an ordered field F and a preordering P of F. Now we state the propositions:

(32) $\bigcap_F P$ is a preordering of F.

(33) $\bigcap_F P = P$.

4. Formally Real Fields

Let R be a ring. We say that R is formally real if and only if

(Def. 3) $-1_R \notin \mathrm{QS}(R)$.

Let us consider a field F. Now we state the propositions:

(34) If $\mathrm{char}(F) \neq 2$, then F is formally real iff $\mathrm{QS}(F)$ is a prepositive cone.

(35) If $\mathrm{char}(F) \neq 2$, then F is formally real iff there exists a subset P of F such that P is a prepositive cone.

(36) If $\mathrm{char}(F) \neq 2$, then F is formally real iff there exists a subset P of F such that P is a positive cone.

(37) If $\mathrm{char}(F) \neq 2$, then F is formally real iff $\mathrm{QS}(F) \neq$ the carrier of F.

Observe that every field which is formally real is also ordered and every field which is ordered is also formally real and every non degenerated ring which is preordered is also formally real and there exists a field which is formally real.

Let F be a formally real field. Note that $\mathrm{QS}(F)$ is negative-disjoint.

Now we state the propositions:

(38) Let us consider a formally real field F. Then $\mathrm{QS}(F)$ is a preordering of F.

(39) Let us consider a formally real field F, and an element a of F. Then for every ordering O of F, $a \in O$ if and only if $a \in \mathrm{QS}(F)$.

(40) Let us consider an element r of $\mathbb{F}_{\mathbb{Q}}$. If $0 \leqslant r$, then r is a sum of squares.

Let R be a zero structure and f be a (the carrier of R)-valued function. We say that f is trivial if and only if

(Def. 4) for every object i such that $i \in \mathrm{dom}\, f$ holds $f(i) = 0_R$.

Let R be a ring and f be a non empty finite sequence of elements of R. We say that f is quadratic if and only if

(Def. 5) for every element i of $\mathrm{dom}\, f$, $f(i)$ is a square.

Let R be a non degenerated ring. Observe that $\langle 1_R \rangle$ is quadratic and non trivial as a non empty finite sequence of elements of R and there exists a non empty finite sequence of elements of R which is quadratic and non trivial.

Now we state the proposition:

(41) Let us consider a field F. Then F is formally real if and only if for every quadratic, non empty finite sequence f of elements of F such that $\sum f = 0_F$ holds f is trivial.

Note that every formally real field is non algebraic closed.

5. Order Relations and Strict Order Relations Revisited

Now we state the propositions:

(42) Let us consider a preordered ring R, a preordering P of R, and elements a, b of R. Then $a \leqslant_P b$ if and only if $-b \leqslant_P -a$.

(43) Let us consider a preordered ring R, a preordering P of R, and an element a of R. Then $a \leqslant_P a$.

(44) Let us consider a preordered ring R, a preordering P of R, and elements a, b of R. If $a \leqslant_P b$ and $b \leqslant_P a$, then $a = b$.

Let us consider a preordered ring R, a preordering P of R, and elements a, b, c of R. Now we state the propositions:

(45) If $a \leqslant_P b$ and $b \leqslant_P c$, then $a \leqslant_P c$.

(46) If $a \leqslant_P b$, then $a + c \leqslant_P b + c$.

(47) If $a \leqslant_P b$ and $0_R \leqslant_P c$, then $a \cdot c \leqslant_P b \cdot c$.

(48) If $a \leqslant_P b$ and $c \leqslant_P 0_R$, then $b \cdot c \leqslant_P a \cdot c$. The theorem is a consequence of (47) and (42).

(49) Let us consider an ordered ring R, an ordering O of R, and elements a, b of R. Then

(i) $a \leqslant_O b$, or

(ii) $b \leqslant_O a$.

Let us consider a preordered field F, a preordering P of F, and non zero elements a, b of F. Now we state the propositions:

(50) If $0_F \leqslant_P a$ and $0_F \leqslant_P b$, then $a \leqslant_P b$ iff $b^{-1} \leqslant_P a^{-1}$. The theorem is a consequence of (47).

(51) If $a \leqslant_P 0_F$ and $b \leqslant_P 0_F$, then $a \leqslant_P b$ iff $b^{-1} \leqslant_P a^{-1}$. The theorem is a consequence of (13) and (48).

Let R be a preordered ring, P be a preordering of R, and a, b be elements of R. We say that $a <_P b$ if and only if

(Def. 6) $a \leqslant_P b$ and $a \neq b$.

Now we state the propositions:

(52) Let us consider a preordered, non degenerated ring R, and a preordering P of R. Then

(i) $0_R <_P 1_R$, and

(ii) $-1_R <_P 0_R$.

(53) Let us consider a preordered ring R, a preordering P of R, and elements a, b of R. Then $a <_P b$ if and only if $-b <_P -a$.

(54) Let us consider an ordered ring R, an ordering O of R, and elements a, b of R. Then

(i) $a <_O b$, or

(ii) $b <_O a$, or

(iii) $a = b$.

Let us consider a preordered ring R, a preordering P of R, and elements a, b, c of R. Now we state the propositions:

(55) If $a <_P b$ and $b \leqslant_P c$, then $a <_P c$.

(56) If $a \leqslant_P b$ and $b <_P c$, then $a <_P c$.

(57) If $a <_P b$, then $a + c <_P b + c$.

Let us consider a preordered integral domain R, a preordering P of R, and elements a, b, c of R. Now we state the propositions:

(58) If $a <_P b$ and $0_R <_P c$, then $a \cdot c <_P b \cdot c$.

(59) If $a <_P b$ and $c <_P 0_R$, then $b \cdot c <_P a \cdot c$. The theorem is a consequence of (42) and (47).

Let us consider a preordered field F, a preordering P of F, and non zero elements a, b of F. Now we state the propositions:

(60) If $0_F \leqslant_P a$ and $0_F \leqslant_P b$, then $a <_P b$ iff $b^{-1} <_P a^{-1}$. The theorem is a consequence of (50).

(61) If $a \leqslant_P 0_F$ and $b \leqslant_P 0_F$, then $a <_P b$ iff $b^{-1} <_P a^{-1}$. The theorem is a consequence of (51).

Let R be a preordered ring, P be a preordering of R, and a be an element of R. We say that a is P-ordered if and only if

(Def. 7) $a \in P \cup -P$.

We say that a is P-positive if and only if

(Def. 8) $a \in P \setminus \{0_R\}$.

We say that a is P-negative if and only if

(Def. 9) $a \in -P \setminus \{0_R\}$.

Note that there exists an element of R which is P-ordered and every element of R which is P-positive is also P-ordered and every element of R which is P-negative is also P-ordered.

Let R be a preordered, non degenerated ring. One can check that there exists an element of R which is P-positive and there exists an element of R which is P-negative and there exists an element of R which is non P-positive and there exists an element of R which is non P-negative and every element of R which is P-positive is also non zero and non P-negative and every element of R which is P-negative is also non zero and non P-positive.

Let a be a P-ordered element of R. One can verify that $-a$ is P-ordered.

Let F be a field and a be a non zero element of F. Let us note that a^{-1} is non zero.

Let F be a preordered field, P be a preordering of F, and a be a non zero, P-ordered element of F. Let us observe that a^{-1} is P-ordered.

Let R be an ordered, non degenerated ring and O be an ordering of R. Note that every element of R which is non zero and non O-positive is also O-negative and every element of R which is non zero and non O-negative is also O-positive.

Let us consider a preordered ring R, a preordering P of R, and an element a of R. Now we state the propositions:

(62) a is P-positive if and only if $0_R <_P a$.

(63) a is P-negative if and only if $a <_P 0_R$.

Let us consider a preordered ring R, a preordering P of R, and a P-ordered element a of R. Now we state the propositions:

(64) a is not P-negative if and only if $0_R \leqslant_P a$. The theorem is a consequence of (43).

(65) a is not P-positive if and only if $a \leqslant_P 0_R$. The theorem is a consequence of (43).

6. Absolute Values

Let R be a preordered ring, P be a preordering of R, and a be an element of R. The functor $|a|_P$ yielding an element of R is defined by the term

(Def. 10) $\begin{cases} a, & \textbf{if } a \in P, \\ -a, & \textbf{if } a \in -P, \\ -1_R, & \textbf{otherwise}. \end{cases}$

Let R be an ordered ring and O be an ordering of R. One can verify that the functor $|a|_O$ yields an element of R and is defined by the term

(Def. 11) $\begin{cases} a, & \textbf{if } a \in O, \\ -a, & \textbf{otherwise}. \end{cases}$

Let us consider a preordered, non degenerated ring R, a preordering P of R, and an element a of R. Now we state the propositions:

(66) $0_R \leqslant_P |a|_P$ if and only if a is P-ordered. The theorem is a consequence of (55) and (52).

(67) a is not P-ordered if and only if $|a|_P = -1_R$. The theorem is a consequence of (66).

(68) $|a|_P = 0_R$ if and only if $a = 0_R$. The theorem is a consequence of (67).

Let us consider a preordered integral domain R, a preordering P of R, and an element a of R. Now we state the propositions:

(69) $|a|_P = a$ if and only if $0_R \leqslant_P a$. The theorem is a consequence of (26) and (43).

(70) $|a|_P = -a$ if and only if $a \leqslant_P 0_R$.

(71) Let us consider a preordered ring R, a preordering P of R, and an element a of R. Then $|a|_P = |-a|_P$.

(72) Let us consider a preordered, non degenerated ring R, a preordering P of R, and an element a of R. Then $-|a|_P \leqslant_P a$ and $a \leqslant_P |a|_P$ if and only if a is P-ordered. The theorem is a consequence of (45), (52), (56), (44), and (66).

(73) Let us consider a preordered field F, a preordering P of F, and a non zero, P-ordered element a of F. Then $|a^{-1}|_P = (|a|_P)^{-1}$.
PROOF: $|a^{-1}|_P \cdot |a|_P = \mathbf{1}_F$. □

(74) Let us consider a preordered ring R, a preordering P of R, and elements a, b of R. Then $|(a-b)|_P = |(b-a)|_P$.

(75) Let us consider a preordered, non degenerated ring R, a preordering P of R, and an element a of R. Then $-|a|_P \leqslant_P a$ and $a \leqslant_P |a|_P$ if and only if a is P-ordered. The theorem is a consequence of (67), (52), (44), (45), and (43).

(76) Let us consider a preordered, non degenerated ring R, a preordering P of R, and P-ordered elements a, b of R. Then $|(a \cdot b)|_P = (|a|_P) \cdot (|b|_P)$. The theorem is a consequence of (18) and (17).

(77) Let us consider a preordered field F, a preordering P of F, a non zero, P-ordered element a of F, and a P-ordered element b of F. Then $|b \cdot (a^{-1})|_P = |b|_P \cdot (|a|_P)^{-1}$. The theorem is a consequence of (76) and (73).

(78) Let us consider a preordered integral domain R, a preordering P of R, a P-ordered element a of R, and a P-ordered, non P-negative element p of R. Then $|a|_P \leqslant_P p$ if and only if $-p \leqslant_P a$ and $a \leqslant_P p$. The theorem is a consequence of (75), (45), (42), (69), and (70).

(79) Let us consider a preordered integral domain R, a preordering P of R, and P-ordered elements a, b of R. Then $|(a+b)|_P \leqslant_P |a|_P + |b|_P$. The theorem is a consequence of (66), (46), (45), (52), (53), (44), (75), and (78).

7. SQUARES AND SQUARE ROOTS

Let R be a ring and a be square element of R.

A square root of a is an element of R defined by

(Def. 12) $it^{\mathbf{2}} = a$.

Let R be a non degenerated ring. Observe that there exists an element of R which is non zero and square.

Let us consider an ordered integral domain R, an ordering O of R, and non O-negative elements a, b of R. Now we state the propositions:

(80) $a \leqslant_O b$ if and only if $a^{\mathbf{2}} \leqslant_O b^{\mathbf{2}}$. The theorem is a consequence of (64), (47), (45), (18), and (9).

(81) $a <_O b$ if and only if $a^{\mathbf{2}} <_O b^{\mathbf{2}}$. The theorem is a consequence of (64) and (80).

(82) Let us consider a preordered integral domain R, a preordering P of R, and a P-ordered element a of R. Then $(|a|_P)^{\mathbf{2}} = a^{\mathbf{2}}$. The theorem is a consequence of (69) and (70).

(83) Let us consider a preordered ring R, a preordering P of R, and an element a of R. If $a \in -P \setminus \{0_R\}$, then a is not square.

(84) Let us consider a preordered ring R, and a preordering P of R. Then $(-P) \cap \mathrm{SQ}(R) = \{0_R\}$. The theorem is a consequence of (83).

(85) Let us consider a preordered integral domain R, a preordering P of R, square element a of R, and square roots b_1, b_2 of a. If $0_R \leqslant_P b_1$ and $0_R \leqslant_P b_2$, then $b_1 = b_2$.

Let R be a preordered ring and P be a preordering of R. Let us observe that every element of R which is P-negative is also non square and every element of R which is non P-positive and square is also zero.

Let R be an ordered integral domain, O be an ordering of R, and a be square element of R. One can check that there exists a square root of a which is non O-negative.

Let a be a non zero, a square element of R. Let us observe that there exists a square root of a which is O-positive and there exists a square root of a which is O-negative.

Let a be square element of R. The functor $\sqrt{a}_O$ yielding a non O-negative square root of a is defined by

(Def. 13) $it^{\mathbf{2}} = a$.

Now we state the proposition:

(86) Let us consider an ordered integral domain R, an ordering O of R, square element a of R, and an element b of R. Then b is a square root of a if and only if $b = \sqrt{a}_O$ or $b = -\sqrt{a}_O$. The theorem is a consequence of (10).

Let R be an ordered integral domain, O be an ordering of R, and a be a non zero, a square element of R. One can check that $\sqrt{a}_O$ is non zero.

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

[3] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. On algebraic hierarchies in mathematical repository of Mizar. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Infor-*

mation Systems (FedCSIS), volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371, 2016. doi:10.15439/2016F520.

[4] Nathan Jacobson. *Lecture Notes in Abstract Algebra, III. Theory of Fields and Galois Theory*. Springer-Verlag, 1964.

[5] Manfred Knebusch and Claus Scheiderer. *Einführung in die reelle Algebra*. Vieweg-Verlag, 1989.

[6] Alexander Prestel. *Lectures on Formally Real Fields*. Springer-Verlag, 1984.

[7] Knut Radbruch. *Geordnete Körper*. Lecture Notes, University of Kaiserslautern, Germany, 1991.

[8] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

[9] Christoph Schwarzweller. Ordered rings and fields. *Formalized Mathematics*, 25(**1**):63–72, 2017. doi:10.1515/forma-2017-0006.

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

[11] Christoph Schwarzweller and Artur Korniłowicz. Characteristic of rings. Prime fields. *Formalized Mathematics*, 23(**4**):333–349, 2015. doi:10.1515/forma-2015-0027.

Received November 29, 2017

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

FORMALIZED MATHEMATICS
Vol. 25, No. 4, Pages 261–268, 2017
DOI: 10.1515/forma-2017-0025

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

Introduction to Stopping Time in Stochastic Finance Theory. Part II

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

Summary. We start proceeding with the stopping time theory in discrete time with the help of the Mizar system [1], [4]. We prove, that the expression for two stopping times k_1 and k_2 not always implies a stopping time $(k_1 + k_2)$ (see Theorem 6 in this paper). If you want to get a stopping time, you have to cut the function e.g. $(k_1 + k_2) \cap T$ (see [2, p. 283 Remark 6.14]).

Next we introduce the stopping time in continuous time. We are focused on the intervals $[0, r]$ where $r \in \mathbb{R}$. We prove, that for $I = [0, r]$ or $I = [0, +\infty[$ the set $\{A \cap I : A \in \text{Borel-Sets}\}$ is a σ-algebra of I (see Definition 6 in this paper, and more general given in [3, p.12 1.8e]). The interval I can be considered as a timeline from now to some point in the future.

This set is necessary to define our next lemma. We prove the existence of the σ-algebra of the τ-past, where τ is a stopping time (see Definition 11 in this paper and [6, p.187, Definition 9.19]). If τ_1 and τ_2 are stopping times with τ_1 is smaller or equal than τ_2 we can prove, that the σ-algebra of the τ_1-past is a subset of the σ-algebra of the τ_2-past (see Theorem 9 in this paper and [6, p.187 Lemma 9.21]).

Suppose, that you want to use Lemma 9.21 with some events, that never occur, see as a comparison the paper [5] and the example for ST(1)=$\{+\infty\}$ in the Summary. We don't have the element $+\infty$ in our above-mentioned time intervals $[0, r[$ and $[0,+\infty[$. This is only possible if we construct a new σ-algebra on $\mathbb{R} \cup \{-\infty, +\infty\}$. This construction is similar to the Borel-Sets and we call this σ-algebra extended Borel sets (see Definition 13 in this paper and [3, p. 21]). It can be proved, that $\{+\infty\}$ is an Element of extended Borel sets (see Theorem 21 in this paper). Now we use the interval $[0, +\infty]$ as a basis. We construct a σ-algebra on $[0, +\infty]$ similar to the book ([3, p. 12 18e]), see Definition 18 in this paper, and call it extended Borel subsets. We prove for stopping times with this given σ-algebra, that for τ_1 and τ_2 are stopping times with τ_1 is smaller or equal than τ_2 we have the σ-algebra of the τ_1-past is a subset of the σ-algebra of the τ_2-past, see Theorem 25 in this paper. It is obvious, that $\{+\infty\} \in$ extended Borel subsets.

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

In general, Lemma 9.21 is important for the proof of the Optional Sampling Theorem, see 10.11 Proof of (i) in [6, p. 203].

MSC: 60G40 03B35

Keywords: stopping time; stochastic process

MML identifier: FINANCE5, version: 8.1.06 5.45.1311

1. Preliminaries

From now on Ω denotes a non empty set, Σ denotes a σ-field of subsets of Ω, S denotes a non empty subset of $\mathbb{R}$, r denotes a real number, and T denotes a natural number.

Let A be a non empty set, I be an extended real-membered set, and k_1, k_2 be functions from A into I. We say that $k_1 \leqslant k_2$ if and only if

(Def. 1) for every element w of A, $k_1(w) \leqslant k_2(w)$.

Let f_1, f_2 be extended real-valued functions. The functor $f_1 + f_2$ yielding a function is defined by

(Def. 2) $\operatorname{dom} it = \operatorname{dom} f_1 \cap \operatorname{dom} f_2$ and for every object x such that $x \in \operatorname{dom} it$ holds $it(x) = f_1(x) + f_2(x)$.

One can check that the functor is commutative.

Let us note that $f_1 + f_2$ is extended real-valued.

Let C be a set, D_1, D_2 be extended real-membered, non empty sets, f_1 be a function from C into D_1, and f_2 be a function from C into D_2. One can verify that $f_1 + f_2$ is total as a partial function from C to $\overline{\mathbb{R}}$.

Let D_1, D_2 be extended real-membered sets, f_1 be a partial function from C to D_1, and f_2 be a partial function from C to D_2. Let us note that the functor $f_1 + f_2$ yields a partial function from C to $\overline{\mathbb{R}}$. Now we state the propositions:

(1) Let us consider non empty sets A, I, y, and a function F from A into I. Then $\{z$, where z is an element of $A : F(z) \in y\} = F^{-1}(y)$.

(2) Let us consider a real number r. If $r > 0$, then there exists a natural number n such that $\frac{1}{n} < r$ and $n > 0$.

(3) Let us consider real numbers a, b. Then $[-\infty, a] \cap [b, +\infty] = [b, a]$.

(4) Let us consider a real number r. Suppose $r \geqslant 0$. Then $[0, +\infty] \setminus [0, r[= [r, +\infty]$.

Let r be an extended real. Observe that $[r, +\infty]$ is non empty.

(5) Let us consider an extended real k. Then $\overline{\mathbb{R}} \setminus [-\infty, k] =]k, +\infty]$.

Let a be a real number. One can check that $]a, +\infty]$ is non empty.

2. STOPPING TIME IN DISCRETE TIME

Let us consider Ω, Σ, and T. Let F_1 be a filtration of $\bigcup_{t\in\mathbb{N}:0\leqslant t\leqslant T}\{t\}$ and Σ and k be a function from Ω into $T_{\{+\infty\}}$. We say that k is like stopping time of F_1 if and only if

(Def. 3) k is StoppingTime(F_1,T).

Let M_1 be a filtration of $\bigcup_{t\in\mathbb{N}:0\leqslant t\leqslant T}\{t\}$ and Σ. Note that there exists a function from Ω into $T_{\{+\infty\}}$ which is like stopping time of M_1.

A stopping time of M_1 is a like stopping time of M_1 function from Ω into $T_{\{+\infty\}}$. Now we state the proposition:

(6) Let us consider a non zero natural number T, and a filtration M_1 of $\bigcup_{t\in\mathbb{N}:0\leqslant t\leqslant T}\{t\}$ and Σ. Then there exist stopping times k_1, k_2 of M_1 such that $k_1 + k_2$ is not a stopping time of M_1.

PROOF: Reconsider $M_2 = T$ as an element of $T_{\{+\infty\}}$. Consider k_1 being a function from Ω into $T_{\{+\infty\}}$ such that $k_1 = \Omega \longmapsto M_2$ and k_1 is StoppingTime(M_1,T). Consider k_2 being a function from Ω into $T_{\{+\infty\}}$ such that $k_2 = \Omega \longmapsto M_2$ and k_2 is StoppingTime(M_1,T). There exists an element w of $\mathrm{dom}(k_1 + k_2)$ such that $w \in \mathrm{dom}(k_1 + k_2)$ and $(k_1 + k_2)(w) \notin T_{\{+\infty\}}$. □

3. STOPPING TIME IN CONTINUOUS TIME

Let r be a real number.

