Contents

Formaliz. Math. 30 (**2**)

Characteristic Subgroups
By Alexander M. Nelson **79**

Transformation Tools for Real Linear Spaces
By Kazuhisa Nakasho **93**

Introduction to Graph Colorings
By Sebastian Koch **99**

Definition of Centroid Method as Defuzzification
By Takashi Mitsuishi **125**

Elementary Number Theory Problems. Part III
By Artur Korniłowicz **135**

Continued on inside back cover

FORMALIZED MATHEMATICS
Vol. 30, No. 2, Pages 79–91, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0007

sciendo
sciendo.com/journal/forma

Characteristic Subgroups

Alexander M. Nelson
Los Angeles, California
United States of America

Summary. We formalize in Mizar [1], [2] the notion of characteristic subgroups using the definition found in Dummit and Foote [3], as subgroups invariant under automorphisms from its parent group. Along the way, we formalize notions of Automorphism and results concerning centralizers. Much of what we formalize may be found sprinkled throughout the literature, in particular Gorenstein [4] and Isaacs [5]. We show all our favorite subgroups turn out to be characteristic: the center, the derived subgroup, the commutator subgroup generated by characteristic subgroups, and the intersection of all subgroups satisfying a generic group property.

MSC: 20E07 20E15 68V20

Keywords: group theory; inner automorphisms; characteristic subgroups

MML identifier: GROUP_22, version: 8.1.12 5.71.1431

1. Preparatory Work

From now on X denotes a set.

Let us consider natural numbers a, b, c. Now we state the propositions:

(1) If $c \neq 0$ and $c \cdot a \mid c \cdot b$, then $a \mid b$.

(2) If $b \neq 0$ and $b \mid c$ and $a \cdot b$ and c are relatively prime, then $b = 1$.

(3) Let us consider groups G_1, G_2, a subgroup H of G_1, a homomorphism f from G_1 to G_2, and an element h of G_1. If $h \in H$, then $(f \restriction H)(h) = f(h)$.

(4) Let us consider non empty sets X, Y, and a function f from X into Y. If f is bijective, then for every element y of Y, $f((f^{-1})(y)) = y$.

(5) Let us consider non empty sets X, Y, a non empty subset A of X, and an element x of X. Suppose $x \notin A$. Let us consider a function f from X into Y. If f is one-to-one, then $f(x) \notin f^{\circ}A$.

2. Nontrivial Groups and Subgroups

Note that there exists a group which is strict and non trivial.

Let G be a group. Observe that there exists a subgroup of G which is trivial.

Let H be a subgroup of G. One can check that there exists a subgroup of H which is trivial.

Let G be a non trivial group. Observe that there exists a subgroup of G which is non trivial and there exists a subgroup of G which is strict and non trivial. Now we state the proposition:

(6) Let us consider a group G. Then G is trivial if and only if the multiplicative magma of $G = \{\mathbf{1}\}_G$.

Proof: If G is trivial, then the multiplicative magma of $G = \{\mathbf{1}\}_G$. □

Note that there exists a finite group which is non trivial.

Now we state the propositions:

(7) Let us consider a group G, and a subgroup H of G. Suppose H is trivial. Then the multiplicative magma of $H = \{\mathbf{1}\}_G$. The theorem is a consequence of (6).

(8) Let us consider a group G, a trivial subgroup H of G, and a trivial subgroup K of G. Then the multiplicative magma of $H =$ the multiplicative magma of K. The theorem is a consequence of (7).

(9) Let us consider a group G, a trivial subgroup K of G, and a subgroup H of G. If H is a subgroup of K, then H is a trivial subgroup of G.

Proof: The carrier of $H = \{\mathbf{1}_G\}$. □

3. Proper Subgroups

Let G be a group and I_1 be a subgroup of G. We say that I_1 is proper if and only if

(Def. 1) the multiplicative magma of $I_1 \neq$ the multiplicative magma of G.

In the sequel G denotes a group and H denotes a subgroup of G.

Now we state the proposition:

(10) H is proper if and only if the carrier of $H \neq$ the carrier of G.

In the sequel h, x, y denote objects. Now we state the proposition:

(11) H is proper if and only if (the carrier of G) $\setminus$ (the carrier of H) is a non empty set. The theorem is a consequence of (10).

Let G be a non trivial group. Let us note that there exists a subgroup of G which is strict and proper and every subgroup of G which is maximal is also proper. Now we state the proposition:

(12) Let us consider a non trivial group G, a proper subgroup H of G, and a subgroup K of G. Suppose H is a subgroup of K and the multiplicative magma of $H \neq$ the multiplicative magma of K. Then K is a non trivial subgroup of G. The theorem is a consequence of (9) and (8).

4. Automorphisms

Let us consider G. An endomorphism of G is a homomorphism from G to G. From now on f denotes an endomorphism of G.

Let us consider G. One can check that there exists an endomorphism of G which is bijective.

An automorphism of G is a bijective endomorphism of G. In the sequel φ denotes an automorphism of G. Now we state the propositions:

(13) $\mathrm{Im}(f \restriction \{\mathbf{1}\}_G) = \{\mathbf{1}\}_G$.

(14) $\mathrm{Im}(\varphi \restriction \{\mathbf{1}\}_G)$ is a subgroup of $\{\mathbf{1}\}_G$. The theorem is a consequence of (13).

(15) Let us consider groups G_1, G_2, a homomorphism f from G_1 to G_2, and a subgroup H of G_1. Then $\mathrm{Ker}(f \restriction H)$ is a subgroup of $\mathrm{Ker}\, f$.

Proof: For every element g of G_1 such that $g \in \mathrm{Ker}(f \restriction H)$ holds $g \in \mathrm{Ker}\, f$. □

(16) Suppose for every automorphism f of G, $\mathrm{Im}(f \restriction H)$ is a subgroup of H. Then there exists an automorphism ψ of G such that

(i) $\psi = \varphi^{-1}$, and

(ii) $\mathrm{Im}(\varphi \restriction \mathrm{Im}(\psi \restriction H))$ is a subgroup of $\mathrm{Im}(\varphi \restriction H)$.

(17) There exists an automorphism ψ of G such that

(i) $\psi = \varphi^{-1}$, and

(ii) $\mathrm{Im}(\varphi \restriction \mathrm{Im}(\psi \restriction H)) =$ the multiplicative magma of H.

Proof: Reconsider $\psi = \varphi^{-1}$ as an automorphism of G. For every element g of G, $g \in \mathrm{Im}(\varphi \restriction \mathrm{Im}(\psi \restriction H))$ iff $g \in H$. □

(18) Let us consider a strict subgroup H of G, and a subgroup K of G. Suppose $\mathrm{Im}(\varphi \restriction H)$ is a subgroup of K. Then there exists an automorphism ψ of G such that

(i) $\psi = \varphi^{-1}$, and

(ii) H is a subgroup of $\mathrm{Im}(\psi \restriction K)$.

The theorem is a consequence of (17).

(19) H and $\varphi^{\circ} H$ are isomorphic.

(20) Let us consider a finite group G, and strict subgroups H_1, H_2 of G. Suppose H_1 and H_2 are isomorphic. Then $|\bullet : H_1|_{\mathbb{N}} = |\bullet : H_2|_{\mathbb{N}}$.

(21) Suppose G is finite. Let us consider a prime natural number p, and a strict subgroup P of G. Suppose P is a Sylow p-subgroup. Then $\mathrm{Im}(\varphi\restriction P)$ is a Sylow p-subgroup. The theorem is a consequence of (19) and (20).

(22) Let us consider an automorphism f of G. Suppose $\mathrm{Im}(f\restriction H) =$ the multiplicative magma of H. Then $f\restriction H$ is an automorphism of H.
PROOF: Set $U_H =$ the carrier of H. Reconsider $f_3 = f\restriction H$ as a function from U_H into U_H. f_3 is bijective. For every elements x, y of H, $f_3(x \cdot y) = f_3(x) \cdot f_3(y)$. $\square$

(23) Let us consider a non trivial group G, a subgroup H of G, and an automorphism φ of G. Suppose H is a proper subgroup of G. Then $\mathrm{Im}(\varphi\restriction H)$ is a proper subgroup of G.
PROOF: Set $U_H =$ the carrier of H. Set $U_G =$ the carrier of G. $U_G \setminus U_H$ is not empty. Consider x such that $x \in U_G \setminus U_H$. $\varphi(x) \notin \varphi^\circ H$ by (5), [8, (8)]. $\varphi(x)$ is an element of G. $\square$

(24) Let us consider a non trivial group G, a strict subgroup H of G, and an automorphism φ of G. If H is maximal, then $\mathrm{Im}(\varphi\restriction H)$ is maximal.
PROOF: $\mathrm{Im}(\varphi\restriction H)$ is a proper subgroup of G. For every strict subgroup K of G such that $\mathrm{Im}(\varphi\restriction H) \neq K$ and $\mathrm{Im}(\varphi\restriction H)$ is a subgroup of K holds $K =$ the multiplicative magma of G. $\square$

5. Inner Automorphisms

Let us consider G. Let a be an element of G and f be a function. We say that a is inner w.r.t. f if and only if

(Def. 2) for every element x of G, $f(x) = x^a$.

Let I_1 be an automorphism of G. We say that I_1 is inner if and only if

(Def. 3) there exists an element a of G such that a is inner w.r.t. I_1.

Let G be a group and f be an automorphism of G. We introduce the notation f is outer as an antonym for f is inner.

Let us consider G. Let us observe that there exists an automorphism of G which is inner.

Let us consider a strict group G and an object f. Now we state the propositions:

(25) $f \in \mathrm{Aut}(G)$ if and only if f is an automorphism of G.

(26) $f \in \mathrm{InnAut}(G)$ if and only if f is an inner automorphism of G.

(27) Let us consider an element a of G, and an inner automorphism f of G. If a is inner w.r.t. f, then $\mathrm{Im}(f \restriction H) = H^a$.

PROOF: For every element h of G such that $h \in H$ holds $(f \restriction H)(h) = h^a$. For every element y of G such that $y \in \mathrm{Im}(f \restriction H)$ holds $y \in H^a$. For every element y of G such that $y \in H^a$ holds $y \in \mathrm{Im}(f \restriction H)$. $\square$

Let us consider an element a of G and an endomorphism f of G. Now we state the propositions:

(28) If a is inner w.r.t. f, then $\mathrm{Ker}\, f = \{\mathbf{1}\}_G$.

PROOF: For every element x of G such that $x \in \mathrm{Ker}\, f$ holds $x \in \{\mathbf{1}\}_G$. $\square$

(29) If a is inner w.r.t. f, then f is an automorphism of G.

PROOF: $\mathrm{Ker}\, f = \{\mathbf{1}\}_G$. There exists an endomorphism f_4 of G such that $f \cdot f_4 = \mathrm{id}_\alpha$, where α is the carrier of G. $\square$

(30) If a is inner w.r.t. f, then f is an inner automorphism of G.

(31) Let us consider an element a of G. Then there exists an inner automorphism f of G such that a is inner w.r.t. f.

PROOF: Define $\mathcal{F}(\text{element of } G) = {\$_1}^a$. Consider f being a function from the carrier of G into the carrier of G such that for every element g of G, $f(g) = \mathcal{F}(g)$. For every elements x_1, x_2 of G, $f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2)$. a is inner w.r.t. f and f is an inner automorphism of G. $\square$

(32) Let us consider a strict subgroup H of G. Then H is normal if and only if for every inner automorphism f of G, $\mathrm{Im}(f \restriction H) = H$. The theorem is a consequence of (27) and (31).

6. Characteristic Subgroups

Let us consider G. Let I_1 be a subgroup of G. We say that I_1 is characteristic if and only if

(Def. 4) for every automorphism f of G, $\mathrm{Im}(f \restriction I_1) =$ the multiplicative magma of I_1.

Note that $\{\mathbf{1}\}_G$ is characteristic and there exists a subgroup of G which is characteristic.

From now on K denotes a characteristic subgroup of G.

Let G be a group. Let us observe that there exists a subgroup of G which is strict and characteristic. Now we state the proposition:

(33) K is a normal subgroup of G. The theorem is a consequence of (31) and (27).

Let G be a group. One can verify that every subgroup of G which is characteristic is also normal. Now we state the propositions:

(34) Let us consider groups G_1, G_2, a subgroup H_1 of G_1, a subgroup K of H_1, a subgroup H_2 of G_2, a homomorphism f from G_1 to G_2, and a homomorphism g from H_1 to H_2. Suppose for every element k of G_1 such that $k \in K$ holds $f(k) = g(k)$. Then $\mathrm{Im}(f \restriction K) = \mathrm{Im}(g \restriction K)$.
PROOF: For every object y, $y \in$ the carrier of $\mathrm{Im}(f \restriction K)$ iff $y \in$ the carrier of $\mathrm{Im}(g \restriction K)$. $\square$

(35) Let us consider a strict subgroup H of G. Suppose for every strict subgroup K of G such that $\overline{\overline{K}} = \overline{\overline{H}}$ holds $H = K$. Then H is characteristic.
PROOF: H is characteristic. $\square$

(36) Let us consider a strict, normal subgroup N of G. Then every characteristic subgroup of N is a normal subgroup of G.
PROOF: For every element a of G, $K^a =$ the multiplicative magma of K. $\square$

(37) Let us consider a characteristic subgroup N of G. Then every characteristic subgroup of N is a characteristic subgroup of G.
PROOF: For every automorphism g of G, $\mathrm{Im}(g \restriction K) =$ the multiplicative magma of K. $\square$

(38) Let us consider a group G, and a strict subgroup H of G. Then H is a characteristic subgroup of G if and only if for every automorphism φ of G, $\mathrm{Im}(\varphi \restriction H)$ is a subgroup of H.
PROOF: If H is a characteristic subgroup of G, then for every automorphism φ of G, $\mathrm{Im}(\varphi \restriction H)$ is a subgroup of H. If for every automorphism φ of G, $\mathrm{Im}(\varphi \restriction H)$ is a subgroup of H, then H is a characteristic subgroup of G. $\square$

(39) $\mathrm{Z}(G)$ is a characteristic subgroup of G.
PROOF: Set $Z = \mathrm{Z}(G)$. For every elements y, z of G such that $z \in Z$ holds $\varphi(z) \cdot y = y \cdot \varphi(z)$. For every element z of G such that $z \in Z$ holds $(\varphi \restriction Z)(z) \in Z$. $\mathrm{Im}(\varphi \restriction Z)$ is a subgroup of Z. $\square$

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

(Sch. 1) For every automorphism φ of $\mathcal{G}$, $\varphi^{\circ}(\bigcap\{A$, where A is a subset of $\mathcal{G}$: there exists a strict subgroup K of $\mathcal{G}$ such that $A =$ the carrier of K and $\mathcal{P}[K]\}) = \bigcap\{A$, where A is a subset of $\mathcal{G}$: there exists a strict subgroup K of $\mathcal{G}$ such that $A =$ the carrier of K and $\mathcal{P}[K]\}$

provided

- for every automorphism φ of $\mathcal{G}$ and for every strict subgroup H of $\mathcal{G}$ such that $\mathcal{P}[H]$ holds $\mathcal{P}[\mathrm{Im}(\varphi \restriction H)]$ and
- there exists a strict subgroup H of $\mathcal{G}$ such that $\mathcal{P}[H]$.

