Contents

Formaliz. Math. 28 (**3**)

Continued on inside back cover

FORMALIZED MATHEMATICS
Vol. 28, No. 3, Pages 227–237, 2020
DOI: 10.2478/forma-2020-0020

sciendo
https://www.sciendo.com/

A Case Study of Transporting Urysohn's Lemma from Topology via Open Sets into Topology via Neighborhoods

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

Summary. Józef Białas and Yatsuka Nakamura has completely formalized a proof of Urysohn's lemma in the article [4], in the context of a topological space defined via open sets. In the Mizar Mathematical Library (MML), the topological space is defined in this way by Beata Padlewska and Agata Darmochwał in the article [18]. In [7] the topological space is defined via neighborhoods. It is well known that these definitions are equivalent [5, 6].

In the definitions, an abstract structure (i.e. the article [17, `STRUCT_0`] and its descendants, all of them directly or indirectly using Mizar structures [3]) have been used (see [10], [9]). The first topological definition is based on the Mizar structure `TopStruct` and the topological space defined via neighborhoods with the Mizar structure: `FMT_Space_Str`. To emphasize the notion of a neighborhood, we rename `FMT_TopSpace` (topology from neighbourhoods) to `NTopSpace` (a neighborhood topological space).

Using Mizar [2], we transport the Urysohn's lemma from `TopSpace` to `NTopSpace`.

In some cases, Mizar allows certain techniques for transporting proofs, definitions or theorems. Generally speaking, there is no such automatic translating.

In Coq, Isabelle/HOL or homotopy type theory transport is also studied, sometimes with a more systematic aim [14], [21], [11], [12], [8], [19]. In [1], two co-existing Isabelle libraries: Isabelle/HOL and Isabelle/Mizar, have been aligned in a single foundation in the Isabelle logical framework.

In the MML, they have been used since the beginning: `reconsider`, `registration`, `cluster`, others were later implemented [13]: `identify`.

In some proofs, it is possible to define particular functors between different structures, mainly useful when results are already obtained in a given structure. This technique is used, for example, in [15] to define two functors `MXR2MXF` and `MXF2MXF` between `Matrix of REAL` and `Matrix of F-Real` and to transport the

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

definition of the addition from one structure to the other: [...] `A + B -> Matrix of REAL equals MXF2MXR ((MXR2MXF A) + (MXR2MXF B))` [...].

In this paper, first we align the necessary topological concepts. For the formalization, we were inspired by the works of Claude Wagschal [20]. It allows us to transport more naturally the Urysohn's lemma ([4, `URYSOHN3:20`]) to the topological space defined via neighborhoods.

Nakasho and Shidama have developed a solution to explore the notions introduced in various ways `https://mimosa-project.github.io/mmlreference/current/` [16].

The definitions can be directly linked in the HTML version of the Mizar library (example: Urysohn's lemma `http://mizar.org/version/current/html/urysohn3.html#T20`).

MSC: 54A05 03B35 68V20

Keywords: filter; topology via neighborhoods; transfer principle; transport of structure; align

MML identifier: `FINTOPO8`, version: `8.1.10 5.64.1388`

1. Some Redefinitions: Neighborhood Topological Space

From now on T denotes a topological space and A, B denote subsets of T.

Now we state the proposition:

(1) If A misses B, then $\operatorname{Int} A$ misses $\operatorname{Int} B$.

A neighborhood topological space is a topology from neighbourhoods. Let X be a non empty topological space. We introduce the notation Top2NTop(X) as a synonym of TopSpace2FMT X.

Let X be a topology from neighbourhoods. We introduce the notation NTop2Top(X) as a synonym of FMT2TopSpace X.

2. Alignment of Topological Space Concepts Defined via Open Sets and Defined via Neighbourhoods

Let N_1 be a non empty neighborhood topological space. Observe that Ω_{N_1} is open and $\emptyset_{N_1}$ is open.

Let N_1 be a U-FMT filter, non empty, strict formal topological space and x be an element of N_1. Note that the functor $U_F(x)$ yields a filter of the carrier of N_1.

[20, definition 2.11.2, p. 89]:

Let N_1 be a U-FMT filter, non empty, strict formal topological space and F be a filter of the carrier of N_1. The functor LimFilter(F) yielding a subset of N_1 is defined by the term

(Def. 1) $\{x$, where x is a point of $N_1 : F$ is finer than $U_F(x)\}$.

[20, DEFINITION 2.11.3, P. 92 AND PROPOSITION 2.11.4, P. 90]:

Let N_1, N_2 be U-FMT filter, non empty, strict formal topological spaces, f be a function from N_1 into N_2, and F be a filter of the carrier of N_1. The functor $\lim_F f$ yielding a subset of N_2 is defined by the term

(Def. 2) LimFilter(the image of filter F under f).

[20, DEFINITION 2.10.1 (1), P. 83]:

Let N be a neighborhood topological space, A be a subset of N, and x be a point of N. We say that x is interior point of A if and only if

(Def. 3) A is a neighbourhood of x.

[20, DEFINITION 2.10.1 (2), P. 83]:

Let N be a neighborhood topological space, A be a subset of N, and x be a point of N. We say that x is adherent point of A if and only if

(Def. 4) for every element V of $U_F(x)$, V meets A.

The functor Int A yielding a subset of N is defined by the term

(Def. 5) $\{x$, where x is a point of $N : x$ is interior point of $A\}$.

[20, DEFINITION 2.13.1, P. 97]:

Let N_1, N_2 be neighborhood topological spaces, f be a function from N_1 into N_2, and x be a point of N_1. We say that f is continuous at x if and only if

(Def. 6) for every filter F of the carrier of N_1 such that $x \in \mathrm{LimFilter}(F)$ holds $f(x) \in \lim_F f$.

We say that f is continuous if and only if

(Def. 7) for every point x of N_1, f is continuous at x.

Note that there exists a function from N_1 into N_2 which is continuous.

Let N be a neighborhood topological space and A be a subset of N.

[20, DEFINITION 2.10.1 (1), P. 83]: Int A is open.

[20, DEFINITION 2.10.1 (2), P. 83]:

Let N be a neighborhood topological space and A be a subset of N. The functor $\overline{A}$ yielding a subset of N is defined by the term

(Def. 8) $\{x$, where x is a point of $N : x$ is adherent point of $A\}$.

[20, DEFINITION 2.9.3, P. 81]:

Let N_1 be a neighborhood topological space and A be a subset of N_1. We say that A is closed if and only if

(Def. 9) $\Omega_{N_1} \setminus A$ is an open subset of N_1.

One can check that there exists a subset of N_1 which is closed and Ω_{N_1} is closed as a subset of N_1 and $\emptyset_{N_1}$ is closed as a subset of N_1 and there exists a subset of N_1 which is non empty and closed.

Let S, T be non empty topological spaces and f be a function from S into T. The functor Top2NTop(f) yielding a function from Top2NTop(S) into Top2NTop(T) is defined by the term

(Def. 10) f.

Let T_1 be a non empty topological space, T_2 be a non empty, strict topological space, and f be a continuous function from T_1 into T_2. Observe that the functor Top2NTop(f) yields a continuous function from Top2NTop(T_1) into Top2NTop(T_2) and is defined by the term

(Def. 11) f.

[20, DEFINITION 2.17.1, P. 111]:

Let N be a neighborhood topological space. We say that N is T_2 if and only if

(Def. 12) for every filter F of the carrier of N, LimFilter(F) is trivial.

One can check that there exists a neighborhood topological space which is T_2.

Let N be a neighborhood topological space. We say that N is normal if and only if

(Def. 13) for every closed subsets A, B of N such that A misses B there exists a neighbourhood V of A and there exists a neighbourhood W of B such that V misses W.

Let x be a point of N. The functor NTop2Top(x) yielding a point of NTop2Top (N) is defined by the term

(Def. 14) x.

Let T be a non empty topological space and x be a point of T. The functor Top2NTop(x) yielding a point of Top2NTop(T) is defined by the term

(Def. 15) x.

Let N be a neighborhood topological space and S be a subset of N. The functor NTop2Top(S) yielding a subset of NTop2Top(N) is defined by the term

(Def. 16) S.

Let T be a non empty topological space and S be a subset of T. The functor Top2NTop(S) yielding a subset of Top2NTop(T) is defined by the term

(Def. 17) S.

One can verify that there exists a neighborhood topological space which is non empty and normal.

Let T_1, T_2 be neighborhood topological spaces and f be a function from T_1 into T_2. The functor NTop2Top(f) yielding a function from NTop2Top(T_1) into NTop2Top(T_2) is defined by the term

(Def. 18) f.

The functor FMT-$\mathbb{R}^1$ yielding a neighborhood topological space is defined by the term

(Def. 19) Top2NTop($\mathbb{R}^{\mathbf{1}}$).

Now we state the proposition:

(2) The carrier of FMT-$\mathbb{R}^1 = \mathbb{R}$.

One can verify that FMT-$\mathbb{R}^1$ is real-membered.

3. Some Properties of a Neighborhood Topology

From now on N, N_1, N_2 denote neighborhood topological spaces, A, B denote subsets of N, O denotes an open subset of N, a denotes a point of N, X denotes a subset of N_1, Y denotes a subset of N_2, x denotes a point of N_1, y denotes a point of N_2, f denotes a function from N_1 into N_2, and f_1 denotes a continuous function from N_1 into N_2.