A stopping event of r is a subset of $\mathbb{R}$ defined by

(Def. 4) (i) $it = [0, +\infty[$, **if** $r \leqslant 0$,

(ii) $it = [0, r]$, **otherwise**.

Let us note that every stopping event of r is non empty.

In the sequel I denotes a stopping event of r.

Now we state the proposition:

(7) I is an event of the Borel sets.

4. BOREL-SETS

Let us consider r and I. Let A be an element of the Borel sets. The intersection of A and I yielding an element of the Borel sets is defined by

(Def. 5) $A \cap I$.

The first Borel subsets with I yielding a σ-field of subsets of I is defined by

(Def. 6) the set of all the intersection of A and I where A is an element of the Borel sets.

Let us consider Ω and Σ. Let M_1 be a function and k be a random variable of Σ and the first Borel subsets with I. We say that k is stopping time of M_1 if and only if

(Def. 7) for every element t of I, $\{w$, where w is an element of $\Omega : k(w) \leqslant t\} \in M_1(t)$.

(8) Let us consider a filtration M_1 of I and Σ, and an element t_1 of I. Then there exists a random variable q of Σ and the first Borel subsets with I such that

(i) $q = \Omega \longmapsto t_1$, and

(ii) q is stopping time of M_1.

Proof: For every element t of I, $\{w$, where w is an element of $\Omega : (\Omega \longmapsto t_1)(w) \leqslant t\} \in M_1(t)$. Set $O = \Omega \longmapsto t_1$. For every set x, $O^{-1}(x) \in \Sigma$. $\square$

Let us consider Ω, Σ, r, and I. Let F_1 be a filtration of I and Σ and k be a random variable of Σ and the first Borel subsets with I. We say that k is like stopping time of F_1 if and only if

(Def. 8) k is stopping time of F_1.

Let M_1 be a filtration of I and Σ. One can check that there exists a random variable of Σ and the first Borel subsets with I which is like stopping time of M_1.

A stopping time of M_1 is a like stopping time of M_1 random variable of Σ and the first Borel subsets with I.

5. σ-Algebra of the τ-Past

Let us consider Ω, Σ, r, and I. Let M_1 be a filtration of I and Σ, τ be a stopping time of M_1, and A_1 be a sequence of subsets of Ω. Assume rng $A_1 \subseteq \{A$, where A is an element of $\Sigma :$ for every element t_1 of $I, A \cap \{w$, where w is an element of $\Omega : \tau(w) \leqslant t_1\} \in M_1(t_1)\}$. Let t be an element of I and n be a natural number. The first set for σ-tau of τ, A_1, n and t yielding an element of the t-$\mathcal{EF}$ of M_1 is defined by the term

(Def. 9) (Complement $A_1)(n) \cap \{w$, where w is an element of $\Omega : \tau(w) \leqslant t\}$.

Let A be a sequence of subsets of Ω. The second set for σ-tau of τ, A and t yielding a sequence of subsets of the t-$\mathcal{EF}$ of M_1 is defined by

(Def. 10) for every natural number n, $it(n) =$ the first set for σ-tau of τ, A, n and t.

The functor Σ-tau(τ) yielding a σ-field of subsets of Ω is defined by the term

(Def. 11) $\{A$, where A is an element of Σ : for every element t of I, $A \cap \{w$, where w is an element of $\Omega : \tau(w) \leqslant t\} \in M_1(t)\}$.

Now we state the proposition:

(9) Let us consider a filtration M_1 of I and Σ, and stopping times k_1, k_2 of M_1. Suppose $k_1 \leqslant k_2$. Then Σ-tau(k_1) $\subseteq$ Σ-tau(k_2).

PROOF: Consider A being an element of Σ such that $x = A$ and for every element t of I, $A \cap \{w_1$, where w_1 is an element of $\Omega : k_1(w_1) \leqslant t\} \in M_1(t)$. $x \in \{A$, where A is an element of $\Sigma :$ for every element t of $I, A \cap \{w_1$, where w_1 is an element of $\Omega : k_2(w_1) \leqslant t\} \in M_1(t)\}$. $\square$

The extended family of halflines yielding a family of subsets of $\overline{\mathbb{R}}$ is defined by the term

(Def. 12) the set of all $[-\infty, r]$ where r is a real number.

The extended Borel sets yielding a σ-field of subsets of $\overline{\mathbb{R}}$ is defined by the term

(Def. 13) σ(the extended family of halflines).

Now we state the proposition:

(10) Let us consider a real number k. Then

(i) $]k, +\infty]$ is an element of the extended Borel sets, and

(ii) $[-\infty, k]$ is an element of the extended Borel sets.

The theorem is a consequence of (5).

Let b be a real number. The extended half open sets of b yielding a sequence of subsets of $\overline{\mathbb{R}}$ is defined by

(Def. 14) $it(0) =]b - 1, +\infty]$ and for every natural number n, $it(n+1) =]b - \frac{1}{n+1}, +\infty]$.

Let us consider a real number b. Now we state the propositions:

(11) Intersection(the extended half open sets of b) is an element of the extended Borel sets.

PROOF: For every natural number n, (Complement(the extended half open sets of b))(n) is an element of the extended Borel sets. $\square$

(12) Intersection(the extended half open sets of b) $= [b, +\infty]$.

PROOF: For every object c, $c \in$ Intersection(the extended half open sets of b) iff $c \in [b, +\infty]$. $\square$

(13) Let us consider real numbers a, b. Then $[b, a]$ is an element of the extended Borel sets.

PROOF: $[-\infty, a]$ is an element of the extended Borel sets. $[-\infty, a] \cap [b, +\infty]$ is an element of the extended Borel sets by (12), (11), [7, (19)]. $\square$

(14) Let us consider a real number a. Then $\{a\}$ is an element of the extended Borel sets. The theorem is a consequence of (13).

(15) Let us consider a real number r. Then $[r, +\infty]$ is an event of the extended Borel sets. The theorem is a consequence of (11) and (12).

Let b be a real number. The extended right closed sets of b yielding a sequence of subsets of $\overline{\mathbb{R}}$ is defined by

(Def. 15) for every natural number n, $it(n) = [-\infty, b - n]$.

Now we state the propositions:

(16) Let us consider a real number b. Then Intersection(the extended right closed sets of b) is an element of the extended Borel sets. The theorem is a consequence of (10).

(17) Intersection(the extended right closed sets of 0) $= \{-\infty\}$.
PROOF: For every object c, $c \in$ Intersection(the extended right closed sets of 0) iff $c \in \{-\infty\}$. □

(18) $\{-\infty\}$ is an element of the extended Borel sets.

Let b be a real number. The extended left closed sets of b yielding a sequence of subsets of $\overline{\mathbb{R}}$ is defined by

(Def. 16) for every natural number n, $it(n) = [b + n, +\infty]$.

Now we state the propositions:

(19) Let us consider a real number b. Then Intersection(the extended left closed sets of b) is an element of the extended Borel sets. The theorem is a consequence of (15).

(20) Intersection(the extended left closed sets of 0) $= \{+\infty\}$.
PROOF: For every object c, $c \in$ Intersection(the extended left closed sets of 0) iff $c \in \{+\infty\}$. □

(21) $\{+\infty\}$ is an element of the extended Borel sets.

(22) $\mathbb{R}$ is an element of the extended Borel sets. The theorem is a consequence of (19), (20), (16), (17), and (2).

(23) Halflines $\subseteq$ the extended Borel sets. The theorem is a consequence of (10), (14), (16), and (17).

Let A be an element of the extended Borel sets. The positive subset of A yielding an element of the extended Borel sets is defined by the term

(Def. 17) $A \cap [0, +\infty]$.

The extended Borel subsets yielding a σ-field of subsets of $[0, +\infty]$ is defined by the term

(Def. 18) the set of all the positive subset of A where A is an element of the extended Borel sets.

Now we state the proposition:

(24) $\{+\infty\}$ is an element of the extended Borel subsets. The theorem is a consequence of (21).

Let us consider Ω and Σ. Let M_1 be a function, S be a non empty, extended real-membered set, and k be a random variable of Σ and the extended Borel subsets. We say that k is StoppingTime(M_1,S) if and only if

(Def. 19) for every element t of S, $\{w$, where w is an element of $\Omega : k(w) \leqslant t\} \in M_1(t)$.

Now we state the proposition:

(25) Let us consider a filtration M_1 of S and Σ, and an element t_1 of $[0, +\infty]$. Then there exists a random variable q of Σ and the extended Borel subsets such that

(i) $q = \Omega \longmapsto t_1$, and

(ii) q is StoppingTime(M_1,S).

PROOF: For every element t of S, $\{w$, where w is an element of $\Omega : (\Omega \longmapsto t_1)(w) \leqslant t\} \in M_1(t)$. Set $O = \Omega \longmapsto t_1$. For every set x, $O^{-1}(x) \in \Sigma$. □

Let us consider Ω, Σ, and S. Let F_1 be a filtration of S and Σ and k be a random variable of Σ and the extended Borel subsets. We say that k is like stopping time of F_1 if and only if

(Def. 20) k is StoppingTime(F_1,S).

Let M_1 be a filtration of S and Σ. Observe that there exists a random variable of Σ and the extended Borel subsets which is like stopping time of M_1.

A stopping time of Σ and M_1 is a like stopping time of M_1 random variable of Σ and the extended Borel subsets. Let τ be a stopping time of Σ and M_1 and A_1 be a sequence of subsets of Ω. Assume rng $A_1 \subseteq \{A$, where A is an element of $\Sigma :$ for every element t_1 of $S, A \cap \{w$, where w is an element of $\Omega : \tau(w) \leqslant t_1\} \in M_1(t_1)\}$. Let t be an element of S and n be a natural number. The first set for σ-tau of M_1, τ, A_1, n and t yielding an element of the t-$\mathcal{EF}$ of M_1 is defined by the term

(Def. 21) (Complement A_1)$(n) \cap \{w$, where w is an element of $\Omega : \tau(w) \leqslant t\}$.

The second set for σ-tau of M_1, τ, A_1 and t yielding a sequence of subsets of the t-$\mathcal{EF}$ of M_1 is defined by

(Def. 22) for every natural number n, $it(n) =$ the first set for σ-tau of M_1, τ, A_1, n and t.

The functor Σ-tau(M_1, τ) yielding a σ-field of subsets of Ω is defined by the term

(Def. 23) $\{A$, where A is an element of $\Sigma :$ for every element t of S, $A \cap \{w$, where w is an element of $\Omega : \tau(w) \leqslant t\} \in M_1(t)\}$.

Now we state the proposition:

(26) Let us consider a filtration M_1 of S and Σ, and stopping times k_1, k_2 of Σ and M_1. Suppose $k_1 \leqslant k_2$. Then $\Sigma\text{-tau}(M_1, k_1) \subseteq \Sigma\text{-tau}(M_1, k_2)$.
PROOF: Consider A being an element of Σ such that $x = A$ and for every element t of S, $A \cap \{w_1$, where w_1 is an element of $\Omega : k_1(w_1) \leqslant t\} \in M_1(t)$. For every element t of S, $x \cap \{w_1$, where w_1 is an element of $\Omega : k_2(w_1) \leqslant t\} \in M_1(t)$. □

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

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

[4] 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.

[5] Peter Jaeger. Introduction to stopping time in stochastic finance theory. *Formalized Mathematics*, 25(**2**):101–105, 2017. doi:10.1515/forma-2017-0010.

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

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

Received November 29, 2017

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

FORMALIZED MATHEMATICS
Vol. 25, No. 4, Pages 269–281, 2017
DOI: 10.1515/forma-2017-0026

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

Implicit Function Theorem. Part I[1]

Kazuhisa Nakasho
Osaka University
Osaka, Japan

Yuichi Futa
Tokyo University of Technology
Tokyo, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize in Mizar [1], [3] the existence and uniqueness part of the implicit function theorem. In the first section, some composition properties of Lipschitz continuous linear function are discussed. In the second section, a definition of closed ball and theorems of several properties of open and closed sets in Banach space are described. In the last section, we formalized the existence and uniqueness of continuous implicit function in Banach space using Banach fixed point theorem. We referred to [7], [8], and [2] in this formalization.

MSC: 26B10 53A07 03B35

Keywords: implicit function theorem; Banach fixed point theorem; Lipschitz continuity

MML identifier: NDIFF_8, version: 8.1.06 5.45.1311

1. Properties of Lipschitz Continuous Linear Function

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

Now we state the propositions:

(1) Let us consider real normed spaces X, Y, a point x of X, a point y of Y, and a point z of $X \times Y$. Suppose $z = \langle x, y \rangle$. Then $\|z\| = \sqrt{\|x\|^2 + \|y\|^2}$.

[1]This study was supported in part by JSPS KAKENHI Grant Number JP17K00182.

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

(2) Let us consider real normed spaces X, Y, a point x of X, and a point z of $X \times Y$. Suppose $z = \langle x, 0_Y \rangle$. Then $\|z\| = \|x\|$. The theorem is a consequence of (1).

(3) Let us consider real normed spaces X, Y, a point y of Y, and a point z of $X \times Y$. Suppose $z = \langle 0_X, y \rangle$. Then $\|z\| = \|y\|$. The theorem is a consequence of (1).

(4) Let us consider real normed spaces X, Y, Z, W, a Lipschitzian linear operator f from Z into W, a Lipschitzian linear operator g from Y into Z, and a Lipschitzian linear operator h from X into Y. Then $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.

(5) Let us consider real normed spaces X, Y, Z, a Lipschitzian linear operator g from X into Y, a Lipschitzian linear operator f from Y into Z, and a Lipschitzian linear operator h from X into Z. Then $h = f \cdot g$ if and only if for every vector x of X, $h(x) = f(g(x))$.

(6) Let us consider real normed spaces X, Y, and a Lipschitzian linear operator f from X into Y. Then

(i) $f \cdot \mathrm{id}_\alpha = f$, and

(ii) $\mathrm{id}_\beta \cdot f = f$,

where α is the carrier of X and β is the carrier of Y.

(7) Let us consider real normed spaces X, Y, Z, W, an element f of $\mathrm{BdLinOps}(Z, W)$, an element g of $\mathrm{BdLinOps}(Y, Z)$, and an element h of $\mathrm{BdLinOps}(X, Y)$. Then $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.

(8) Let us consider real normed spaces X, Y, and an element f of $\mathrm{BdLinOps}(X, Y)$. Then

(i) $f \cdot \mathrm{FuncUnit}(X) = f$, and

(ii) $\mathrm{FuncUnit}(Y) \cdot f = f$.

The theorem is a consequence of (6).

(9) Let us consider real normed spaces X, Y, Z, an element f of the real norm space of bounded linear operators from Y into Z, and elements g, h of the real norm space of bounded linear operators from X into Y. Then $f \cdot (g + h) = f \cdot g + f \cdot h$.

PROOF: Set $m_1 = \mathrm{PartFuncs}(f, Y, Z)$. Set $m_2 = \mathrm{PartFuncs}(g, X, Y)$. Set $m_4 = \mathrm{PartFuncs}(h, X, Y)$. Set $m_3 = \mathrm{PartFuncs}(g + h, X, Y)$. For every vector x of X, $(m_1 \cdot m_3)(x) = (m_1 \cdot m_2)(x) + (m_1 \cdot m_4)(x)$ by [9, (35)], (5). □

(10) Let us consider real normed spaces X, Y, Z, an element f of the real norm space of bounded linear operators from X into Y, and elements g, h

of the real norm space of bounded linear operators from Y into Z. Then $(g + h) \cdot f = g \cdot f + h \cdot f$.

PROOF: Set $m_1 = \mathrm{PartFuncs}(f, X, Y)$. Set $m_2 = \mathrm{PartFuncs}(g, Y, Z)$. Set $m_4 = \mathrm{PartFuncs}(h, Y, Z)$. Set $m_3 = \mathrm{PartFuncs}(g + h, Y, Z)$. For every vector x of X, $(m_3 \cdot m_1)(x) = (m_2 \cdot m_1)(x) + (m_4 \cdot m_1)(x)$. □

(11) Let us consider real normed spaces X, Y, Z, an element f of the real norm space of bounded linear operators from Y into Z, an element g of the real norm space of bounded linear operators from X into Y, and real numbers a, b. Then $(a \cdot b) \cdot (f \cdot g) = a \cdot f \cdot (b \cdot g)$.

PROOF: Set $m_1 = \mathrm{PartFuncs}(f, Y, Z)$. Set $m_2 = \mathrm{PartFuncs}(g, X, Y)$. Set $m_5 = \mathrm{PartFuncs}(a \cdot f, Y, Z)$. Set $m_6 = \mathrm{PartFuncs}(b \cdot g, X, Y)$. For every vector x of X, $(m_5 \cdot m_6)(x) = a \cdot b \cdot (m_1 \cdot m_2)(x)$. □

(12) Let us consider real normed spaces X, Y, Z, an element f of the real norm space of bounded linear operators from Y into Z, an element g of the real norm space of bounded linear operators from X into Y, and a real number a. Then $a \cdot (f \cdot g) = (a \cdot f) \cdot g$. The theorem is a consequence of (11).

2. PROPERTIES OF OPEN AND CLOSED SETS IN BANACH SPACE

Let M be a real normed space, p be an element of M, and r be a real number. The functor $\overline{\mathrm{Ball}}(p, r)$ yielding a subset of M is defined by the term

(Def. 1) $\{q$, where q is an element of $M : \|p - q\| \leqslant r\}$.

Let us consider an element p of S and a real number r. Now we state the propositions:

(13) If $0 < r$, then $p \in \mathrm{Ball}(p, r)$ and $p \in \overline{\mathrm{Ball}}(p, r)$.

(14) If $0 < r$, then $\mathrm{Ball}(p, r) \neq \emptyset$ and $\overline{\mathrm{Ball}}(p, r) \neq \emptyset$.

Let us consider a real normed space M, an element p of M, and real numbers r_1, r_2. Now we state the propositions:

(15) Suppose $r_1 \leqslant r_2$. Then

(i) $\overline{\mathrm{Ball}}(p, r_1) \subseteq \overline{\mathrm{Ball}}(p, r_2)$, and

(ii) $\mathrm{Ball}(p, r_1) \subseteq \overline{\mathrm{Ball}}(p, r_2)$, and

(iii) $\mathrm{Ball}(p, r_1) \subseteq \mathrm{Ball}(p, r_2)$.

(16) If $r_1 < r_2$, then $\overline{\mathrm{Ball}}(p, r_1) \subseteq \mathrm{Ball}(p, r_2)$.

Let us consider an element p of S and a real number r. Now we state the propositions:

(17) $\mathrm{Ball}(p,r) = \{y$, where y is a point of $S : \|y-p\| < r\}$.
PROOF: Define $\mathcal{F}$(object) $= \$_1$. Define $\mathcal{P}$[element of S] $\equiv \|p - \$_1\| < r$. Define $\mathcal{Q}$[element of S] $\equiv \|\$_1 - p\| < r$. $\{\mathcal{F}(y)$, where y is an element of the carrier of $S : \mathcal{P}[y]\} = \{\mathcal{F}(y)$, where y is an element of the carrier of $S : \mathcal{Q}[y]\}$. □

(18) $\overline{\mathrm{Ball}}(p,r) = \{y$, where y is a point of $S : \|y-p\| \leqslant r\}$.
PROOF: Define $\mathcal{F}$(object) $= \$_1$. Define $\mathcal{P}$[element of S] $\equiv \|p - \$_1\| \leqslant r$. Define $\mathcal{Q}$[element of S] $\equiv \|\$_1 - p\| \leqslant r$. $\{\mathcal{F}(y)$, where y is an element of the carrier of $S : \mathcal{P}[y]\} = \{\mathcal{F}(y)$, where y is an element of the carrier of $S : \mathcal{Q}[y]\}$. □

(19) If $0 < r$, then $\mathrm{Ball}(p,r)$ is a neighbourhood of p. The theorem is a consequence of (17).

Let X be a real normed space, x be a point of X, and r be a real number. One can check that $\mathrm{Ball}(x,r)$ is open and $\overline{\mathrm{Ball}}(x,r)$ is closed.

Now we state the propositions:

(20) Let us consider a real normed space X, and a subset V of X. Then V is open if and only if for every point x of X such that $x \in V$ there exists a real number r such that $r > 0$ and $\mathrm{Ball}(x,r) \subseteq V$.

(21) Let us consider real normed spaces X, Y, a point x of X, a point y of Y, and a point z of $X \times Y$. Suppose $z = \langle x, y\rangle$. Then

(i) $\|x\| \leqslant \|z\|$, and

(ii) $\|y\| \leqslant \|z\|$.

The theorem is a consequence of (1).

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

(i) $0 < r_2 < r_1$, and

(ii) $\mathrm{Ball}(x,r_2) \times \mathrm{Ball}(y,r_2) \subseteq \mathrm{Ball}(z,r_1)$.

PROOF: $\mathrm{Ball}(x,r_2) \times \mathrm{Ball}(y,r_2) \subseteq \mathrm{Ball}(z,r_1)$. □

(23) Let us consider real normed spaces X, Y, a point x of X, a point y of Y, and a subset V of $X \times Y$. Suppose V is open and $\langle x, y\rangle \in V$. Then there exists a real number r such that

(i) $0 < r$, and

(ii) $\mathrm{Ball}(x,r) \times \mathrm{Ball}(y,r) \subseteq V$.

The theorem is a consequence of (20) and (22).