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

(Sch. 2) There exists a strict subgroup K of $\mathcal{G}$ such that the carrier of $K = \bigcap\{A$, where A is a subset of $\mathcal{G}$: there exists a strict subgroup H of $\mathcal{G}$ such that $A =$ the carrier of H and $\mathcal{P}[H]\}$ and K is characteristic

provided

- for every automorphism φ of $\mathcal{G}$ and for every strict subgroup H of $\mathcal{G}$ such that $\mathcal{P}[H]$ holds $\mathcal{P}[\mathrm{Im}(\varphi\restriction H)]$ and

- there exists a strict subgroup H of $\mathcal{G}$ such that $\mathcal{P}[H]$.

Now we state the propositions:

(40) Let us consider a non trivial group G. Suppose there exists a strict subgroup H of G such that H is maximal. Then $\Phi(G)$ is a characteristic subgroup of G.
Proof: Define $\mathcal{P}[\text{subgroup of } G] \equiv \$_1$ is maximal. For every automorphism φ of G and for every strict subgroup H of G such that $\mathcal{P}[H]$ holds $\mathcal{P}[\mathrm{Im}(\varphi\restriction H)]$. Consider K being a strict subgroup of G such that the carrier of $K = \bigcap\{A$, where A is a subset of G : there exists a strict subgroup H of G such that $A =$ the carrier of H and $\mathcal{P}[H]\}$ and K is characteristic. □

(41) Let us consider an automorphism φ of G. Then φ°(the commutators of G) = the commutators of G.
Proof: For every object g such that $g \in$ the commutators of G holds $g \in \varphi^\circ$(the commutators of G). For every object h such that $h \in \varphi^\circ$(the commutators of G) holds $h \in$ the commutators of G. □

(42) Let us consider a group G, an automorphism φ of G, and a subgroup H of G. Suppose for every element h of H, $\varphi(h) \in H$. Then $\mathrm{Im}(\varphi\restriction H)$ is a subgroup of H.
Proof: For every object y such that $y \in \mathrm{rng}(\varphi\restriction H)$ holds $y \in$ the carrier of H. □

(43) Let us consider a group G, and a non empty subset A of G. Suppose for every automorphism φ of G, $\varphi^\circ A = A$. Then $\mathrm{gr}(A)$ is characteristic.
Proof: For every automorphism φ of G and for every element a of A, $\varphi(a) \in A$. Set $H = \mathrm{gr}(A)$. For every automorphism φ of G, $\mathrm{Im}(\varphi\restriction H)$ is a subgroup of H by [7, (28)], [6, (125)]. □

(44) G^{c} is characteristic. The theorem is a consequence of (41) and (43).

Let us consider groups G_1, G_2, a subgroup H of G_1, an element a of G_1, and a homomorphism f from G_1 to G_2. Now we state the propositions:

(45) $f^\circ(a \cdot H) = f(a) \cdot (f^\circ H)$.
PROOF: For every object y such that $y \in f^\circ(a \cdot H)$ holds $y \in f(a) \cdot (f^\circ H)$. For every object y such that $y \in f(a) \cdot (f^\circ H)$ holds $y \in f^\circ(a \cdot H)$. □

(46) $f^\circ(H \cdot a) = (f^\circ H) \cdot f(a)$.
PROOF: For every object y such that $y \in f^\circ(H \cdot a)$ holds $y \in (f^\circ H) \cdot f(a)$. For every object y such that $y \in (f^\circ H) \cdot f(a)$ holds $y \in f^\circ(H \cdot a)$. □

(47) Let us consider a group G, a strict, normal subgroup N of G, and an automorphism φ of G. Then $\mathrm{Im}(\varphi \restriction N)$ is a normal subgroup of G.
PROOF: Set $H = \mathrm{Im}(\varphi \restriction N)$. For every element g of G, $g \cdot H = H \cdot g$. □

(48) Let us consider a group G, and a strict subgroup H of G. Then H is characteristic if and only if for every automorphism φ of G and for every element x of G such that $x \in H$ holds $\varphi(x) \in H$.
PROOF: If H is characteristic, then for every automorphism φ of G and for every element x of G such that $x \in H$ holds $\varphi(x) \in H$. If for every automorphism φ of G for every element x of G such that $x \in H$ holds $\varphi(x) \in H$, then H is characteristic. □

Let us consider a group G and strict, characteristic subgroups H, K of G. Now we state the propositions:

(49) $H \cap K$ is a characteristic subgroup of G.
PROOF: For every automorphism φ of G and for every element x of G such that $x \in H \cap K$ holds $\varphi(x) \in H \cap K$. □

(50) $H \sqcup K$ is a characteristic subgroup of G.
PROOF: For every automorphism φ of G and for every element g of G such that $g \in H \sqcup K$ holds $\varphi(g) \in H \sqcup K$. □

(51) Let us consider a group G, strict, characteristic subgroups H, K of G, and an automorphism φ of G. Then φ°(the commutators of H & K) = the commutators of H & K.
PROOF: For every object x such that $x \in$ the commutators of H & K holds $x \in \varphi^\circ$(the commutators of H & K). For every object y such that $y \in \varphi^\circ$(the commutators of H & K) holds $y \in$ the commutators of H & K. □

(52) Let us consider a group G, and strict, characteristic subgroups H, K of G. Then $[H, K]$ is a characteristic subgroup of G. The theorem is a consequence of (51) and (43).

7. Appendix 1: Results Concerning Meets

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

(Sch. 3) There exists a strict subgroup H of $\mathcal{G}$ such that the carrier of $H = \bigcap\{A$, where A is a subset of $\mathcal{G}$: there exists a strict subgroup K of $\mathcal{G}$ such-that $A =$ the carrier of K and $\mathcal{P}[K]\}$ and for every strict subgroup K of $\mathcal{G}$ such that $\mathcal{P}[K]$ holds H is a subgroup of K

provided

- there exists a strict subgroup H of $\mathcal{G}$ such that $\mathcal{P}[H]$.

Now we state the proposition:

(53) Let us consider a group G, and subgroups H_1, H_2 of G. Suppose H_1 is a subgroup of H_2. Let us consider an element a of G. Then ${H_1}^a$ is a subgroup of ${H_2}^a$.

Proof: For every element h of G such that $h \in {H_1}^a$ holds $h \in {H_2}^a$. □

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

(Sch. 4) For every strict subgroup H of $\mathcal{G}$ such that the carrier of $H = \bigcap\{A$, where A is a subset of $\mathcal{G}$: there exists a strict subgroup N of $\mathcal{G}$ such that $A =$ the carrier of N and N is normal and $\mathcal{P}[N]\}$ holds H is a strict, normal subgroup of $\mathcal{G}$

provided

- there exists a strict, normal subgroup H of $\mathcal{G}$ such that $\mathcal{P}[H]$.

Now we state the proposition:

(54) Let us consider a group G, and a finite set X. Suppose $X \neq \emptyset$ and for every element A of X, there exists a strict, normal subgroup N of G such that $A =$ the carrier of N. Then there exists a strict, normal subgroup N of G such that the carrier of $N = \bigcap X$.

Proof: Define $\mathcal{P}[\text{group}] \equiv \$_1$ is a normal subgroup of G and the carrier of $\$_1 \in X$. Set $F_1 = \{A$, where A is a subset of G : there exists a strict subgroup N of G such that $A =$ the carrier of N and $\mathcal{P}[N]\}$. Set $F_2 = \{A$, where A is a subset of G : there exists a strict subgroup N of G such that $A =$ the carrier of N and N is normal and $\mathcal{P}[N]\}$.

There exists a strict subgroup H of G such that $\mathcal{P}[H]$. Consider N being a strict subgroup of G such that the carrier of $N = \bigcap F_1$. For every object A, $A \in F_1$ iff $A \in F_2$. For every strict subgroup H of G such that the carrier of $H = \bigcap F_2$ holds H is a strict, normal subgroup of G. For every object A, $A \in F_1$ iff $A \in X$. □

8. Appendix 2: Centralizer of Characteristic Subgroups is Characteristic

Let G be a group and A be a subset of G. The functor Centralizer(A) yielding a strict subgroup of G is defined by

(Def. 5) the carrier of $it = \{b$, where b is an element of G : for every element a of G such that $a \in A$ holds $a \cdot b = b \cdot a\}$.

Now we state the propositions:

(55) Let us consider a group G, a subset A of G, and an element g of G. Then for every element a of G such that $a \in A$ holds $g \cdot a = a \cdot g$ if and only if g is an element of Centralizer(A).

(56) Let us consider a group G, and subsets A, B of G. Suppose $A \subseteq B$. Then Centralizer(B) is a subgroup of Centralizer(A). The theorem is a consequence of (55).

Let G be a group and H be a subgroup of G. The functor Centralizer(H) yielding a strict subgroup of G is defined by

(Def. 6) $it =$ Centralizer$(\overline{H})$.

Now we state the propositions:

(57) Let us consider a group G, and a subgroup H of G. Then the carrier of Centralizer$(H) = \{b$, where b is an element of G : for every element a of G such that $a \in H$ holds $b \cdot a = a \cdot b\}$.

(58) Let us consider a group G, a subgroup H of G, and an element g of G. Then for every element a of G such that $a \in H$ holds $g \cdot a = a \cdot g$ if and only if g is an element of Centralizer(H). The theorem is a consequence of (57).

(59) Let us consider a group G. Then every subset of G is a subset of Centralizer(Centralizer(A)). The theorem is a consequence of (55) and (58).

(60) Let us consider a group G, and a strict, characteristic subgroup K of G. Then Centralizer(K) is a characteristic subgroup of G.

Proof: For every automorphism φ of G and for every element x of G such that $x \in$ Centralizer(K) holds $\varphi(x) \in$ Centralizer(K). $\square$

Let G be a group and a be an element of G. Let us observe that the functor $\{a\}$ yields a subset of G. The functor N(a) yielding a strict subgroup of G is defined by the term

(Def. 7) N$(\{a\})$.

Now we state the propositions:

(61) Let us consider a group G, and elements a, x of G. Then $x \in \mathrm{N}(a)$ if and only if there exists an element h of G such that $x = h$ and $a^h = a$.

(62) Let us consider a group G, and a non empty subset A of G. Then the carrier of $\mathrm{Centralizer}(A) = \bigcap\{B$, where B is a subset of G : there exists a strict subgroup H of G such that $B =$ the carrier of H and there exists an element a of G such that $a \in A$ and $H = \mathrm{N}(a)\}$.

PROOF: Define $\mathcal{P}[\text{strict subgroup of } G] \equiv$ there exists an element a of G such that $a \in A$ and $\$_1 = \mathrm{N}(a)$. Set $F_1 = \{B$, where B is a subset of G : there exists a strict subgroup H of G such that $B =$ the carrier of H and $\mathcal{P}[H]\}$. $F_1 \neq \emptyset$. For every object x such that $x \in$ the carrier of $\mathrm{Centralizer}(A)$ holds $x \in \bigcap F_1$. For every object x such that $x \in \bigcap F_1$ holds $x \in$ the carrier of $\mathrm{Centralizer}(A)$. □

(63) Let us consider a finite group G, and strict subgroups H_1, H_2 of G. Suppose $\overline{\overline{H_1 \cap H_2}} = \overline{\overline{H_1}}$ and $\overline{\overline{H_1 \cap H_2}} = \overline{\overline{H_2}}$. Then $H_1 = H_2$.

PROOF: $H_1 \cap H_2 = H_1$. $H_1 \cap H_2 = H_2$. □

(64) Let us consider finite groups G_1, G_2, a normal subgroup N_1 of G_1, and a normal subgroup N_2 of G_2. Suppose ${}^{G_1}/_{N_1}$ and ${}^{G_2}/_{N_2}$ are isomorphic. Then $\overline{\overline{N_2}} \cdot \overline{\overline{G_1}} = \overline{\overline{N_1}} \cdot \overline{\overline{G_2}}$.

(65) Let us consider a finite group G, strict, normal subgroups K, N of G, and natural numbers m, d. Suppose $m = \overline{\overline{N}}$ and $m = \overline{\overline{K}}$ and $d = \overline{\overline{K \cap N}}$. Then $d \cdot \overline{\overline{N \sqcup K}} = m \cdot m$. The theorem is a consequence of (64).

(66) Let us consider a finite group G, and a strict, normal subgroup N of G. Suppose $\overline{\overline{N}}$ and $|\bullet : N|_{\mathbb{N}}$ are relatively prime. Then N is a characteristic subgroup of G.

PROOF: Consider m being a natural number such that $m = \overline{\overline{N}}$. Consider n being a natural number such that $n = |\bullet : N|_{\mathbb{N}}$. For every automorphism φ of G, $\mathrm{Im}(\varphi \restriction N) = N$. □

(67) Let us consider groups G_1, G_2, G_3, a homomorphism f_1 from G_1 to G_2, a homomorphism f_2 from G_2 to G_3, and a subgroup A of G_1. Then the multiplicative magma of $f_2{}^\circ(f_1{}^\circ A) =$ the multiplicative magma of $f_2 \cdot f_1{}^\circ A$.

PROOF: For every element z of G_3, $z \in f_2{}^\circ(f_1{}^\circ A)$ iff $z \in f_2 \cdot f_1{}^\circ A$. □

(68) Let us consider a group G, a strict, normal subgroup N of G, and an automorphism φ of G. Suppose $\mathrm{Im}(\varphi \restriction N) = N$. Then there exists an automorphism σ of ${}^{G}/_{N}$ such that for every element x of G, $\sigma(x \cdot N) = \varphi(x) \cdot N$.