Now we state the propositions:

(3) O is an open subset of NTop2Top(N).

(4) A is a subset of NTop2Top(N).

(5) (i) Ω_N is open, and

(ii) $\emptyset_N$ is open.

(6) $N \longmapsto y$ is continuous.

(7) a is interior point of A if and only if there exists an open subset O of N such that $a \in O$ and $O \subseteq A$.

(8) If $a \in O$, then a is interior point of O.

(9) $\operatorname{Int} A = \bigcup\{O$, where O is an open subset of $N : O \subseteq A\}$.

(10) $\operatorname{Int} A \subseteq A$.

(11) [20, definition 2.10.1, p. 83]:
If $A \subseteq B$, then $\operatorname{Int} A \subseteq \operatorname{Int} B$.

(12) [20, definition 2.10.2, p. 83]:
A is open if and only if $\operatorname{Int} A = A$.

(13) $\operatorname{Int} A = \operatorname{Int} \operatorname{Int} A$.

(14) Let us consider a non empty, strict neighborhood topological space N, a subset A of N, and a point x of N. Suppose A is a neighbourhood of x. Then $\operatorname{Int} A$ is an open neighbourhood of x. The theorem is a consequence of (12).

(15) The image of filter $U_F(x)$ under $f = \{M$, where M is a subset of $N_2 : f^{-1}(M) \in U_F(x)\}$.

(16) If f is continuous at x and $y = f(x)$, then for every element V of $U_F(y)$, there exists an element W of $U_F(x)$ such that $f^\circ W \subseteq V$.

(17) If $y = f(x)$ and for every element V of $U_F(y)$, there exists an element W of $U_F(x)$ such that $f^\circ W \subseteq V$, then f is continuous at x.

(18) [20, DEFINITION 2.13.1, P. 97]:
If $y = f(x)$, then f is continuous at x iff for every element V of $U_F(y)$, there exists an element W of $U_F(x)$ such that $f^\circ W \subseteq V$.

(19) [20, PROPOSITION 2.13.3, P. 99]:
If f is continuous at x and x is adherent point of X and $y = f(x)$ and $Y = f^\circ X$, then y is adherent point of Y.

(20) [20, THEOREM 2.13.4, P. 99, (1) $\Rightarrow$ (2)]:
${f_1}^\circ \overline{X} \subseteq \overline{{f_1}^\circ X}$.

(21) Every closed subset of N is a closed subset of NTop2Top(N).

(22) [20, PROPOSITION 2.10.2, P. 84]:
If $B = \Omega_N \setminus A$, then $\Omega_N \setminus \overline{A} = \operatorname{Int} B$.

(23) [20, PROPOSITION 2.10.2, P. 84]:
If $B = \Omega_N \setminus A$, then $\Omega_N \setminus (\operatorname{Int} A) = \overline{B}$.

(24) $A \subseteq \overline{A}$.

(25) [20, 2.10.6, P. 84]:
A is closed if and only if $\overline{A} = A$.

(26) [20, 2.10.5, P.84]:
If $A \subseteq B$, then $\overline{A} \subseteq \overline{B}$.

(27) [20, THEOREM 2.13.4, P. 99, (2) $\Rightarrow$ (3)]:
If for every subset X of N_1, $f^\circ \overline{X} \subseteq \overline{f^\circ X}$, then for every closed subset S of N_2, $f^{-1}(S)$ is a closed subset of N_1.

(28) [20, DEFINITION 2.9.3, P. 81]:
If $B = \Omega_N \setminus A$, then A is open iff B is closed.

(29) If $A = \Omega_N \setminus B$, then A is open iff B is closed.

(30) [20, THEOREM 2.13.4, P. 99, (3) $\Rightarrow$ (4)]:
If for every closed subset S of N_2, $f^{-1}(S)$ is a closed subset of N_1, then for every open subset S of N_2, $f^{-1}(S)$ is an open subset of N_1.

(31) [20, THEOREM 2.13.4, P. 99, (4) $\Rightarrow$ (1)]:
If for every open subset S of N_2, $f^{-1}(S)$ is an open subset of N_1, then f is continuous.

(32) [20, THEOREM 2.13.4, P. 99, (1) $\Leftrightarrow$ (4)]:
f is continuous if and only if for every open subset O of N_2, $f^{-1}(O)$ is an open subset of N_1.

(33) [20, THEOREM 2.13.4, P. 99, (1) $\Leftrightarrow$ (3)]:
f is continuous if and only if for every closed subset O of N_2, $f^{-1}(O)$ is a closed subset of N_1.

(34) $\operatorname{Int} A = \operatorname{Int} \mathrm{NTop2Top}(A)$.

(35) If A is a neighbourhood of a, then $\mathrm{NTop2Top}(A)$ is a neighbourhood of $\mathrm{NTop2Top}(a)$. The theorem is a consequence of (34).

(36) If A is a neighbourhood of B, then $\mathrm{NTop2Top}(A)$ is a neighbourhood of $\mathrm{NTop2Top}(B)$.

(37) If A misses B, then $\mathrm{NTop2Top}(A)$ misses $\mathrm{NTop2Top}(B)$.

(38) If A misses B, then $\operatorname{Int} A$ misses $\operatorname{Int} B$.

From now on N denotes a T_2 neighborhood topological space.

Now we state the propositions:

(39) Let us consider points x, y of N. Suppose $x \neq y$. Then there exists an element V_1 of $U_F(x)$ and there exists an element V_2 of $U_F(y)$ such that V_1 misses V_2.

(40) $\mathrm{NTop2Top}(N)$ is a T_2, non empty, strict topological space. The theorem is a consequence of (39).

(41) Let us consider a non empty, normal neighborhood topological space N. Then $\mathrm{NTop2Top}(N)$ is normal. The theorem is a consequence of (36) and (1).

Let N be a non empty, normal neighborhood topological space. One can verify that $\mathrm{NTop2Top}(N)$ is normal.

4. Some Connections between Neighborhood Topology and Open-Set Topology

In the sequel T denotes a non empty topological space, A, B denote subsets of T, F denotes a closed subset of T, and O denotes an open subset of T.

Now we state the propositions:

(42) A is a subset of $\mathrm{Top2NTop}(T)$.

(43) F is a closed subset of $\mathrm{Top2NTop}(T)$.

(44) O is an open subset of $\mathrm{Top2NTop}(T)$.

(45) If A misses B, then $\mathrm{Top2NTop}(A)$ misses $\mathrm{Top2NTop}(B)$.

(46) Let us consider a T_2, non empty topological space T. Then $\mathrm{Top2NTop}(T)$ is a T_2 neighborhood topological space.

In the sequel T denotes a non empty, strict topological space, A, B denote subsets of T, and x denotes a point of T.

Now we state the propositions:

(47) $\operatorname{Int} A = \operatorname{Int} \operatorname{Top2NTop}(A)$.

(48) If A is a neighbourhood of B, then $\operatorname{Top2NTop}(A)$ is a neighbourhood of $\operatorname{Top2NTop}(B)$.

(49) If A is a neighbourhood of x, then $\operatorname{Top2NTop}(A)$ is a neighbourhood of $\operatorname{Top2NTop}(x)$.

(50) Let us consider a non empty, normal, strict topological space T. Then $\operatorname{Top2NTop}(T)$ is normal.

Let T be a non empty, normal, strict topological space. Note that $\operatorname{Top2NTop}(T)$ is normal.

5. Transport from $\mathbb{R}^1$ to FMT-$\mathbb{R}^1$

From now on A denotes a subset of FMT-$\mathbb{R}^1$, x denotes a point of FMT-$\mathbb{R}^1$, y denotes a point of the metric space of real numbers, z denotes a point of $(\text{the metric space of real numbers})_{\text{top}}$, and r denotes a real number.

Now we state the propositions:

(51) $\operatorname{NTop2Top}(\text{FMT-}\mathbb{R}^1) = \mathbb{R}^{\mathbf{1}}$.

(52) The carrier of FMT-$\mathbb{R}^1 = \mathbb{R}$.

(53) Let us consider a neighborhood topological space N, and a function f from N into FMT-$\mathbb{R}^1$. Then $\operatorname{NTop2Top}(f)$ is a function from $\operatorname{NTop2Top}(N)$ into $\mathbb{R}^{\mathbf{1}}$.

(54) Let us consider a non empty topological space T, and a function f from T into $\mathbb{R}^{\mathbf{1}}$. Then $\operatorname{Top2NTop}(f)$ is a function from $\operatorname{Top2NTop}(T)$ into $\operatorname{Top2NTop}(\mathbb{R}^{\mathbf{1}})$.

(55) A is open if and only if for every real number x such that $x \in A$ there exists r such that $r > 0$ and $]x - r, x + r[\subseteq A$.

(56) $\{]a, b[,$ where a, b are real numbers : $a < b\}$ is a basis of $\mathbb{R}^{\mathbf{1}}$.

(57) $\{]a, b[,$ where a, b are real numbers : $a < b\}$ is a basis of FMT-$\mathbb{R}^1$.