(24) Let us consider real normed spaces X, Y, a point x of X, a point y of Y, a subset V of $X \times Y$, and a real number r. Suppose $V = \mathrm{Ball}(x, r) \times \mathrm{Ball}(y, r)$. Then V is open.

PROOF: For every point z of $X \times Y$ such that $z \in V$ there exists a real number s such that $s > 0$ and $\mathrm{Ball}(z, s) \subseteq V$ by [5, (18)]. □

(25) Let us consider real normed spaces E, F, a linear operator Q from E into F, and a point v of E. If Q is one-to-one, then $Q(v) = 0_F$ iff $v = 0_E$.

Let us consider a real normed space E, subsets X, Y of E, and a point v of E. Now we state the propositions:

(26) If X is open and $Y = \{x + v$, where x is a point of $E : x \in X\}$, then Y is open.

PROOF: Define $\mathcal{C}(\text{point of } E) = 1 \cdot \$_1 + -v$. Consider H being a function from E into E such that for every point p of E, $H(p) = \mathcal{C}(p)$. For every object s, $s \in H^{-1}(X)$ iff $s \in Y$. □

(27) If X is open and $Y = \{x - v$, where x is a point of $E : x \in X\}$, then Y is open.

PROOF: Set $w = -v$. $\{x + w$, where x is a point of $E : x \in X\} \subseteq$ the carrier of E. Define $\mathcal{F}(\text{point of } E) = \$_1 + w$. Define $\mathcal{G}(\text{point of } E) = \$_1 - v$. Define $\mathcal{P}[\text{point of } E] \equiv \$_1 \in X$. $\{\mathcal{F}(v_1)$, where v_1 is an element of the carrier of $E : \mathcal{P}[v_1]\} = \{\mathcal{G}(v_2)$, where v_2 is an element of the carrier of $E : \mathcal{P}[v_2]\}$. □

3. Existence and Uniqueness of Continuous Implicit Function

Now we state the propositions:

(28) Let us consider a real Banach space X, a non empty subset S of X, and a partial function f from X to X. Suppose S is closed and $\mathrm{dom}\, f = S$ and $\mathrm{rng}\, f \subseteq S$ and there exists a real number k such that $0 < k < 1$ and for every points x, y of X such that x, $y \in S$ holds $\|f_x - f_y\| \leqslant k \cdot \|x - y\|$. Then

(i) there exists a point x_0 of X such that $x_0 \in S$ and $f(x_0) = x_0$, and

(ii) for every points x_0, y_0 of X such that x_0, $y_0 \in S$ and $f(x_0) = x_0$ and $f(y_0) = y_0$ holds $x_0 = y_0$.

PROOF: Consider x_0 being an object such that $x_0 \in S$. Consider K being a real number such that $0 < K$ and $K < 1$ and for every points x, y of X such that x, $y \in S$ holds $\|f_x - f_y\| \leqslant K \cdot \|x - y\|$. Define $\mathcal{G}(\mathrm{set}, \mathrm{set}) = f(\$_2)$. Consider g being a function such that $\mathrm{dom}\, g = \mathbb{N}$ and $g(0) = x_0$ and for every natural number n, $g(n+1) = \mathcal{G}(n, g(n))$. Define $\mathcal{P}[\text{natural number}] \equiv$

$g(\$_1) \in S$ and $g(\$_1)$ is an element of X. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number n, $\mathcal{P}[n]$. For every object n such that $n \in \mathbb{N}$ holds $g(n) \in$ the carrier of X. For every natural number n, $\|g(n+1) - g(n)\| \leqslant \|g(1) - g(0)\| \cdot (K^n)$. For every natural numbers k, n, $\|g(n+k) - g(n)\| \leqslant \|g(1) - g(0)\| \cdot (\frac{K^n - K^{n+k}}{1-K})$. For every natural numbers k, n, $\|g(n+k) - g(n)\| \leqslant \|g(1) - g(0)\| \cdot (\frac{K^n}{1-K})$. For every real number e such that $e > 0$ there exists a natural number n such that for every natural number m such that $n \leqslant m$ holds $\|(g\uparrow 1)(m) - f_{\lim g}\| < e$. For every points x_0, y_0 of X such that x_0, $y_0 \in S$ and $f(x_0) = x_0$ and $f(y_0) = y_0$ holds $x_0 = y_0$. □

(29) Let us consider a real normed space E, a real Banach space F, a non empty subset E_0 of E, a non empty subset F_0 of F, and a partial function F_1 from $E \times F$ to F. Suppose F_0 is closed and $E_0 \times F_0 \subseteq \operatorname{dom} F_1$ and for every point x of E and for every point y of F such that $x \in E_0$ and $y \in F_0$ holds $F_1(x, y) \in F_0$ and for every point y of F such that $y \in F_0$ for every point x_0 of E such that $x_0 \in E_0$ for every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every point x_1 of E such that $x_1 \in E_0$ and $\|x_1 - x_0\| < d$ holds $\|F_1\langle x_1, y\rangle - F_1\langle x_0, y\rangle\| < e$ and there exists a real number k such that $0 < k < 1$ and for every point x of E such that $x \in E_0$ for every points y_1, y_2 of F such that y_1, $y_2 \in F_0$ holds $\|F_1\langle x, y_1\rangle - F_1\langle x, y_2\rangle\| \leqslant k \cdot \|y_1 - y_2\|$. Then

(i) for every point x of E such that $x \in E_0$ holds there exists a point y of F such that $y \in F_0$ and $F_1(x, y) = y$ and for every points y_1, y_2 of F such that y_1, $y_2 \in F_0$ and $F_1(x, y_1) = y_1$ and $F_1(x, y_2) = y_2$ holds $y_1 = y_2$, and

(ii) for every point x_0 of E and for every point y_0 of F such that $x_0 \in E_0$ and $y_0 \in F_0$ and $F_1(x_0, y_0) = y_0$ for every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every point x_1 of E and for every point y_1 of F such that $x_1 \in E_0$ and $y_1 \in F_0$ and $F_1(x_1, y_1) = y_1$ and $\|x_1 - x_0\| < d$ holds $\|y_1 - y_0\| < e$.

PROOF: Consider k being a real number such that $0 < k < 1$ and for every point x of E such that $x \in E_0$ for every points y_1, y_2 of F such that y_1, $y_2 \in F_0$ holds $\|F_1\langle x, y_1\rangle - F_1\langle x, y_2\rangle\| \leqslant k \cdot \|y_1 - y_2\|$. For every point x of E such that $x \in E_0$ holds there exists a point y of F such that $y \in F_0$ and $F_1(x, y) = y$ and for every points y_1, y_2 of F such that y_1, $y_2 \in F_0$ and $F_1(x, y_1) = y_1$ and $F_1(x, y_2) = y_2$ holds $y_1 = y_2$. For every point x_0 of E and for every point y_0 of F such that $x_0 \in E_0$ and $y_0 \in F_0$ and $F_1(x_0, y_0) = y_0$ for every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every point x_1 of E and for every

point y_1 of F such that $x_1 \in E_0$ and $y_1 \in F_0$ and $F_1(x_1, y_1) = y_1$ and $\|x_1 - x_0\| < d$ holds $\|y_1 - y_0\| < e$. $\square$

(30) Let us consider a real normed space E, a real Banach space F, a non empty subset A of E, a non empty subset B of F, and a partial function F_1 from $E \times F$ to F. Suppose B is closed and $A \times B \subseteq \operatorname{dom} F_1$ and for every point x of E and for every point y of F such that $x \in A$ and $y \in B$ holds $F_1(x, y) \in B$ and for every point y of F such that $y \in B$ for every point x_0 of E such that $x_0 \in A$ for every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every point x_1 of E such that $x_1 \in A$ and $\|x_1 - x_0\| < d$ holds $\|F_1{}_{\langle x_1, y\rangle} - F_1{}_{\langle x_0, y\rangle}\| < e$ and there exists a real number k such that $0 < k < 1$ and for every point x of E such that $x \in A$ for every points y_1, y_2 of F such that y_1, $y_2 \in B$ holds $\|F_1{}_{\langle x, y_1\rangle} - F_1{}_{\langle x, y_2\rangle}\| \leqslant k \cdot \|y_1 - y_2\|$. Then

(i) there exists a partial function g from E to F such that g is continuous on A and $\operatorname{dom} g = A$ and $\operatorname{rng} g \subseteq B$ and for every point x of E such that $x \in A$ holds $F_1(x, g(x)) = g(x)$, and

(ii) for every partial functions g_1, g_2 from E to F such that $\operatorname{dom} g_1 = A$ and $\operatorname{rng} g_1 \subseteq B$ and $\operatorname{dom} g_2 = A$ and $\operatorname{rng} g_2 \subseteq B$ and for every point x of E such that $x \in A$ holds $F_1(x, g_1(x)) = g_1(x)$ and for every point x of E such that $x \in A$ holds $F_1(x, g_2(x)) = g_2(x)$ holds $g_1 = g_2$.

PROOF: There exists a partial function g from E to F such that g is continuous on A and $\operatorname{dom} g = A$ and $\operatorname{rng} g \subseteq B$ and for every point x of E such that $x \in A$ holds $F_1(x, g(x)) = g(x)$ by (29), [4, (19)]. For every object x such that $x \in \operatorname{dom} g_1$ holds $g_1(x) = g_2(x)$. $\square$

Let us consider real normed spaces E, F and points s_1, s_2 of $E \times F$. Now we state the propositions:

(31) If $(s_1)_{\mathbf{2}} = (s_2)_{\mathbf{2}}$, then $\operatorname{reproj1}(s_1) = \operatorname{reproj1}(s_2)$.

(32) If $(s_1)_{\mathbf{1}} = (s_2)_{\mathbf{1}}$, then $\operatorname{reproj2}(s_1) = \operatorname{reproj2}(s_2)$.

(33) Let us consider a real normed space E, a real number r, and points z, y_1, y_2 of E. Suppose y_1, $y_2 \in \overline{\operatorname{Ball}}(z, r)$. Then $[y_1, y_2] \subseteq \overline{\operatorname{Ball}}(z, r)$.

(34) Let us consider a real normed space E, points x, b of E, and a neighbourhood N of x. Then $\{z - b$, where z is a point of $E : z \in N\}$ is neighbourhood of $x - b$ and neighbourhood of $x + b$.

PROOF: Consider g being a real number such that $0 < g$ and $\{y$, where y is a point of $E : \|y - x\| < g\} \subseteq N$. $\{z - b$, where z is a point of $E : z \in N\} \subseteq$ the carrier of E. $\{z + b$, where z is a point of $E : z \in N\} \subseteq$ the carrier of E. $\{y$, where y is a point of $E : \|y - (x - b)\| < g\} \subseteq \{z - b$, where z is a point of $E : z \in N\}$. $\{y$, where y is a point of

$E : \|y - (x + b)\| < g\} \subseteq \{z + b$, where z is a point of $E : z \in N\}$. □

Let us consider real normed spaces E, G, a real Banach space F, a subset Z of $E \times F$, a partial function f from $E \times F$ to G, a point a of E, a point b of F, a point c of G, and a point z of $E \times F$. Now we state the propositions:

(35) Suppose Z is open and $\operatorname{dom} f = Z$ and f is continuous on Z and f is partially differentiable on Z w.r.t. 2 and $f \upharpoonright^2 Z$ is continuous on Z and $z = \langle a, b\rangle$ and $z \in Z$ and $f(a, b) = c$ and $\operatorname{partdiff}(f, z)$ w.r.t. 2 is one-to-one and $(\operatorname{partdiff}(f, z)$ w.r.t. $2)^{-1}$ is a Lipschitzian linear operator from G into F. Then there exist real numbers r_1, r_2 such that

(i) $0 < r_1$, and

(ii) $0 < r_2$, and

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

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

(v) for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ for every points y_1, y_2 of F such that y_1, $y_2 \in \overline{\operatorname{Ball}}(b, r_2)$ and $f(x, y_1) = c$ and $f(x, y_2) = c$ holds $y_1 = y_2$, and

(vi) there exists a partial function g from E to F such that g is continuous on $\operatorname{Ball}(a, r_1)$ and $\operatorname{dom} g = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g \subseteq \overline{\operatorname{Ball}}(b, r_2)$ and $g(a) = b$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g(x)) = c$, and

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

PROOF: Consider Q_1 being a Lipschitzian linear operator from G into F such that $Q_1 = (\operatorname{partdiff}(f, z)$ w.r.t. $2)^{-1}$. Reconsider $Q = Q_1$ as a point of the real norm space of bounded linear operators from G into F. Reconsider $z_1 = \langle a, 0_F\rangle$ as a point of $E \times F$. Reconsider $e_0 = \langle 0_E, b\rangle$ as a point of $E \times F$. Define $\mathcal{C}(\text{point of } E \times F) = 1 \cdot \$_1 + -e_0$. Consider H being a function from the carrier of $E \times F$ into the carrier of $E \times F$ such that for every point p of $E \times F$, $H(p) = \mathcal{C}(p)$. For every point x of E and for every point y of F, $H(x, y) = \langle x, y - b\rangle$. Define $\mathcal{D}(\text{point of } E \times F) = 1 \cdot \$_1 + e_0$. Consider K being a function from the carrier of $E \times F$ into the carrier of $E \times F$ such that for every point p of $E \times F$, $K(p) = \mathcal{D}(p)$. For every point p of $E \times F$, $K \cdot H(p) = p$. For every point p of $E \times F$, $H \cdot K(p) = p$. Reconsider $Z_1 = H^\circ Z$ as a subset of $E \times F$. For every point x of E and for every

point y of F, $\langle x, y+b\rangle \in Z$ iff $\langle x, y\rangle \in Z_1$. Reconsider $e_0 = \langle 0_E, b\rangle$ as a point of $E \times F$. For every object p, $p \in Z_1$ iff $p \in \{y - e_0$, where y is a point of $E \times F : y \in Z\}$. Z_1 is open. Define $\mathcal{J}$[object, object] $\equiv$ there exists a point x of E and there exists a point y of F such that $\$_1 = \langle x, y\rangle$ and $\$_2 = f_{\langle x, y+b\rangle} - c$. For every object p such that $p \in Z_1$ there exists an object w such that $w \in$ the carrier of G and $\mathcal{J}[p, w]$. Consider f_1 being a function from Z_1 into G such that for every object p such that $p \in Z_1$ holds $\mathcal{J}[p, f_1(p)]$. For every point x of E and for every point y of F such that $\langle x, y\rangle \in Z_1$ holds $f_1(x, y) = f_{\langle x, y+b\rangle} - c$. Define $\mathcal{O}$[object, object] $\equiv$ there exists a point x of E and there exists a point y of F such that $\$_1 = \langle x, y\rangle$ and $\$_2 = Q(f_1(x, y))$. For every object p such that $p \in Z_1$ there exists an object w such that $w \in$ the carrier of F and $\mathcal{O}[p, w]$. Consider f_2 being a function from Z_1 into F such that for every object p such that $p \in Z_1$ holds $\mathcal{O}[p, f_2(p)]$. For every point x of E and for every point y of F such that $\langle x, y\rangle \in Z_1$ holds $f_2(x, y) = Q(f_1(x, y))$. Define $\mathcal{U}$[object, object] $\equiv$ there exists a point x of E and there exists a point y of F such that $\$_1 = \langle x, y\rangle$ and $\$_2 = y - f_{2\langle x, y\rangle}$. For every object p such that $p \in Z_1$ there exists an object w such that $w \in$ the carrier of F and $\mathcal{U}[p, w]$.

Consider F_1 being a function from Z_1 into F such that for every object p such that $p \in Z_1$ holds $\mathcal{U}[p, F_1(p)]$. For every point x of E and for every point y of F such that $\langle x, y\rangle \in Z_1$ holds $F_1(x, y) = y - f_{2\langle x, y\rangle}$. For every point z_0 of $E \times F$ and for every real number r such that $z_0 \in Z_1$ and $0 < r$ there exists a real number s such that $0 < s$ and for every point z_1 of $E \times F$ such that $z_1 \in Z_1$ and $\|z_1 - z_0\| < s$ holds $\|F_{1z_1} - F_{1z_0}\| < r$. For every point w_0 of $E \times F$ such that $w_0 \in Z$ holds $f \cdot (\mathrm{reproj2}(w_0))$ is differentiable in $(w_0)_{\mathbf{2}}$. For every point w_0 of $E \times F$ such that $w_0 \in Z$ there exists a neighbourhood N of $(w_0)_{\mathbf{2}}$ such that $N \subseteq \mathrm{dom}\, f \cdot (\mathrm{reproj2}(w_0))$ and there exists a rest R of F, G such that for every point w_1 of F such that $w_1 \in N$ holds $f \cdot (\mathrm{reproj2}(w_0))_{w_1} - f \cdot (\mathrm{reproj2}(w_0))_{(w_0)_{\mathbf{2}}} = f \cdot (\mathrm{reproj2}(w_0))'((w_0)_{\mathbf{2}})(w_1 - (w_0)_{\mathbf{2}}) + R_{w_1 - (w_0)_{\mathbf{2}}}$. For every point z_0 of $E \times F$ such that $z_0 \in Z_1$ holds $F_1 \cdot (\mathrm{reproj2}(z_0))$ is differentiable in $(z_0)_{\mathbf{2}}$ and there exist points L_0, I of the real norm space of bounded linear operators from F into F such that $L_0 = Q \cdot ((f \restriction^2 Z)_{z_0+e_0})$ and $I = \mathrm{id}_\alpha$ and $F_1 \cdot (\mathrm{reproj2}(z_0))'((z_0)_{\mathbf{2}}) = I - L_0$, where α is the carrier of F. $\mathrm{dom}(F_1 \restriction^2 Z_1) = Z_1$ and for every point z of $E \times F$ such that $z \in Z_1$ there exist points L, I of the real norm space of bounded linear operators from F into F such that $L = Q \cdot ((f \restriction^2 Z)_{z+e_0})$ and $I = \mathrm{id}_\alpha$ and $(F_1 \restriction^2 Z_1)_z = I - L$, where α is the carrier of F. Set $F_2 = F_1 \restriction^2 Z_1$. For every point z_0 of $E \times F$ and for every real number r such that $z_0 \in Z_1$ and $0 < r$ there exists

a real number s such that $0 < s$ and for every point z_1 of $E \times F$ such that $z_1 \in Z_1$ and $\|z_1 - z_0\| < s$ holds $\|F_{2z_1} - F_{2z_0}\| < r$. $F_1(a, 0_F) = 0_F$ by [6, (3)]. Reconsider $a_0 = \langle a,\, 0_F \rangle$ as a point of $E \times F$. Consider r_4 being a real number such that $0 < r_4$ and for every point s of $E \times F$ such that $s \in Z_1$ and $\|s - a_0\| < r_4$ holds $\|(F_1 \restriction^2 Z_1)_s - (F_1 \restriction^2 Z_1)_{a_0}\| < \frac{1}{4}$. Consider r_5 being a real number such that $0 < r_5$ and $\mathrm{Ball}(a_0, r_5) \subseteq Z_1$. Reconsider $r_6 = \min(r_4, r_5)$ as a real number. $\mathrm{Ball}(a_0, r_6) \subseteq \mathrm{Ball}(a_0, r_5)$.

Consider r_1 being a real number such that $0 < r_1 < r_6$ and $\mathrm{Ball}(a, r_1) \times \mathrm{Ball}(0_F, r_1) \subseteq \mathrm{Ball}(a_0, r_6)$. For every point x of $E \times F$ such that $x \in Z_1$ holds $(F_1 \restriction^2 Z_1)_x = F_1 \cdot (\mathrm{reproj2}(x))'((x)_{\mathbf{2}})$. $a \in \mathrm{Ball}(a, r_1)$. $0_F \in \mathrm{Ball}(0_F, r_1)$. Reconsider $a_0 = \langle a,\, 0_F \rangle$ as a point of $E \times F$. Consider L_1, I_1 being points of the real norm space of bounded linear operators from F into F such that $L_1 = Q \cdot ((f \restriction^2 Z)_{a_0 + e_0})$ and $I_1 = \mathrm{id}_\alpha$ and $(F_1 \restriction^2 Z_1)_{a_0} = I_1 - L_1$, where α is the carrier of F. For every point x of E and for every point y of F such that $x \in \mathrm{Ball}(a, r_1)$ and $y \in \mathrm{Ball}(0_F, r_1)$ holds $\|(F_1 \restriction^2 Z_1)_{\langle x, y \rangle}\| < \frac{1}{4}$. Reconsider $r_2 = \frac{r_1}{2}$ as a real number. Consider a_2 being a real number such that $0 < a_2$ and for every point s of $E \times F$ such that $s \in Z_1$ and $\|s - a_0\| < a_2$ holds $\|F_{1s} - F_{1a_0}\| < (\frac{1}{2}) \cdot r_2$. Consider a_4 being a real number such that $0 < a_4 < a_2$ and $\mathrm{Ball}(a, a_4) \times \mathrm{Ball}(0_F, a_4) \subseteq \mathrm{Ball}(a_0, a_2)$. Reconsider $a_3 = \min(a_2, a_4)$ as a real number. $\mathrm{Ball}(a, a_3) \subseteq \mathrm{Ball}(a, a_4)$. Reconsider $a_1 = \min(a_3, r_1)$ as a real number. $\mathrm{Ball}(a, a_1) \subseteq \mathrm{Ball}(a, r_1)$. $\mathrm{Ball}(a, a_1) \subseteq \mathrm{Ball}(a, a_3)$. For every point x of E such that $x \in \mathrm{Ball}(a, a_1)$ holds $\|F_{1\langle x, 0_F \rangle}\| \leqslant (\frac{1}{2}) \cdot r_2$. Reconsider $r_0 = \min(\frac{r_1}{2}, a_1)$ as a real number. $\mathrm{Ball}(a, r_0) \subseteq \mathrm{Ball}(a, r_1)$. For every point x of E such that $x \in \mathrm{Ball}(a, r_0)$ holds $\|F_{1\langle x, 0_F \rangle}\| \leqslant (\frac{1}{2}) \cdot r_2$. $\overline{\mathrm{Ball}}(0_F, r_2) \subseteq \mathrm{Ball}(0_F, r_1)$. For every point x of E such that $x \in \mathrm{Ball}(a, r_0)$ for every points y_1, y_2 of F such that $y_1, y_2 \in \overline{\mathrm{Ball}}(0_F, r_2)$ holds $\|F_{1\langle x, y_1 \rangle} - F_{1\langle x, y_2 \rangle}\| \leqslant (\frac{1}{2}) \cdot \|y_1 - y_2\|$. For every point x of E and for every point y of F such that $x \in \mathrm{Ball}(a, r_0)$ and $y \in \overline{\mathrm{Ball}}(0_F, r_2)$ holds $F_1(x, y) \in \overline{\mathrm{Ball}}(0_F, r_2)$. $\mathrm{Ball}(a, r_0) \neq \emptyset$. $\overline{\mathrm{Ball}}(0_F, r_2) \neq \emptyset$. For every point y of F such that $y \in \overline{\mathrm{Ball}}(0_F, r_2)$ for every point x_0 of E such that $x_0 \in \mathrm{Ball}(a, r_0)$ for every real number e such that $0 < e$ there exists a real number d such that $0 < d$ and for every point x_1 of E such that $x_1 \in \mathrm{Ball}(a, r_0)$ and $\|x_1 - x_0\| < d$ holds $\|F_{1\langle x_1, y \rangle} - F_{1\langle x_0, y \rangle}\| < e$.