PROOF: Define $\mathcal{P}[\text{set}, \text{set}] \equiv$ there exists an element a of G such that $\$_1 = a \cdot N$ and $\$_2 = \varphi(a) \cdot N$. For every element x of ${}^{G}/_{N}$, there exists an element y of ${}^{G}/_{N}$ such that $\mathcal{P}[x, y]$. Consider σ being a function from ${}^{G}/_{N}$ into ${}^{G}/_{N}$ such that for every element x of ${}^{G}/_{N}$, $\mathcal{P}[x, \sigma(x)]$. For every element a of G, $\sigma(a \cdot N) = \varphi(a) \cdot N$. For every elements x, y of ${}^{G}/_{N}$, $\sigma(x \cdot y) = \sigma(x) \cdot \sigma(y)$. σ is bijective. $\square$

Let us consider a finite group G, a strict, characteristic subgroup H of G, and a strict subgroup K of G. Now we state the propositions:

(69) If H is a subgroup of K, then H is a normal subgroup of K.

PROOF: For every element k of K, $k \in H$ iff $k \in$ Ker((the canonical homomorphism onto cosets of H)$\restriction K$). $\square$

(70) If H is a subgroup of K and ${}^{K}/_{(H)_K}$ is a characteristic subgroup of ${}^{G}/_{H}$, then K is a characteristic subgroup of G.

PROOF: For every automorphism φ of G and for every element k of G such that $k \in K$ holds $\varphi(k) \in K$. $\square$

(71) Let us consider a group G, and a subgroup H of G. Then H is a subgroup of Centralizer(H) if and only if H is a commutative group.

PROOF: If H is a subgroup of Centralizer(H), then H is a commutative group. If H is a commutative group, then H is a subgroup of Centralizer(H). $\square$

(72) Let us consider a group G. Then Centralizer(Ω_G) $=$ Z(G).

PROOF: For every element g of G, $g \in$ Centralizer(Ω_G) iff $g \in$ Z(G). $\square$

(73) Let us consider a group G, and a normal subgroup N of G. Then Centralizer(N) is a normal subgroup of G.

PROOF: For every elements g, n of G such that $n \in N$ holds $n^g \in N$. For every elements g, x, n of G such that $x \in$ Centralizer(N) and $n \in N$ holds $x^g \cdot n = n \cdot (x^g)$. For every elements g, z of G such that $z \in$ Centralizer(N) holds $z^g \in$ Centralizer(N). For every element g of G, (Centralizer(N))$^g =$ Centralizer(N). $\square$

(74) Let us consider a group G, a subgroup H of G, and elements h, n of G. If $h \in H$ and $n \in$ N(H), then $h^n \in H$.

(75) Let us consider a group G. Then every subgroup of G is a subgroup of N(H).

PROOF: For every element g of G such that $g \in H$ for every element x of G such that $x \in \overline{H}^g$ holds $x \in \overline{H}$. For every element g of G such that $g \in H$ holds $g \in$ N(H). $\square$

(76) Let us consider a group G, and a subgroup H of G. Then Centralizer(H) is a strict, normal subgroup of N(H).

PROOF: Centralizer(H) is a normal subgroup of N(H). $\square$

ACKNOWLEDGEMENT: The author would like to thank Adam Grabowski for his invaluable help and kindness.

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] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley and Sons, Third edition, 2004.

[4] Daniel Gorenstein. *Finite Groups*. Chelsea Publishing Company, Second edition, 1980.

[5] I. Martin Isaacs. *Finite Group Theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, 2008.

[6] Marco Riccardi. The Jordan-Hölder theorem. *Formalized Mathematics*, 15(**2**):35–51, 2007. doi:10.2478/v10037-007-0005-8.

[7] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.

[8] Katarzyna Zawadzka. Solvable groups. *Formalized Mathematics*, 5(**1**):145–147, 1996.

Accepted July 23, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 2, Pages 93–98, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0008

sciendo.com/journal/forma

Transformation Tools for Real Linear Spaces

Kazuhisa Nakasho
Yamaguchi University
Yamaguchi, Japan

Summary. This paper, using the Mizar system [1], [2], provides useful tools for working with real linear spaces and real normed spaces. These include the identification of a real number set with a one-dimensional real normed space, the relationships between real linear spaces and real Euclidean spaces, the transformation from a real linear space to a real vector space, and the properties of basis and dimensions of real linear spaces. We referred to [6], [10], [8], [9] in this formalization.

MSC: 46A19 46A35 68V20

Keywords: real linear space; real normed space; real Euclidean space; real vector space

MML identifier: `LOPBAN15`, version: `8.1.12 5.71.1431`

1. Lipschitz Continuity of Linear Maps from Finite-Dimensional Spaces

Let n be a natural number. One can check that $\langle \mathcal{E}^n, \|\cdot\| \rangle$ is finite dimensional. Now we state the propositions:

(1) Let us consider real linear spaces X, Y, a linear operator L from X into Y, and a finite sequence F of elements of X. Then $L(\sum F) = \sum(L \cdot F)$.
PROOF: Define $\mathcal{S}[\text{set}] \equiv$ for every finite sequence H of elements of X such that $\operatorname{len} H = \$_1$ holds $L(\sum H) = \sum(L \cdot H)$. $\mathcal{S}[0]$. For every natural number n such that $\mathcal{S}[n]$ holds $\mathcal{S}[n+1]$. For every natural number n, $\mathcal{S}[n]$. □

(2) Let us consider a finite dimensional real normed space X, a real normed space Y, and a linear operator L from X into Y. If $\dim(X) \neq 0$, then L is Lipschitzian.

Proof: Set $b =$ the ordered basis of RLSp2RVSp(X). Consider r_1, r_2 being real numbers such that $0 < r_1$ and $0 < r_2$ and for every point x of X, $\|x\| \leqslant r_1 \cdot (\text{max-norm}(X, b))(x)$ and $(\text{max-norm}(X, b))(x) \leqslant r_2 \cdot \|x\|$. Reconsider $e = b$ as a finite sequence of elements of X. Define $\mathcal{N}(\text{natural number}) = \|L(e_{/\$_1})\| (\in \mathbb{R})$. Consider k being a finite sequence of elements of $\mathbb{R}$ such that $\operatorname{len} k = \operatorname{len} b$ and for every natural number i such that $i \in \operatorname{dom} k$ holds $k(i) = \mathcal{N}(i)$. Set $k_1 = \sum k$. For every natural number i such that $i \in \operatorname{dom} k$ holds $0 \leqslant k(i)$. For every point x of X, $\|L(x)\| \leqslant r_2 \cdot (k_1 + 1) \cdot \|x\|$. $\square$

(3) Let us consider a finite dimensional real normed space X, and a real normed space Y. Suppose $\dim(X) \neq 0$. Then LinearOperators$(X, Y) =$ BdLinOps(X, Y). The theorem is a consequence of (2).

2. Identification of a Real Number Set with a One-Dimensional Real Normed Space

One can check that the real normed space of $\mathbb{R}$ is non empty, right complementable, Abelian, add-associative, right zeroed, vector distributive, scalar distributive, scalar associative, scalar unital, discernible, reflexive, and real normed space-like. Now we state the propositions:

(4) Let us consider elements v, w of the real normed space of $\mathbb{R}$, and elements v_1, w_1 of $\mathbb{R}$. If $v = v_1$ and $w = w_1$, then $v + w = v_1 + w_1$.

(5) Let us consider an element v of the real normed space of $\mathbb{R}$, an element v_1 of $\mathbb{R}$, and a real number a. If $v = v_1$, then $a \cdot v = a \cdot v_1$.

(6) Let us consider an element v of the real normed space of $\mathbb{R}$, and an element v_1 of $\mathbb{R}$. If $v = v_1$, then $\|v\| = |v_1|$.

3. Identification of Real Euclidean Space and Real Normed Space

Now we state the propositions:

(7) There exists a linear operator f from the real normed space of $\mathbb{R}$ into $\langle \mathcal{E}^1, \|\cdot\| \rangle$ such that

   (i) f is isomorphism, and

   (ii) for every element x of the real normed space of $\mathbb{R}$, $f(x) = \langle x \rangle$.

Proof: Define $\mathcal{H}(\text{real number}) = \langle \$_1 \rangle (\in \mathcal{R}^1)$. Consider f being a function from $\mathbb{R}$ into $\mathcal{R}^1$ such that for every element x of $\mathbb{R}$, $f(x) = \mathcal{H}(x)$. For every element x of the real normed space of $\mathbb{R}$, $f(x) = \langle x \rangle$. For every elements v,

w of the real normed space of $\mathbb{R}$, $f(v+w) = f(v)+f(w)$. For every vector x of the real normed space of $\mathbb{R}$ and for every real number r, $f(r\cdot x) = r\cdot f(x)$. For every point x of the real normed space of $\mathbb{R}$, $\|x\| = \|f(x)\|$ by [3, (1)], [5, (2)]. $\square$

(8) (i) the real normed space of $\mathbb{R}$ is finite dimensional, and

(ii) dim(the real normed space of $\mathbb{R}$) $= 1$.

The theorem is a consequence of (7).

(9) Let us consider a real linear space sequence X, elements v, w of $\prod \overline{X}$, and an element i of dom $\overline{X}$. Then

(i) $(\prod^{\circ}\langle +_{X_i}\rangle_i)(v, w)(i) =$ (the addition of $X(i))(v(i), w(i))$, and

(ii) for every vectors v_2, w_2 of $X(i)$ such that $v_2 = v(i)$ and $w_2 = w(i)$ holds $(\prod^{\circ}\langle +_{X_i}\rangle_i)(v, w)(i) = v_2 + w_2$.

(10) Let us consider a real linear space sequence X, an element r of $\mathbb{R}$, an element v of $\prod \overline{X}$, and an element i of dom $\overline{X}$. Then

(i) $(\prod^{\circ} \operatorname{multop} X)(r, v)(i) =$ (the external multiplication of $X(i))(r, v(i))$, and

(ii) for every vector v_2 of $X(i)$ such that $v_2 = v(i)$ holds $(\prod^{\circ} \operatorname{multop} X)(r, v)(i) = r \cdot v_2$.

Let us consider a natural number n and a real norm space sequence X. Now we state the propositions:

(11) If $X = n \mapsto$ (the real normed space of $\mathbb{R}$), then $\prod X = \langle \mathcal{E}^n, \|\cdot\|\rangle$.

Proof: Set $P_1 = \prod X$. For every natural number i such that $i \in \operatorname{Seg} n$ holds $\overline{X}(i) = \mathbb{R}$. For every object x, $x \in \prod \overline{X}$ iff $x \in \mathcal{R}^n$. For every element j of dom $\overline{X}$, $\langle \underbrace{0, \ldots, 0}_{n} \rangle(j) = 0_{X(j)}$. For every elements a, b of $\mathcal{R}^n$, (the addition of $P_1)(a, b) = a + b$. For every real number r and for every element a of $\mathcal{R}^n$, (the external multiplication of $P_1)(r, a) = r \cdot a$. For every element a of $\mathcal{R}^n$, (the norm of $P_1)(a) = |a|$ by [4, (7)]. $\square$

(12) Suppose $X = n \mapsto$ (the real normed space of $\mathbb{R}$). Then

(i) $\prod X$ is finite dimensional, and

(ii) $\dim(\prod X) = n$.

The theorem is a consequence of (11).

4. Transformation to Real Vector Space

Let X be a real linear space and Y be a subspace of X. One can verify that the functor RLSp2RVSp(Y) yields a subspace of RLSp2RVSp(X). Now we state the proposition:

(13) Let us consider a real linear space X, and a subspace Y of X. Then RLSp2RVSp(Y) is a subspace of RLSp2RVSp(X).

Let us consider a real linear space X and subspaces Y_1, Y_2 of X. Now we state the propositions:

(14) $\mathrm{RLSp2RVSp}(Y_1 + Y_2) = \mathrm{RLSp2RVSp}(Y_1) + \mathrm{RLSp2RVSp}(Y_2)$.

(15) $\mathrm{RLSp2RVSp}(Y_1 \cap Y_2) = \mathrm{RLSp2RVSp}(Y_1) \cap \mathrm{RLSp2RVSp}(Y_2)$.

(16) Let us consider a real linear space X.
Then $\mathrm{RLSp2RVSp}(\mathbf{0}_X) = \mathbf{0}_{\mathrm{RLSp2RVSp}(X)}$.

5. Basis and Dimension Properties of Real Linear Spaces

Now we state the propositions:

(17) Let us consider a real linear space X, and subspaces Y_1, Y_2 of X. Suppose $Y_1 \cap Y_2 = \mathbf{0}_X$. Let us consider a linearly independent subset B_1 of Y_1, and a linearly independent subset B_2 of Y_2. Then $B_1 \cup B_2$ is a linearly independent subset of $Y_1 + Y_2$. The theorem is a consequence of (15), (16), and (14).

(18) Let us consider a real linear space X, and subspaces Y_1, Y_2 of X. Suppose $Y_1 \cap Y_2 = \mathbf{0}_X$. Let us consider a basis B_1 of Y_1, and a basis B_2 of Y_2. Then $B_1 \cup B_2$ is a basis of $Y_1 + Y_2$. The theorem is a consequence of (15), (16), and (14).

(19) Let us consider real linear spaces X, Y, a subspace X_1 of X, and a subspace Y_1 of Y. Then $X_1 \times Y_1$ is a subspace of $X \times Y$.
Proof: Set $V = X \times Y$. Set $X_2 = X_1 \times Y_1$. Set $f =$ the addition of X_2. Set $g =$ (the addition of V) $\restriction$ (the carrier of X_2). For every object z such that $z \in \operatorname{dom} f$ holds $f(z) = g(z)$. Set $f =$ the external multiplication of X_2. Set $g =$ (the external multiplication of V)$\restriction$($\mathbb{R} \times$ (the carrier of X_2)). For every object z such that $z \in \operatorname{dom} f$ holds $f(z) = g(z)$. □

(20) Let us consider real linear spaces X, Y, and subspaces X_1, Y_1 of $X \times Y$. Suppose $X_1 = X \times \mathbf{0}_Y$ and $Y_1 = \mathbf{0}_X \times Y$. Then

(i) $X_1 + Y_1 = X \times Y$, and

(ii) $X_1 \cap Y_1 = \mathbf{0}_{X \times Y}$.