Proof: Set $B = \{]a, b[,$ where a, b are real numbers : $a < b\}$. $B \subseteq 2^{\alpha}$, where α is the carrier of FMT-$\mathbb{R}^1$. $B \subseteq$ the open set family of FMT-$\mathbb{R}^1$. □

(58) If $r > 0$, then $]x - r, x + r[$ is a neighbourhood of x. The theorem is a consequence of (57).

(59) Let us consider an object x. Then x is a point of FMT-$\mathbb{R}^1$ if and only if x is a point of the metric space of real numbers.

(60) If $x = y$, then $\operatorname{Ball}(y, r) =]x - r, x + r[$.

(61) If $x = y$ and $r > 0$, then $\operatorname{Ball}(y, r)$ is a neighbourhood of x. The theorem is a consequence of (58).

(62) If $x = z$, then Balls z is a family of subsets of FMT-$\mathbb{R}^1$.

(63) Let us consider a family S of subsets of FMT-$\mathbb{R}^1$. If $x = z$ and $S =$ Balls z, then $[S] = U_F(x)$. The theorem is a consequence of (61), (14), and (55).

The functor gen-NS-$\mathbb{R}^1$ yielding a function from the carrier of FMT-$\mathbb{R}^1$ into $2^{2^{(\text{the carrier of FMT-}\mathbb{R}^1)}}$ is defined by

(Def. 20) for every real number r, there exists a point x of (the metric space of real numbers)$_{\text{top}}$ such that $x = r$ and $it(r) =$ Balls x.

The functor gen-$\mathbb{R}^1$ yielding a non empty, strict formal topological space is defined by the term

(Def. 21) $\langle$the carrier of FMT-$\mathbb{R}^1$, gen-NS-$\mathbb{R}^1\rangle$.

Now we state the propositions:

(64) The carrier of gen-$\mathbb{R}^1 = \mathbb{R}$.

(65) Let us consider an element x of gen-$\mathbb{R}^1$. Then there exists a point y of (the metric space of real numbers)$_{\text{top}}$ such that

(i) $x = y$, and

(ii) $U_F(x) =$ Balls y.

(66) dom[gen-$\mathbb{R}^1$] $= \mathbb{R}$.

(67) gen-filter gen-$\mathbb{R}^1$ = FMT-$\mathbb{R}^1$. The theorem is a consequence of (64), (65), and (58).

6. Transporting Urysohn's Lemma ([4, URYSOHN3:20]) from an Open-Set Topological Space to the Associated Neighborhood Topological Space

Now we state the proposition:

(68) **Main result** Urysohn's lemma in a neighborhood topological space:
Let us consider a non empty, normal neighborhood topological space N, and closed subsets A, B of N. Suppose A misses B. Then there exists a function F from N into FMT-$\mathbb{R}^1$ such that

(i) F is continuous, and

(ii) for every point x of N, $0 \leqslant F(x) \leqslant 1$ and if $x \in A$, then $F(x) = 0$ and if $x \in B$, then $F(x) = 1$.

Acknowledgement: I would like to thank the Mizar Team for allowing me to present, during my visit to Białystok in July 2016, the main ideas (the

transport of theorems) that where used to write this article. Their advice and listening enabled this work to be completed.

References

[1] *Higher-Order Tarski Grothendieck as a Foundation for Formal Proof*, Sep. 2019. Zenodo. doi:10.4230/lipics.itp.2019.9.

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

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

[4] Józef Białas and Yatsuka Nakamura. The Urysohn lemma. *Formalized Mathematics*, 9 (**3**):631–636, 2001.

[5] Nicolas Bourbaki. *General Topology: Chapters 1–4*. Springer Science and Business Media, 2013.

[6] Nicolas Bourbaki. *Topologie générale: Chapitres 1 à 4*. Eléments de mathématique. Springer Science & Business Media, 2007.

[7] Roland Coghetto. Topology from neighbourhoods. *Formalized Mathematics*, 23(**4**):289–296, 2015. doi:10.1515/forma-2015-0023.

[8] Thierry Coquand. Théorie des types dépendants et axiome d'univalence. *Séminaire Bourbaki*, 66:1085, 2014.

[9] Adam Grabowski and Roland Coghetto. *Extending Formal Topology in Mizar by Uniform Spaces*, pages 77–105. Springer, Cham, 2020. ISBN 978-3-030-41425-2. doi:10.1007/978-3-030-41425-2_2.

[10] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. *Refining Algebraic Hierarchy in Mathematical Repository of Mizar*, pages 49–75. Springer, Cham, 2020. ISBN 978-3-030-41425-2. doi:10.1007/978-3-030-41425-2_2.

[11] Brian Huffman and Ondřej Kunčar. Lifting and transfer: A modular design for quotients in Isabelle/HOL. In *International Conference on Certified Programs and Proofs*, pages 131–146. Springer, 2013.

[12] Einar Broch Johnsen and Christoph Lüth. Theorem reuse by proof term transformation. In *International Conference on Theorem Proving in Higher Order Logics*, pages 152–167. Springer, 2004.

[13] Artur Korniłowicz. How to define terms in Mizar effectively. *Studies in Logic, Grammar and Rhetoric*, 18:67–77, 2009.

[14] Nicolas Magaud. Changing data representation within the Coq system. In *International Conference on Theorem Proving in Higher Order Logics*, pages 87–102. Springer, 2003.

[15] Yatsuka Nakamura, Nobuyuki Tamura, and Wenpai Chang. A theory of matrices of real elements. *Formalized Mathematics*, 14(**1**):21–28, 2006. doi:10.2478/v10037-006-0004-1.

[16] Kazuhisa Nakasho and Yasunari Shidama. Documentation generator focusing on symbols for the HTML-ized Mizar library. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics, CICM 2015*, volume 9150 of *Lecture Notes in Computer Science*, pages 343–347. Springer, Cham, 2015. doi:10.1007/978-3-319-20615-8_25.

[17] Library Committee of the Association of Mizar Users. Preliminaries to structures. *Mizar Mathematical Library*, 1995.

[18] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.

[19] Nicolas Tabareau, Éric Tanter, and Matthieu Sozeau. Equivalences for free: univalent

parametricity for effective transport. *Proceedings of the ACM on Programming Languages*, 2(ICFP):1–29, 2018.

[20] Claude Wagschal. *Topologie et analyse fonctionnelle*. Hermann, 1995.

[21] Theo Zimmermann and Hugo Herbelin. Automatic and transparent transfer of theorems along isomorphisms in the Coq proof assistant. *arXiv preprint arXiv:1505.05028*, 2015.

Accepted September 25, 2020

FORMALIZED MATHEMATICS
Vol. 28, No. 3, Pages 239–249, 2020
DOI: 10.2478/forma-2020-0021

sciendo
https://www.sciendo.com/

Extended Natural Numbers and Counters

Sebastian Koch
Johannes Gutenberg University
Mainz, Germany[1]

Summary. This article introduces extended natural numbers, i.e. the set $\mathbb{N} \cup \{+\infty\}$, in Mizar [4], [3] and formalizes a way to list a cardinal numbers of cardinals. Both concepts have applications in graph theory.

MSC: 03E10 68V20

Keywords: cardinal; sequence; extended natural numbers

MML identifier: `COUNTERS`, version: `8.1.10 5.64.1388`

0. Introduction

Extended natural numbers have often been used in the literature to define distances in graphs that are not necessarily connected, to set the distance between vertices of different components to $+\infty$, see e.g. [5], [7], [8]. Therefore it is only natural to formalize these numbers in preparation for a formalization of distances in graphs. On the other hand, one usually does not see the list of counters from the second part of this article in the literature. The generalistic motivation to introduce these is a rather simple one, however. n-partite finite graphs are rather known and constructions like $K_{\omega,\omega}$ arise sometimes. The index objects of these alone could be formalized using `Cardinal-yielding XFinSequence` (cf. [14], [1]), but a generalization for the index object to be any cardinality long seemed to be appropriate. This allows for easy notation of more graphs than just with the finite amount of indices. For example $K_{1,2,3,\ldots}$, where the index ranges over all natural numbers, is an easy notation for a graph that does not

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

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

have a finite independence number and also no infinite subset of vertices that form an independent set.

In the first section the set $\overline{\mathbb{N}} = \mathbb{N} \cup \{+\infty\}$ of extended natural numbers is introduced to the Mizar system [6] as a subset of the extended real numbers $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ defined in [12]. Basic theorems will be proven, often specializations of theorems from [10], [13] or generalizations of theorems from [2]. The second section will introduce sets of extended natural numbers and proceed in a similar fashion to [11]. The third section does the same with relations that only have extended natural numbers in their range, similar to [9]. Section 4 deals with some ordinal preliminaries. Not all are needed for the last section, but the author felt they would fit better here than into a graph preliminary article. Finally, the last section introduces relations with cardinal domain, as only a cardinal domain (in lieu of an ordinal one) is needed for counting purposes. The article ends with the definition of `Counters` and `Counters+`, two expandable modes with the latter not allowing 0 in its range.

1. Extended Natural Numbers

The functor $\overline{\mathbb{N}}$ yielding a subset of $\overline{\mathbb{R}}$ is defined by the term

(Def. 1) $\mathbb{N} \cup \{+\infty\}$.