Consider Ψ being a partial function from E to F such that Ψ is continuous on $\mathrm{Ball}(a, r_0)$ and $\mathrm{dom}\, \Psi = \mathrm{Ball}(a, r_0)$ and $\mathrm{rng}\, \Psi \subseteq \overline{\mathrm{Ball}}(0_F, r_2)$ and for every point x of E such that $x \in \mathrm{Ball}(a, r_0)$ holds $F_1(x, \Psi(x)) = \Psi(x)$. For every object z, $z \in \overline{\mathrm{Ball}}(b, r_2)$ iff $z \in \{y + b$, where y is a point of $F : y \in \overline{\mathrm{Ball}}(0_F, r_2)\}$. For every object y, $y \in \mathrm{Ball}(a, r_0) \times \overline{\mathrm{Ball}}(b, r_2)$

iff there exists an object x such that $x \in \operatorname{dom} K$ and $x \in \operatorname{Ball}(a, r_0) \times \overline{\operatorname{Ball}}(0_F, r_2)$ and $y = K(x)$. Define $\mathcal{W}(\text{object}) = \Psi_{\$_1} + b$. For every object y such that $y \in \operatorname{Ball}(a, r_0)$ holds $\mathcal{W}(y) \in \overline{\operatorname{Ball}}(b, r_2)$. Consider E_3 being a function from $\operatorname{Ball}(a, r_0)$ into $\overline{\operatorname{Ball}}(b, r_2)$ such that for every object y such that $y \in \operatorname{Ball}(a, r_0)$ holds $E_3(y) = \mathcal{W}(y)$. $\overline{\operatorname{Ball}}(b, r_2) \neq \emptyset$. For every point x_0 of E and for every real number r such that $x_0 \in \operatorname{Ball}(a, r_0)$ and $0 < r$ there exists a real number s such that $0 < s$ and for every point x_1 of E such that $x_1 \in \operatorname{Ball}(a, r_0)$ and $\|x_1 - x_0\| < s$ holds $\|E_{3x_1} - E_{3x_0}\| < r$. For every point x of E such that $x \in \operatorname{Ball}(a, r_0)$ holds $f(x, E_3(x)) = c$. For every point x of E such that $x \in \operatorname{Ball}(a, r_0)$ there exists a point y of F such that $y \in \overline{\operatorname{Ball}}(b, r_2)$ and $f(x, y) = c$. For every point x of E such that $x \in \operatorname{Ball}(a, r_0)$ for every points y_1, y_2 of F such that y_1, $y_2 \in \overline{\operatorname{Ball}}(b, r_2)$ and $f(x, y_1) = c$ and $f(x, y_2) = c$ holds $y_1 = y_2$. $a \in \operatorname{Ball}(a, r_0)$ and $b \in \overline{\operatorname{Ball}}(b, r_2)$. $E_3(a) \in \operatorname{rng} E_3$. $f(a, E_3(a)) = c$. For every partial functions E_1, E_2 from E to F such that $\operatorname{dom} E_1 = \operatorname{Ball}(a, r_0)$ and $\operatorname{rng} E_1 \subseteq \overline{\operatorname{Ball}}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_0)$ holds $f(x, E_1(x)) = c$ and $\operatorname{dom} E_2 = \operatorname{Ball}(a, r_0)$ and $\operatorname{rng} E_2 \subseteq \overline{\operatorname{Ball}}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_0)$ holds $f(x, E_2(x)) = c$ holds $E_1 = E_2$. □

(36) Suppose Z is open and $\operatorname{dom} f = Z$ and f is continuous on Z and f is partially differentiable on Z w.r.t. 2 and $f \restriction^2 Z$ is continuous on Z and $z = \langle a, b \rangle$ and $z \in Z$ and $f(a, b) = c$ and $\operatorname{partdiff}(f, z)$ w.r.t. 2 is one-to-one and $(\operatorname{partdiff}(f, z) \text{ w.r.t. } 2)^{-1}$ is a Lipschitzian linear operator from G into F. Then there exist real numbers r_1, r_2 such that

(i) $0 < r_1$, and

(ii) $0 < r_2$, and

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

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

(v) for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ for every points y_1, y_2 of F such that y_1, $y_2 \in \operatorname{Ball}(b, r_2)$ and $f(x, y_1) = c$ and $f(x, y_2) = c$ holds $y_1 = y_2$, and

(vi) there exists a partial function g from E to F such that g is continuous on $\operatorname{Ball}(a, r_1)$ and $\operatorname{dom} g = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g \subseteq \operatorname{Ball}(b, r_2)$ and $g(a) = b$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g(x)) = c$, and

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

and $\operatorname{rng} g_2 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_2(x)) = c$ holds $g_1 = g_2$.

PROOF: Consider r_1, r_2 being real numbers such that $0 < r_1$ and $0 < r_2$ and $\operatorname{Ball}(a, r_1) \times \overline{\operatorname{Ball}}(b, r_2) \subseteq Z$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ there exists a point y of F such that $y \in \overline{\operatorname{Ball}}(b, r_2)$ and $f(x, y) = c$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ for every points y_1, y_2 of F such that y_1, $y_2 \in \overline{\operatorname{Ball}}(b, r_2)$ and $f(x, y_1) = c$ and $f(x, y_2) = c$ holds $y_1 = y_2$ and there exists a partial function g from E to F such that g is continuous on $\operatorname{Ball}(a, r_1)$ and $\operatorname{dom} g = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g \subseteq \overline{\operatorname{Ball}}(b, r_2)$ and $g(a) = b$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g(x)) = c$ and for every partial functions g_1, g_2 from E to F such that $\operatorname{dom} g_1 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_1 \subseteq \overline{\operatorname{Ball}}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_1(x)) = c$ and $\operatorname{dom} g_2 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_2 \subseteq \overline{\operatorname{Ball}}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_2(x)) = c$ holds $g_1 = g_2$.

Consider g being a partial function from E to F such that g is continuous on $\operatorname{Ball}(a, r_1)$ and $\operatorname{dom} g = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g \subseteq \overline{\operatorname{Ball}}(b, r_2)$ and $g(a) = b$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g(x)) = c$ and for every partial functions g_1, g_2 from E to F such that $\operatorname{dom} g_1 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_1 \subseteq \overline{\operatorname{Ball}}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_1(x)) = c$ and $\operatorname{dom} g_2 = \operatorname{Ball}(a, r_1)$ and $\operatorname{rng} g_2 \subseteq \overline{\operatorname{Ball}}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_1)$ holds $f(x, g_2(x)) = c$ holds $g_1 = g_2$. $a \in \operatorname{Ball}(a, r_1)$. Consider r_3 being a real number such that $0 < r_3$ and for every point x_1 of E such that $x_1 \in \operatorname{dom} g$ and $\|x_1 - a\| < r_3$ holds $\|g_{x_1} - g_a\| < r_2$. Reconsider $r_0 = \min(r_1, r_3)$ as a real number. $\operatorname{Ball}(a, r_0) \subseteq \operatorname{Ball}(a, r_1)$ and $\operatorname{Ball}(a, r_0) \subseteq \operatorname{Ball}(a, r_3)$. For every point x of E such that $x \in \operatorname{Ball}(a, r_0)$ there exists a point y of F such that $y \in \operatorname{Ball}(b, r_2)$ and $f(x, y) = c$.

For every point x of E such that $x \in \operatorname{Ball}(a, r_0)$ for every points y_1, y_2 of F such that y_1, $y_2 \in \operatorname{Ball}(b, r_2)$ and $f(x, y_1) = c$ and $f(x, y_2) = c$ holds $y_1 = y_2$. Reconsider $g_1 = g \restriction \operatorname{Ball}(a, r_0)$ as a partial function from E to F. $\operatorname{dom} g_1 = \operatorname{Ball}(a, r_0)$. For every object y such that $y \in \operatorname{rng} g_1$ holds $y \in \operatorname{Ball}(b, r_2)$. $g_1(a) = b$. For every point x of E such that $x \in \operatorname{Ball}(a, r_0)$ holds $f(x, g_1(x)) = c$. For every partial functions g_1, g_2 from E to F such that $\operatorname{dom} g_1 = \operatorname{Ball}(a, r_0)$ and $\operatorname{rng} g_1 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_0)$ holds $f(x, g_1(x)) = c$ and $\operatorname{dom} g_2 = \operatorname{Ball}(a, r_0)$ and $\operatorname{rng} g_2 \subseteq \operatorname{Ball}(b, r_2)$ and for every point x of E such that $x \in \operatorname{Ball}(a, r_0)$ holds $f(x, g_2(x)) = c$ holds $g_1 = g_2$. □

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

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

[5] 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.

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

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

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

[9] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.

Received November 29, 2017

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

FORMALIZED MATHEMATICS
Vol. 25, No. 4, Pages 283–288, 2017
DOI: 10.1515/forma-2017-0027

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

Introduction to Diophantine Approximation. Part II

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

Summary. In the article we present in the Mizar system [1], [2] the formalized proofs for Hurwitz' theorem [4, 1891] and Minkowski's theorem [5]. Both theorems are well explained as a basic result of the theory of Diophantine approximations appeared in [3], [6].

A formal proof of Dirichlet's theorem, namely an inequation $|\theta - y/x| \leqslant 1/x^2$ has infinitely many integer solutions (x, y) where θ is an irrational number, was given in [8]. A finer approximation is given by Hurwitz' theorem: $|\theta - y/x| \leqslant 1/\sqrt{5}x^2$.

Minkowski's theorem concerns an inequation of a product of non-homogeneous binary linear forms such that $|a_1x + b_1y + c_1| \cdot |a_2x + b_2y + c_2| \leqslant \Delta/4$ where $\Delta = |a_1b_2 - a_2b_1| \neq 0$, has at least one integer solution.

MSC: 11J20 11J25 03B35

Keywords: Diophantine approximation; rational approximation; Dirichlet; Hurwitz; Minkowski

MML identifier: DIOPHAN2, version: 8.1.06 5.45.1311

1. Preliminaries

From now on r_1, r_2, r_3 denote non negative real numbers, n, m_1 denote natural numbers, s denotes a real number, i, j, i_1, j_1 denote integers, r denotes an irrational real number, and q denotes a rational number.

Now we state the propositions:

(1) If $r_1 \cdot r_2 \leqslant r_3$, then $r_1 \leqslant \sqrt{r_3}$ or $r_2 \leqslant \sqrt{r_3}$.

(2) $\sqrt{r_1 \cdot r_2} = \frac{r_1+r_2}{2}$ if and only if $r_1 = r_2$.

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

(3) $r_1 \cdot r_2 = (\frac{r_1+r_2}{2})^{\mathbf{2}}$ if and only if $r_1 = r_2$. The theorem is a consequence of (2).

(4) If i_1 and j_1 are relatively prime, then there exist integers s, t such that $s \cdot i_1 + t \cdot j_1 = 1$.

(5) If $1 < s$ and $s + \frac{1}{s} < \sqrt{5}$, then $s < \frac{\sqrt{5}+1}{2}$ and $\frac{1}{s} > \frac{\sqrt{5}-1}{2}$.

(6) If $q = \frac{i_1}{m_1}$ and $m_1 \neq 0$ and i_1 and m_1 are relatively prime, then $i_1 = \operatorname{num} q$ and $m_1 = \operatorname{den} q$.

Let f be a function. The functor ZeroPointSet(f) yielding a set is defined by the term

(Def. 1) $\operatorname{dom} f \setminus \operatorname{support} f$. Now we state the proposition:

(7) Let us consider a function f, and objects o_1. Then $o_1 \in \text{ZeroPointSet}(f)$ if and only if $o_1 \in \operatorname{dom} f$ and $f(o_1) = 0$.

2. Hurwitz' Theorem [4, 1891]

Let r be an irrational real number and n be a natural number. Note that $(cd\,r)(n)$ is positive and natural. Now we state the propositions:

(8) Suppose $n > 1$ and $|r - \frac{(cn\,r)(n)}{(cd\,r)(n)}| \geqslant \frac{1}{\sqrt{5}\cdot((cd\,r)(n)^2)}$ and $|r - \frac{(cn\,r)(n+1)}{(cd\,r)(n+1)}| \geqslant \frac{1}{\sqrt{5}\cdot((cd\,r)(n+1)^2)}$. Then $\sqrt{5} > \frac{(cd\,r)(n+1)}{(cd\,r)(n)} + \frac{1}{\frac{(cd\,r)(n+1)}{(cd\,r)(n)}}$.

(9) If $i = (cn\,r)(n)$ and $j = (cd\,r)(n)$, then i and j are relatively prime.

(10) Suppose $n > 1$. Then

(i) $|r - \frac{(cn\,r)(n)}{(cd\,r)(n)}| < \frac{1}{\sqrt{5}\cdot((cd\,r)(n)^2)}$, or

(ii) $|r - \frac{(cn\,r)(n+1)}{(cd\,r)(n+1)}| < \frac{1}{\sqrt{5}\cdot((cd\,r)(n+1)^2)}$, or

(iii) $|r - \frac{(cn\,r)(n+2)}{(cd\,r)(n+2)}| < \frac{1}{\sqrt{5}\cdot((cd\,r)(n+2)^2)}$.

The theorem is a consequence of (8) and (5).

Let us consider r. The functor HWZSet(r) yielding a subset of $\mathbb{Q}$ is defined by the term

(Def. 2) $\{p$, where p is a rational number : $|r - p| < \frac{1}{\sqrt{5}\cdot((\operatorname{den} p)^2)}\}$.

The functor HWZSet1(r) yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 3) $\{x$, where x is a natural number : there exists a rational number p such that $p \in \text{HWZSet}(r)$ and $x = \operatorname{den} p\}$.

The functor TRANQN yielding a function from $\mathbb{Q}$ into $\mathbb{N}$ is defined by

(Def. 4) for every rational number x, $it(x) = \operatorname{den} x$.

(11) $(\text{TRANQN})^{\circ}(\text{HWZSet}(r)) = \text{HWZSet1}(r)$.

(12) If HWZSet(r) is finite, then HWZSet1(r) is finite. The theorem is a consequence of (11).

Let us consider r. One can check that HWZSet1(r) is non empty.

(13) Let us consider a natural number h. If $h \in$ HWZSet1(r), then $h > 0$.

Let us consider r. Note that HWZSet1(r) is infinite.

(14) HURWITZ'S THEOREM (NUMBER THEORY): $\{q : |r-q| < \frac{1}{\sqrt{5}\cdot((\operatorname{den} q)^2)}\}$ is infinite. The theorem is a consequence of (12).

From now on c_0, c_1, c_2, u, a_0, b_0 denote real numbers.

Let a_0, b_0, c_0 be real numbers. The functor LF(a_0, b_0, c_0) yielding a function from $\mathbb{Z} \times \mathbb{Z}$ into $\mathbb{R}$ is defined by

(Def. 5) for every integers x, y, $it(x, y) = a_0 \cdot x + b_0 \cdot y + c_0$.

3. MINKOWSKI'S THEOREM [5, ZWEITES KAPITEL, §11, 1907]

Now we state the proposition:

(15) Let us consider an element ρ of $\mathbb{R}$, and integers p, q. Suppose p and q are relatively prime. Then there exist elements x, y of $\mathbb{Z}$ such that $|p \cdot x - q \cdot y + \rho| \leqslant \frac{1}{2}$. The theorem is a consequence of (4).

In the sequel a, b denote real numbers and n denotes an integer.

(16) If $n \leqslant b \leqslant n+1$, then $|n-b| \cdot |n+1-b| \leqslant \frac{1}{4}$.

(17) If a is not an integer and ($n = \lfloor a \rfloor$ or $n = \lfloor a \rfloor + 1$), then $|a - n| < 1$.

(18) Suppose $|n-a| \cdot |n+1-a| \leqslant \frac{1}{4}$ and $|n-b| \cdot |n+1-b| \leqslant \frac{1}{4}$. Then

(i) $|n-a| \cdot |n-b| \leqslant \frac{1}{4}$, or

(ii) $|n+1-a| \cdot |n+1-b| \leqslant \frac{1}{4}$.

The theorem is a consequence of (1).

(19) Suppose $|a-n| \cdot |b-n| \cdot |a-n-1| \cdot |b-n-1| \leqslant \frac{|a-b|^2}{4}$. Then

(i) $|a-n| \cdot |b-n| \leqslant \frac{|a-b|}{2}$, or

(ii) $|a-n-1| \cdot |b-n-1| \leqslant \frac{|a-b|}{2}$.

The theorem is a consequence of (1).

(20) Suppose $(n-b) \cdot (n+1-a) > 0$ and $(a-n) \cdot (n+1-b) > 0$. Then

(i) $(n-b) \cdot (n+1-a) + (a-n) \cdot (n+1-b) = a-b$, and

(ii) $|a-n| \cdot |b-n| \cdot |a-n-1| \cdot |b-n-1| \leqslant \frac{|a-b|^2}{4}$.

(21) If $b < n < a < n+1$, then $|a-n| \cdot |b-n| \cdot |a-n-1| \cdot |b-n-1| \leqslant \frac{|a-b|^2}{4}$. The theorem is a consequence of (20).

(22) Suppose $(n-a)\cdot(n+1-b)>0$ and $(b-n)\cdot(n+1-a)>0$. Then

(i) $(n-a)\cdot(n+1-b)+(b-n)\cdot(n+1-a)=b-a$, and

(ii) $|a-n|\cdot|b-n|\cdot|a-n-1|\cdot|b-n-1|\leqslant\frac{|a-b|^2}{4}$.

(23) If $n+1<b$ and $n<a<n+1$, then $|a-n|\cdot|b-n|\cdot|a-n-1|\cdot|b-n-1|\leqslant\frac{|a-b|^2}{4}$. The theorem is a consequence of (22).

(24) Suppose a is not an integer and $\lfloor a\rfloor\leqslant b\leqslant\lfloor a\rfloor+1$. Then there exists an integer u such that

(i) $|a-u|<1$, and

(ii) $|a-u|\cdot|b-u|\leqslant\frac{1}{4}$.

The theorem is a consequence of (16), (18), and (17).

(25) Suppose $|a-\lfloor a\rfloor|\cdot|b-\lfloor a\rfloor|\geqslant\frac{|a-b|}{2}$ and $|a-(\lfloor a\rfloor+1)|\cdot|b-(\lfloor a\rfloor+1)|\geqslant\frac{|a-b|}{2}$. Then

(i) a is an integer, or

(ii) $\lfloor a\rfloor\leqslant b$.

The theorem is a consequence of (21), (19), and (3).

(26) Suppose a is not an integer and $\lfloor a\rfloor>b$. Then there exists an integer u such that

(i) $|a-u|<1$, and

(ii) $|a-u|\cdot|b-u|<\frac{|a-b|}{2}$.

The theorem is a consequence of (17) and (25).

(27) Suppose $|a-\lfloor a\rfloor|\cdot|b-\lfloor a\rfloor|\geqslant\frac{|a-b|}{2}$ and $|a-(\lfloor a\rfloor+1)|\cdot|b-(\lfloor a\rfloor+1)|\geqslant\frac{|a-b|}{2}$. Then

(i) a is an integer, or

(ii) $\lfloor a\rfloor+1\geqslant b$.

The theorem is a consequence of (23), (19), and (3).

(28) Suppose a is not an integer and $\lfloor a\rfloor+1<b$. Then there exists an integer u such that

(i) $|a-u|<1$, and

(ii) $|a-u|\cdot|b-u|<\frac{|a-b|}{2}$.

The theorem is a consequence of (17) and (27).

(29) There exists an integer u such that

(i) $|a-u|<1$, and

(ii) $|a-u|\cdot|b-u|\leqslant\frac{1}{4}$ or $|a-u|\cdot|b-u|<\frac{|a-b|}{2}$.

The theorem is a consequence of (24), (26), and (28).