PROOF: For every object x, $x \in$ the carrier of $X_1 + Y_1$ iff $x \in$ the carrier of $X \times Y$. For every object x, $x \in$ (the carrier of $X \times \mathbf{0}_Y$) $\cap$ (the carrier of $\mathbf{0}_X \times Y$) iff $x \in \{\langle 0_X, 0_Y \rangle\}$ by [7, (9)]. $\square$

Let us consider real linear spaces X, Y. Now we state the propositions:

(21) There exists a linear operator f from X into $X \times \mathbf{0}_Y$ such that

(i) f is bijective, and

(ii) for every element x of X, $f(x) = \langle x, 0_Y \rangle$.

PROOF: Set $A =$ the carrier of X. Set $B =$ the carrier of $X \times \mathbf{0}_Y$. Define $\mathcal{H}(\text{element of } A) = \langle \$_1, 0_Y \rangle (\in B)$. Consider f being a function from A into B such that for every element x of A, $f(x) = \mathcal{H}(x)$. For every element x of X, $f(x) = \langle x, 0_Y \rangle$. For every elements x_1, x_2 of X, $f(x_1 + x_2) = f(x_1)+f(x_2)$. For every vector x of X and for every real number r, $f(r \cdot x) = r \cdot f(x)$. $\square$

(22) There exists a linear operator f from Y into $\mathbf{0}_X \times Y$ such that

(i) f is bijective, and

(ii) for every element y of Y, $f(y) = \langle 0_X, y \rangle$.

PROOF: Set $A =$ the carrier of Y. Set $B =$ the carrier of $\mathbf{0}_X \times Y$. Define $\mathcal{H}(\text{element of } A) = \langle 0_X, \$_1 \rangle (\in B)$. Consider f being a function from A into B such that for every element y of A, $f(y) = \mathcal{H}(y)$. For every element y of Y, $f(y) = \langle 0_X, y \rangle$. For every elements y_1, y_2 of Y, $f(y_1+y_2) = f(y_1)+f(y_2)$. For every vector y of Y and for every real number r, $f(r \cdot y) = r \cdot f(y)$. $\square$

(23) Let us consider real linear spaces X, Y, a basis B_6 of X, and a basis B_7 of Y. Then $B_6 \times \{0_Y\} \cup \{0_X\} \times B_7$ is a basis of $X \times Y$.

PROOF: Reconsider $B_4 = B_6 \times \{0_Y\}$ as a subset of the carrier of $X \times Y$. Reconsider $B_5 = \{0_X\} \times B_7$ as a subset of the carrier of $X \times Y$. Consider T_1 being a linear operator from X into $X \times \mathbf{0}_Y$ such that T_1 is bijective and for every element x of X, $T_1(x) = \langle x, 0_Y \rangle$. For every object y, $y \in T_1{}^{\circ}B_6$ iff $y \in B_4$.

Consider T_2 being a linear operator from Y into $\mathbf{0}_X \times Y$ such that T_2 is bijective and for every element y of Y, $T_2(y) = \langle 0_X, y \rangle$. For every object y, $y \in T_2{}^{\circ}B_7$ iff $y \in B_5$. Reconsider $W_1 = X \times \mathbf{0}_Y$ as a subspace of $X \times Y$. Reconsider $W_2 = \mathbf{0}_X \times Y$ as a subspace of $X \times Y$. $W_1 + W_2 = X \times Y$ and $W_1 \cap W_2 = \mathbf{0}_{X \times Y}$. $\square$

(24) Let us consider finite dimensional real linear spaces X, Y. Then

(i) $X \times Y$ is finite dimensional, and

(ii) $\dim(X \times Y) = \dim(X) + \dim(Y)$.

The theorem is a consequence of (23).

(25) Let us consider a finite dimensional real linear space X. Then

(i) $\prod\langle X\rangle$ is finite dimensional, and

(ii) $\dim(\prod\langle X\rangle) = \dim(X)$.

(26) Let us consider a real linear space sequence X, and a finite sequence d of elements of $\mathbb{N}$. Suppose $\operatorname{len} d = \operatorname{len} X$ and for every element i of $\operatorname{dom} X$, $X(i)$ is finite dimensional and $d(i) = \dim(X(i))$. Then

(i) $\prod X$ is finite dimensional, and

(ii) $\dim(\prod X) = \sum d$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every real linear space sequence X for every finite sequence d of elements of $\mathbb{N}$ such that $\operatorname{len} X = \$_1$ and $\operatorname{len} d = \operatorname{len} X$ and for every element i of $\operatorname{dom} X$, $X(i)$ is finite dimensional and $d(i) = \dim(X(i))$ holds $\prod X$ is finite dimensional and $\dim(\prod X) = \sum d$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. $\square$

References

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

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

[3] Noboru Endou and Yasunari Shidama. Completeness of the real Euclidean space. *Formalized Mathematics*, 13(**4**):577–580, 2005.

[4] Noboru Endou, Yasunari Shidama, and Keiichi Miyajima. The product space of real normed spaces and its properties. *Formalized Mathematics*, 15(**3**):81–85, 2007. doi:10.2478/v10037-007-0010-y.

[5] Takao Inoué, Adam Naumowicz, Noboru Endou, and Yasunari Shidama. Partial differentiation, differentiation and continuity on n-dimensional real normed linear spaces. *Formalized Mathematics*, 19(**2**):65–68, 2011. doi:10.2478/v10037-011-0011-8.

[6] Miyadera Isao. *Functional Analysis.* Riko-Gaku-Sya, 1972.

[7] 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.

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

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

[10] Kôsaku Yosida. *Functional Analysis.* Springer, 1980.

Accepted July 23, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 2, Pages 99–124, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0009

sciendo
sciendo.com/journal/forma

Introduction to Graph Colorings

Sebastian Koch[1]
Mainz, Germany

Summary. In this article vertex, edge and total colorings of graphs are formalized in the Mizar system [4] and [1], based on the formalization of graphs in [5].

MSC: 68V20 05C15

Keywords: graph coloring; edge coloring; total coloring

MML identifier: `GLCOLO00`, version: `8.1.12 5.71.1431`

Introduction

Graph coloring has a long history in mathematics and is introduced in almost every introductory book on graph theory (cf. [2], [6], [3]). In this article, the basic notions of vertex, edge and total colorings of graphs are formalized in sections 1, 2 and 3 respectively. These sections have the same basic structure.

At first the (not necessarily proper) coloring is defined as a function defined on the vertices or edges of a graph. The total coloring of a graph is defined as a pair of the other two.

The next definition is about proper colorings, i.e. that no two adjacent vertices or edges are colored the same. A proper total coloring also requires that vertices and edges who are incident with each other are not colored the same as well. In the context of this formalization, the vertex of a loop is considered adjacent to itself, but the edge of a loop is not considered adjacent to itself.

After that an attribute for proper colorability with a cardinal amount of colors is provided. It is important to note that the definition expresses how

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

many colors are sufficient. Given that cardinalities can be infinite, an attribute indicating that only finitely many colors are needed is given as well.

In the last part of each section the chromatic number or index is introduced, indicating how many colors are at least necessary for a proper coloring.

1. Vertex Colorings

From now on E, V denote sets, G, G_1, G_2 denote graphs, c, c_1, c_2 denote cardinal numbers, and n denotes a natural number.

Let us consider G.

A vertex coloring of G is a many sorted set indexed by the vertices of G. One can check that every vertex coloring of G is non empty.

From now on f denotes a vertex coloring of G.

Now we state the proposition:

(1) Let us consider a function f'. Suppose $\operatorname{rng} f \subseteq \operatorname{dom} f'$. Then $f' \cdot f$ is a vertex coloring of G.

Let us consider G and f. Let f' be a many sorted set indexed by $\operatorname{rng} f$. One can check that the functor $f' \cdot f$ yields a vertex coloring of G. Now we state the propositions:

(2) Let us consider a vertex v of G, and an object x. Then $f{+}\cdot(v \dot{\longmapsto} x)$ is a vertex coloring of G.

(3) Let us consider a subgraph H of G. Then $f \restriction$(the vertices of H) is a vertex coloring of H.

(4) Let us consider a supergraph G_1 of G_2 extended by the vertices from V, a vertex coloring f of G_2, and a function h. Suppose $\operatorname{dom} h = V \setminus$ (the vertices of G_2). Then $f{+}\cdot h$ is a vertex coloring of G_1.

(5) Let us consider objects v, e, x, a vertex w of G_2, a supergraph G_1 of G_2 extended by v, w and e between them, and a vertex coloring f of G_2. Suppose $e \notin$ the edges of G_2 and $v \notin$ the vertices of G_2. Then $f{+}\cdot(v \dot{\longmapsto} x)$ is a vertex coloring of G_1.

(6) Let us consider a vertex v of G_2, objects e, w, x, a supergraph G_1 of G_2 extended by v, w and e between them, and a vertex coloring f of G_2. Suppose $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2. Then $f{+}\cdot(w \dot{\longmapsto} x)$ is a vertex coloring of G_1.

(7) Let us consider objects v, x, a subset V of the vertices of G_2, a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2, and a vertex coloring f_2 of G_2. Suppose $v \notin$ the vertices of G_2. Then $f_2{+}\cdot(v \dot{\longmapsto} x)$ is a vertex coloring of G_1.

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

(8) If $\mathrm{dom}(F_{\mathbb{V}})$ = the vertices of G_1, then $f \cdot (F_{\mathbb{V}})$ is a vertex coloring of G_1.

(9) If F is total, then $f \cdot (F_{\mathbb{V}})$ is a vertex coloring of G_1. The theorem is a consequence of (8).

Let us consider G and f. We say that f is proper if and only if

(Def. 1) for every vertices v, w of G such that v and w are adjacent holds $f(v) \neq f(w)$.

Now we state the propositions:

(10) f is proper if and only if for every objects e, v, w such that e joins v and w in G holds $f(v) \neq f(w)$.

(11) f is proper if and only if for every objects e, v, w such that e joins v to w in G holds $f(v) \neq f(w)$. The theorem is a consequence of (10).

(12) Let us consider a one-to-one function f', and a vertex coloring f_2 of G. Suppose $f_2 = f' \cdot f$ and f is proper and $\mathrm{rng}\, f \subseteq \mathrm{dom}\, f'$. Then f_2 is proper. The theorem is a consequence of (10).

(13) Let us consider a one-to-one many sorted set f' indexed by $\mathrm{rng}\, f$. If f is proper, then $f' \cdot f$ is proper. The theorem is a consequence of (12).

(14) If there exists f such that f is proper, then G is loopless. The theorem is a consequence of (10).

Let G be a non loopless graph. Observe that every vertex coloring of G is non proper.

Let G be a loopless graph. Let us observe that every vertex coloring of G which is one-to-one is also proper and there exists a vertex coloring of G which is one-to-one and proper.

Now we state the propositions:

(15) Let us consider a subgraph H of G, and a vertex coloring f' of H. Suppose $f' = f{\restriction}$(the vertices of H) and f is proper. Then f' is proper. The theorem is a consequence of (10).

(16) Let us consider a vertex coloring f_1 of G_1, and a vertex coloring f_2 of G_2. Suppose $G_1 \approx G_2$ and $f_1 = f_2$ and f_1 is proper. Then f_2 is proper. The theorem is a consequence of (10).

(17) Let us consider a vertex coloring f_1 of G_1, a vertex coloring f_2 of G_2, a vertex v of G_1, and an object x. Suppose $G_1 \approx G_2$ and $f_2 = f_1 {+\cdot} (v \,\dot{\longmapsto}\, x)$ and $x \notin \mathrm{rng}\, f_1$ and f_1 is proper. Then f_2 is proper. The theorem is a consequence of (10).

(18) Let us consider a graph G_2 given by reversing directions of the edges E of G_1, a vertex coloring f_1 of G_1, and a vertex coloring f_2 of G_2. If $f_1 = f_2$,

then f_1 is proper iff f_2 is proper.

(19) Let us consider a supergraph G_1 of G_2 extended by the vertices from V, a vertex coloring f_1 of G_1, a vertex coloring f_2 of G_2, and a function h. Suppose $\operatorname{dom} h = V \setminus$ (the vertices of G_2) and $f_1 = f_2 {+}\!\cdot h$ and f_2 is proper. Then f_1 is proper. The theorem is a consequence of (10).

(20) Let us consider vertices v, w of G_2, an object e, a supergraph G_1 of G_2 extended by e between vertices v and w, a vertex coloring f_1 of G_1, and a vertex coloring f_2 of G_2. Suppose $f_1 = f_2$ and v and w are adjacent and f_2 is proper. Then f_1 is proper. The theorem is a consequence of (10) and (16).

(21) Let us consider a vertex v of G_2, objects e, w, a supergraph G_1 of G_2 extended by e between vertices v and w, a vertex coloring f_1 of G_1, a vertex coloring f_2 of G_2, and an object x. Suppose $f_1 = f_2 {+}\!\cdot (v \dot{\longmapsto} x)$ and $v \neq w$ and $x \notin \operatorname{rng} f_2$ and f_2 is proper. Then f_1 is proper. The theorem is a consequence of (10) and (17).

(22) Let us consider objects v, e, a vertex w of G_2, a supergraph G_1 of G_2 extended by e between vertices v and w, a vertex coloring f_1 of G_1, a vertex coloring f_2 of G_2, and an object x. Suppose $f_1 = f_2 {+}\!\cdot (w \dot{\longmapsto} x)$ and $v \neq w$ and $x \notin \operatorname{rng} f_2$ and f_2 is proper. Then f_1 is proper. The theorem is a consequence of (21), (18), and (17).

Let us consider objects v, e, w, a supergraph G_1 of G_2 extended by v, w and e between them, a vertex coloring f_1 of G_1, a vertex coloring f_2 of G_2, and an object x. Now we state the propositions:

(23) Suppose $v \notin$ the vertices of G_2 and $f_1 = f_2 {+}\!\cdot (v \dot{\longmapsto} x)$ and $x \neq f_2(w)$. Then if f_2 is proper, then f_1 is proper. The theorem is a consequence of (11).

(24) Suppose $w \notin$ the vertices of G_2 and $f_1 = f_2 {+}\!\cdot (w \dot{\longmapsto} x)$ and $x \neq f_2(v)$. Then if f_2 is proper, then f_1 is proper. The theorem is a consequence of (23) and (18).