Now we state the proposition:

(1) $\mathbb{N} \subset \overline{\mathbb{N}} \subset \overline{\mathbb{R}}$.

PROOF: $-\infty \notin \overline{\mathbb{N}}$. □

Observe that $\overline{\mathbb{N}}$ is non empty and infinite.

Let x be an object. We say that x is extended natural if and only if

(Def. 2) $x \in \overline{\mathbb{N}}$.

Let us observe that $+\infty$ is extended natural and every object which is extended natural is also extended real and every object which is natural is also extended natural and every set which is finite and extended natural is also natural.

There exists an object which is zero and extended natural and there exists an object which is non zero and extended natural and there exists a number which is extended natural and every element of $\overline{\mathbb{N}}$ is extended natural.

An extended natural is an extended natural extended real. Let x be an extended natural. Note that $x(\in \overline{\mathbb{N}})$ reduces to x.

One can check that sethood property holds for extended naturals.

Now we state the proposition:

(2) Let us consider an object x. Then x is an extended natural if and only if x is a natural number or $x = +\infty$.

Note that every object which is zero is also extended natural and every extended real which is extended natural is also non negative and every extended natural is non negative and every extended natural which is non zero is also positive.

From now on N, M, K denote extended naturals.

Let us consider N and M. Observe that $\min(N, M)$ is extended natural and $\max(N, M)$ is extended natural and $N + M$ is extended natural and $N \cdot M$ is extended natural.

Now we state the propositions:

(3) $0 \leqslant N$.

(4) If $0 \neq N$, then $0 < N$.

(5) $0 < N + 1$.

(6) If $M \in \mathbb{N}$ and $N \leqslant M$, then $N \in \mathbb{N}$.

(7) If $N < M$, then $N \in \mathbb{N}$.

(8) If $N \leqslant M$, then $N \cdot K \leqslant M \cdot K$.

(9) (i) $N = 0$, or

(ii) there exists K such that $N = K + 1$.

The theorem is a consequence of (2).

(10) If $N + M = 0$, then $N = 0$ and $M = 0$.

Let M be an extended natural and N be a non zero extended natural. One can check that $M + N$ is non zero and $N + M$ is non zero.

Now we state the propositions:

(11) If $N \leqslant M + 1$, then $N \leqslant M$ or $N = M + 1$.

(12) If $N \leqslant M \leqslant N + 1$, then $N = M$ or $M = N + 1$.

(13) If $N \leqslant M$, then there exists K such that $M = N + K$.

(14) $N \leqslant N + M$.

(15) If $N \leqslant M$, then $N \leqslant M + K$.

(16) If $N < 1$, then $N = 0$.

(17) If $N \cdot M = 1$, then $N = 1$.

(18) $K < K + N$ if and only if $1 \leqslant N$ and $K \neq +\infty$.

(19) If $K \neq 0$ and $N = M \cdot K$, then $M \leqslant N$.

(20) If $M \leqslant N$, then $M \cdot K \leqslant N \cdot K$.

(21) $(K + M) + N = K + (M + N)$.

(22) $K \cdot (N + M) = K \cdot N + K \cdot M$.

2. Sets of Extended Natural Numbers

Let X be a set. We say that X is extended natural-membered if and only if

(Def. 3) for every object x such that $x \in X$ holds x is extended natural.

Note that every set which is empty is also extended natural-membered and every set which is natural-membered is also extended natural-membered.

Every set which is extended natural-membered is also extended real-membered and $\overline{\mathbb{N}}$ is extended natural-membered and there exists a set which is non empty and extended natural-membered. Now we state the proposition:

(23) Let us consider a set X. Then X is extended natural-membered if and only if $X \subseteq \overline{\mathbb{N}}$.

In the sequel X denotes an extended natural-membered set.

Let us consider X. Let us observe that every element of X is extended natural. Now we state the propositions:

(24) Let us consider a non empty, extended natural-membered set X. Then there exists N such that $N \in X$.

(25) If for every N, $N \in X$, then $X = \overline{\mathbb{N}}$.

(26) Let us consider a set Y. If $Y \subseteq X$, then Y is extended natural-membered.

Let us consider X. One can verify that every subset of X is extended natural-membered. Let us consider N. Let us observe that $\{N\}$ is extended natural-membered. Let us consider M. Let us note that $\{N, M\}$ is extended natural-membered. Let us consider K. One can verify that $\{N, M, K\}$ is extended natural-membered.

Let us consider X. Let Y be an extended natural-membered set. One can verify that $X \cup Y$ is extended natural-membered.

Let Y be a set. One can verify that $X \cap Y$ is extended natural-membered and $X \setminus Y$ is extended natural-membered.

Let Y be an extended natural-membered set. One can check that $X \dot{-} Y$ is extended natural-membered.

Let Y be a set. One can check that $X \subseteq Y$ if and only if the condition (Def. 4) is satisfied.

(Def. 4) if $N \in X$, then $N \in Y$.

Let Y be an extended natural-membered set. One can check that $X = Y$ if and only if the condition (Def. 5) is satisfied.

(Def. 5) $N \in X$ iff $N \in Y$.

One can verify that X misses Y if and only if the condition (Def. 6) is satisfied.

(Def. 6) there exists no N such that $N \in X$ and $N \in Y$.

Now we state the propositions:

(27) Let us consider a set F. Suppose for every set X such that $X \in F$ holds X is extended natural-membered. Then $\bigcup F$ is extended natural-membered.

(28) Let us consider sets F, X. Suppose $X \in F$ and X is extended natural-membered. Then $\bigcap F$ is extended natural-membered.

The scheme *ENMSeparation* deals with a unary predicate $\mathcal{P}$ and states that

(Sch. 1) There exists an extended natural-membered set X such that for every N, $N \in X$ iff $\mathcal{P}[N]$.

Let X be an extended natural-membered set. Let us note that an upper bound of X can equivalently be formulated as follows:

(Def. 7) for every N such that $N \in X$ holds $N \leqslant it$.

One can check that a lower bound of X can equivalently be formulated as follows:

(Def. 8) for every N such that $N \in X$ holds $it \leqslant N$.

Let us note that every extended natural-membered set is lower bounded and every extended natural-membered set which is non empty is also left-ended.

Let us consider X. Note that there exists an upper bound of X which is extended natural and there exists a lower bound of X which is extended natural and $\inf X$ is extended natural.

Let X be a non empty, extended natural-membered set. Let us note that $\sup X$ is extended natural and every extended natural-membered set which is non empty and upper bounded is also right-ended.

Let X be a left-ended, extended natural-membered set. One can verify that the functor $\min X$ yields an extended natural and is defined by

(Def. 9) $it \in X$ and for every N such that $N \in X$ holds $it \leqslant N$.

Let X be a right-ended, extended natural-membered set. One can verify that the functor $\max X$ yields an extended natural and is defined by

(Def. 10) $it \in X$ and for every N such that $N \in X$ holds $N \leqslant it$.

3. Relations with Extended Natural Numbers in Range

Let R be a binary relation. We say that R is extended natural-valued if and only if

(Def. 11) $\operatorname{rng} R \subseteq \overline{\mathbb{N}}$.

Let us note that every binary relation which is empty is also extended natural-valued and every binary relation which is natural-valued is also extended natural-valued and every binary relation which is extended natural-valued is also $(\overline{\mathbb{N}})$-valued and extended real-valued.

Every binary relation which is $(\overline{\mathbb{N}})$-valued is also extended natural-valued and there exists a function which is extended natural-valued.

Let R be an extended natural-valued binary relation. One can check that $\operatorname{rng} R$ is extended natural-membered.

Now we state the proposition:

(29) Let us consider a binary relation R, and an extended natural-valued binary relation S. If $R \subseteq S$, then R is extended natural-valued.

Let R be an extended natural-valued binary relation. Observe that every subset of R is extended natural-valued.

Let R, S be extended natural-valued binary relations. One can verify that $R \cup S$ is extended natural-valued.

Let R be an extended natural-valued binary relation and S be a binary relation. One can check that $R \cap S$ is extended natural-valued and $R \setminus S$ is extended natural-valued and $S \cdot R$ is extended natural-valued.

Let R, S be extended natural-valued binary relations. Note that $R \dot{-} S$ is extended natural-valued.

Let R be an extended natural-valued binary relation and X be a set. Let us note that $R^\circ X$ is extended natural-membered and $R{\restriction}X$ is extended natural-valued and $X{\restriction}R$ is extended natural-valued.

Let x be an object. Let us observe that $R^\circ x$ is extended natural-membered.

Let us consider X. One can check that id_X is extended natural-valued.

Let f be a function. Note that f is extended natural-valued if and only if the condition (Def. 12) is satisfied.

(Def. 12) for every object x such that $x \in \operatorname{dom} f$ holds $f(x)$ is extended natural.

Now we state the proposition:

(30) Let us consider a function f. Then f is extended natural-valued if and only if for every object x, $f(x)$ is extended natural.

Let f be an extended natural-valued function and x be an object. Observe that $f(x)$ is extended natural.

Let X be a set. Let us consider N. One can verify that $X \longmapsto N$ is extended natural-valued.