In the sequel a_1, a_2, b_1, b_2, c_1, c_2 denote elements of $\mathbb{R}$, ϵ denotes a positive real number, r_1 denotes a non negative real number, and q, q_1 denote elements of $\mathbb{Q}$. Now we state the propositions:

(30) There exists an element q of $\mathbb{Q}$ such that

(i) $\operatorname{den} q > \lfloor r_1 \rfloor + 1$, and

(ii) $q \in \operatorname{HWZSet}(r)$.

PROOF: Reconsider $m = \lfloor r_1 \rfloor + 1$ as a natural number. There exists n such that $n \in \operatorname{HWZSet1}(r)$ and $n > m$ by (13), [7, (3)]. Consider n such that $n \in \operatorname{HWZSet1}(r)$ and $n > m$. □

(31) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $q \neq q_1$ and $a_2 \cdot (\operatorname{den} q) + b_2 \cdot (\operatorname{num} q) = 0$. Then $a_2 \cdot (\operatorname{den} q_1) + b_2 \cdot (\operatorname{num} q_1) \neq 0$.

(32) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$. Then there exists an element q of $\mathbb{Q}$ such that

(i) $\operatorname{den} q > \lfloor r_1 \rfloor + 1$, and

(ii) $q \in \operatorname{HWZSet}(r)$, and

(iii) $a_2 \cdot (\operatorname{den} q) + b_2 \cdot (\operatorname{num} q) \neq 0$.

The theorem is a consequence of (30) and (31).

(33) Let us consider real numbers a_1, b_1, and integers n_1, d_1. Suppose $d_1 > 0$ and $|\frac{a_1}{b_1} + \frac{n_1}{d_1}| < \frac{1}{\sqrt{5} \cdot ({d_1}^2)}$. Then there exists a real number d such that

(i) $\frac{n_1}{d_1} = -\frac{a_1}{b_1} + \frac{d}{{d_1}^2}$, and

(ii) $|d| < \frac{1}{\sqrt{5}}$.

(34) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $\frac{a_1}{b_1}$ is irrational. Then there exist elements x, y of $\mathbb{Z}$ such that

(i) $|(\operatorname{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\operatorname{LF}(a_2, b_2, c_2))(x, y)| < \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$, and

(ii) $|(\operatorname{LF}(a_1, b_1, c_1))(x, y)| < \epsilon$.

The theorem is a consequence of (32), (15), (29), and (33).

(35) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $\frac{a_2}{b_2}$ is irrational. Then there exist elements x, y of $\mathbb{Z}$ such that

(i) $|(\operatorname{LF}(a_2, b_2, c_2))(x, y)| \cdot |(\operatorname{LF}(a_1, b_1, c_1))(x, y)| < \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$, and

(ii) $|(\operatorname{LF}(a_2, b_2, c_2))(x, y)| < \epsilon$.

The theorem is a consequence of (34).

(36) Suppose $\operatorname{ZeroPointSet}(\operatorname{LF}(a_1, b_1, c_1)) \neq \emptyset$. Then there exist elements x, y of $\mathbb{Z}$ such that $|(\operatorname{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\operatorname{LF}(a_2, b_2, c_2))(x, y)| \leqslant \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$. The theorem is a consequence of (7).

(37) Suppose ZeroPointSet(LF(a_2, b_2, c_2)) $\neq \emptyset$. Then there exist elements x, y of $\mathbb{Z}$ such that $|(\mathrm{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\mathrm{LF}(a_2, b_2, c_2))(x, y)| \leqslant \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$. The theorem is a consequence of (7).

(38) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $b_1 \neq 0$ and $\frac{a_1}{b_1}$ is rational. Then there exist elements x, y of $\mathbb{Z}$ such that $|(\mathrm{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\mathrm{LF}(a_2, b_2, c_2))(x, y)| \leqslant \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$. The theorem is a consequence of (15).

(39) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $b_2 \neq 0$ and $\frac{a_2}{b_2}$ is rational. Then there exist elements x, y of $\mathbb{Z}$ such that $|(\mathrm{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\mathrm{LF}(a_2, b_2, c_2))(x, y)| \leqslant \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$. The theorem is a consequence of (38).

(40) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$ and $b_1 = 0$. Then there exist elements x, y of $\mathbb{Z}$ such that $|(\mathrm{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\mathrm{LF}(a_2, b_2, c_2))(x, y)| \leqslant \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$. The theorem is a consequence of (35), (37), and (39).

(41) Suppose $|a_1 \cdot b_2 - a_2 \cdot b_1| \neq 0$. Then there exist elements x, y of $\mathbb{Z}$ such that $|(\mathrm{LF}(a_1, b_1, c_1))(x, y)| \cdot |(\mathrm{LF}(a_2, b_2, c_2))(x, y)| \leqslant \frac{|a_1 \cdot b_2 - a_2 \cdot b_1|}{4}$. The theorem is a consequence of (34), (36), (40), and (38).

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

[3] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 6th edition, 2008.

[4] Adolf Hurwitz. Ueber die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche. *Mathematische Annalen*, 39(2):279–284, B.G.Teubner Verlag, Leipzig, 1891.

[5] Hermann Minkowski. *Diophantische Approximationen: eine Einführung in die Zahlentheorie*. Teubner, Leipzig, 1907.

[6] Ivan Niven. *Diophantine Approximation*. Dover, 2008.

[7] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.

[8] Yasushige Watase. Introduction to Diophantine approximation. *Formalized Mathematics*, 23(**2**):101–106, 2015. doi:10.1515/forma-2015-0010.

Received November 29, 2017

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

FORMALIZED MATHEMATICS
Vol. 25, No. 4, Pages 289–313, 2017
DOI: 10.1515/forma-2017-0028

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

Tarski Geometry Axioms. Part III

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

Adam Grabowski
Institute of Informatics
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. After we prepared some introductory formal framework in our two previous Mizar articles, we focus on the regular translation of underlying items faithfully following the abovementioned book (our encoding covers first seven chapters). Our development utilizes also other formalization efforts of the same topic, e.g. Isabelle/HOL by Makarios, Metamath or even proof objects obtained directly from Prover9.

In addition, using the native Mizar constructions (cluster registrations) the propositions ("Satz") are reformulated under weaker conditions, i.e. by using fewer axioms or by proposing an alternative version that uses just another axioms (ex. Satz 2.1 or Satz 2.2).

MSC: 51A05 51M04 03B35

Keywords: Tarski's geometry axioms; foundations of geometry; Euclidean plane

MML identifier: GTARSKI3, version: 8.1.06 5.45.1311

0. Introduction

Some chapters of the book "Metamathematische Methoden in der Geometrie" by W. Schwabhäuser, W. Szmielew, and A. Tarski (SST) [12] have been formalized within the classical two-valued logic with proof checkers: Isabelle/HOL by Makarios [7, 8] (Chapter 2 and 3), Metamath (Chapters 2 to 6), Mizar ([11, 3], [5]) or by means of Coq [10, 2]. Some of the results were obtained with the help of other automatic proof assistants, either partially [4], or completely [1].

In the first part of this article, we use the Mizar system to systematically formalize Chapters 2 to 7 of the SST book.

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

In addition, using the native Mizar constructions (cluster registrations) the propositions ("Satz") are reformulated with fewer hypotheses, i.e. by using fewer number of axioms or by proposing an alternative version that uses just another axioms (e.g., Satz 2.1 or Satz 2.2).

The proposition "6.28 Satz" introduced by Beeson (*"This is used in Satz 11.4, but is never proved in the book, and belongs in Chapter 6, so we give it the name "Satz 6.28""* following Beeson[1]) has been added.

The proof of the 2 lemmas: 5.12 Lemma 3 and 4 were directly inspired by Narboux Lemma (see Thm. 26 from [11]) and "endofsegidand" from Metamath. One of the theorems was taken from [6].

In the following section, the equivalence between the simplified axiomatic system of Makarios [9] is proved with axioms defined in [11] and [3]. This equivalence has already been shown (by means of GeoCoq).

To recall using the notations of Makarios:

- Reflexivity axiom for equidistance (RE)

$$\forall_{a,b}\ ab \equiv ba$$

- Transitivity axiom for equidistance (TE)

$$\forall_{a,b,p,q,r,s}\ ab \equiv pq \wedge ab \equiv rs \Rightarrow pq \equiv rs$$

- Identity axiom for equidistance (IE)

$$\forall_{a,b,c}\ ab \equiv cc \Rightarrow a = b$$

- Axiom of segment construction (SC)

$$\forall_{a,b,c,q} \exists_x\ \mathrm{B}qax \wedge ax \equiv bc$$

- Five-segments axiom (FS)

$$\forall_{a,b,c,d,a',b',c',d'}\ a \neq b \wedge \mathrm{B}abc \wedge \mathrm{B}a'b'c' \wedge ab \equiv a'b' \wedge bc \equiv b'c' \wedge ad \equiv a'd' \wedge$$

$$\wedge\ bd \equiv b'd' \ \Rightarrow\ cd \equiv c'd'$$

- Identity axiom for betweenness (IB)

$$\forall_{a,b}\ \mathrm{B}aba \Rightarrow a = b$$

[1] Tarski Formalization Project Archives maintained by Michael Beeson are available at `http://www.michaelbeeson.com/research/FormalTarski/index.php?include=archive6.php`

- Axiom of Pasch (IP)

$$\forall_{a,b,c,p,q}\ \mathrm{B}apc \wedge \mathrm{B}bqc \Rightarrow \exists_x \mathrm{B}pxb \wedge \mathrm{B}qxa$$

- Lower 2-dimensional axiom (LO_2)

$$\exists_{a,b,c}\ \neg\mathrm{B}abc \wedge \neg\mathrm{B}bca \wedge \neg\mathrm{B}cab$$

- Upper 2-dimensional axiom (Up_2)

$$\forall_{a,b,c,p,q}\ p \neq q \wedge ap \equiv aq \wedge bp \equiv bq \wedge cp \equiv cq \Rightarrow (\mathrm{B}abc \vee \mathrm{B}bca \vee \mathrm{B}cab)$$

- Euclidean axiom (Eu)

$$\forall_{a,b,c,d,t}\ \mathrm{B}adt\ \wedge\ \mathrm{B}bdc\ \wedge\ a \neq d\ \Rightarrow\ \exists_{x,y}\ \mathrm{B}abx\ \wedge\ \mathrm{B}acy\ \wedge\ \mathrm{B}xty$$

- Axiom of continuity (Co)

$$\forall_{X,Y}(\exists_a \forall_{x,y}\ x \in X \wedge y \in Y \Rightarrow \mathrm{B}axy) \Rightarrow (\exists_b \forall_{x,y}\ x \in X \wedge y \in Y \Rightarrow \mathrm{B}xby)$$

- (FS')

$$\forall_{a,b,c,d,a',b',c',d'}\ a \neq b\ \wedge\ \mathrm{B}abc\ \wedge\ \mathrm{B}a'b'c'\ \wedge\ ab \equiv a'b'\ \wedge\ bc \equiv b'c' \wedge$$

$$\wedge\ ad \equiv a'd'\ \wedge\ bd \equiv b'd'\ \Rightarrow\ dc \equiv c'd'$$

We show that $\mathsf{CE}_2 = \{$(RE), (TE), (IE), (FS), (IB), (IP), (Lo_2), (Up_2), (Eu), (Co)$\}$ is equivalent to the system defined in [11] and [3].

Moreover, it can be shown that the real Euclidean plane is a model for the axiom system $\mathsf{CE}'_2 = \{$(TE), (IE), (SC), (FS'), (IB), (IP), (Lo_2), (Up_2), (Eu), (Co)$\}$ of the system proposed by Makarios.

Like Makarios we show the equivalence between CE_2 and CE'_2, but using less axioms, more particularly we show that

- $\{$(RE), (TE), (FS)$\} \vdash$ (FS')
- $\{$(TE), (IE), (SC), (FS')$\} \vdash$ (FS)

Additionally, we prove that

$$\{\text{(TE), (IE), (SC), (FS')}\} \vdash \text{(RE).}$$

We don't use (IB) and (IP).

1. Congruence Properties

From now on S denotes Tarski plane satisfying the axiom of congruence symmetry and the axiom of congruence equivalence relation, and a, b, c, d, e, f denote points of S.

Now we state the propositions:

(1) 2.1 Satz:
$\overline{ab} \cong \overline{ab}$.

(2) 2.1 Satz bis:
Let us consider Tarski plane S satisfying the axiom of congruence equivalence relation and the axiom of segment construction, and points a, b of S. Then $\overline{ab} \cong \overline{ab}$.

(3) 2.2 Satz:
If $\overline{ab} \cong \overline{cd}$, then $\overline{cd} \cong \overline{ab}$. The theorem is a consequence of (1).

(4) 2.2 Satz bis:
Let us consider Tarski plane S satisfying the axiom of congruence equivalence relation and the axiom of segment construction, and points a, b, c, d of S. If $\overline{ab} \cong \overline{cd}$, then $\overline{cd} \cong \overline{ab}$. The theorem is a consequence of (2).

(5) 2.3 Satz:
If $\overline{ab} \cong \overline{cd}$ and $\overline{cd} \cong \overline{ef}$, then $\overline{ab} \cong \overline{ef}$. The theorem is a consequence of (3).

(6) 2.4 Satz:
If $\overline{ab} \cong \overline{cd}$, then $\overline{ba} \cong \overline{cd}$. The theorem is a consequence of (5).

(7) 2.5 Satz:
If $\overline{ab} \cong \overline{cd}$, then $\overline{ab} \cong \overline{dc}$. The theorem is a consequence of (5).

(8) 2.8 Satz:
Let us consider Tarski plane S satisfying the axiom of congruence identity and the axiom of segment construction, and points a, b of S. Then $\overline{aa} \cong \overline{bb}$.

Let S be a Tarski plane. We say that S satisfies (A5) from SST if and only if

(Def. 1) for every points a, b, c, d, a', b', c', d' of S such that $a \neq b$ and b lies between a and c and b' lies between a' and c' and $\overline{ab} \cong \overline{a'b'}$ and $\overline{bc} \cong \overline{b'c'}$ and $\overline{ad} \cong \overline{a'd'}$ and $\overline{bd} \cong \overline{b'd'}$ holds $\overline{cd} \cong \overline{c'd'}$.

Now we state the proposition:

(9) S satisfies the axiom of SAS if and only if S satisfies (A5) from SST. The theorem is a consequence of (6) and (7).

One can check that every Tarski plane satisfying the axiom of congruence symmetry and the axiom of congruence equivalence relation which satisfies (A5)

from SST satisfies also the axiom of SAS and every Tarski plane satisfying the axiom of congruence symmetry and the axiom of congruence equivalence relation which satisfies the axiom of SAS satisfies also (A5) from SST.

Let S be a Tarski plane and a, b, c, d, a', b', c', d' be points of S. We say that AFS $\binom{a,\,b,\,c,\,d}{a',\,b',\,c',\,d'}$ if and only if

(Def. 2) b lies between a and c and b' lies between a' and c' and $\overline{ab} \cong \overline{a'b'}$ and $\overline{bc} \cong \overline{b'c'}$ and $\overline{ad} \cong \overline{a'd'}$ and $\overline{bd} \cong \overline{b'd'}$.

Now we state the proposition:

(10) Let us consider Tarski plane S satisfying the axiom of congruence symmetry, the axiom of congruence equivalence relation, and the axiom of SAS, and points a, b, c, d, a', b', c', d' of S. Suppose AFS $\binom{a,\,b,\,c,\,d}{a',\,b',\,c',\,d'}$ and $a \neq b$. Then $\overline{cd} \cong \overline{c'd'}$.

From now on S denotes Tarski plane satisfying the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of congruence identity, the axiom of segment construction, and the axiom of SAS and q, a, b, c, a', b', c', x_1, x_2 denote points of S. Now we state the propositions:

(11) 2.11 SATZ:
If b lies between a and c and b' lies between a' and c' and $\overline{ab} \cong \overline{a'b'}$ and $\overline{bc} \cong \overline{b'c'}$, then $\overline{ac} \cong \overline{a'c'}$. The theorem is a consequence of (6), (7), (8), and (3).

(12) 2.12 SATZ:
Suppose $q \neq a$. If a lies between q and x_1 and $\overline{ax_1} \cong \overline{bc}$ and a lies between q and x_2 and $\overline{ax_2} \cong \overline{bc}$, then $x_1 = x_2$. The theorem is a consequence of (3), (5), (1), and (11).

2. BETWEENNESS RELATION

Now we state the proposition:

(13) 3.1 SATZ:
Let us consider Tarski plane S satisfying the axiom of congruence identity and the axiom of segment construction, and points a, b of S. Then b lies between a and b.

From now on S denotes Tarski plane satisfying the axiom of congruence identity, the axiom of segment construction, the axiom of betweenness identity, and the axiom of Pasch and a, b, c, d denote points of S.

Now we state the propositions:

(14) 3.2 SATZ:
If b lies between a and c, then b lies between c and a. The theorem is

a consequence of (13).

(15) 3.3 Satz:
a lies between a and b.

(16) 3.4 Satz:
Let us consider Tarski plane S satisfying the axiom of betweenness identity and the axiom of Pasch, and points a, b, c of S. If b lies between a and c and a lies between b and c, then $a = b$.

From now on S denotes Tarski plane satisfying seven Tarski's geometry axioms and a, b, c, d denote points of S. Now we state the propositions:

(17) 3.5 Satz:
If b lies between a and d and c lies between b and d, then b lies between a and c and c lies between a and d.

(18) 3.6 Satz:
If b lies between a and c and c lies between a and d, then c lies between b and d and b lies between a and d.

(19) 3.7 Satz:
If b lies between a and c and c lies between b and d and $b \neq c$, then c lies between a and d and b lies between a and d.

Let S be a Tarski plane and a, b, c, d be points of S.

We say that between4(a, b, c, d) if and only if

(Def. 3) b lies between a and c and b lies between a and d and c lies between a and d and c lies between b and d.

Let S be a Tarski plane and a, b, c, d, e be points of S. We say that between5(a, b, c, d, e) if and only if

(Def. 4) b lies between a and c and b lies between a and d and b lies between a and e and c lies between a and d and c lies between a and e and d lies between a and e and c lies between b and d and c lies between b and e and d lies between b and e and d lies between c and e.

From now on S denotes Tarski plane satisfying the axiom of congruence identity, the axiom of segment construction, the axiom of betweenness identity, and the axiom of Pasch and a, b, c, d, e denote points of S.

Now we state the propositions:

(20) 3.9 Satz (N = 3):
If b lies between a and c, then b lies between c and a.

(21) 3.9 Satz (N = 4):
If between4(a, b, c, d), then between4(d, c, b, a).

(22) 3.9 Satz (N = 5):
If between5(a, b, c, d, e), then between5(e, d, c, b, a).

(23) 3.10 SATZ (N = 4):
Let us consider Tarski plane S satisfying the axiom of congruence identity, the axiom of segment construction, the axiom of betweenness identity, and the axiom of Pasch, and points a, b, c, d of S. Suppose between4(a, b, c, d). Then

(i) b lies between a and c, and

(ii) b lies between a and d, and

(iii) c lies between a and d, and

(iv) c lies between b and d.

(24) 3.10 SATZ (N = 5):
Suppose between5(a, b, c, d, e). Then

(i) b lies between a and c, and

(ii) b lies between a and d, and

(iii) b lies between a and e, and

(iv) c lies between a and d, and

(v) c lies between a and e, and

(vi) d lies between a and e, and

(vii) c lies between b and d, and

(viii) c lies between b and e, and

(ix) d lies between b and e, and

(x) d lies between c and e, and

(xi) between4(a, b, c, d), and

(xii) between4(a, b, c, e), and

(xiii) between4(a, c, d, e), and

(xiv) between4(b, c, d, e).

From now on S denotes Tarski plane satisfying seven Tarski's geometry axioms and a, b, c, d, p denote points of S. Now we state the propositions:

(25) 3.11 SATZ (N = 3, L = 1):
If b lies between a and c and p lies between a and b, then between4(a, p, b, c).

(26) 3.11 SATZ (N = 3, L = 2):
If b lies between a and c and p lies between b and c, then between4(a, b, p, c).

(27) 3.11 SATZ (N = 3, L = 1):
If between4(a, b, c, d) and p lies between a and b, then between5(a, p, b, c, d).

(28) 3.11 SATZ (N = 3, L = 2):
If between4(a, b, c, d) and p lies between b and c, then between5(a, b, p, c, d).

(29) 3.11 Satz (n = 3, l = 3):
If between4(a, b, c, d) and p lies between c and d, then between5(a, b, c, p, d).

(30) 3.12 Satz (n = 3, l = 1):
If b lies between a and c and c lies between a and p, then between4(a, b, c, p) and if $a \neq c$, then between4(a, b, c, p).

(31) 3.12 Satz (n = 3, l = 2):
If b lies between a and c and c lies between b and p, then c lies between b and p and if $b \neq c$, then between4(a, b, c, p).

(32) 3.12 Satz (n = 4, l = 1):
If between4(a, b, c, d) and d lies between a and p, then between5(a, b, c, d, p) and if $a \neq d$, then between5(a, b, c, d, p).

(33) 3.12 Satz (n = 4, l = 2):
If between4(a, b, c, d) and d lies between b and p, then between4(b, c, d, p) and if $b \neq d$, then between5(a, b, c, d, p).

(34) 3.12 Satz (n = 4, l = 3):
If between4(a, b, c, d) and d lies between c and p, then d lies between c and p and if $c \neq d$, then between5(a, b, c, d, p).