(25) Let us consider objects v, x, a subset V of the vertices of G_2, a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2, a vertex coloring f_1 of G_1, and a vertex coloring f_2 of G_2. Suppose $v \notin$ the vertices of G_2 and $f_1 = f_2 {+}\!\cdot (v \dot{\longmapsto} x)$ and $x \notin \operatorname{rng} f_2$. If f_2 is proper, then f_1 is proper. The theorem is a consequence of (10).

(26) Let us consider a partial graph mapping F from G_1 to G, and a vertex coloring f' of G_1. Suppose F is total and $f' = f \cdot (F_{\mathbb{V}})$ and f is proper. Then f' is proper. The theorem is a consequence of (10).

Let us consider c and G. We say that G is c-vertex-colorable if and only if

(Def. 2) there exists a vertex coloring f of G such that f is proper and $\overline{\overline{\operatorname{rng} f}} \subseteq c$.

Now we state the propositions:

(27) If $c_1 \subseteq c_2$ and G is c_1-vertex-colorable, then G is c_2-vertex-colorable.

(28) If there exists c such that G is c-vertex-colorable, then G is loopless.

Let us consider c. Note that every graph which is c-vertex-colorable is also loopless and every graph which is loopless and c-vertex is also c-vertex-colorable and every graph is non 0-vertex-colorable.

Now we state the propositions:

(29) If G is loopless, then G is (G.order())-vertex-colorable.

(30) G is edgeless if and only if G is 1-vertex-colorable. The theorem is a consequence of (10).

Let c be a non zero cardinal number. One can verify that there exists a graph which is c-vertex-colorable.

Now we state the proposition:

(31) Let us consider a subgraph H of G. If G is c-vertex-colorable, then H is c-vertex-colorable. The theorem is a consequence of (3) and (15).

One can verify that every graph which is edgeless is also 1-vertex-colorable and every graph which is 1-vertex-colorable is also edgeless.

Let c be a non zero cardinal number and G be a c-vertex-colorable graph. Let us observe that every subgraph of G is c-vertex-colorable.

Now we state the propositions:

(32) If $G_1 \approx G_2$ and G_1 is c-vertex-colorable, then G_2 is c-vertex-colorable. The theorem is a consequence of (16).

(33) Let us consider a graph G_2 given by reversing directions of the edges E of G_1. Then G_1 is c-vertex-colorable if and only if G_2 is c-vertex-colorable.

Let c be a non zero cardinal number and G_1 be a c-vertex-colorable graph. Let us consider E. One can verify that every graph given by reversing directions of the edges E of G_1 is c-vertex-colorable.

Now we state the proposition:

(34) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then G_1 is c-vertex-colorable if and only if G_2 is c-vertex-colorable. The theorem is a consequence of (31), (4), and (19).

Let c be a non zero cardinal number and G_2 be a c-vertex-colorable graph. Let us consider V. One can verify that every supergraph of G_2 extended by the vertices from V is c-vertex-colorable.

Now we state the propositions:

(35) Let us consider vertices v, w of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v and w. Suppose v and w are adjacent.

Then G_1 is c-vertex-colorable if and only if G_2 is c-vertex-colorable. The theorem is a consequence of (31) and (20).

(36) Let us consider objects v, e, w, and a supergraph G_1 of G_2 extended by e between vertices v and w. Suppose $v \neq w$ and G_2 is c-vertex-colorable. Then G_1 is $(c+1)$-vertex-colorable. The theorem is a consequence of (22), (32), and (27).

(37) Let us consider a non edgeless graph G_2, objects v, e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Then G_1 is c-vertex-colorable if and only if G_2 is c-vertex-colorable. The theorem is a consequence of (31), (33), and (32).

(38) Let us consider an edgeless graph G_2, and objects v, e, w. Then every supergraph of G_2 extended by v, w and e between them is 2-vertex-colorable. The theorem is a consequence of (33), (32), and (27).

(39) Let us consider an object v, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. If G_2 is c-vertex-colorable, then G_1 is $(c+1)$-vertex-colorable. The theorem is a consequence of (7), (25), (32), and (27).

(40) Let us consider a subgraph G_2 of G_1 with parallel edges removed. Then G_1 is c-vertex-colorable if and only if G_2 is c-vertex-colorable. The theorem is a consequence of (31).

Let c be a non zero cardinal number and G_1 be a c-vertex-colorable graph. Note that every subgraph of G_1 with parallel edges removed is c-vertex-colorable.

Now we state the proposition:

(41) Let us consider a subgraph G_2 of G_1 with directed-parallel edges removed. Then G_1 is c-vertex-colorable if and only if G_2 is c-vertex-colorable. The theorem is a consequence of (31) and (40).

Let c be a non zero cardinal number and G_1 be a c-vertex-colorable graph. One can check that every subgraph of G_1 with directed-parallel edges removed is c-vertex-colorable.

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

(42) If F is weak subgraph embedding and G_2 is c-vertex-colorable, then G_1 is c-vertex-colorable. The theorem is a consequence of (9) and (26).

(43) If F is isomorphism, then G_1 is c-vertex-colorable iff G_2 is c-vertex-colorable. The theorem is a consequence of (42).

Let c be a non zero cardinal number and G be a c-vertex-colorable graph. Let us note that every graph which is G-isomorphic is also c-vertex-colorable.

Let us consider G. We say that G is finitely vertex-colorable if and only if

(Def. 3) there exists n such that G is n-vertex-colorable.

One can verify that every graph which is finitely vertex-colorable is also loopless and every graph which is vertex-finite and loopless is also finitely vertex-colorable and every graph which is edgeless is also finitely vertex-colorable.

Let us consider n. Let us note that every graph which is n-vertex-colorable is also finitely vertex-colorable and there exists a graph which is finitely vertex-colorable and there exists a graph which is non finitely vertex-colorable.

Let G be a finitely vertex-colorable graph. Observe that every subgraph of G is finitely vertex-colorable.

Let G be a non finitely vertex-colorable graph. One can verify that every supergraph of G is non finitely vertex-colorable.

Now we state the propositions:

(44) If $G_1 \approx G_2$ and G_1 is finitely vertex-colorable, then G_2 is finitely vertex-colorable. The theorem is a consequence of (32).

(45) Let us consider a graph G_2 given by reversing directions of the edges E of G_1. Then G_1 is finitely vertex-colorable if and only if G_2 is finitely vertex-colorable.

Let G_1 be a finitely vertex-colorable graph. Let us consider E. Observe that every graph given by reversing directions of the edges E of G_1 is finitely vertex-colorable.

Let G_1 be a non finitely vertex-colorable graph. Note that every graph given by reversing directions of the edges E of G_1 is non finitely vertex-colorable.

Now we state the proposition:

(46) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then G_1 is finitely vertex-colorable if and only if G_2 is finitely vertex-colorable. The theorem is a consequence of (34).

Let G_2 be a finitely vertex-colorable graph. Let us consider V. One can verify that every supergraph of G_2 extended by the vertices from V is finitely vertex-colorable.

Now we state the propositions:

(47) Let us consider objects v, e, w, and a supergraph G_1 of G_2 extended by e between vertices v and w. Suppose $v \neq w$. Then G_1 is finitely vertex-colorable if and only if G_2 is finitely vertex-colorable. The theorem is a consequence of (36).

(48) Let us consider objects v, e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Then G_1 is finitely vertex-colorable if and only if G_2 is finitely vertex-colorable. The theorem is a consequence of (37) and (38).

Let G_2 be a finitely vertex-colorable graph and v, e, w be objects. Observe that every supergraph of G_2 extended by v, w and e between them is finitely vertex-colorable.

Now we state the proposition:

(49) Let us consider an object v, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Then G_1 is finitely vertex-colorable if and only if G_2 is finitely vertex-colorable. The theorem is a consequence of (39).

Let G_2 be a finitely vertex-colorable graph and v be an object. Let us consider V. Let us note that every supergraph of G_2 extended by vertex v and edges between v and V of G_2 is finitely vertex-colorable.

Now we state the proposition:

(50) Let us consider a subgraph G_2 of G_1 with parallel edges removed. Then G_1 is finitely vertex-colorable if and only if G_2 is finitely vertex-colorable. The theorem is a consequence of (40).

Let G_1 be a non finitely vertex-colorable graph. One can verify that every subgraph of G_1 with parallel edges removed is non finitely vertex-colorable.

Now we state the proposition:

(51) Let us consider a subgraph G_2 of G_1 with directed-parallel edges removed. Then G_1 is finitely vertex-colorable if and only if G_2 is finitely vertex-colorable. The theorem is a consequence of (41).

Let G_1 be a non finitely vertex-colorable graph. One can verify that every subgraph of G_1 with directed-parallel edges removed is non finitely vertex-colorable.

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

(52) If F is weak subgraph embedding and G_2 is finitely vertex-colorable, then G_1 is finitely vertex-colorable. The theorem is a consequence of (42).

(53) If F is isomorphism, then G_1 is finitely vertex-colorable iff G_2 is finitely vertex-colorable. The theorem is a consequence of (52).

Let G be a finitely vertex-colorable graph. Observe that every graph which is G-isomorphic is also finitely vertex-colorable.

Let G be a graph. The functor $\chi(G)$ yielding a cardinal number is defined by the term

(Def. 4) $\bigcap\{c$, where c is a cardinal subset of $G.\mathrm{order}() : G$ is c-vertex-colorable$\}$.

Now we state the propositions:

(54) If G is loopless, then G is $\chi(G)$-vertex-colorable. The theorem is a consequence of (29).

(55) G is not loopless if and only if $\chi(G) = 0$. The theorem is a consequence of (29).

Let G be a loopless graph. One can verify that $\chi(G)$ is non zero.

Let G be a non loopless graph. Let us observe that $\chi(G)$ is zero.

Now we state the propositions:

(56) $\chi(G) \subseteq G.\mathrm{order}()$. The theorem is a consequence of (29).

(57) If G is c-vertex-colorable, then $\chi(G) \subseteq c$. The theorem is a consequence of (56).

(58) If G is c-vertex-colorable and for every cardinal number d such that G is d-vertex-colorable holds $c \subseteq d$, then $\chi(G) = c$. The theorem is a consequence of (57) and (29).

Let G be a finitely vertex-colorable graph. Note that $\chi(G)$ is natural.

Let us note that the functor $\chi(G)$ yields a natural number. Now we state the propositions:

(59) Let us consider a loopless graph G. Then $1 \subseteq \chi(G)$.

(60) G is edgeless if and only if $\chi(G) = 1$. The theorem is a consequence of (57), (59), and (54).

(61) Let us consider a loopless, non edgeless graph G. Then $2 \subseteq \chi(G)$. The theorem is a consequence of (60).

(62) Let us consider a loopless graph G. If G is complete, then $\chi(G) = G.\mathrm{order}()$. The theorem is a consequence of (29) and (56).

(63) Let us consider a loopless graph G, and a subgraph H of G. Then $\chi(H) \subseteq \chi(G)$. The theorem is a consequence of (54) and (57).

(64) If $G_1 \approx G_2$, then $\chi(G_1) = \chi(G_2)$. The theorem is a consequence of (32).

(65) Let us consider a graph G_2 given by reversing directions of the edges E of G_1. Then $\chi(G_1) = \chi(G_2)$. The theorem is a consequence of (33).

(66) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then $\chi(G_1) = \chi(G_2)$. The theorem is a consequence of (54), (34), (57), and (58).

(67) Let us consider a non edgeless graph G_2, objects v, e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Then $\chi(G_1) = \chi(G_2)$. The theorem is a consequence of (54), (37), (57), and (58).

(68) Let us consider an edgeless graph G_2, a vertex v of G_2, objects e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Suppose $w \notin$ the vertices of G_2. Then $\chi(G_1) = 2$. The theorem is a consequence of (38) and (58).

(69) Let us consider an edgeless graph G_2, objects v, e, a vertex w of G_2, and a supergraph G_1 of G_2 extended by v, w and e between them. Suppose

$v \notin$ the vertices of G_2. Then $\chi(G_1) = 2$. The theorem is a consequence of (38) and (58).

(70) Let us consider an object v, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Then $\chi(G_1) \subseteq \chi(G_2) + 1$. The theorem is a consequence of (54), (39), and (57).

(71) Let us consider a loopless graph G_2, an object v, and a supergraph G_1 of G_2 extended by vertex v and edges between v and the vertices of G_2. Suppose $v \notin$ the vertices of G_2. Then $\chi(G_1) = \chi(G_2) + 1$. The theorem is a consequence of (70), (63), (54), (3), (15), and (57).

(72) Let us consider a subgraph G_2 of G_1 with parallel edges removed. Then $\chi(G_1) = \chi(G_2)$. The theorem is a consequence of (40), (54), (57), and (58).

(73) Let us consider a subgraph G_2 of G_1 with directed-parallel edges removed. Then $\chi(G_1) = \chi(G_2)$. The theorem is a consequence of (41), (54), (57), and (58).

(74) Let us consider a graph G_1, a loopless graph G_2, and a partial graph mapping F from G_1 to G_2. If F is weak subgraph embedding, then $\chi(G_1) \subseteq \chi(G_2)$. The theorem is a consequence of (42), (54), and (57).

(75) Let us consider a partial graph mapping F from G_1 to G_2. If F is isomorphism, then $\chi(G_1) = \chi(G_2)$. The theorem is a consequence of (54), (43), (57), and (58).

(76) Let us consider a G_1-isomorphic graph G_2. Then $\chi(G_1) = \chi(G_2)$. The theorem is a consequence of (75).

2. Edge Colorings

Let us consider G.

An edge coloring of G is a many sorted set indexed by the edges of G. In the sequel g denotes an edge coloring of G.

Now we state the proposition:

(77) Let us consider a function g'. Suppose $\operatorname{rng} g \subseteq \operatorname{dom} g'$. Then $g' \cdot g$ is an edge coloring of G.

Let us consider G and g. Let g' be a many sorted set indexed by $\operatorname{rng} g$. Note that the functor $g' \cdot g$ yields an edge coloring of G. Now we state the propositions:

(78) Let us consider a subgraph H of G. Then $g \restriction$(the edges of H) is an edge coloring of H.