Let f, g be extended natural-valued functions. Note that $f + \cdot g$ is extended natural-valued.

Let x be an object. Let us consider N. Let us observe that $x \dot{\longmapsto} N$ is extended natural-valued.

Let Z be a set. Let us consider X. Note that every relation between Z and X is extended natural-valued and $Z \times X$ is extended natural-valued as a relation between Z and X and there exists a function which is non empty, constant, and extended natural-valued.

Now we state the proposition:

(31) Let us consider a non empty, constant, extended natural-valued function f. Then there exists N such that for every object x such that $x \in \operatorname{dom} f$ holds $f(x) = N$.

4. Ordinal Preliminaries

Now we state the proposition:

(32) Let us consider a function f. Then f is ordinal yielding if and only if for every object x such that $x \in \operatorname{dom} f$ holds $f(x)$ is an ordinal number.

One can check that every set which is ordinal is also $\subseteq$-linear.

Let f be an ordinal yielding function and x be an object. Observe that $f(x)$ is ordinal.

Let A, B be non-empty transfinite sequences. Note that $A^\frown B$ is non-empty.

Now we state the propositions:

(33) Let us consider a set X, and an object x. Then $\overline{\overline{X \longmapsto x}} = \overline{\overline{X}}$.

(34) Let us consider a cardinal number c, and an object x. Then $\overline{\overline{c \longmapsto x}} = c$. The theorem is a consequence of (33).

Let X be a trivial set. One can verify that $\overline{\overline{X}}$ is trivial.

Let c_1 be a cardinal number and c_2 be a non empty cardinal number. Note that $c_1 + c_2$ is non empty.

Now we state the propositions:

(35) Let us consider an ordinal number A. Then $A \neq 0$ and $A \neq 1$ if and only if A is not trivial.

(36) Let us consider an ordinal number A, and an infinite cardinal number B. If $A \in B$, then $A + B = B$.

PROOF: Define $\mathcal{F}(\text{ordinal number}) = A + \$_1$. Consider f being a sequence of ordinal numbers such that $\operatorname{dom} f = B$ and for every ordinal number C such that $C \in B$ holds $f(C) = \mathcal{F}(C)$. $\square$

Let f be a cardinal yielding function and g be a function. Observe that $f \cdot g$ is cardinal yielding and every function which is natural-valued is also cardinal yielding.

Let f be an empty function. Let us observe that disjoint f is empty.

Let f be an empty yielding function. One can verify that disjoint f is empty yielding.

Let f be a non empty yielding function. One can check that disjoint f is non empty yielding.

Let f be an empty yielding function. One can verify that $\bigcup f$ is empty and every function which is cardinal yielding is also ordinal yielding.

Now we state the proposition:

(37) Let us consider a function f, and a permutation p of $\operatorname{dom} f$. Then $\operatorname{Card}(f \cdot p) = (\operatorname{Card} f) \cdot p$.

Let A be a transfinite sequence. Note that $\operatorname{Card} A$ is transfinite sequence-like.

Now we state the proposition:

(38) Let us consider transfinite sequences A, B. Then $\operatorname{Card}(A^\frown B) = \operatorname{Card} A^\frown \operatorname{Card} B$.

Let f be a trivial function. One can check that $\operatorname{Card} f$ is trivial.

Let f be a non trivial function. Note that $\operatorname{Card} f$ is non trivial.

Let A, B be cardinal yielding transfinite sequences. Note that $A \frown B$ is cardinal yielding.

Let c_1 be a cardinal number. Note that $\langle c_1 \rangle$ is cardinal yielding.

Let c_2 be a cardinal number. Let us observe that $\langle c_1, c_2 \rangle$ is cardinal yielding.

Let c_3 be a cardinal number. One can verify that $\langle c_1, c_2, c_3 \rangle$ is cardinal yielding.

Let X_1, X_2, X_3 be non empty sets. One can verify that $\langle X_1, X_2, X_3 \rangle$ is non-empty.

Let A be an infinite ordinal number. Let us note that $\langle A \rangle$ is non natural-valued.

Let x be an object. Let us observe that $\langle A, x \rangle$ is non natural-valued and $\langle x, A \rangle$ is non natural-valued.

Let y be an object. Observe that $\langle A, x, y \rangle$ is non natural-valued and $\langle x, A, y \rangle$ is non natural-valued and $\langle x, y, A \rangle$ is non natural-valued and there exists a finite 0-sequence which is non empty, non-empty, and natural-valued and $\langle x \rangle$ is one-to-one.

Now we state the propositions:

(39) Let us consider objects x, y. Then

(i) $\operatorname{dom}\langle x, y \rangle = \{0, 1\}$, and

(ii) $\operatorname{rng}\langle x, y \rangle = \{x, y\}$.

(40) Let us consider objects x, y, z. Then

(i) $\operatorname{dom}\langle x, y, z \rangle = \{0, 1, 2\}$, and

(ii) $\operatorname{rng}\langle x, y, z \rangle = \{x, y, z\}$.

Let x be an object. One can verify that $\langle x \rangle$ is trivial.

Let y be an object. Let us note that $\langle x, y \rangle$ is non trivial.

Let z be an object. Let us note that $\langle x, y, z \rangle$ is non trivial and there exists a finite 0-sequence which is non empty and trivial.

Let D be a non empty set. One can check that there exists a finite 0-sequence of D which is non empty and trivial.

Now we state the propositions:

(41) Let us consider a non empty, trivial transfinite sequence p. Then there exists an object x such that $p = \langle x \rangle$.

(42) Let us consider a non empty set D, and a non empty, trivial transfinite sequence p of elements of D. Then there exists an element x of D such that $p = \langle x \rangle$. The theorem is a consequence of (41).

(43) $\langle 0 \rangle = \mathrm{id}_1$.

(44) $\langle 0, 1 \rangle = \mathrm{id}_2$. The theorem is a consequence of (39).

(45) $\langle 0, 1, 2 \rangle = \mathrm{id}_3$. The theorem is a consequence of (40).

(46) Let us consider objects x, y. Then $\langle x, y \rangle \cdot \langle 1, 0 \rangle = \langle y, x \rangle$. The theorem is a consequence of (39).

Let us consider objects x, y, z. Now we state the propositions:

(47) $\langle x, y, z \rangle \cdot \langle 0, 2, 1 \rangle = \langle x, z, y \rangle$. The theorem is a consequence of (40).

(48) $\langle x, y, z \rangle \cdot \langle 1, 0, 2 \rangle = \langle y, x, z \rangle$. The theorem is a consequence of (40).

(49) $\langle x, y, z \rangle \cdot \langle 1, 2, 0 \rangle = \langle y, z, x \rangle$. The theorem is a consequence of (40).

(50) $\langle x, y, z \rangle \cdot \langle 2, 0, 1 \rangle = \langle z, x, y \rangle$. The theorem is a consequence of (40).

(51) $\langle x, y, z \rangle \cdot \langle 2, 1, 0 \rangle = \langle z, y, x \rangle$. The theorem is a consequence of (40).

(52) Let us consider objects x, y. If $x \neq y$, then $\langle x, y \rangle$ is one-to-one. The theorem is a consequence of (39).

(53) Let us consider objects x, y, z. If $x \neq y$ and $x \neq z$ and $y \neq z$, then $\langle x, y, z \rangle$ is one-to-one. The theorem is a consequence of (40).

5. Relations with Cardinal Domain

Let R be a binary relation. We say that R is with cardinal domain if and only if

(Def. 13) there exists a cardinal number c such that $\operatorname{dom} R = c$.

One can verify that every binary relation which is empty is also with cardinal domain and every binary relation which is finite and transfinite sequence-like is also with cardinal domain and every binary relation which is with cardinal domain is also transfinite sequence-like.

Let c be a cardinal number. Let us observe that every many sorted set indexed by c is with cardinal domain.

Let x be an object. Let us note that $c \longmapsto x$ is with cardinal domain.

Let X be a set. Let us note that every denumeration of X is with cardinal domain.

Let c be a cardinal number. One can verify that every permutation of c is with cardinal domain and there exists a function which is non empty, trivial, non-empty, with cardinal domain, and cardinal yielding and there exists a function which is non empty, non trivial, non-empty, finite, with cardinal domain, and cardinal yielding.

There exists a function which is non empty, non-empty, infinite, with cardinal domain, and natural-valued and there exists a function which is non trivial, non-empty, with cardinal domain, cardinal yielding, and non natural-valued.

Let R be a with cardinal domain binary relation. One can check that $\operatorname{dom} R$ is cardinal.

Let f be a with cardinal domain function. We identify $\overline{\overline{f}}$ with $\operatorname{dom} f$. Let R be a with cardinal domain binary relation and P be a total, $(\operatorname{rng} R)$-defined binary relation. One can verify that $R \cdot P$ is with cardinal domain.

Let g be a function and f be a denumeration of $\operatorname{dom} g$. Let us observe that $g \cdot f$ is with cardinal domain.

Let f be a with cardinal domain function and p be a permutation of $\operatorname{dom} f$. Observe that $f \cdot p$ is with cardinal domain.

Now we state the proposition:

(54) Let us consider with cardinal domain transfinite sequences A, B. Suppose $\operatorname{dom} A \in \operatorname{dom} B$. Then $A \frown B$ is with cardinal domain. The theorem is a consequence of (36).