Let us note that there exists Tarski plane satisfying seven Tarski's geometry axioms which satisfies Lower Dimension Axiom. Now we state the propositions:

(35) 3.13 Satz:
Let us consider Tarski plane S satisfying the axiom of congruence identity, the axiom of segment construction, and Lower Dimension Axiom. Then there exist points a, b, c of S such that

(i) b does not lie between a and c, and

(ii) c does not lie between b and a, and

(iii) a does not lie between c and b, and

(iv) $a \neq b$, and

(v) $b \neq c$, and

(vi) $c \neq a$.

The theorem is a consequence of (13).

(36) 3.14 Satz:
Let us consider Tarski plane S satisfying the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of congruence identity, the axiom of segment construction, and Lower Dimension Axiom, and points a, b of S. Then there exists a point c of S such that

(i) b lies between a and c, and

(ii) $b \neq c$.

The theorem is a consequence of (35) and (3).

(37) 3.15 SATZ (N = 3):
Let us consider Tarski plane S satisfying the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of congruence identity, the axiom of segment construction, the axiom of betweenness identity, and Lower Dimension Axiom, and points a_1, a_2 of S. Suppose $a_1 \neq a_2$. Then there exists a point a_3 of S such that

(i) a_2 lies between a_1 and a_3, and

(ii) a_1, a_2, a_3 are mutually different.

The theorem is a consequence of (36).

(38) 3.15 SATZ (N = 4):
Let us consider Tarski plane S satisfying seven Tarski's geometry axioms and Lower Dimension Axiom, and points a_1, a_2 of S. Suppose $a_1 \neq a_2$. Then there exist points a_3, a_4 of S such that

(i) between4(a_1, a_2, a_3, a_4), and

(ii) a_1, a_2, a_3, a_4 are mutually different.

The theorem is a consequence of (37).

(39) 3.15 SATZ (N = 5):
Let us consider Tarski plane S satisfying seven Tarski's geometry axioms and Lower Dimension Axiom, and points a_1, a_2 of S. Suppose $a_1 \neq a_2$. Then there exist points a_3, a_4, a_5 of S such that

(i) between5$(a_1, a_2, a_3, a_4, a_5)$, and

(ii) a_1,a_2,a_3,a_4,a_5 are mutually different.

The theorem is a consequence of (38) and (37).

(40) 3.17 SATZ:
Let us consider Tarski plane S satisfying seven Tarski's geometry axioms, and points a, b, c, p, a', b', c' of S. Suppose b lies between a and c and b' lies between a' and c and p lies between a and a'. Then there exists a point q of S such that

(i) q lies between p and c, and

(ii) q lies between b and b'.

The theorem is a consequence of (14).

3. Collinearity

Let S be a Tarski plane and a, b, c, d, a', b', c', d' be points of S. We say that IFS $\binom{a,\,b,\,c,\,d}{a',\,b',\,c',\,d'}$ if and only if

(Def. 5) b lies between a and c and b' lies between a' and c' and $\overline{ac} \cong \overline{a'c'}$ and $\overline{bc} \cong \overline{b'c'}$ and $\overline{ad} \cong \overline{a'd'}$ and $\overline{cd} \cong \overline{c'd'}$.

From now on S denotes Tarski plane satisfying seven Tarski's geometry axioms and a, b, c, d, a', b', c', d' denote points of S.

Now we state the propositions:

(41) 4.2 Satz:
If IFS $\binom{a,\,b,\,c,\,d}{a',\,b',\,c',\,d'}$, then $\overline{bd} \cong \overline{b'd'}$. The theorem is a consequence of (3), (6), (7), and (14).

(42) 4.3 Satz:
If b lies between a and c and b' lies between a' and c' and $\overline{ac} \cong \overline{a'c'}$ and $\overline{bc} \cong \overline{b'c'}$, then $\overline{ab} \cong \overline{a'b'}$. The theorem is a consequence of (6), (8), (7), and (41).

(43) 4.5 Satz:
If b lies between a and c and $\overline{ac} \cong \overline{a'c'}$, then there exists b' such that b' lies between a' and c' and $\triangle abc \cong \triangle a'b'c'$. The theorem is a consequence of (3), (8), (13), (14), (11), and (12).

(44) 4.6 Satz:
If b lies between a and c and $\triangle abc \cong \triangle a'b'c'$, then b' lies between a' and c'. The theorem is a consequence of (43), (3), (5), (6), (1), (7), and (41).

(45) 4.11 Satz:
Let us consider Tarski plane S satisfying the axiom of congruence identity, the axiom of segment construction, the axiom of betweenness identity, and the axiom of Pasch, and points a, b, c of S. Suppose a, b and c are collinear. Then

(i) b, c and a are collinear, and

(ii) c, a and b are collinear, and

(iii) c, b and a are collinear, and

(iv) b, a and c are collinear, and

(v) a, c and b are collinear.

(46) 4.12 Satz:
Let us consider Tarski plane S satisfying the axiom of congruence identity and the axiom of segment construction, and points a, b of S. Then a, a and b are collinear.

(47) Let us consider Tarski plane S satisfying the axiom of congruence symmetry and the axiom of congruence equivalence relation, and points a, b, c, a', b', c' of S. Suppose $\triangle abc \cong \triangle a'b'c'$. Then $\triangle bca \cong \triangle b'c'a'$. The theorem is a consequence of (6) and (7).

(48) 4.13 SATZ:
Let us consider Tarski plane S satisfying seven Tarski's geometry axioms, and points a, b, c, a', b', c' of S. Suppose a, b and c are collinear and $\triangle abc \cong \triangle a'b'c'$. Then a', b' and c' are collinear. The theorem is a consequence of (47) and (44).

Let us consider Tarski plane S satisfying the axiom of congruence symmetry and the axiom of congruence equivalence relation and points a, b, c, a', b', c' of S. Now we state the propositions:

(49) If $\triangle bac \cong \triangle b'a'c'$, then $\triangle abc \cong \triangle a'b'c'$. The theorem is a consequence of (6) and (7).

(50) If $\triangle acb \cong \triangle a'c'b'$, then $\triangle abc \cong \triangle a'b'c'$. The theorem is a consequence of (6) and (7).

From now on S denotes Tarski plane satisfying seven Tarski's geometry axioms and a, b, c, d, a', b', c', d', p, q denote points of S.

Now we state the proposition:

(51) 4.14 SATZ:
If a, b and c are collinear and $\overline{ab} \cong \overline{a'b'}$, then there exists a point c' of S such that $\triangle abc \cong \triangle a'b'c'$. The theorem is a consequence of (3), (11), (14), (6), (7), (49), (43), and (50).

Let S be a Tarski plane and a, b, c, d, a', b', c', d' be points of S. We say that FS $\binom{a,\,b,\,c,\,d}{a',\,b',\,c',\,d'}$ if and only if

(Def. 6) a, b and c are collinear and $\triangle abc \cong \triangle a'b'c'$ and $\overline{ad} \cong \overline{a'd'}$ and $\overline{bd} \cong \overline{b'd'}$.

Now we state the propositions:

(52) 4.16 SATZ:
If FS $\binom{a,\,b,\,c,\,d}{a',\,b',\,c',\,d'}$ and $a \neq b$, then $\overline{cd} \cong \overline{c'd'}$. The theorem is a consequence of (44), (47), (41), (14), and (49).

(53) 4.17 SATZ:
If $a \neq b$ and a, b and c are collinear and $\overline{ap} \cong \overline{aq}$ and $\overline{bp} \cong \overline{bq}$, then $\overline{cp} \cong \overline{cq}$. The theorem is a consequence of (1) and (52).

(54) 4.18 SATZ:
If $a \neq b$ and a, b and c are collinear and $\overline{ac} \cong \overline{ac'}$ and $\overline{bc} \cong \overline{bc'}$, then $c = c'$. The theorem is a consequence of (53) and (3).

(55) 4.19 SATZ:
If c lies between a and b and $\overline{ac} \cong \overline{ac'}$ and $\overline{bc} \cong \overline{bc'}$, then $c = c'$. The

theorem is a consequence of (3), (14), and (54).

4. Line Segments

From now on S denotes Tarski plane satisfying seven Tarski's geometry axioms and a, b, c, d, e, f, a', b', c', d' denote points of S.

Now we state the propositions:

(56) 5.1 Satz:
If $a \neq b$ and b lies between a and c and b lies between a and d, then c lies between a and d or d lies between a and c.

(57) 5.2 Satz:
If $a \neq b$ and b lies between a and c and b lies between a and d, then c lies between b and d or d lies between b and c. The theorem is a consequence of (56).

(58) 5.3 Satz:
If b lies between a and d and c lies between a and d, then b lies between a and c or c lies between a and b. The theorem is a consequence of (13), (14), (3), and (57).

Let S be a Tarski plane and a, b, c, d be points of S. We say that $a, b \leqslant c, d$ if and only if

(Def. 7) there exists a point y of S such that y lies between c and d and $\overline{ab} \cong \overline{cy}$.

Now we state the propositions:

(59) 5.5 Satz:
$a, b \leqslant c, d$ if and only if there exists a point x of S such that b lies between a and x and $\overline{ax} \cong \overline{cd}$. The theorem is a consequence of (3), (51), (44), (6), and (7).

(60) 5.6 Satz:
If $a, b \leqslant c, d$ and $\overline{ab} \cong \overline{a'b'}$ and $\overline{cd} \cong \overline{c'd'}$, then $a', b' \leqslant c', d'$. The theorem is a consequence of (59), (51), (3), (5), and (44).

(61) 5.7 Satz:
$a, b \leqslant a, b$. The theorem is a consequence of (13) and (1).

(62) 5.8 Satz:
If $a, b \leqslant c, d$ and $c, d \leqslant e, f$, then $a, b \leqslant e, f$. The theorem is a consequence of (59), (3), (51), (44), and (5).

(63) 5.9 Satz:
If $a, b \leqslant c, d$ and $c, d \leqslant a, b$, then $\overline{ab} \cong \overline{cd}$. The theorem is a consequence of (59), (14), (3), (12), and (16).

(64) 5.10 SATZ:

(i) $a, b \leqslant c, d$, or

(ii) $c, d \leqslant a, b$.

The theorem is a consequence of (3), (59), (14), and (56).

(65) 5.11 SATZ:
$a, a \leqslant b, c$. The theorem is a consequence of (59).

(66) 5.12 LEMMA 1:
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, the axiom of congruence symmetry, and the axiom of congruence equivalence relation, and points a, b, c, d of S. If $a, b \leqslant c, d$, then $b, a \leqslant c, d$.

(67) 5.12 LEMMA 2:
If $a, b \leqslant c, d$, then $a, b \leqslant d, c$. The theorem is a consequence of (59) and (7).

(68) 5.12 LEMMA 3:
If b lies between a and c and $\overline{ac} \cong \overline{ab}$, then $c = b$. The theorem is a consequence of (14), (6), (3), (7), (44), and (16).

(69) 5.12 LEMMA 4:
If c lies between a and b and $a, b \leqslant a, c$, then $b = c$. The theorem is a consequence of (59) and (68).

(70) 5.12 SATZ:
If a, b and c are collinear, then b lies between a and c iff $a, b \leqslant a, c$ and $b, c \leqslant a, c$. The theorem is a consequence of (1), (14), (6), (67), (69), and (13).

5. LINES AND HALFLINES

Let S be a Tarski plane and a, b, p be points of S. We say that $a \tilde{p} b$ if and only if

(Def. 8) $p \neq a$ and $p \neq b$ and (a lies between p and b or b lies between p and a).

From now on p denotes a point of S. Now we state the proposition:

(71) 6.2 SATZ:
If $a \neq p$ and $b \neq p$ and $c \neq p$ and p lies between a and c, then p lies between b and c iff $a \tilde{p} b$. The theorem is a consequence of (14) and (57).

(72) 6.3 SATZ:
$a \tilde{p} b$ if and only if $a \neq p$ and $b \neq p$ and there exists c such that $c \neq p$

and p lies between a and c and p lies between b and c. The theorem is a consequence of (3) and (71).

(73) 6.4 Satz:
$a \mathrel{\tilde{p}} b$ if and only if a, p and b are collinear and p does not lie between a and b. The theorem is a consequence of (14), (16), and (13).

(74) 6.5 Satz:
If $a \neq p$, then $a \mathrel{\tilde{p}} a$.

(75) 6.6 Satz:
If $a \mathrel{\tilde{p}} b$, then $b \mathrel{\tilde{p}} a$.

(76) 6.7 Satz:
If $a \mathrel{\tilde{p}} b$ and $b \mathrel{\tilde{p}} c$, then $a \mathrel{\tilde{p}} c$.

(77) METAMATH, segcon2:
There exists a point x of S such that

(i) a lies between p and x or x lies between p and a, and

(ii) $\overline{px} \cong \overline{bc}$.

The theorem is a consequence of (3), (14), and (57).

In the sequel r denotes a point of S. Now we state the proposition:

(78) 6.11 Satz a):
If $r \neq a$ and $b \neq c$, then there exists a point x of S such that $x \mathrel{\tilde{a}} r$ and $\overline{ax} \cong \overline{bc}$. The theorem is a consequence of (77) and (3).

Let S be a Tarski plane and a, p be points of S. The functor HalfLine(p, a) yielding a set is defined by the term

(Def. 9) $\{x$, where x is a point of $S : x \mathrel{\tilde{p}} a\}$.

From now on x, y denote points of S. Now we state the propositions:

(79) 6.11 Satz b):
If $r \neq a$ and $b \neq c$ and $x \mathrel{\tilde{a}} r$ and $\overline{ax} \cong \overline{bc}$ and $y \mathrel{\tilde{a}} r$ and $\overline{ay} \cong \overline{bc}$, then $x = y$. The theorem is a consequence of (72), (14), (12), and (57).

(80) 6.13 Satz:
If $a \mathrel{\tilde{p}} b$, then $p, a \leqslant p, b$ iff a lies between p and b. The theorem is a consequence of (1), (79), and (70).

Let S be a non empty Tarski plane and p, q be points of S. The functor Line(p, q) yielding a subset of S is defined by the term

(Def. 10) $\{x$, where x is a point of $S : p$, q and x are collinear$\}$.

In the sequel S denotes a non empty Tarski plane satisfying seven Tarski's geometry axioms and p, q, r, s denote points of S.

Now we state the proposition:

(81) 6.15 SATZ:

If $p \neq q$ and $p \neq r$ and p lies between q and r, then $\mathrm{Line}(p,q) = (\mathrm{HalfLine}(p,q) \cup \{p\}) \cup \mathrm{HalfLine}(p,r)$. The theorem is a consequence of (14), (57), and (13).

Let S be a non empty Tarski plane and A be a subset of S. We say that A is a line if and only if

(Def. 11) there exist points p, q of S such that $p \neq q$ and $A = \mathrm{Line}(p,q)$.

Now we state the proposition:

(82) 6.16 SATZ:

If $p \neq q$ and $s \neq p$ and $s \in \mathrm{Line}(p,q)$, then $\mathrm{Line}(p,q) = \mathrm{Line}(p,s)$. The theorem is a consequence of (56), (14), (58), and (57).

In the sequel 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 and a, b, p, q denote points of S.

Now we state the proposition:

(83) 6.17 SATZ:

(i) $p, q \in \mathrm{Line}(p,q)$, and

(ii) $\mathrm{Line}(p,q) = \mathrm{Line}(q,p)$.

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

In the sequel S denotes a non empty Tarski plane satisfying seven Tarski's geometry axioms, A, B denote subsets of S, and a, b, c, p, q, r, s denote points of S.

Now we state the proposition:

(84) Let us consider Tarski plane S satisfying seven Tarski's geometry axioms, and elements a, b, c of S. Then $a \neq b$ and a, b and c are collinear if and only if c lies on the line passing through a and b.

Let us consider a non empty Tarski plane S satisfying seven Tarski's geometry axioms and points a, b, x, y of S. Now we state the propositions:

(85) If the line passing through a and b is equal to the line passing through x and y, then $\mathrm{Line}(a,b) = \mathrm{Line}(x,y)$. The theorem is a consequence of (84).

(86) If $a \neq b$ and $x \neq y$ and $\mathrm{Line}(a,b) = \mathrm{Line}(x,y)$, then the line passing through a and b is equal to the line passing through x and y.

(87) 6.18 SATZ:

If A is a line and $a \neq b$ and $a, b \in A$, then $A = \mathrm{Line}(a,b)$. The theorem is a consequence of (85).

(88) 6.19 SATZ:

If $a \neq b$ and A is a line and $a, b \in A$ and B is a line and $a, b \in B$, then $A = B$. The theorem is a consequence of (87).

(89) 6.21 Satz:
If A is a line and B is a line and $A \neq B$ and $a \in A$ and $a \in B$ and $b \in A$ and $b \in B$, then $a = b$.

(90) 6.23 Satz:
If there exists p and there exists q such that $p \neq q$, then a, b and c are collinear iff there exists A such that A is a line and a, b, $c \in A$. The theorem is a consequence of (87) and (13).

(91) 6.24 Satz:
Let us consider Tarski plane S satisfying (A8). Then there exist points a, b, c of S such that a, b and c are not collinear.

(92) 6.25 Satz:
Let us consider a non empty Tarski plane S satisfying seven Tarski's geometry axioms, and points a, b of S. Suppose S satisfies (A8) and $a \neq b$. Then there exists a point c of S such that a, b and c are not collinear. The theorem is a consequence of (91), (13), and (87).

(93) Let us consider Tarski plane S satisfying seven Tarski's geometry axioms, and points p, a, b of S. If $a \overset{\cong}{p} b$ and $p, a \leqslant p, b$, then a lies between p and b.

(94) Let us consider Tarski plane S satisfying seven Tarski's geometry axioms, and elements a, b, c, d, e, f, g, h of S. Suppose $c, d \not\leqslant a, b$ and $\overline{ab} \cong \overline{ef}$ and $\overline{cd} \cong \overline{gh}$. Then $e, f \leqslant g, h$. The theorem is a consequence of (64) and (60).

(95) 6.28 Satz, introduced by Beeson:
Let us consider Tarski plane S satisfying seven Tarski's geometry axioms, and elements a, b, c, a_1, b_1, c_1 of S. Suppose $a \overset{\cong}{b} c$ and $a_1 \overset{\cong}{b_1} c_1$ and $\overline{ba} \cong \overline{b_1 a_1}$ and $\overline{bc} \cong \overline{b_1 c_1}$. Then $\overline{ac} \cong \overline{a_1 c_1}$. The theorem is a consequence of (7), (6), (42), (94), (93), and (14).

6. Point Reflection

Let S be a Tarski plane and a, b, m be points of S. We say that Middle(a, m, b) if and only if

(Def. 12) m lies between a and b and $\overline{ma} \cong \overline{mb}$.

From now on S denotes Tarski plane satisfying the axiom of congruence identity, the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of segment construction, the axiom of betweenness identity, and the axiom of Pasch and a, b, m denote points of S.

Now we state the proposition:

(96) 7.2 SATZ:
If Middle(a, m, b), then Middle(b, m, a).

From now on S denotes Tarski plane satisfying the axiom of congruence identity, the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of segment construction, and the axiom of betweenness identity and a, b, m denote points of S.

Now we state the propositions:

(97) 7.3 SATZ:
Middle(a, m, a) if and only if $m = a$.

(98) 7.4 EXISTENCE:
Let us consider a point p of S. Then there exists a point p' of S such that Middle(p, a, p'). The theorem is a consequence of (7), (3), and (97).

From now on S denotes Tarski plane satisfying the axiom of congruence identity, the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of segment construction, and the axiom of SAS and a denotes a point of S.

(99) 7.4 UNIQUENESS:
Let us consider points p, p_1, p_2 of S. If Middle(p, a, p_1) and Middle(p, a, p_2), then $p_1 = p_2$. The theorem is a consequence of (3) and (12).

Let S be Tarski plane satisfying the axiom of congruence identity, the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of segment construction, the axiom of betweenness identity, and the axiom of SAS and a, p be points of S. The functor $\mathrm{S}_a(p)$ yielding a point of S is defined by

(Def. 13) Middle(p, a, it).

From now on S denotes Tarski plane satisfying the axiom of congruence identity, the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of segment construction, the axiom of betweenness identity, and the axiom of SAS and a, p, p' denote points of S.

Now we state the proposition:

(100) 7.6 SATZ:
$\mathrm{S}_a(p) = p'$ if and only if Middle(p, a, p').

From now on S denotes Tarski plane satisfying the axiom of congruence identity, the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of segment construction, the axiom of betweenness identity, the axiom of SAS, and the axiom of Pasch and a, p, p' denote points of S.

Now we state the propositions:

(101) 7.7 Satz:
$\mathrm{S}_a((\mathrm{S}_a(p))) = p$. The theorem is a consequence of (14) and (3).

(102) 7.8 Satz:
There exists p such that $\mathrm{S}_a(p) = p'$. The theorem is a consequence of (101).

(103) 7.9 Satz:
If $\mathrm{S}_a(p) = \mathrm{S}_a(p')$, then $p = p'$. The theorem is a consequence of (101).

From now on S denotes Tarski plane satisfying the axiom of congruence identity, the axiom of congruence symmetry, the axiom of congruence equivalence relation, the axiom of segment construction, the axiom of betweenness identity, and the axiom of SAS and a, p denote points of S.

Now we state the proposition:

(104) 7.10 Satz:
$\mathrm{S}_a(p) = p$ if and only if $p = a$. The theorem is a consequence of (13) and (1).

From now on S denotes Tarski plane satisfying seven Tarski's geometry axioms and a, b, c, d, m, p, p', q, r, s denote points of S.

Now we state the propositions:

(105) 7.13 Satz:
$\overline{pq} \cong \overline{\mathrm{S}_a(p)\mathrm{S}_a(q)}$. The theorem is a consequence of (104), (14), (26), (28), (3), (6), (7), (11), (5), (1), and (41).