(79) Let us consider an object e, vertices v, w of G_2, a supergraph G_1 of G_2 extended by e between vertices v and w, an edge coloring g of G_2, and

an object x. Suppose $e \notin$ the edges of G_2. Then $g{+\cdot}(e \dot{\longmapsto} x)$ is an edge coloring of G_1.

(80) Let us consider objects v, e, a vertex w of G_2, a supergraph G_1 of G_2 extended by v, w and e between them, an edge coloring g of G_2, and an object x. Suppose $e \notin$ the edges of G_2 and $v \notin$ the vertices of G_2. Then $g{+\cdot}(e \dot{\longmapsto} x)$ is an edge coloring of G_1.

(81) Let us consider a vertex v of G_2, objects e, w, a supergraph G_1 of G_2 extended by v, w and e between them, an edge coloring g of G_2, and an object x. Suppose $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2. Then $g{+\cdot}(e \dot{\longmapsto} x)$ is an edge coloring of G_1.

(82) Let us consider an object v, a subset V of the vertices of G_2, a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2, an edge coloring g_2 of G_2, and a function h. Suppose $v \notin$ the vertices of G_2 and $\operatorname{dom} h = G_1.\mathrm{edgesBetween}(V, \{v\})$. Then $g_2{+\cdot}h$ is an edge coloring of G_1.

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

(83) If $\operatorname{dom}(F_{\mathbb{E}}) =$ the edges of G_1, then $g \cdot (F_{\mathbb{E}})$ is an edge coloring of G_1.

(84) If F is total, then $g \cdot (F_{\mathbb{E}})$ is an edge coloring of G_1. The theorem is a consequence of (83).

Let us consider G and g. We say that g is proper if and only if

(Def. 5) for every vertex v of G, $g{\restriction}v.\mathrm{edgesInOut}()$ is one-to-one.

Now we state the propositions:

(85) g is proper if and only if for every vertex v of G and for every objects e_1, e_2 such that $e_1, e_2 \in v.\mathrm{edgesInOut}()$ and $g(e_1) = g(e_2)$ holds $e_1 = e_2$.

(86) g is proper if and only if for every objects e_1, e_2, v, w_1, w_2 such that e_1 joins v and w_1 in G and e_2 joins v and w_2 in G and $g(e_1) = g(e_2)$ holds $e_1 = e_2$. The theorem is a consequence of (85).

(87) Let us consider a one-to-one function g', and an edge coloring g_2 of G. If $g_2 = g' \cdot g$ and g is proper, then g_2 is proper.

(88) Let us consider a one-to-one many sorted set g' indexed by $\operatorname{rng} g$. If g is proper, then $g' \cdot g$ is proper.

Let us consider G. One can verify that every edge coloring of G which is one-to-one is also proper and there exists an edge coloring of G which is one-to-one and proper.

Now we state the propositions:

(89) Let us consider a subgraph H of G, and an edge coloring g' of H. Suppose $g' = g{\restriction}$(the edges of H) and g is proper. Then g' is proper. The theorem is a consequence of (85).

(90) Let us consider an edge coloring g_1 of G_1, and an edge coloring g_2 of G_2. Suppose $G_1 \approx G_2$ and $g_1 = g_2$ and g_1 is proper. Then g_2 is proper.

(91) Let us consider a graph G_2 given by reversing directions of the edges E of G_1, an edge coloring g_1 of G_1, and an edge coloring g_2 of G_2. If $g_1 = g_2$, then g_1 is proper iff g_2 is proper.

(92) Let us consider a supergraph G_1 of G_2 extended by the vertices from V, an edge coloring g_1 of G_1, and an edge coloring g_2 of G_2. If $g_1 = g_2$, then if g_2 is proper, then g_1 is proper.

(93) Let us consider objects v, e, w, a supergraph G_1 of G_2 extended by e between vertices v and w, an edge coloring g_1 of G_1, an edge coloring g_2 of G_2, and an object x. Suppose $g_1 = g_2 {+\cdot} (e \dot{\longmapsto} x)$ and $e \notin$ the edges of G_2 and $x \notin \operatorname{rng} g_2$. If g_2 is proper, then g_1 is proper.

(94) Let us consider objects v, e, a vertex w of G_2, a supergraph G_1 of G_2 extended by v, w and e between them, an edge coloring g_1 of G_1, an edge coloring g_2 of G_2, and an object x. Suppose $g_1 = g_2 {+\cdot} (e \dot{\longmapsto} x)$ and $x \notin \operatorname{rng} g_2$ and $e \notin$ the edges of G_2 and $v \notin$ the vertices of G_2. If g_2 is proper, then g_1 is proper. The theorem is a consequence of (92) and (93).

(95) Let us consider a vertex v of G_2, objects e, w, a supergraph G_1 of G_2 extended by v, w and e between them, an edge coloring g_1 of G_1, an edge coloring g_2 of G_2, and an object x. Suppose $g_1 = g_2 {+\cdot} (e \dot{\longmapsto} x)$ and $x \notin \operatorname{rng} g_2$ and $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2. If g_2 is proper, then g_1 is proper. The theorem is a consequence of (92) and (93).

(96) Let us consider an object v, a subset V of the vertices of G_2, a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2, an edge coloring g_2 of G_2, an edge coloring g_1 of G_1, and sets X, E. Suppose $E = G_1.\mathrm{edgesBetween}(V, \{v\})$ and $\operatorname{rng} g_2 \subseteq X$ and $g_1 = g_2 {+\cdot} \langle E \longmapsto X, \mathrm{id}_E\rangle$ and $v \notin$ the vertices of G_2 and g_2 is proper. Then g_1 is proper. The theorem is a consequence of (85) and (86).

Let us consider a partial graph mapping F from G_1 to G and an edge coloring g' of G_1. Now we state the propositions:

(97) Suppose $\mathrm{dom}(F_{\mathbb{E}})$ = the edges of G_1 and $F_{\mathbb{E}}$ is one-to-one and $g' = g \cdot (F_{\mathbb{E}})$ and g is proper. Then g' is proper. The theorem is a consequence of (85).

(98) If F is weak subgraph embedding and $g' = g \cdot (F_{\mathbb{E}})$ and g is proper, then g' is proper. The theorem is a consequence of (97).

Let us consider c and G. We say that G is c-edge-colorable if and only if

(Def. 6) there exists a proper edge coloring g of G such that $\overline{\overline{\operatorname{rng} g}} \subseteq c$.

Now we state the propositions:

(99) If $c_1 \subseteq c_2$ and G is c_1-edge-colorable, then G is c_2-edge-colorable.

(100) G is (G.size())-edge-colorable.

(101) G is edgeless if and only if G is 0-edge-colorable. The theorem is a consequence of (100).

Let us observe that every graph which is edgeless is also 0-edge-colorable and every graph which is 0-edge-colorable is also edgeless.

Let us consider c. Note that every graph which is c-edge is also c-edge-colorable and there exists a graph which is c-edge-colorable.

Now we state the proposition:

(102) Let us consider a subgraph H of G. If G is c-edge-colorable, then H is c-edge-colorable. The theorem is a consequence of (78) and (89).

Let us consider c. Let G be a c-edge-colorable graph. Note that every subgraph of G is c-edge-colorable.

Now we state the propositions:

(103) If $G_1 \approx G_2$ and G_1 is c-edge-colorable, then G_2 is c-edge-colorable. The theorem is a consequence of (90).

(104) Let us consider a graph G_2 given by reversing directions of the edges E of G_1. Then G_1 is c-edge-colorable if and only if G_2 is c-edge-colorable.

Let us consider c. Let G_1 be a c-edge-colorable graph. Let us consider E. Let us note that every graph given by reversing directions of the edges E of G_1 is c-edge-colorable.

Now we state the proposition:

(105) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then G_1 is c-edge-colorable if and only if G_2 is c-edge-colorable. The theorem is a consequence of (92).

Let us consider c. Let G_2 be a c-edge-colorable graph. Let us consider V. Let us note that every supergraph of G_2 extended by the vertices from V is c-edge-colorable.

Let us consider a c-edge-colorable graph G_2 and objects v, e, w. Now we state the propositions:

(106) Every supergraph of G_2 extended by e between vertices v and w is $(c+1)$-edge-colorable. The theorem is a consequence of (79), (93), (103), and (99).

(107) Every supergraph of G_2 extended by v, w and e between them is $(c+1)$-edge-colorable. The theorem is a consequence of (106), (103), and (99).

Now we state the proposition:

(108) Let us consider an edgeless graph G_2, and objects v, e, w. Then every supergraph of G_2 extended by v, w and e between them is 1-edge-colorable. The theorem is a consequence of (104) and (99).

Let us consider c. Let G_2 be a c-edge-colorable graph and v, e, w be objects. Note that every supergraph of G_2 extended by e between vertices v and w is $(c+1)$-edge-colorable and every supergraph of G_2 extended by v, w and e between them is $(c+1)$-edge-colorable.

Now we state the proposition:

(109) Let us consider a c-edge-colorable graph G_2, and an object v. Then every supergraph of G_2 extended by vertex v and edges between v and V of G_2 is $(c+\overline{\overline{V}})$-edge-colorable. The theorem is a consequence of (82), (96), (103), and (99).

Let us consider c. Let G_2 be a c-edge-colorable graph and v be an object. Let us consider V. One can verify that every supergraph of G_2 extended by vertex v and edges between v and V of G_2 is $(c+\overline{\overline{V}})$-edge-colorable.

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

(110) If F is weak subgraph embedding and G_2 is c-edge-colorable, then G_1 is c-edge-colorable. The theorem is a consequence of (84) and (98).

(111) If F is isomorphism, then G_1 is c-edge-colorable iff G_2 is c-edge-colorable. The theorem is a consequence of (110).

Let us consider c. Let G be a c-edge-colorable graph. Note that every graph which is G-isomorphic is also c-edge-colorable.

Let us consider G. We say that G is finitely edge-colorable if and only if

(Def. 7) there exists n such that G is n-edge-colorable.

Let us observe that every graph which is edge-finite is also finitely edge-colorable and every graph which is edgeless is also finitely edge-colorable and every graph which is finitely edge-colorable is also locally-finite.

Let us consider n. One can check that every graph which is n-edge-colorable is also finitely edge-colorable and there exists a graph which is finitely edge-colorable and there exists a graph which is non finitely edge-colorable.

Let G be a finitely edge-colorable graph. Note that every subgraph of G is finitely edge-colorable.

Now we state the propositions:

(112) If $G_1 \approx G_2$ and G_1 is finitely edge-colorable, then G_2 is finitely edge-colorable. The theorem is a consequence of (103).

(113) Let us consider a graph G_2 given by reversing directions of the edges E of G_1. Then G_1 is finitely edge-colorable if and only if G_2 is finitely edge-colorable.

Let G_1 be a finitely edge-colorable graph. Let us consider E. One can verify that every graph given by reversing directions of the edges E of G_1 is finitely edge-colorable.

Let G_1 be a non finitely edge-colorable graph. Observe that every graph given by reversing directions of the edges E of G_1 is non finitely edge-colorable.

Now we state the proposition:

(114) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then G_1 is finitely edge-colorable if and only if G_2 is finitely edge-colorable. The theorem is a consequence of (105).

Let G_2 be a finitely edge-colorable graph. Let us consider V. One can verify that every supergraph of G_2 extended by the vertices from V is finitely edge-colorable.

Let G_2 be a non finitely edge-colorable graph. Observe that every supergraph of G_2 extended by the vertices from V is non finitely edge-colorable.

Now we state the proposition:

(115) Let us consider objects v, e, w, and a supergraph G_1 of G_2 extended by e between vertices v and w. Then G_1 is finitely edge-colorable if and only if G_2 is finitely edge-colorable. The theorem is a consequence of (107).

Let G_2 be a finitely edge-colorable graph and v, e, w be objects. Note that every supergraph of G_2 extended by e between vertices v and w is finitely edge-colorable.

Let G_2 be a non finitely edge-colorable graph. One can verify that every supergraph of G_2 extended by e between vertices v and w is non finitely edge-colorable.

Now we state the proposition:

(116) Let us consider objects v, e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Then G_1 is finitely edge-colorable if and only if G_2 is finitely edge-colorable.

Let G_2 be a finitely edge-colorable graph and v, e, w be objects. Observe that every supergraph of G_2 extended by v, w and e between them is finitely edge-colorable.

Let G_2 be a non finitely edge-colorable graph. Note that every supergraph of G_2 extended by v, w and e between them is non finitely edge-colorable.

Now we state the proposition:

(117) Let us consider an object v, a finite set V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Then G_1 is finitely edge-colorable if and only if G_2 is finitely edge-colorable.

Let G_2 be a finitely edge-colorable graph, v be an object, and V be a finite set. Let us observe that every supergraph of G_2 extended by vertex v and edges between v and V of G_2 is finitely edge-colorable.

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

(118) If F is weak subgraph embedding and G_2 is finitely edge-colorable, then G_1 is finitely edge-colorable. The theorem is a consequence of (110).

(119) If F is isomorphism, then G_1 is finitely edge-colorable iff G_2 is finitely edge-colorable. The theorem is a consequence of (118).

Let G be a finitely edge-colorable graph. One can verify that every graph which is G-isomorphic is also finitely edge-colorable.

Let us consider G. The functor $\chi'(G)$ yielding a cardinal number is defined by the term

(Def. 8) $\bigcap\{c$, where c is a cardinal subset of G.size() : G is c-edge-colorable$\}$.

Now we state the propositions:

(120) $\chi'(G) \subseteq G$.size(). The theorem is a consequence of (100).

(121) G is edgeless if and only if $\chi'(G) = 0$. The theorem is a consequence of (120).

Let G be an edgeless graph. One can check that $\chi'(G)$ is zero.

Let G be a non edgeless graph. One can check that $\chi'(G)$ is non zero.

Now we state the proposition:

(122) G is c-edge-colorable and for every cardinal number d such that G is d-edge-colorable holds $c \subseteq d$ if and only if $\chi'(G) = c$. The theorem is a consequence of (100).

Let G be a finitely edge-colorable graph. Let us observe that $\chi'(G)$ is natural.

Let us observe that the functor $\chi'(G)$ yields a natural number. Now we state the propositions:

(123) Let us consider a loopless graph G. Then $\bar{\Delta}(G) \subseteq \chi'(G)$.

(124) If $G_1 \approx G_2$, then $\chi'(G_1) = \chi'(G_2)$. The theorem is a consequence of (103) and (122).