Let p be a finite 0-sequence and B be a with cardinal domain transfinite sequence. Observe that $p \frown B$ is with cardinal domain.

A Counters is a non empty, with cardinal domain, cardinal yielding function.

A Counters_{+} is a non empty, non-empty, with cardinal domain, cardinal yielding function.

References

[1] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

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

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

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

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

[6] 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.

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

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

[9] Library Committee of the Association of Mizar Users. Number-valued functions. *Mizar Mathematical Library*, 2007.

[10] Library Committee of the Association of Mizar Users. Introduction to arithmetic of extended real numbers. *Mizar Mathematical Library*, 2006.

[11] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[12] Andrzej Trybulec. Subsets of complex numbers. *Mizar Mathematical Library*, 2003.

[13] Andrzej Trybulec. Basic operations on extended real numbers. *Mizar Mathematical Library*, 2008.

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

Accepted September 25, 2020

FORMALIZED MATHEMATICS
Vol. 28, No. 3, Pages 251–261, 2020
DOI: 10.2478/forma-2020-0022

sciendo
https://www.sciendo.com/

Ring and Field Adjunctions, Algebraic Elements and Minimal Polynomials

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In [6], [7] we presented a formalization of Kronecker's construction of a field extension of a field F in which a given polynomial $p \in F[X]\backslash F$ has a root [4], [5], [3]. As a consequence for every field F and every polynomial there exists a field extension E of F in which p splits into linear factors. It is well-known that one gets the smallest such field extension – the splitting field of p – by adjoining the roots of p to F.

In this article we start the Mizar formalization [1], [2] towards splitting fields: we define ring and field adjunctions, algebraic elements and minimal polynomials and prove a number of facts necessary to develop the theory of splitting fields, in particular that for an algebraic element a over F a basis of the vector space $F(a)$ over F is given by $a^0, \ldots, a^{n-1}$, where n is the degree of the minimal polynomial of a over F.

MSC: 12F05 68V20

Keywords: ring and field adjunctions; algebraic elements and minimal polynomials

MML identifier: FIELD_6, version: 8.1.10 5.64.1388

1. Preliminaries

Now we state the proposition:

(1) Let us consider a ring R. Then R is degenerated if and only if the carrier of $R = \{0_R\}$.

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

Let F be a field. Note that $\{0_F\}$–ideal is maximal.

Let R be a non degenerated, non almost left invertible commutative ring. Let us note that $\{0_R\}$–ideal is non maximal.

Let R be a ring. We say that R has a subfield if and only if

(Def. 1) there exists a field F such that F is a subring of R.

Observe that there exists a ring which has a subfield.

Let R be a ring which has a subfield.

A subfield of R is a field defined by

(Def. 2) *it* is a subring of R.

Now we state the proposition:

(2) Let us consider a non degenerated ring R, and a non zero polynomial p over R. Then $p(\deg p) = \mathrm{LC}\, p$.

Let R be a non degenerated ring and p be a non zero polynomial over R. One can verify that $\mathrm{LM}(p)$ is non zero.

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

(3) $\deg \mathrm{LM}(p) = \deg p$.

(4) $\mathrm{LC}\, \mathrm{LM}(p) = \mathrm{LC}\, p$.

(5) Let us consider a non degenerated ring R, and a non zero polynomial p over R. Then $\deg(p - \mathrm{LM}(p)) < \deg p$. The theorem is a consequence of (2), (3), and (4).

(6) Let us consider a ring R, a polynomial p over R, and a natural number i. Then $(\langle 0_R, 1_R\rangle * p)(i+1) = p(i)$.

(7) Let us consider a ring R, and a polynomial p over R. Then $(\langle 0_R, 1_R\rangle * p)(0) = 0_R$.

(8) Let us consider an integral domain R, and a non zero polynomial p over R. Then $\deg(\langle 0_R, 1_R\rangle * p) = \deg p + 1$.

(9) Let us consider a commutative ring R, a polynomial p over R, and an element a of R. Then $\mathrm{eval}(\langle 0_R, 1_R\rangle * p, a) = a \cdot (\mathrm{eval}(p, a))$. The theorem is a consequence of (1).

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

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

Let L be a non empty zero structure, a, b be elements of L, f be a (the carrier of L)-valued function, and x, y be objects. Observe that $f + \cdot [x \longmapsto a, y \longmapsto b]$ is

(the carrier of L)-valued.

Let f be a finite-Support sequence of L. One can verify that $f+\cdot[x \longmapsto a, y \longmapsto b]$ is finite-Support as a sequence of L.

2. On Subrings and Subfields

Now we state the propositions:

(12) Let us consider strict rings R_1, R_2. Suppose R_1 is a subring of R_2 and R_2 is a subring of R_1. Then $R_1 = R_2$.

(13) Let us consider a ring S, and subrings R_1, R_2 of S. Then R_1 is a subring of R_2 if and only if the carrier of $R_1 \subseteq$ the carrier of R_2.

(14) Let us consider a ring S, and strict subrings R_1, R_2 of S. Then $R_1 = R_2$ if and only if the carrier of $R_1 =$ the carrier of R_2. The theorem is a consequence of (13) and (12).

Let us consider a ring S, a subring R of S, elements x, y of S, and elements x_1, y_1 of R. Now we state the propositions:

(15) If $x = x_1$ and $y = y_1$, then $x + y = x_1 + y_1$.

(16) If $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.

(17) Let us consider a ring S, a subring R of S, an element x of S, and an element x_1 of R. If $x = x_1$, then $-x = -x_1$. The theorem is a consequence of (15).

(18) Let us consider a field E, a subfield F of E, a non zero element x of E, and an element x_1 of F. If $x = x_1$, then $x^{-1} = {x_1}^{-1}$. The theorem is a consequence of (16).

(19) Let us consider a ring S, a subring R of S, an element x of S, an element x_1 of R, and an element n of $\mathbb{N}$. If $x = x_1$, then $x^n = {x_1}^n$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every element x of S for every element x_1 of R such that $x = x_1$ holds $x^{\$_1} = {x_1}^{\$_1}$. For every natural number k, $\mathcal{P}[k]$. $\square$

(20) Let us consider a ring S, a subring R of S, elements x_1, x_2 of S, and elements y_1, y_2 of R. Suppose $x_1 = y_1$ and $x_2 = y_2$. Then $\langle x_1, x_2\rangle = \langle y_1, y_2\rangle$.

(21) Let us consider a commutative ring R, a commutative ring extension S of R, elements x_1, x_2 of S, elements y_1, y_2 of R, and an element n of $\mathbb{N}$. Suppose $x_1 = y_1$ and $x_2 = y_2$. Then $\langle x_1, x_2\rangle^n = \langle y_1, y_2\rangle^n$.

(22) Let us consider an integral domain R, a domain ring extension S of R, a non zero element n of $\mathbb{N}$, and an element a of S.
Then $\mathrm{ExtEval}(\langle 0_R, 1_R\rangle^n, a) = a^n$. The theorem is a consequence of (21).

(23) Let us consider a ring R, a ring extension S of R, an element a of R, and an element b of S. If $a = b$, then $a\restriction R = b\restriction S$.

(24) Let us consider a field F, an extension E of F, an element p of the carrier of PolyRing(F), and an element q of the carrier of PolyRing(E). If $p = q$, then NormPoly p = NormPoly q. The theorem is a consequence of (18) and (16).

(25) Let us consider a field F, an extension E of F, an element p of the carrier of PolyRing(F), and an element a of E. Then ExtEval$(p, a) = 0_E$ if and only if ExtEval(NormPoly $p, a) = 0_E$. The theorem is a consequence of (24).

(26) Let us consider a ring R, a ring extension S of R, an element a of S, and a polynomial p over R. Then ExtEval$(-p, a) = -$ExtEval(p, a). The theorem is a consequence of (17).

(27) Let us consider a ring R, a ring extension S of R, an element a of S, and polynomials p, q over R. Then ExtEval$(p - q, a) =$ ExtEval$(p, a) -$ ExtEval(q, a). The theorem is a consequence of (26).

(28) Let us consider a ring R, a ring extension S of R, an element a of S, and a constant polynomial p over R. Then ExtEval$(p, a) =$ LC p.

(29) Let us consider a non degenerated ring R, a ring extension S of R, elements a, b of S, and a non zero polynomial p over R. Suppose $b =$ LC p. Then ExtEval(Leading-Monomial $p, a) = b \cdot (a^{\deg p})$.

3. Ring and Field Adjunctions

Let R be a ring, S be a ring extension of R, and T be a subset of S. The functor /\\(R, T) yielding a non empty subset of S is defined by the term

(Def. 3) $\{x$, where x is an element of S : for every subring U of S such that R is a subring of U and T is a subset of U holds $x \in U\}$.

The functor RingAdjunction(R, T) yielding a strict double loop structure is defined by

(Def. 4) the carrier of it = /\\(R, T) and the addition of it = (the addition of S) $\restriction$ /\\(R, T) and the multiplication of it = (the multiplication of S) $\restriction$ /\\(R, T) and the one of $it = 1_S$ and the zero of $it = 0_S$.