(106) 7.15 Satz:
q lies between p and r if and only if $\mathrm{S}_a(q)$ lies between $\mathrm{S}_a(p)$ and $\mathrm{S}_a(r)$. The theorem is a consequence of (101).

(107) 7.16 Satz:
$\overline{pq} \cong \overline{rs}$ if and only if $\overline{\mathrm{S}_a(p)\mathrm{S}_a(q)} \cong \overline{\mathrm{S}_a(r)\mathrm{S}_a(s)}$. The theorem is a consequence of (101).

(108) 7.17 Satz:
If $\mathrm{Middle}(p, a, p')$ and $\mathrm{Middle}(p, b, p')$, then $a = b$. The theorem is a consequence of (105), (101), (5), (6), (7), (55), and (104).

(109) 7.18 Satz:
If $\mathrm{S}_a(p) = \mathrm{S}_b(p)$, then $a = b$. The theorem is a consequence of (108).

(110) 7.19 Satz:
$\mathrm{S}_b((\mathrm{S}_a(p))) = \mathrm{S}_a((\mathrm{S}_b(p)))$ if and only if $a = b$. The theorem is a consequence of (106), (107), (101), (108), and (104).

(111) 7.20 Satz:
If a, m and b are collinear and $\overline{ma} \cong \overline{mb}$, then $a = b$ or $\mathrm{Middle}(a, m, b)$. The theorem is a consequence of (14), (13), (7), (6), (1), (42), and (3).

From now on S denotes a non empty Tarski plane satisfying seven Tarski's geometry axioms and a, b, c, d, p denote points of S.

Now we state the proposition:

(112) 7.21 SATZ:

Suppose a, b and c are not collinear and $b \neq d$ and $\overline{ab} \cong \overline{cd}$ and $\overline{bc} \cong \overline{da}$ and a, p and c are collinear and b, p and d are collinear. Then

(i) Middle(a, p, c), and

(ii) Middle(b, p, d).

The theorem is a consequence of (14), (51), (48), (7), (6), (3), (52), (13), (83), (88), and (111).

From now on a_1, a_2, b_1, b_2, m_1, m_2 denote points of S.

Now we state the propositions:

(113) 7.22 SATZ, PART 1:

Suppose c lies between a_1 and a_2 and c lies between b_1 and b_2 and $\overline{ca_1} \cong \overline{cb_1}$ and $\overline{ca_2} \cong \overline{cb_2}$ and Middle(a_1, m_1, b_1) and Middle(a_2, m_2, b_2) and $c, a_1 \leqslant c, a_2$. Then c lies between m_1 and m_2. The theorem is a consequence of (59), (3), (13), (1), (105), (104), (60), (14), (103), (56), (80), (106), (40), (107), (7), (6), (41), (53), and (108).

(114) 7.22 SATZ, PART 2:

Suppose c lies between a_1 and a_2 and c lies between b_1 and b_2 and $\overline{ca_1} \cong \overline{cb_1}$ and $\overline{ca_2} \cong \overline{cb_2}$ and Middle(a_1, m_1, b_1) and Middle(a_2, m_2, b_2) and $c, a_2 \leqslant c, a_1$. Then c lies between m_1 and m_2. The theorem is a consequence of (59), (3), (13), (14), (1), (105), (104), (60), (103), (56), (80), (106), (40), (107), (7), (6), (41), (53), and (108).

(115) 7.22 SATZ, KRIPPENLEMMA, (GUPTA 1965, 3.45 THEOREM):

Suppose c lies between a_1 and a_2 and c lies between b_1 and b_2 and $\overline{ca_1} \cong \overline{cb_1}$ and $\overline{ca_2} \cong \overline{cb_2}$ and Middle(a_1, m_1, b_1) and Middle(a_2, m_2, b_2). Then c lies between m_1 and m_2. The theorem is a consequence of (64), (113), and (114).

Let S be a Tarski plane and a_1, a_2, b_1, b_2, c, m_1, m_2 be points of S. We say that Krippenfigur$(a_1, m_1, b_1, c, b_2, m_2, a_2)$ if and only if

(Def. 14) c lies between a_1 and a_2 and c lies between b_1 and b_2 and $\overline{ca_1} \cong \overline{cb_1}$ and $\overline{ca_2} \cong \overline{cb_2}$ and Middle(a_1, m_1, b_1) and Middle(a_2, m_2, b_2).

Now we state the proposition:

(116) KRIPPENFIGUR:

If Krippenfigur$(a_1, m_1, b_1, c, b_2, m_2, a_2)$, then c lies between m_1 and m_2.

Let us observe that there exists Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms which is non empty.

In the sequel S denotes a non empty Tarski plane satisfying Lower Dimension Axiom and seven Tarski's geometry axioms and a, b, c, p, q, r denote points of S. Now we state the proposition:

(117) If $\overline{ca} \cong \overline{cb}$, then there exists a point x of S such that Middle(a, x, b). The theorem is a consequence of (14), (111), (13), (1), (36), (3), (7), (10), (6), (43), (41), (48), (88), (83), (87), and (53).

7. Note about Simplification of Tarski's Axioms of Geometry by Makarios

Let S be a Tarski plane. We say that S satisfies (RE) if and only if

(Def. 15) for every points a, b of S, $\overline{ab} \cong \overline{ba}$.

We say that S satisfies (TE) if and only if

(Def. 16) for every points a, b, p, q, r, s of S such that $\overline{ab} \cong \overline{pq}$ and $\overline{ab} \cong \overline{rs}$ holds $\overline{pq} \cong \overline{rs}$.

We say that S satisfies (IE) if and only if

(Def. 17) for every points a, b, c of S such that $\overline{ab} \cong \overline{cc}$ holds $a = b$.

We say that S satisfies (SC) if and only if

(Def. 18) for every points a, b, c, q of S, there exists a point x of S such that a lies between q and x and $\overline{ax} \cong \overline{bc}$.

We say that S satisfies (FS) if and only if

(Def. 19) for every points a, b, c, d, a', b', c', d' of S such that $a \neq b$ and b lies between a and c and b' lies between a' and c' and $\overline{ab} \cong \overline{a'b'}$ and $\overline{bc} \cong \overline{b'c'}$ and $\overline{ad} \cong \overline{a'd'}$ and $\overline{bd} \cong \overline{b'd'}$ holds $\overline{cd} \cong \overline{c'd'}$.

We say that S satisfies (IB) if and only if

(Def. 20) for every points a, b of S such that b lies between a and a holds $a = b$.

We say that S satisfies (IP) if and only if

(Def. 21) for every points a, b, c, p, q of S such that p lies between a and c and q lies between b and c there exists a point x of S such that x lies between p and b and x lies between q and a.

We say that S satisfies (Lo_2) if and only if

(Def. 22) there exist points a, b, c of S such that b does not lie between a and c and c does not lie between b and a and a does not lie between c and b.

We say that S satisfies (Up_2) if and only if

(Def. 23) for every points a, b, c, p, q of S such that $p \neq q$ and $\overline{ap} \cong \overline{aq}$ and $\overline{bp} \cong \overline{bq}$ and $\overline{cp} \cong \overline{cq}$ holds b lies between a and c or c lies between b and a or a lies between c and b.

We say that S satisfies (Eu) if and only if

(Def. 24) for every points a, b, c, d, t of S such that d lies between a and t and d lies between b and c and $a \neq d$ there exist points x, y of S such that b lies between a and x and c lies between a and y and t lies between x and y.

We say that S satisfies (Co) if and only if

(Def. 25) for every sets X, Y such that there exists a point a of S such that for every points x, y of S such that $x \in X$ and $y \in Y$ holds x lies between a and y there exists a point b of S such that for every points x, y of S such that $x \in X$ and $y \in Y$ holds b lies between x and y.

We say that S satisfies (FS') if and only if

(Def. 26) for every points a, b, c, d, a', b', c', d' of S such that $a \neq b$ and b lies between a and c and b' lies between a' and c' and $\overline{ab} \cong \overline{a'b'}$ and $\overline{bc} \cong \overline{b'c'}$ and $\overline{ad} \cong \overline{a'd'}$ and $\overline{bd} \cong \overline{b'd'}$ holds $\overline{dc} \cong \overline{c'd'}$.

In the sequel S denotes a Tarski plane. Now we state the propositions:

(118) S satisfies the axiom of congruence symmetry if and only if S satisfies (RE).

(119) S satisfies the axiom of congruence equivalence relation if and only if S satisfies (TE).

(120) S satisfies the axiom of congruence identity if and only if S satisfies (IE).

(121) S satisfies the axiom of segment construction if and only if S satisfies (SC).

(122) S satisfies the axiom of betweenness identity if and only if S satisfies (IB).

(123) S satisfies the axiom of Pasch if and only if S satisfies (IP).

(124) S satisfies Lower Dimension Axiom if and only if S satisfies (Lo_2).

(125) S satisfies Upper Dimension Axiom if and only if S satisfies (Up_2).

(126) S satisfies Euclid Axiom if and only if S satisfies (Eu).

(127) Let us consider Tarski plane S satisfying the axiom of congruence symmetry and the axiom of congruence equivalence relation. Then S satisfies the axiom of SAS if and only if S satisfies (FS).

(128) Let us consider a non empty Tarski plane S. Then S satisfies Continuity Axiom if and only if S satisfies (Co).

One can verify that every Tarski plane which satisfies (RE) satisfies also the axiom of congruence symmetry and every Tarski plane which satisfies (TE) satisfies also the axiom of congruence equivalence relation and every Tarski plane which satisfies (IE) satisfies also the axiom of congruence identity and every Tarski plane which satisfies (SC) satisfies also the axiom of segment construction.

Every Tarski plane which satisfies (IB) satisfies also the axiom of betweenness identity and every Tarski plane which satisfies (IP) satisfies also the axiom of Pasch and every Tarski plane which satisfies (Lo_2) satisfies also Lower Dimension Axiom and every Tarski plane which satisfies (Up_2) satisfies also Upper Dimension Axiom and every Tarski plane which satisfies (Eu) satisfies also Euclid Axiom.

Every Tarski plane which satisfies (Co) satisfies also Continuity Axiom and every Tarski plane which satisfies the axiom of congruence symmetry satisfies also (RE) and every Tarski plane which satisfies the axiom of congruence equivalence relation satisfies also (TE) and every Tarski plane which satisfies the axiom of congruence identity satisfies also (IE) and every Tarski plane which satisfies the axiom of segment construction satisfies also (SC) and every Tarski plane which satisfies the axiom of betweenness identity satisfies also (IB). Every Tarski plane which satisfies the axiom of Pasch satisfies also (IP) and every Tarski plane which satisfies Lower Dimension Axiom satisfies also (Lo_2) and every Tarski plane which satisfies Upper Dimension Axiom satisfies also (Up_2) and every Tarski plane which satisfies Euclid Axiom satisfies also (Eu) and every non empty Tarski plane which satisfies Continuity Axiom satisfies also (Co) and there exists a Tarski plane which satisfies (RE) and (TE).

(129) Let us consider Tarski plane S satisfying (RE) and (TE). Then S satisfies the axiom of SAS if and only if S satisfies (FS).

One can check that every Tarski plane satisfying (RE) and (TE) which satisfies (FS) satisfies also the axiom of SAS and there exists Tarski plane satisfying (RE) and (TE) which satisfies (FS).

From now on S denotes a Tarski plane. Now we state the propositions:

(130) Makarios, Lemma 6:
Let us consider a Tarski plane S. Suppose S satisfies (RE) and (TE). Then S satisfies (FS) if and only if S satisfies (FS').

(131) Let us consider Tarski plane S satisfying (RE) and (TE). Then S satisfies (FS) if and only if S satisfies (FS').

Let us note that every Tarski plane satisfying (RE) and (TE) which satisfies (FS') satisfies also (FS) and there exists a Tarski plane which satisfies (TE) and (SC) and there exists Tarski plane satisfying (RE) and (TE) which satisfies (FS') and there exists Tarski plane satisfying (RE), (TE), and (FS') which satisfies (SC). Now we state the propositions:

(132) Let us consider Tarski plane S satisfying (TE) and (SC), and points a, b of S. Then $\overline{ab} \cong \overline{ab}$.

(133) Let us consider Tarski plane S satisfying (IE) and (SC), and points a, b of S. Then b lies between a and b.

(134) Let us consider Tarski plane S satisfying (TE) and (SC), and points a, b, c, d of S. If $\overline{ab} \cong \overline{cd}$, then $\overline{cd} \cong \overline{ab}$.

(135) Let us consider Tarski plane S satisfying (TE), (SC), and (FS'), and points a, b, c, d, e, f of S. Suppose $a \neq b$ and a lies between b and c and a lies between d and e and $\overline{ba} \cong \overline{da}$ and $\overline{ac} \cong \overline{ae}$ and $\overline{bf} \cong \overline{df}$. Then $\overline{fc} \cong \overline{ef}$. The theorem is a consequence of (2).

Let S be a Tarski plane. We say that S satisfies (RE') if and only if

(Def. 27) for every points a, b, c, d of S such that $a \neq b$ and a lies between b and c holds $\overline{dc} \cong \overline{cd}$.

Now we state the proposition:

(136) Every Tarski plane satisfying (TE), (SC), and (FS') satisfies (RE'). The theorem is a consequence of (2) and (135).

Let us note that every Tarski plane which satisfies (TE), (SC), and (FS') satisfies also (RE') and there exists Tarski plane satisfying (IE) which satisfies (RE') and there exists Tarski plane satisfying (RE') and (IE) which satisfies (SC) and there exists a non empty Tarski plane satisfying (IE) which is trivial and there exists a non empty Tarski plane satisfying (IE) and (SC) which is trivial. Now we state the proposition:

(137) Every trivial, non empty Tarski plane satisfying (IE) and (SC) satisfies (RE). The theorem is a consequence of (8).

One can verify that there exists a non empty Tarski plane satisfying (TE), (IE), and (SC) which satisfies (RE'). Now we state the proposition:

(138) Every non empty Tarski plane satisfying (RE'), (TE), (IE), and (SC) satisfies (RE). The theorem is a consequence of (8), (13), and (4).

Note that there exists a non empty Tarski plane satisfying (TE), (IE), and (SC) which satisfies (FS'). Now we state the propositions:

(139) Every non empty Tarski plane satisfying (TE), (IE), (SC), and (FS') satisfies (RE).

(140) Every non empty Tarski plane satisfying (TE), (IE), (SC), and (FS') satisfies (FS). The theorem is a consequence of (138).

8. MAIN RESULTS AND COROLLARIES

Let us note that every Tarski plane which satisfies (RE), (TE), and (FS) satisfies also (FS') and every non empty Tarski plane which satisfies (TE), (IE), (SC), and (FS') satisfies also (FS) and every non empty Tarski plane which satisfies (TE), (IE), (SC), and (FS') satisfies also (RE) and every non empty Tarski plane which satisfies (TE), (IE), (SC), and (FS') satisfies also the axiom

of SAS and there exists a non empty Tarski plane which satisfies (RE), (TE), (IE), (SC), (FS), (IB), (IP), (Lo_2), (Up_2), (Eu), and (Co).

An axiomatic system CE_2 is a non empty Tarski plane satisfying (RE), (TE), (IE), (SC), (FS), (IB), (IP), (Lo_2), (Up_2), (Eu), and (Co).

An axiomatic system CE'_2 is a non empty Tarski plane satisfying (TE), (IE), (SC), (FS'), (IB), (IP), (Lo_2), (Up_2), (Eu), and (Co). Now we state the propositions:

(141) Every axiomatic system CE_2 is an axiomatic system CE'_2.

(142) Every axiomatic system CE'_2 is an axiomatic system CE_2.

(143) Every axiomatic system CE_2 satisfies seven Tarski's geometry axioms, Lower Dimension Axiom, Upper Dimension Axiom, Euclid Axiom, and Continuity Axiom.

(144) Every axiomatic system CE'_2 satisfies seven Tarski's geometry axioms, Lower Dimension Axiom, Upper Dimension Axiom, Euclid Axiom, and Continuity Axiom.

References

[1] 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.

[2] 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.

[3] Roland Coghetto and Adam Grabowski. Tarski geometry axioms – Part II. *Formalized Mathematics*, 24(**2**):157–166, 2016. doi:10.1515/forma-2016-0012.

[4] 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.

[5] 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.

[6] Haragauri Narayan Gupta. *Contributions to the Axiomatic Foundations of Geometry*. PhD thesis, University of California-Berkeley, 1965.

[7] 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.

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

[9] Timothy James McKenzie Makarios. A further simplification of Tarski's axioms of geometry. *Note di Matematica*, 33(2):123–132, 2014.

[10] 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.

[11] William Richter, Adam Grabowski, and Jesse Alama. Tarski geometry axioms. *Formalized Mathematics*, 22(**2**):167–176, 2014. doi:10.2478/forma-2014-0017.

[12] Wolfram Schwabhäuser, Wanda Szmielew, and Alfred Tarski. *Metamathematische Methoden in der Geometrie*. Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1983.

Received November 29, 2017

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

FORMALIZED MATHEMATICS
Vol. 25, No. 4, Pages 315–322, 2017
DOI: 10.1515/forma-2017-0029

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

The Matiyasevich Theorem. Preliminaries[1]

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Summary. In this article, we prove selected properties of Pell's equation that are essential to finally prove the Diophantine property of two equations. These equations are explored in the proof of Matiyasevich's negative solution of Hilbert's tenth problem.

MSC: 11D45 03B35

Keywords: Pell's equation; Diophantine equation; Hilbert's 10th problem

MML identifier: HILB10_1, version: 8.1.06 5.45.1311

0. Introduction

In this article, we prove, using the Mizar formalism, a number of properties that correspond to the Pell's Equation to prove finally two basic lemmas that are essential in the proof of Matiyasevich's negative solution of Hilbert's tenth problem.

For this purpose, first, we focus on a special case of the Pell's Equation, which has the form

$$x^2 - (a^2 - 1)y^2 = 1, \tag{0.1}$$

where $a > 1$ and integer numerical solutions are sought for x and y. We develop the Pell's Equation theory formalized for the general case in [1]. Note that $\mathtt{x}_a(0) = 1$, $\mathtt{y}_a(0) = 0$ is an obvious solution. Additionally, if we know a solution of the Pell's equation, we can determine all solutions as well as we can order

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

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

them. In our case the $n+1$-solution $\mathtt{x}_a(n+1)$, $\mathtt{y}_a(n+1)$ as shown Theorem 6 can be simply determined in terms of the n-solution as follows:

$$\begin{array}{rcl} \mathtt{x}_a(n+1) & = & a \cdot \mathtt{x}_a(n) + (a^2-1) \cdot \mathtt{y}_a(n) \\ \mathtt{y}_a(n+1) & = & \mathtt{x}_a(n) + a \cdot \mathtt{y}_a(n) \end{array} \tag{0.2}$$

We show a number of dependency between the elements of these sequences to provide that the equality $\mathtt{y}_a(z) = y$ is Diophantine. For this purpose we justify in Theorem 38 that for a given a, z, y holds $\mathtt{y}_a(z) = y$ if and only if the following system has a solution for natural numbers x, x_1, y_1, A, x_2, y_2:

$$\begin{array}{l} a > 1 \ \wedge \ y_1 \geqslant y \ \wedge \ A > y \ \wedge \ y \geqslant z \ \wedge \\ x^2 - (a^2-1)y^2 = 1 \ \wedge \ x_1^2 - (a^2-1)y_1^2 = 1 \ \wedge \\ x_2^2 - (A^2-1)y_2^2 = 1 \ \wedge \ y_2 \equiv y \bmod x_1 \ \wedge \ A \equiv a \bmod x_1 \ \wedge \\ y_2 \equiv z \bmod 2y \ \wedge \ A \equiv 1 \bmod 2y \ \wedge \ y_1 \equiv 0 \bmod y^2 \end{array} \tag{0.3}$$

Based on this result we prove in Theorem 39 that the equality $y = x^z$ is Diophantine. For this purpose we justify that for a given x, y, z that $y = x^z$ if and only if

$$\begin{array}{l} (y = 1 \wedge z = 0) \vee \\ (x = 0 \wedge y = 0 \wedge z > 0) \ \vee \ (x = 1 \wedge y = 1 \wedge z > 0) \vee \\ (x > 1 \wedge z > 0 \wedge \exists_{y_1,y_2,y_3,K \in \mathbb{N}} \\ \qquad y_1 = y_{z+1}(x) \wedge K > 2zy_1 \wedge y_2 = y_{z+1}(K) \wedge y_3 = y_{z+1}(Kx) \wedge \\ \qquad (0 \leqslant y - \frac{y_3}{y_2} < \frac{1}{2} \vee 0 \leqslant \frac{y_3}{y_2} - y < \frac{1}{2})). \end{array} \tag{0.4}$$

The formalization follows Z.Adamowicz, P.Zbierski [2] as well as M.Davis [3].

1. Preliminaries

From now on i, j, n, n_1, n_2, m, k, u denote natural numbers, r, r_1, r_2 denote real numbers, x, y denote integers, and a, b denote non trivial natural numbers.