(125) Let us consider a graph G_2 given by reversing directions of the edges E of G_1. Then $\chi'(G_1) = \chi'(G_2)$. The theorem is a consequence of (104) and (122).

(126) Let us consider a subgraph H of G. Then $\chi'(H) \subseteq \chi'(G)$.

(127) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then $\chi'(G_1) = \chi'(G_2)$. The theorem is a consequence of (105) and (122).

(128) Let us consider objects v, e, w, and a supergraph G_1 of G_2 extended by e between vertices v and w. Then $\chi'(G_1) \subseteq \chi'(G_2) + 1$. The theorem is a consequence of (106).

(129) Let us consider objects v, e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Then $\chi'(G_1) \subseteq \chi'(G_2) + 1$. The theorem is a consequence of (107).

(130) Let us consider an edgeless graph G_2, a vertex v of G_2, objects e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Suppose $w \notin$ the vertices of G_2. Then $\chi'(G_1) = 1$. The theorem is a consequence of (122).

(131) Let us consider an edgeless graph G_2, objects v, e, a vertex w of G_2, and a supergraph G_1 of G_2 extended by v, w and e between them. Suppose $v \notin$ the vertices of G_2. Then $\chi'(G_1) = 1$. The theorem is a consequence of (130) and (125).

(132) Let us consider an object v, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Then $\chi'(G_1) \subseteq \chi'(G_2) + \overline{\overline{V}}$.

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

(133) If F is weak subgraph embedding, then $\chi'(G_1) \subseteq \chi'(G_2)$. The theorem is a consequence of (110).

(134) If F is isomorphism, then $\chi'(G_1) = \chi'(G_2)$. The theorem is a consequence of (133).

(135) Let us consider a G_1-isomorphic graph G_2. Then $\chi'(G_1) = \chi'(G_2)$. The theorem is a consequence of (134).

(136) If G is trivial, then $\chi'(G) = G$.size(). The theorem is a consequence of (100) and (122).

3. Total Colorings

Let us consider G.

A total coloring of G is an object defined by

(Def. 9) there exists a vertex coloring f of G and there exists an edge coloring g of G such that $it = \langle f, g \rangle$.

Note that every total coloring of G is pair.

From now on t denotes a total coloring of G.

Let us consider G and t. We introduce the notation $t_{\mathbb{V}}$ as a synonym of $(t)_{\mathbf{1}}$ and $t_{\mathbb{E}}$ as a synonym of $(t)_{\mathbf{2}}$.

One can check that $\langle t_{\mathbb{V}}, t_{\mathbb{E}} \rangle$ reduces to t.

One can verify that the functor $t_{\mathbb{V}}$ yields a vertex coloring of G. Let us observe that the functor $t_{\mathbb{E}}$ yields an edge coloring of G. Let us consider f and g. Note that the functor $\langle f, g \rangle$ yields a total coloring of G. Now we state the propositions:

(137) If G is edgeless, then $\langle f, \emptyset \rangle$ is a total coloring of G.

(138) Let us consider a subgraph H of G. Then $\langle t_{\mathbb{V}} \restriction$(the vertices of H), $t_{\mathbb{E}} \restriction$(the edges of H)$\rangle$ is a total coloring of H. The theorem is a consequence of (3) and (78).

(139) Let us consider a supergraph G_1 of G_2 extended by the vertices from V, a total coloring t of G_2, and a function h. Suppose $\mathrm{dom}\, h = V \setminus$ (the vertices of G_2). Then $\langle t_{\mathbb{V}} {+\cdot} h, t_{\mathbb{E}} \rangle$ is a total coloring of G_1. The theorem is a consequence of (4).

(140) Let us consider objects v, x, a supergraph G_1 of G_2 extended by v, and a total coloring t of G_2. Then $\langle t_{\mathbb{V}} {+\cdot} (v \mathrel{\dot{\longmapsto}} x), t_{\mathbb{E}} \rangle$ is a total coloring of G_1.

(141) Let us consider an object e, vertices v, w of G_2, a supergraph G_1 of G_2 extended by e between vertices v and w, a total coloring t of G_2, and an object y. Suppose $e \notin$ the edges of G_2. Then $\langle t_{\mathbb{V}}, t_{\mathbb{E}} {+\cdot} (e \mathrel{\dot{\longmapsto}} y) \rangle$ is a total coloring of G_1.

(142) Let us consider an object e, vertices v, w, u of G_2, a supergraph G_1 of G_2 extended by e between vertices v and w, a total coloring t of G_2, and objects x, y. Suppose $e \notin$ the edges of G_2. Then $\langle t_{\mathbb{V}} {+\cdot} (u \mathrel{\dot{\longmapsto}} x), t_{\mathbb{E}} {+\cdot} (e \mathrel{\dot{\longmapsto}} y) \rangle$ is a total coloring of G_1. The theorem is a consequence of (141).

(143) Let us consider objects v, e, a vertex w of G_2, a supergraph G_1 of G_2 extended by v, w and e between them, a total coloring t of G_2, and objects x, y. Suppose $e \notin$ the edges of G_2 and $v \notin$ the vertices of G_2. Then $\langle t_{\mathbb{V}} {+\cdot} (v \mathrel{\dot{\longmapsto}} x), t_{\mathbb{E}} {+\cdot} (e \mathrel{\dot{\longmapsto}} y) \rangle$ is a total coloring of G_1. The theorem is a consequence of (140) and (141).

(144) Let us consider a vertex v of G_2, objects e, w, a supergraph G_1 of G_2 extended by v, w and e between them, a total coloring t of G_2, and objects x, y. Suppose $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2. Then $\langle t_{\mathbb{V}} {+\cdot} (w \mathrel{\dot{\longmapsto}} x), t_{\mathbb{E}} {+\cdot} (e \mathrel{\dot{\longmapsto}} y) \rangle$ is a total coloring of G_1. The theorem is a consequence of (140) and (141).

(145) Let us consider a partial graph mapping F from G_1 to G. Suppose F is total. Then $\langle (t_{\mathbb{V}}) \cdot (F_{\mathbb{V}}), (t_{\mathbb{E}}) \cdot (F_{\mathbb{E}}) \rangle$ is a total coloring of G_1. The theorem is a consequence of (9) and (84).

Let us consider G and t. We say that t is proper if and only if

(Def. 10) $t_{\mathbb{V}}$ is proper and $t_{\mathbb{E}}$ is proper and for every vertex v of G, $(t_{\mathbb{V}})(v) \notin (t_{\mathbb{E}})^{\circ}(v.\mathrm{edgesInOut}())$.

Now we state the propositions:

(146) t is proper if and only if $t_{\mathbb{V}}$ is proper and $t_{\mathbb{E}}$ is proper and for every objects e, v, w such that e joins v and w in G holds $(t_{\mathbb{V}})(v) \neq (t_{\mathbb{E}})(e)$.

(147) If $t_{\mathbb{V}}$ is proper and $t_{\mathbb{E}}$ is proper and $\mathrm{rng}\, t_{\mathbb{V}}$ misses $\mathrm{rng}\, t_{\mathbb{E}}$, then t is proper. The theorem is a consequence of (146).

(148) t is proper if and only if for every objects e_1, e_2, v, w_1, w_2 such that e_1 joins v and w_1 in G and e_2 joins v and w_2 in G holds $(t_{\mathbb{V}})(v) \neq (t_{\mathbb{V}})(w_1)$ and $(t_{\mathbb{V}})(v) \neq (t_{\mathbb{E}})(e_1)$ and if $e_1 \neq e_2$, then $(t_{\mathbb{E}})(e_1) \neq (t_{\mathbb{E}})(e_2)$. The theorem is a consequence of (10), (86), and (146).

(149) Suppose g is proper. Then there exists a proper edge coloring g' of G such that

(i) $\operatorname{rng} f$ misses $\operatorname{rng} g'$, and

(ii) $\overline{\overline{\operatorname{rng} g}} = \overline{\overline{\operatorname{rng} g'}}$.

The theorem is a consequence of (77) and (87).

(150) Suppose f is proper. Then there exists a vertex coloring f' of G such that

(i) f' is proper, and

(ii) $\operatorname{rng} f'$ misses $\operatorname{rng} g$, and

(iii) $\overline{\overline{\operatorname{rng} f}} = \overline{\overline{\operatorname{rng} f'}}$.

The theorem is a consequence of (1) and (12).

Let G be a loopless graph. Observe that there exists a total coloring of G which is proper.

Let t be a proper total coloring of G. One can verify that $t_{\mathbb{V}}$ is proper as a vertex coloring of G and $t_{\mathbb{E}}$ is proper as an edge coloring of G.

Now we state the propositions:

(151) Let us consider a subgraph H of G, and a total coloring t' of H. Suppose $t' = \langle t_{\mathbb{V}} \restriction (\text{the vertices of } H), t_{\mathbb{E}} \restriction (\text{the edges of } H) \rangle$ and t is proper. Then t' is proper. The theorem is a consequence of (15), (89), and (146).

(152) Let us consider a total coloring t^1 of G_1, and a total coloring t^2 of G_2. Suppose $G_1 \approx G_2$ and $t^1 = t^2$ and t^1 is proper. Then t^2 is proper. The theorem is a consequence of (16), (90), and (146).

(153) Let us consider a graph G_2 given by reversing directions of the edges E of G_1, a total coloring t^1 of G_1, and a total coloring t^2 of G_2. If $t^1 = t^2$, then t^1 is proper iff t^2 is proper.

(154) Let us consider a supergraph G_1 of G_2 extended by the vertices from V, a total coloring t^1 of G_1, a total coloring t^2 of G_2, and a function h. Suppose $\operatorname{dom} h = V \setminus (\text{the vertices of } G_2)$ and ${t^1}_{\mathbb{V}} = {t^2}_{\mathbb{V}} {+\cdot} h$ and ${t^1}_{\mathbb{E}} = {t^2}_{\mathbb{E}}$ and t^2 is proper. Then t^1 is proper. The theorem is a consequence of (19) and (92).

(155) Let us consider objects y, e, vertices v, w of G_2, a supergraph G_1 of G_2 extended by e between vertices v and w, a total coloring t^1 of G_1, and a total coloring t^2 of G_2. Suppose $e \notin$ the edges of G_2 and v and w are

adjacent and ${t^1}_{\mathbb{V}} = {t^2}_{\mathbb{V}}$ and ${t^1}_{\mathbb{E}} = {t^2}_{\mathbb{E}} {+\cdot} (e \dot{\longmapsto} y)$ and $y \notin \operatorname{rng} {t^2}_{\mathbb{V}} \cup \operatorname{rng} {t^2}_{\mathbb{E}}$ and t^2 is proper. Then t^1 is proper. The theorem is a consequence of (20), (93), and (146).

(156) Let us consider objects v, e, a vertex w of G_2, a supergraph G_1 of G_2 extended by e between vertices v and w, a total coloring t^1 of G_1, a total coloring t^2 of G_2, and objects x, y. Suppose $e \notin$ the edges of G_2 and $v \neq w$ and ${t^1}_{\mathbb{V}} = {t^2}_{\mathbb{V}} {+\cdot} (v \dot{\longmapsto} x)$ and ${t^1}_{\mathbb{E}} = {t^2}_{\mathbb{E}} {+\cdot} (e \dot{\longmapsto} y)$ and $\{x, y\}$ misses $\operatorname{rng} {t^2}_{\mathbb{V}} \cup \operatorname{rng} {t^2}_{\mathbb{E}}$ and $x \neq y$ and t^2 is proper. Then t^1 is proper. The theorem is a consequence of (21), (93), and (146).

(157) Let us consider a vertex v of G_2, objects e, w, a supergraph G_1 of G_2 extended by e between vertices v and w, a total coloring t^1 of G_1, a total coloring t^2 of G_2, and objects x, y. Suppose $e \notin$ the edges of G_2 and $v \neq w$ and ${t^1}_{\mathbb{V}} = {t^2}_{\mathbb{V}} {+\cdot} (w \dot{\longmapsto} x)$ and ${t^1}_{\mathbb{E}} = {t^2}_{\mathbb{E}} {+\cdot} (e \dot{\longmapsto} y)$ and $\{x, y\}$ misses $\operatorname{rng} {t^2}_{\mathbb{V}} \cup \operatorname{rng} {t^2}_{\mathbb{E}}$ and $x \neq y$ and t^2 is proper. Then t^1 is proper. The theorem is a consequence of (156) and (153).

(158) Let us consider objects v, e, a vertex w of G_2, a supergraph G_1 of G_2 extended by v, w and e between them, a total coloring t^1 of G_1, a total coloring t^2 of G_2, and objects x, y. Suppose $e \notin$ the edges of G_2 and $v \notin$ the vertices of G_2 and ${t^1}_{\mathbb{V}} = {t^2}_{\mathbb{V}} {+\cdot} (v \dot{\longmapsto} x)$ and ${t^1}_{\mathbb{E}} = {t^2}_{\mathbb{E}} {+\cdot} (e \dot{\longmapsto} y)$ and $y \notin \operatorname{rng} {t^2}_{\mathbb{V}} \cup \operatorname{rng} {t^2}_{\mathbb{E}}$ and $x \neq y$ and $x \neq ({t^2}_{\mathbb{V}})(w)$ and t^2 is proper. Then t^1 is proper. The theorem is a consequence of (23), (94), and (146).

(159) Let us consider a vertex v of G_2, objects e, w, a supergraph G_1 of G_2 extended by v, w and e between them, a total coloring t^1 of G_1, a total coloring t^2 of G_2, and objects x, y. Suppose $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2 and ${t^1}_{\mathbb{V}} = {t^2}_{\mathbb{V}} {+\cdot} (w \dot{\longmapsto} x)$ and ${t^1}_{\mathbb{E}} = {t^2}_{\mathbb{E}} {+\cdot} (e \dot{\longmapsto} y)$ and $y \notin \operatorname{rng} {t^2}_{\mathbb{V}} \cup \operatorname{rng} {t^2}_{\mathbb{E}}$ and $x \neq y$ and $x \neq ({t^2}_{\mathbb{V}})(v)$ and t^2 is proper. Then t^1 is proper. The theorem is a consequence of (158) and (153).