We introduce the notation RAdj(R, T) as a synonym of RingAdjunction(R, T).

One can check that RAdj(R, T) is non empty.

Let R be a non degenerated ring. Let us observe that RAdj(R, T) is non degenerated.

Let R be a ring. Observe that $\mathrm{RAdj}(R,T)$ is Abelian, add-associative, right zeroed, and right complementable.

Let R be a commutative ring and S be a commutative ring extension of R. One can check that $\mathrm{RAdj}(R,T)$ is commutative.

Let R be a ring and S be a ring extension of R. Let us observe that $\mathrm{RAdj}(R,T)$ is associative, well unital, and distributive.

Now we state the propositions:

(30) Let us consider a ring R, and a ring extension S of R. Then every subset T of S is a subset of $\mathrm{RAdj}(R,T)$.

(31) Let us consider a ring R, a ring extension S of R, and a subset T of S. Then R is a subring of $\mathrm{RAdj}(R,T)$.

(32) Let us consider a ring R, a ring extension S of R, a subset T of S, and a subring U of S. Suppose R is a subring of U and T is a subset of U. Then $\mathrm{RAdj}(R,T)$ is a subring of U.

(33) Let us consider a strict ring R, a ring extension S of R, and a subset T of S. Then $\mathrm{RAdj}(R,T) = R$ if and only if T is a subset of R. The theorem is a consequence of (30).

Let R be a ring, S be a ring extension of R, and T be a subset of S. Let us note that the functor $\mathrm{RAdj}(R,T)$ yields a strict subring of S. One can check that $\mathrm{RAdj}(R,T)$ is R-extending.

Let F be a field, R be a ring extension of F, and T be a subset of R. Let us note that $\mathrm{RAdj}(F,T)$ has a subfield.

Now we state the proposition:

(34) Let us consider a field F, a ring extension R of F, and a subset T of R. Then F is a subfield of $\mathrm{RAdj}(F,T)$. The theorem is a consequence of (31).

Let F be a field, E be an extension of F, and T be a subset of E. The functor $/\backslash(\mathrm{F},T)$ yielding a non empty subset of E is defined by the term

(Def. 5) $\{x$, where x is an element of E : for every subfield U of E such that F is a subfield of U and T is a subset of U holds $x \in U\}$.

The functor $\mathrm{FieldAdjunction}(F,T)$ yielding a strict double loop structure is defined by

(Def. 6) the carrier of $it = /\backslash(\mathrm{F},T)$ and the addition of $it =$ (the addition of E) $\restriction /\backslash(\mathrm{F},T)$ and the multiplication of $it =$ (the multiplication of E) $\restriction /\backslash(\mathrm{F},T)$ and the one of $it = 1_E$ and the zero of $it = 0_E$.

We introduce the notation $\mathrm{FAdj}(F,T)$ as a synonym of $\mathrm{FieldAdjunction}(F,T)$. One can check that $\mathrm{FAdj}(F,T)$ is non degenerated and $\mathrm{FAdj}(F,T)$ is Abelian, add-associative, right zeroed, and right complementable and $\mathrm{FieldAdjunction}(F,$

T) is commutative, associative, well unital, distributive, and almost left invertible.

Now we state the propositions:

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

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

(37) Let us consider a field F, an extension E of F, a subset T of E, and a subfield U of E. Suppose F is a subfield of U and T is a subset of U. Then $\mathrm{FAdj}(F, T)$ is a subfield of U.

(38) Let us consider a strict field F, an extension E of F, and a subset T of E. Then $\mathrm{FAdj}(F, T) = F$ if and only if T is a subset of F. The theorem is a consequence of (35).

Let F be a field, E be an extension of F, and T be a subset of E. Let us observe that the functor $\mathrm{FAdj}(F, T)$ yields a strict subfield of E. Let us note that $\mathrm{FAdj}(F, T)$ is F-extending.

Let us consider a field F, an extension E of F, and a subset T of E. Now we state the propositions:

(39) $\mathrm{RAdj}(F, T)$ is a subring of $\mathrm{FAdj}(F, T)$.

(40) $\mathrm{RAdj}(F, T) = \mathrm{FAdj}(F, T)$ if and only if $\mathrm{RAdj}(F, T)$ is a field. The theorem is a consequence of (31), (30), (37), (39), and (12).

4. Algebraic Elements

Let R be a non degenerated commutative ring, S be a commutative ring extension of R, and a be an element of S. Observe that $\mathrm{HomExtEval}(a, R)$ is additive, multiplicative, and unity-preserving and every commutative ring extension of R is $(\mathrm{PolyRing}(R))$-homomorphic.

Let F be a field. Let us note that there exists an extension of F which is $(\mathrm{PolyRing}(F))$-homomorphic.

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

(Def. 7) $\ker \mathrm{HomExtEval}(a, F) \neq \{0_{\mathrm{PolyRing}(F)}\}$.

We introduce the notation a is F-transcendental as an antonym for a is F-algebraic. Now we state the proposition:

(41) Let us consider a ring R, a ring extension S of R, and an element a of S. Then $\mathrm{AnnPoly}(a, R) = \ker \mathrm{HomExtEval}(a, R)$.

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

(42) a is F-algebraic if and only if a is integral over F. The theorem is a consequence of (25).

(43) a is F-algebraic if and only if there exists a non zero polynomial p over F such that $\mathrm{ExtEval}(p, a) = 0_E$. The theorem is a consequence of (42).

Let F be a field and E be an extension of F. Note that there exists an element of E which is F-algebraic.

Let us consider a field F, a $(\mathrm{PolyRing}(F))$-homomorphic extension E of F, and an element a of E. Now we state the propositions:

(44) $\mathrm{RAdj}(F, \{a\}) = \operatorname{Im} \mathrm{HomExtEval}(a, F)$. The theorem is a consequence of (20), (32), and (14).

(45) The carrier of $\mathrm{RAdj}(F, \{a\})$ = the set of all $\mathrm{ExtEval}(p, a)$ where p is a polynomial over F. The theorem is a consequence of (44).

5. On Linear Combinations and Polynomials

Now we state the propositions:

(46) Let us consider a field F, a vector space V over F, a subspace W of V, and a linear combination l_1 of W. Then there exists a linear combination l_2 of V such that

(i) the support of l_2 = the support of l_1, and

(ii) for every element v of V such that $v \in$ the support of l_2 holds $l_2(v) = l_1(v)$.

PROOF: Consider f being a function such that $l_1 = f$ and $\operatorname{dom} f =$ the carrier of W and $\operatorname{rng} f \subseteq$ the carrier of F. Define $\mathcal{P}[\text{element of } V, \text{element of } F] \equiv \$_1 \in$ the support of l_1 and $\$_2 = f(\$_1)$ or $\$_1 \notin$ the support of l_1 and $\$_2 = 0_F$. For every element x of the carrier of V, there exists an element y of the carrier of F such that $\mathcal{P}[x, y]$. Consider g being a function from V into F such that for every element x of V, $\mathcal{P}[x, g(x)]$. □

(47) Let us consider a field F, an extension E of F, an element a of E, an element n of $\mathbb{N}$, and a linear combination l of $\mathrm{VecSp}(E, F)$. Then there exists a polynomial p over F such that

(i) $\deg p \leqslant n$, and

(ii) for every element i of $\mathbb{N}$ such that $i \leqslant n$ holds $p(i) = l(a^i)$.

PROOF: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a natural number i such that $i \leqslant n$ and $\$_1 = i$ and $\$_2 = l(a^i)$ or there exists a natural number i such that $i > n$ and $\$_1 = i$ and $\$_2 = 0_F$. For every element x of $\mathbb{N}$, there exists an element y of the carrier of F such that $\mathcal{P}[x, y]$. Consider p being a function from $\mathbb{N}$ into the carrier of F such that for every element x of $\mathbb{N}$, $\mathcal{P}[x, p(x)]$. For every natural number i such that $i \leqslant n$ holds $p(i) = l(a^i)$. For every natural number i such that $i \geqslant n + 1$ holds $p(i) = 0_F$. □

(48) Let us consider a field F, an extension E of F, an element a of E, an element n of $\mathbb{N}$, a linear combination l of $\mathrm{VecSp}(E, F)$, and a non zero polynomial p over F. Suppose $l(a^{\deg p}) = \mathrm{LC}\, p$ and the support of $l = \{a^{\deg p}\}$. Then $\sum l = \mathrm{ExtEval}(\mathrm{LM}(p), a)$. The theorem is a consequence of (35) and (29).

(49) Let us consider a field F, an extension E of F, an element a of E, an element n of $\mathbb{N}$, and a subset M of $\mathrm{VecSp}(E, F)$. Suppose $M = \{a^i$, where i is an element of $\mathbb{N} : i \leqslant n\}$ and for every elements i, j of $\mathbb{N}$ such that $i < j \leqslant n$ holds $a^i \neq a^j$. Let us consider a linear combination l of M, and a polynomial p over F. Suppose $\deg p \leqslant n$ and for every element i of $\mathbb{N}$ such that $i \leqslant n$ holds $p(i) = l(a^i)$. Then $\mathrm{ExtEval}(p, a) = \sum l$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every linear combination l of M such that $\overline{\overline{\text{the support of } l}} = \$_1$ for every polynomial p over F such that $\deg p \leqslant n$ and for every element i of $\mathbb{N}$ such that $i \leqslant n$ holds $p(i) = l(a^i)$ holds $\sum l = \mathrm{ExtEval}(p, a)$. $\mathcal{P}[0]$ by [8, (13)]. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{\alpha}} = n$, where α is the support of l. □

6. Minimal Polynomials

Let F be a field, E be an extension of F, and a be an F-algebraic element of E. We introduce the notation $\mathrm{MinPoly}(a, F)$ as a synonym of the minimal polynomial of a over F.