Now we state the propositions:

(1) Let us consider a finite sequence F of elements of $\mathbb{N}$. Suppose for every k such that $1 < k \leqslant \operatorname{len} F$ holds $F(k) \bmod n = 0$. Then $\sum F \bmod n = F(1) \bmod n$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence F of elements of $\mathbb{N}$ such that $\operatorname{len} F = \$_1$ and for every k such that $1 < k \leqslant \operatorname{len} F$ holds $F(k) \bmod n = 0$ holds $\sum F \bmod n = F(1) \bmod n$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. $\square$

(2) Let us consider a complex-valued finite sequence f. Then there exist complex-valued finite sequences e, o such that

(i) $\operatorname{len} e = \lfloor \frac{\operatorname{len} f}{2} \rfloor$, and

(ii) $\operatorname{len} o = \lceil \frac{\operatorname{len} f}{2} \rceil$, and

(iii) $\sum f = \sum e + \sum o$, and

(iv) for every n, $e(n) = f(2 \cdot n)$ and $o(n) = f(2 \cdot n - 1)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every complex-valued finite sequence f such that $\operatorname{len} f = \$_1$ there exist complex-valued finite sequences e, o such that $\operatorname{len} e = \lfloor \frac{\operatorname{len} f}{2} \rfloor$ and $\operatorname{len} o = \lceil \frac{\operatorname{len} f}{2} \rceil$ and $\sum f = \sum e + \sum o$ and for every n, $e(n) = f(2 \cdot n)$ and $o(n) = f(2 \cdot n - 1)$. $\mathcal{P}[0]$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$. $\mathcal{P}[n]$. $\square$

Let us consider a. Let us observe that $a^{\mathbf{2}} -' 1$ is non square.

2. SOLUTIONS OF PELL'S EQUATION – SPECIAL CASE

Let a, n be natural numbers. Assume a is not trivial. The functor $\mathtt{x}_a(n)$ yielding a natural number is defined by

(Def. 1) for every non trivial natural number b such that $b = a$ there exists a natural number y such that
$it + y \cdot \sqrt{b^{\mathbf{2}} -' 1} = ((\text{the minimal Pell's solution of } (b^{\mathbf{2}} -' 1))_{\mathbf{1}} +$
$(\text{the minimal Pell's solution of } (b^{\mathbf{2}} -' 1))_{\mathbf{2}} \cdot \sqrt{b^{\mathbf{2}} -' 1})^n$.

Assume a is not trivial. The functor $\mathtt{y}_a(n)$ yielding a natural number is defined by

(Def. 2) for every non trivial natural number b such that $b = a$ holds $\mathtt{x}_b(n) + it \cdot \sqrt{b^{\mathbf{2}} -' 1} = ((\text{the minimal Pell's solution of } (b^{\mathbf{2}} -' 1))_{\mathbf{1}} +$
$(\text{the minimal Pell's solution of } (b^{\mathbf{2}} -' 1))_{\mathbf{2}} \cdot \sqrt{b^{\mathbf{2}} -' 1})^n$.

Now we state the propositions:

(3) (i) $\mathtt{x}_a(0) = 1$, and

(ii) $\mathtt{y}_a(0) = 0$.

(4) Suppose $\langle n_1, n_2 \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$. Then there exists n such that

(i) $n_1 = \mathtt{x}_a(n)$, and

(ii) $n_2 = \mathtt{y}_a(n)$.

The theorem is a consequence of (3).

(5) $\langle a, 1 \rangle =$ the minimal Pell's solution of $(a^{\mathbf{2}} -' 1)$.

(6) (i) $\mathtt{x}_a(n+1) = \mathtt{x}_a(n) \cdot a + \mathtt{y}_a(n) \cdot (a^{\mathbf{2}} -' 1)$, and

(ii) $\mathtt{y}_a(n+1) = \mathtt{x}_a(n) + \mathtt{y}_a(n) \cdot a$.

The theorem is a consequence of (5).

(7) $(\mathtt{x}_a(n))^{\mathbf{2}} - (a^{\mathbf{2}} -' 1) \cdot (\mathtt{y}_a(n))^{\mathbf{2}} = 1$. The theorem is a consequence of (3).

(8) (i) $\mathtt{x}_a(n) + \mathtt{y}_a(n) \cdot \sqrt{a^{\mathbf{2}} -' 1} = (a + \sqrt{a^{\mathbf{2}} -' 1})^n$, and

(ii) $\mathtt{x}_a(n) + -\mathtt{y}_a(n) \cdot \sqrt{a^{\mathbf{2}} -' 1} = (a - \sqrt{a^{\mathbf{2}} -' 1})^n$.

The theorem is a consequence of (5).

(9) There exist finite sequences F_2, F_1 of elements of $\mathbb{N}$ such that

(i) $\sum F_2 = \mathtt{y}_a(n)$, and

(ii) $\operatorname{len} F_2 = \lfloor \frac{n+1}{2} \rfloor$, and

(iii) for every i such that $1 \leqslant i \leqslant \frac{n+1}{2}$ holds $F_2(i) = \binom{n}{2 \cdot i -' 1} \cdot (a^{n+1-'2 \cdot i}) \cdot (a^{\mathbf{2}} -' 1)^{i-'1}$, and

(iv) $a^n + \sum F_1 = \mathtt{x}_a(n)$, and

(v) $\operatorname{len} F_1 = \lfloor \frac{n}{2} \rfloor$, and

(vi) for every i such that $1 \leqslant i \leqslant \frac{n}{2}$ holds $F_1(i) = \binom{n}{2 \cdot i} \cdot (a^{n-'2 \cdot i}) \cdot (a^{\mathbf{2}} -' 1)^i$.

PROOF: Set $A = a^{\mathbf{2}} -' 1$. Define $\mathcal{P}[\text{natural number}] \equiv$ there exist finite sequences F_2, F_1 of elements of $\mathbb{N}$ such that $\sum F_2 = \mathtt{y}_a(\$_1)$ and $\operatorname{len} F_2 = \lfloor \frac{\$_1+1}{2} \rfloor$ and for every natural number i such that $1 \leqslant i \leqslant \frac{\$_1+1}{2}$ holds $F_2(i) = \binom{\$_1}{2 \cdot i -' 1} \cdot (a^{\$_1+1-'2 \cdot i}) \cdot (A^{i-'1})$ and $a^{\$_1} + \sum F_1 = \mathtt{x}_a(\$_1)$ and $\operatorname{len} F_1 = \lfloor \frac{\$_1}{2} \rfloor$ and for every natural number i such that $1 \leqslant i \leqslant \frac{\$_1}{2}$ holds $F_1(i) = \binom{\$_1}{2 \cdot i} \cdot (a^{\$_1-'2 \cdot i}) \cdot (A^i)$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every n, $\mathcal{P}[n]$. □

3. Solutions of Pell's Equation – Inequalities

Now we state the proposition:

(10) If $k \leqslant n$, then $\mathtt{x}_a(k) \leqslant \mathtt{x}_a(n)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \mathtt{x}_a(k) \leqslant \mathtt{x}_a(k + \$_1)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$ by (6), [6, (29)]. $\mathcal{P}[n_1]$. □

Let us consider a and k. One can verify that $\mathtt{x}_a(k)$ is positive.

Now we state the propositions:

(11) If $k < n$, then $\mathtt{y}_a(k) < \mathtt{y}_a(n)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 > 0$, then $\mathtt{y}_a(k) < \mathtt{y}_a(k + \$_1)$. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i+1]$. $\mathcal{P}[n_1]$. □

(12) If $\mathtt{y}_a(k) = \mathtt{y}_a(n)$, then $k = n$. The theorem is a consequence of (11).

(13) $\mathtt{y}_a(n) \geqslant n$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \mathtt{y}_a(\$_1) \geqslant \$_1$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$. $\mathcal{P}[k]$. □

Let us consider a. Let k be a non zero natural number. Observe that $\mathtt{y}_a(k)$ is non zero.

Let a be a non trivial natural number and x be a positive natural number. Note that $a \cdot x$ is non trivial.

Now we state the propositions:

(14) If $a \neq 2$ and $k \leqslant n$, then $2 \cdot (\mathtt{y}_a(k)) < \mathtt{x}_a(n)$. The theorem is a consequence of (7) and (10).

(15) If $a = 2$ and $k \leqslant n$, then $\sqrt{3} \cdot (\mathtt{y}_a(k)) < \mathtt{x}_a(n)$. The theorem is a consequence of (7) and (10).

(16) If $a = 2$ and $k < n$, then $(3 + 2 \cdot \sqrt{3}) \cdot \mathtt{y}_a(k) < \mathtt{x}_a(n)$. The theorem is a consequence of (6) and (15).

(17) (i) $(2 \cdot a - 1)^n \cdot (a - 1) \leqslant \mathtt{x}_a(n + 1) \leqslant a \cdot (2 \cdot a)^n$, and

(ii) $(2 \cdot a - 1)^n \leqslant \mathtt{y}_a(n + 1) \leqslant 2 \cdot a^n$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv (2 \cdot a - 1)^{\$_1} \leqslant \mathtt{y}_a(\$_1 + 1) \leqslant 2 \cdot a^{\$_1}$ and $(2 \cdot a - 1)^{\$_1} \cdot (a-1) \leqslant \mathtt{x}_a(\$_1+1) \leqslant a \cdot (2 \cdot a^{\$_1})$. $\mathtt{y}_a(0) = 0$ and $\mathtt{x}_a(0) = 1$. $\mathtt{y}_a(1 + 0) = 1 + 0 \cdot a$ and $\mathtt{x}_a(1 + 0) = 1 \cdot a + 0 \cdot (a^{\mathbf{2}} -' 1)$. If $\mathcal{P}[k]$, then $\mathcal{P}[k + 1]$. $\mathcal{P}[k]$. $\square$

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

(18) $x^n \cdot (1 - \frac{1}{2 \cdot a \cdot x})^n \leqslant \frac{\mathtt{y}_{a \cdot x}(n+1)}{\mathtt{y}_a(n+1)} \leqslant x^n \cdot \frac{1}{(1 - \frac{1}{2 \cdot a})^n}$. The theorem is a consequence of (17).

(19) If $a > 2 \cdot n \cdot x^n$, then $x^n - \frac{1}{2} < \frac{\mathtt{y}_{a \cdot x}(n+1)}{\mathtt{y}_a(n+1)} < x^n + \frac{1}{2}$. The theorem is a consequence of (18).

4. SOLUTIONS OF PELL'S EQUATION – EQUALITY

Now we state the propositions:

(20) If $x \geqslant 0$, then $(\operatorname{sgn} x) \cdot (\mathtt{y}_a(|x|)) = \mathtt{y}_a(|x|)$. The theorem is a consequence of (3).

(21) If $x \leqslant 0$, then $(\operatorname{sgn} x) \cdot (\mathtt{y}_a(|x|)) = -\mathtt{y}_a(|x|)$. The theorem is a consequence of (3).

(22) (i) $\mathtt{x}_a(|x+y|) = (\mathtt{x}_a(|x|)) \cdot (\mathtt{x}_a(|y|)) + (a^{\mathbf{2}} -' 1) \cdot (\operatorname{sgn} x) \cdot (\mathtt{y}_a(|x|)) \cdot (\operatorname{sgn} y) \cdot (\mathtt{y}_a(|y|))$, and

(ii) $(\operatorname{sgn}(x + y)) \cdot (\mathtt{y}_a(|x + y|)) = (\mathtt{x}_a(|x|)) \cdot (\operatorname{sgn} y) \cdot (\mathtt{y}_a(|y|)) + (\operatorname{sgn} x) \cdot (\mathtt{y}_a(|x|)) \cdot (\mathtt{x}_a(|y|))$.

The theorem is a consequence of (20), (8), and (21).

5. Solutions of Pell's Equation – Congruences

Now we state the propositions:

(23) $\mathtt{x}_a(n)$ and $\mathtt{y}_a(n)$ are relatively prime.
PROOF: Define $\mathcal{P}$[natural number] $\equiv \gcd(\mathtt{x}_a(\$_1), \mathtt{y}_a(\$_1)) = 1$. $\mathtt{x}_a(0) = 1$ and $\mathtt{y}_a(0) = 0$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (6), [4, (8)], [7, (1), (5)]. For every n, $\mathcal{P}[n]$. □

(24) $\mathtt{y}_a(n) \equiv n \pmod{a-1}$. The theorem is a consequence of (9), (3), and (1).

(25) (i) $\mathtt{x}_a(n) \equiv \mathtt{x}_b(n) \pmod{a-b}$, and
(ii) $\mathtt{y}_a(n) \equiv \mathtt{y}_b(n) \pmod{a-b}$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv \mathtt{x}_a(\$_1) \equiv \mathtt{x}_b(\$_1) \pmod{a-b}$ and $\mathtt{y}_a(\$_1) \equiv \mathtt{y}_b(\$_1) \pmod{a-b}$. $\mathtt{x}_a(0) = 1 = \mathtt{x}_b(0)$ and $\mathtt{y}_a(0) = 0 = \mathtt{y}_b(0)$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every n, $\mathcal{P}[n]$. □

(26) If $a \equiv b \pmod{k}$, then $\mathtt{y}_a(n) \equiv \mathtt{y}_b(n) \pmod{k}$. The theorem is a consequence of (25).

(27) $\operatorname{sgn}(2\cdot x+y)\cdot \mathtt{y}_a(|2\cdot x+y|) \equiv -(\operatorname{sgn} y)\cdot \mathtt{y}_a(|y|) \pmod{\mathtt{x}_a(|x|)}$. The theorem is a consequence of (22) and (7).

(28) $(\operatorname{sgn}(4\cdot x\cdot n+y))\cdot(\mathtt{y}_a(|4\cdot x\cdot n+y|)) \equiv (\operatorname{sgn} y)\cdot(\mathtt{y}_a(|y|)) \pmod{\mathtt{x}_a(|x|)}$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv (\operatorname{sgn}(4\cdot x\cdot \$_1+y))\cdot(\mathtt{y}_a(|4\cdot x\cdot \$_1+y|)) \equiv (\operatorname{sgn} y)\cdot(\mathtt{y}_a(|y|)) \pmod{\mathtt{x}_a(|x|)}$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every n, $\mathcal{P}[n]$. □

(29) $(\operatorname{sgn}(x+y))\cdot(\mathtt{y}_a(|x+y|)) \equiv (\operatorname{sgn}(x-y))\cdot(\mathtt{y}_a(|x-y|)) \pmod{\mathtt{x}_a(|x|)}$. The theorem is a consequence of (27).

(30) If $n_1 < n_2 \leqslant n$ and $|x| = \mathtt{y}_a(n_1)$ and $|y| = \mathtt{y}_a(n_2)$ and $x \equiv y \pmod{\mathtt{x}_a(n)}$, then $x = y$.
PROOF: Consider i being an integer such that $x-y = (\mathtt{x}_a(n))\cdot i$. $-\mathtt{x}_a(n) < x-y < \mathtt{x}_a(n)$. □

(31) Suppose $n_1 \leqslant 2\cdot n$ and $n_2 \leqslant 2\cdot n$ and $|x| = \mathtt{y}_a(n_1)$ and $|y| = \mathtt{y}_a(n_2)$ and $x \equiv y \pmod{\mathtt{x}_a(n)}$. Then
(i) $n_1 \equiv n_2 \pmod{2\cdot n}$, or
(ii) $n_1 \equiv -n_2 \pmod{2\cdot n}$.

(32) Suppose $n_1 \leqslant 4\cdot n$ and $n_2 \leqslant 4\cdot n$ and $|x| = \mathtt{y}_a(n_1)$ and $|y| = \mathtt{y}_a(n_2)$ and $x \equiv y \pmod{\mathtt{x}_a(n)}$. Then
(i) $n_1 \equiv n_2 \pmod{2\cdot n}$, or
(ii) $n_1 \equiv -n_2 \pmod{2\cdot n}$.
The theorem is a consequence of (31).

(33) Suppose $\mathtt{y}_a(n_1) \equiv \mathtt{y}_a(n_2) \pmod{\mathtt{x}_a(n)}$ and $n > 0$. Then

(i) $n_1 \equiv n_2 \pmod{2 \cdot n}$, or

(ii) $n_1 \equiv -n_2 \pmod{2 \cdot n}$.

The theorem is a consequence of (28), (20), and (32).

6. Solutions of Pell's Equation – Divisibility

Now we state the propositions:

(34) $\mathtt{y}_a(n) \mid \mathtt{y}_a(n \cdot k)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv \mathtt{y}_a(n) \mid \mathtt{y}_a(n \cdot \$_1)$. $(\mathtt{y}_a(n)) \cdot 0 = \mathtt{y}_a(n \cdot 0)$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every k, $\mathcal{P}[k]$. $\square$

(35) $\mathtt{y}_a(n \cdot k) \equiv k \cdot ((\mathtt{x}_a(n))^{k-'1}) \cdot (\mathtt{y}_a(n)) \pmod{(\mathtt{y}_a(n))^{\mathbf{2}}}$. The theorem is a consequence of (3), (2), and (1).

(36) If $k > 0$ and $\mathtt{y}_a(k) \mid \mathtt{y}_a(n)$, then $k \mid n$.

PROOF: Set $P = \mathtt{y}_a(k)$. Set $r = n \bmod k$. Set $q = n \operatorname{div} k$. $(\operatorname{sgn} n) \cdot (\mathtt{y}_a(|n|)) = (\mathtt{x}_a(|r|)) \cdot (\operatorname{sgn} q \cdot k) \cdot (\mathtt{y}_a(|q \cdot k|)) + (\operatorname{sgn} r) \cdot (\mathtt{y}_a(|r|)) \cdot (\mathtt{x}_a(|q \cdot k|))$. $\mathtt{y}_a(n) = (\mathtt{x}_a(|r|)) \cdot ((\operatorname{sgn} q \cdot k) \cdot (\mathtt{y}_a(|q \cdot k|))) + (\operatorname{sgn} r) \cdot (\mathtt{y}_a(|r|)) \cdot (\mathtt{x}_a(|q \cdot k|))$. $P \mid \mathtt{y}_a(q \cdot k)$. $P \mid (\mathtt{x}_a(r)) \cdot (\mathtt{y}_a(q \cdot k))$. P and $\mathtt{x}_a(k \cdot q)$ are relatively prime. $r = 0$ by [5, (6)], (11). $\square$

(37) If $(\mathtt{y}_a(k))^{\mathbf{2}} \mid \mathtt{y}_a(n)$, then $\mathtt{y}_a(k) \mid n$. The theorem is a consequence of (3), (36), (35), and (23).

7. Special Case of Pell's Equation is Diophantine

Now we state the proposition:

(38) Let us consider natural numbers y, z, a. Then $y = \mathtt{y}_a(z)$ and $a > 1$ if and only if there exist natural numbers x, x_1, y_1, A, x_2, y_2 such that $a > 1$ and $\langle x, y \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $\langle x_1, y_1 \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $y_1 \geqslant y$ and $A > y \geqslant z$ and $\langle x_2, y_2 \rangle$ is a Pell's solution of $A^{\mathbf{2}} -' 1$ and $y_2 \equiv y \pmod{x_1}$ and $A \equiv a \pmod{x_1}$ and $y_2 \equiv z \pmod{2 \cdot y}$ and $A \equiv 1 \pmod{2 \cdot y}$ and $y_1 \equiv 0 \pmod{y^{\mathbf{2}}}$.

PROOF: If $y = \mathtt{y}_a(z)$ and $a > 1$, then there exist natural numbers x, x_1, y_1, A, x_2, y_2 such that $a > 1$ and $\langle x, y \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $\langle x_1, y_1 \rangle$ is a Pell's solution of $a^{\mathbf{2}} -' 1$ and $y_1 \geqslant y$ and $A > y \geqslant z$ and $\langle x_2, y_2 \rangle$ is a Pell's solution of $A^{\mathbf{2}} -' 1$ and $y_2 \equiv y \pmod{x_1}$ and $A \equiv a \pmod{x_1}$ and $y_2 \equiv z \pmod{2 \cdot y}$ and $A \equiv 1 \pmod{2 \cdot y}$ and $y_1 \equiv 0 \pmod{y^{\mathbf{2}}}$. $\square$

8. Exponential Function is Diophantine

Now we state the proposition:

(39) Let us consider natural numbers x, y, z. Then $y = x^z$ if and only if $y = 1$ and $z = 0$ or $x = 0$ and $y = 0$ and $z > 0$ or $x = 1$ and $y = 1$ and $z > 0$ or $x > 1$ and $z > 0$ and there exist natural numbers y_1, y_2, y_3, K such that $y_1 = \mathtt{y}_x(z+1)$ and $K > 2 \cdot z \cdot y_1$ and $y_2 = \mathtt{y}_K(z+1)$ and $y_3 = \mathtt{y}_{K \cdot x}(z+1)$ and $(0 \leqslant y - \frac{y_3}{y_2} < \frac{1}{2}$ or $0 \leqslant \frac{y_3}{y_2} - y < \frac{1}{2})$.

Proof: If $y = x^z$, then $y = 1$ and $z = 0$ or $x = 0$ and $y = 0$ and $z > 0$ or $x = 1$ and $y = 1$ and $z > 0$ or $x > 1$ and $z > 0$ and there exist natural numbers y_1, y_2, y_3, K such that $y_1 = \mathtt{y}_x(z+1)$ and $K > 2 \cdot z \cdot y_1$ and $y_2 = \mathtt{y}_K(z+1)$ and $y_3 = \mathtt{y}_{K \cdot x}(z+1)$ and $(0 \leqslant y - \frac{y_3}{y_2} < \frac{1}{2}$ or $0 \leqslant \frac{y_3}{y_2} - y < \frac{1}{2})$. □

References

[1] Marcin Acewicz and Karol Pąk. Pell's equation. *Formalized Mathematics*, 25(**3**):197–204, 2017. doi:10.1515/forma-2017-0019.

[2] Zofia Adamowicz and Paweł Zbierski. *Logic of Mathematics: A Modern Course of Classical Logic*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley-Interscience, 1997.

[3] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly, Mathematical Association of America*, 80(3):233–269, 1973. doi:10.2307/2318447.

[4] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6 (**4**):549–551, 1997.

[5] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(**4**):181–187, 2007. doi:10.2478/v10037-007-0022-7.

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

[7] 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.

Received November 29, 2017

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