Note that $\mathrm{MinPoly}(a, F)$ is monic and irreducible.

Let us consider a field F, an extension E of F, an F-algebraic element a of E, and an element p of the carrier of $\mathrm{PolyRing}(F)$. Now we state the propositions:

(50) $p = \mathrm{MinPoly}(a, F)$ if and only if p is monic and irreducible and $\ker \mathrm{Hom}\text{-}\mathrm{ExtEval}(a, F) = \{p\}$–ideal. The theorem is a consequence of (42) and (41).

(51) $p = \mathrm{MinPoly}(a, F)$ if and only if p is monic and $\mathrm{ExtEval}(p, a) = 0_E$ and for every non zero polynomial q over F such that $\mathrm{ExtEval}(q, a) = 0_E$ holds $\deg p \leqslant \deg q$. The theorem is a consequence of (42) and (50).

(52) $p = \mathrm{MinPoly}(a, F)$ if and only if p is monic and irreducible and $\mathrm{ExtEval}(p,$

$a) = 0_E$. The theorem is a consequence of (42) and (50).

(53) $\mathrm{ExtEval}(p, a) = 0_E$ if and only if $\mathrm{MinPoly}(a, F) \mid p$. The theorem is a consequence of (50) and (51).

(54) Let us consider a field F, an extension E of F, and an F-algebraic element a of E. Then $\mathrm{MinPoly}(a, F) = \mathrm{rpoly}(1, a)$ if and only if $a \in$ the carrier of F. The theorem is a consequence of (10), (52), and (17).

(55) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and elements i, j of $\mathbb{N}$. If $i < j < \deg \mathrm{MinPoly}(a, F)$, then $a^i \neq a^j$. The theorem is a consequence of (7), (6), (17), (52), and (53).

(56) Let us consider a field F, a (PolyRing(F))-homomorphic extension E of F, and an element a of E. Then a is F-algebraic if and only if $\mathrm{FAdj}(F, \{a\}) = \mathrm{RAdj}(F, \{a\})$. The theorem is a consequence of (50), (44), and (40).

(57) Let us consider a field F, a (PolyRing(F))-homomorphic extension E of F, and a non zero element a of E. Then a is F-algebraic if and only if $a^{-1} \in \mathrm{RAdj}(F, \{a\})$. The theorem is a consequence of (56), (35), (18), (45), (17), (28), and (43).

(58) Let us consider a field F, an extension E of F, and an element a of E. Then a is F-transcendental if and only if $\mathrm{RAdj}(F, \{a\})$ and PolyRing(F) are isomorphic. The theorem is a consequence of (44) and (56).

(59) Let us consider a field F, a (PolyRing(F))-homomorphic extension E of F, and an F-algebraic element a of E.
Then PolyRing(F)/$\{\mathrm{MinPoly}(a, F)\}$–ideal and $\mathrm{FAdj}(F, \{a\})$ are isomorphic. The theorem is a consequence of (50), (44), and (56).

7. A Basis of the Vector Space $\mathrm{VecSp}(\mathrm{FAdj}(F, \{a\}), F)$

Let F be a field, E be an extension of F, and a be an F-algebraic element of E. The functor $\mathrm{Base}(a)$ yielding a non empty subset of $\mathrm{VecSp}(\mathrm{FAdj}(F, \{a\}), F)$ is defined by the term

(Def. 8) $\{a^n$, where n is an element of $\mathbb{N} : n < \deg \mathrm{MinPoly}(a, F)\}$.

One can verify that $\mathrm{Base}(a)$ is finite. Now we state the propositions:

(60) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and a polynomial p over F. Then $\mathrm{ExtEval}(p, a) \in \mathrm{Lin}(\mathrm{Base}(a))$. The theorem is a consequence of (51).

(61) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and a linear combination l of $\mathrm{Base}(a)$. Then there exists a polynomial p over F such that

(i) $\deg p < \deg \mathrm{MinPoly}(a, F)$, and

(ii) for every element i of $\mathbb{N}$ such that $i < \deg \mathrm{MinPoly}(a, F)$ holds $p(i) = l(a^i)$.

The theorem is a consequence of (46) and (47).

(62) Let us consider a field F, an extension E of F, an F-algebraic element a of E, a linear combination l of $\mathrm{Base}(a)$, and a non zero polynomial p over F. Suppose $l(a^{\deg p}) = \mathrm{LC}\, p$ and the support of $l = \{a^{\deg p}\}$. Then $\sum l = \mathrm{ExtEval}(\mathrm{LM}(p), a)$. The theorem is a consequence of (35), (36), (19), and (29).

(63) Let us consider a field F, an extension E of F, an F-algebraic element a of E, a linear combination l of $\mathrm{Base}(a)$, and a polynomial p over F. Suppose $\deg p < \deg \mathrm{MinPoly}(a, F)$ and for every element i of $\mathbb{N}$ such that $i < \deg \mathrm{MinPoly}(a, F)$ holds $p(i) = l(a^i)$. Then $\sum l = \mathrm{ExtEval}(p, a)$.

Proof: Define $\mathcal{P}[\underline{\text{natural number}}] \equiv$ for every linear combination l of $\mathrm{Base}(a)$ such that $\overline{\overline{\text{the support of } l}} = \$_1$ for every polynomial p over F such that $\deg p < \deg \mathrm{MinPoly}(a, F)$ and for every element i of $\mathbb{N}$ such that $i < \deg \mathrm{MinPoly}(a, F)$ holds $p(i) = l(a^i)$ holds $\sum l = \mathrm{ExtEval}(p, a)$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{\alpha}} = n$, where α is the support of l. □

(64) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and a linear combination l of $\mathrm{Base}(a)$. Suppose $\sum l = 0_F$. Then $l = \mathbf{0}_{\mathrm{LC}_{\mathrm{VecSp}(\mathrm{FAdj}(F, \{a\}), F)}}$. The theorem is a consequence of (61), (63), and (53).

(65) Let us consider a field F, a $(\mathrm{PolyRing}(F))$-homomorphic extension E of F, and an F-algebraic element a of E. Then $\mathrm{Base}(a)$ is a basis of $\mathrm{VecSp}(\mathrm{FAdj}(F, \{a\}), F)$. The theorem is a consequence of (64), (56), (45), and (60).

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

(66) $\overline{\overline{\mathrm{Base}(a)}} = \deg \mathrm{MinPoly}(a, F)$.

Proof: Set $m = \deg \mathrm{MinPoly}(a, F)$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists an element x of $\mathrm{Seg}\, m$ and there exists an element y of $\mathbb{N}$ such that $\$_1 = x$ and $y = x - 1$ and $\$_2 = a^y$. Consider f being a function such that $\mathrm{dom}\, f = \mathrm{Seg}\, m$ and for every object x such that $x \in \mathrm{Seg}\, m$ holds $\mathcal{P}[x, f(x)]$. □

(67) $\deg(\mathrm{FAdj}(F, \{a\}), F) = \deg \mathrm{MinPoly}(a, F)$. The theorem is a consequence of (66) and (65).

Let F be a field, E be an extension of F, and a be an F-algebraic element of E. Let us note that $\mathrm{FAdj}(F, \{a\})$ is F-finite.

Now we state the proposition:

(68) Let us consider a field F, an extension E of F, and an element a of E. Then a is F-algebraic if and only if $\mathrm{FAdj}(F, \{a\})$ is F-finite. The theorem is a consequence of (27), (22), (43), (35), (19), (47), (11), and (49).

REFERENCES

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

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

[3] Nathan Jacobson. *Basic Algebra I.* Dover Books on Mathematics, 1985.

[4] Heinz Lüneburg. *Gruppen, Ringe, Körper: Die grundlegenden Strukturen der Algebra.* Oldenbourg Verlag, 1999.

[5] Knut Radbruch. *Algebra I.* Lecture Notes, University of Kaiserslautern, Germany, 1991.

[6] Christoph Schwarzweller. Renamings and a condition-free formalization of Kronecker's construction. *Formalized Mathematics*, 28(**2**):129–135, 2020. doi:10.2478/forma-2020-0012.

[7] Christoph Schwarzweller. Representation matters: An unexpected property of polynomial rings and its consequences for formalizing abstract field theory. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2018 Federated Conference on Computer Science and Information Systems*, volume 15 of *Annals of Computer Science and Information Systems*, pages 67–72. IEEE, 2018. doi:10.15439/2018F88.

[8] Yasushige Watase. Algebraic numbers. *Formalized Mathematics*, 24(**4**):291–299, 2016. doi:10.1515/forma-2016-0025.

Accepted September 25, 2020