(160) Let us consider a partial graph mapping F from G_1 to G, and a total coloring t' of G_1. Suppose F is weak subgraph embedding and $t' = \langle (t_{\mathbb{V}}) \cdot (F_{\mathbb{V}}), (t_{\mathbb{E}}) \cdot (F_{\mathbb{E}}) \rangle$ and t is proper. Then t' is proper. The theorem is a consequence of (26), (98), and (146).

Let us consider c and G. We say that G is c-total-colorable if and only if

(Def. 11) there exists a total coloring t of G such that t is proper and $\operatorname{rng} t_{\mathbb{V}} \cup \operatorname{rng} t_{\mathbb{E}} \subseteq c$.

Now we state the propositions:

(161) If $c_1 \subseteq c_2$ and G is c_1-total-colorable, then G is c_2-total-colorable.

(162) If G is c-total-colorable, then G is c-vertex-colorable and c-edge-colorable.

(163) If G is c_1-vertex-colorable and c_2-edge-colorable, then G is (c_1+c_2)-total-

colorable. The theorem is a consequence of (150) and (147).

(164) If G is edgeless and f is proper and $t = \langle f, \emptyset \rangle$, then t is proper.

(165) G is edgeless if and only if G is 1-total-colorable. The theorem is a consequence of (137) and (162).

Let c be a non zero cardinal number. One can check that there exists a graph which is c-total-colorable.

Now we state the proposition:

(166) Let us consider a subgraph H of G. If G is c-total-colorable, then H is c-total-colorable. The theorem is a consequence of (138) and (151).

Let us note that every graph is non 0-total-colorable and every graph which is edgeless is also 1-total-colorable and every graph which is 1-total-colorable is also edgeless.

Let c be a non zero cardinal number and G be a c-total-colorable graph. Note that every subgraph of G is c-total-colorable.

Let us consider c. Observe that every graph which is c-total-colorable is also loopless.

Now we state the propositions:

(167) If $G_1 \approx G_2$ and G_1 is c-total-colorable, then G_2 is c-total-colorable. The theorem is a consequence of (152).

(168) Let us consider a graph G_2 given by reversing directions of the edges E of G_1. Then G_1 is c-total-colorable if and only if G_2 is c-total-colorable.

Let c be a non zero cardinal number and G_1 be a c-total-colorable graph. Let us consider E. One can check that every graph given by reversing directions of the edges E of G_1 is c-total-colorable.

Now we state the proposition:

(169) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then G_1 is c-total-colorable if and only if G_2 is c-total-colorable. The theorem is a consequence of (166), (139), and (154).

Let c be a non zero cardinal number and G_2 be a c-total-colorable graph. Let us consider V. Let us observe that every supergraph of G_2 extended by the vertices from V is c-total-colorable.

Now we state the propositions:

(170) Let us consider an object e, vertices v, w of G_2, and a supergraph G_1 of G_2 extended by e between vertices v and w. Suppose v and w are adjacent and G_2 is c-total-colorable. Then G_1 is $(c+1)$-total-colorable. The theorem is a consequence of (141), (155), (167), and (161).

(171) Let us consider objects v, e, w, and a supergraph G_1 of G_2 extended by e between vertices v and w. Suppose $v \neq w$ and G_2 is c-total-colorable.

Then G_1 is $(c+2)$-total-colorable. The theorem is a consequence of (142), (156), (167), and (161).

(172) Let us consider a non edgeless graph G_2, objects v, e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. If G_2 is c-total-colorable, then G_1 is $(c+1)$-total-colorable. The theorem is a consequence of (168), (167), and (161).

(173) Let us consider a vertex v of G_2, objects e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Suppose $e \notin$ the edges of G_2 and $w \notin$ the vertices of G_2 and v is endvertex. If G_2 is c-total-colorable, then G_1 is c-total-colorable. The theorem is a consequence of (144) and (148).

(174) Let us consider an edgeless graph G_2, and objects v, e, w. Then every supergraph of G_2 extended by v, w and e between them is 3-total-colorable. The theorem is a consequence of (38) and (163).

(175) Let us consider an object v, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose G_2 is c-total-colorable. Then G_1 is $((c+1)+\overline{\overline{V}})$-total-colorable. The theorem is a consequence of (82), (7), (96), (25), (146), (167), and (161).

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

(176) If F is weak subgraph embedding and G_2 is c-total-colorable, then G_1 is c-total-colorable. The theorem is a consequence of (145) and (160).

(177) If F is isomorphism, then G_1 is c-total-colorable iff G_2 is c-total-colorable. The theorem is a consequence of (176).

Let c be a non zero cardinal number and G be a c-total-colorable graph. One can verify that every graph which is G-isomorphic is also c-total-colorable.

Let us consider G. We say that G is finitely total-colorable if and only if

(Def. 12) there exists n such that G is n-total-colorable.

Let us note that every graph which is finitely total-colorable is also loopless and every graph which is edgeless is also finitely total-colorable.

Let us consider n. One can verify that every graph which is n-total-colorable is also finitely total-colorable and there exists a graph which is finitely total-colorable and there exists a graph which is non finitely total-colorable.

Let G be a finitely total-colorable graph. One can check that every subgraph of G is finitely total-colorable.

Now we state the propositions:

(178) If $G_1 \approx G_2$ and G_1 is finitely total-colorable, then G_2 is finitely total-colorable. The theorem is a consequence of (167).

(179) Let us consider a graph G_2 given by reversing directions of the edges E of G_1. Then G_1 is finitely total-colorable if and only if G_2 is finitely total-colorable. The theorem is a consequence of (168).

Let G_1 be a finitely total-colorable graph. Let us consider E. Observe that every graph given by reversing directions of the edges E of G_1 is finitely total-colorable.

Let G_1 be a non finitely total-colorable graph. Note that every graph given by reversing directions of the edges E of G_1 is non finitely total-colorable.

Now we state the proposition:

(180) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then G_1 is finitely total-colorable if and only if G_2 is finitely total-colorable. The theorem is a consequence of (169).

Let G_2 be a finitely total-colorable graph. Let us consider V. One can verify that every supergraph of G_2 extended by the vertices from V is finitely total-colorable.

Let G_2 be a non finitely total-colorable graph. Observe that every supergraph of G_2 extended by the vertices from V is non finitely total-colorable.

Now we state the propositions:

(181) Let us consider objects v, e, w, and a supergraph G_1 of G_2 extended by e between vertices v and w. Suppose $v \neq w$. Then G_1 is finitely total-colorable if and only if G_2 is finitely total-colorable. The theorem is a consequence of (171).

(182) Let us consider objects v, e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Then G_1 is finitely total-colorable if and only if G_2 is finitely total-colorable. The theorem is a consequence of (172) and (174).

Let G_2 be a finitely total-colorable graph and v, e, w be objects. One can check that every supergraph of G_2 extended by v, w and e between them is finitely total-colorable.

Let G_2 be a non finitely total-colorable graph. Let us observe that every supergraph of G_2 extended by v, w and e between them is non finitely total-colorable.

Now we state the proposition:

(183) Let us consider an object v, a finite set V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Then G_1 is finitely total-colorable if and only if G_2 is finitely total-colorable. The theorem is a consequence of (175).

Let G_2 be a finitely total-colorable graph, v be an object, and V be a finite set. Note that every supergraph of G_2 extended by vertex v and edges between

v and V of G_2 is finitely total-colorable.

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

(184) If F is weak subgraph embedding and G_2 is finitely total-colorable, then G_1 is finitely total-colorable. The theorem is a consequence of (176).

(185) If F is isomorphism, then G_1 is finitely total-colorable iff G_2 is finitely total-colorable. The theorem is a consequence of (184).

Let G be a finitely total-colorable graph. Let us note that every graph which is G-isomorphic is also finitely total-colorable.

Let G be a graph. The functor $\chi''(G)$ yielding a cardinal number is defined by the term

(Def. 13) $\bigcap\{c$, where c is a cardinal subset of $G.\mathrm{order}() + G.\mathrm{size}() : G$ is c-total-colorable$\}$.

Now we state the propositions:

(186) If G is loopless, then G is $\chi''(G)$-total-colorable. The theorem is a consequence of (29), (100), and (163).

(187) G is not loopless if and only if $\chi''(G) = 0$. The theorem is a consequence of (29), (100), and (163).

Let G be a loopless graph. Let us observe that $\chi''(G)$ is non zero.

Let G be a non loopless graph. Observe that $\chi''(G)$ is zero.

Now we state the propositions:

(188) $\chi''(G) \subseteq G.\mathrm{order}() + G.\mathrm{size}()$. The theorem is a consequence of (29), (100), and (163).

(189) If G is c-total-colorable, then $\chi''(G) \subseteq c$. The theorem is a consequence of (188).

(190) If G is c-total-colorable and for every cardinal number d such that G is d-total-colorable holds $c \subseteq d$, then $\chi''(G) = c$. The theorem is a consequence of (189), (29), (100), and (163).

Let G be a finitely total-colorable graph. One can check that $\chi''(G)$ is natural.

Note that the functor $\chi''(G)$ yields a natural number. Now we state the propositions:

(191) $\chi(G) \subseteq \chi''(G)$. The theorem is a consequence of (186), (57), and (162).

(192) Let us consider a loopless graph G. Then $\chi'(G) \subseteq \chi''(G)$. The theorem is a consequence of (186) and (162).

(193) $\chi''(G) \subseteq \chi(G) + \chi'(G)$. The theorem is a consequence of (54), (122), (163), and (189).

(194) Let us consider a loopless graph G. Then $\bar{\Delta}(G)+1 \subseteq \chi''(G)$. The theorem is a consequence of (186), (123), and (192).

(195) G is edgeless if and only if $\chi''(G) = 1$. The theorem is a consequence of (190), (186), and (187).

(196) Let us consider a loopless, non edgeless graph G. Then $3 \subseteq \chi''(G)$. The theorem is a consequence of (195), (186), and (148).

(197) Let us consider a loopless graph G, and a subgraph H of G. Then $\chi''(H) \subseteq \chi''(G)$. The theorem is a consequence of (186) and (189).

(198) If $G_1 \approx G_2$, then $\chi''(G_1) = \chi''(G_2)$. The theorem is a consequence of (167), (186), (189), and (190).

(199) Let us consider a graph G_2 given by reversing directions of the edges E of G_1. Then $\chi''(G_1) = \chi''(G_2)$. The theorem is a consequence of (168), (186), (189), and (190).

(200) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then $\chi''(G_1) = \chi''(G_2)$. The theorem is a consequence of (169), (186), (189), and (190).

(201) Let us consider a non edgeless graph G_2, objects v, e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Then $\chi''(G_1) \subseteq \chi''(G_2) + 1$. The theorem is a consequence of (186), (172), and (189).

(202) Let us consider an edgeless graph G_2, a vertex v of G_2, objects e, w, and a supergraph G_1 of G_2 extended by v, w and e between them. Suppose $w \notin$ the vertices of G_2. Then $\chi''(G_1) = 3$. The theorem is a consequence of (196), (174), and (189).

(203) Let us consider an edgeless graph G_2, objects v, e, a vertex w of G_2, and a supergraph G_1 of G_2 extended by v, w and e between them. Suppose $v \notin$ the vertices of G_2. Then $\chi''(G_1) = 3$. The theorem is a consequence of (196), (174), and (189).

(204) Let us consider an object v, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Then $\chi''(G_1) \subseteq (\chi''(G_2)+1)+\overline{\overline{V}}$. The theorem is a consequence of (186), (175), and (189).

(205) Let us consider a graph G_1, a loopless graph G_2, and a partial graph mapping F from G_1 to G_2. If F is weak subgraph embedding, then $\chi''(G_1) \subseteq \chi''(G_2)$. The theorem is a consequence of (186), (176), and (189).

(206) Let us consider a partial graph mapping F from G_1 to G_2. If F is isomorphism, then $\chi''(G_1) = \chi''(G_2)$. The theorem is a consequence of (186), (177), (189), and (190).

(207) Let us consider a G_1-isomorphic graph G_2. Then $\chi''(G_1) = \chi''(G_2)$. The theorem is a consequence of (206).

References

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

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

[3] Reinhard Diestel. *Graph theory*. Graduate Texts in Mathematics; 173. Springer, New York, 2nd edition, 2000. ISBN 0-387-98976-5; 0-387-98976-5.

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

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

Accepted July 23, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 2, Pages 125–134, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0010

sciendo
sciendo.com/journal/forma

Definition of Centroid Method as Defuzzification

Takashi Mitsuishi
Faculty of Business and Informatics
Nagano University, Japan

Summary. In this study, using the Mizar system [1], [2], we reuse formalization efforts in fuzzy sets described in [5] and [6]. This time the centroid method which is one of the fuzzy inference processes is formulated [10]. It is the most popular of all defuzzied methods ([11], [13], [7]) – here, defuzzified crisp value is obtained from domain of membership function as weighted average [8]. Since the integral is used in centroid method, the integrability and bounded properties of membership functions are also mentioned to fill the formalization gaps present in the Mizar Mathematical Library, as in the case of another fuzzy operators [4]. In this paper, the properties of piecewise linear functions consisting of two straight lines are mainly described.

MSC: 68V20 93C42

Keywords: defuzzification; centroid; piecewise linear function

MML identifier: FUZZY_6, version: 8.1.12 5.71.1431

From now on A denotes a non empty, closed interval subset of $\mathbb{R}$.

Let A be a non empty, closed interval subset of $\mathbb{R}$ and f be a function from $\mathbb{R}$ into $\mathbb{R}$. The functor centroid(f, A) yielding a real number is defined by the term

(Def. 1) $$\frac{\int\limits_{A} (\mathrm{id}_{\mathbb{R}} \cdot f)(x)dx}{\int\limits_{A} f(x)dx}.$$

Now we state the propositions:

(1) Let us consider real numbers a, b, c. Suppose $a < b$ and $c > 0$. Then centroid(AffineMap$(0, c), [a, b]) = \frac{a+b}{2}$.

Proof: Set $F = \frac{c}{2} \cdot (\square^2)$. For every element x of $\mathbb{R}$ such that $x \in \mathrm{dom}(F'_{\restriction \Omega_{\mathbb{R}}})$ holds $(F'_{\restriction \Omega_{\mathbb{R}}})(x) = (\mathrm{id}_{\mathbb{R}} \cdot (\mathrm{AffineMap}(0, c)))(x)$ by [12, (2)]. For every element x of $\mathbb{R}$ such that $x \in \mathrm{dom}((\mathrm{AffineMap}(c, 0))'_{\restriction \Omega_{\mathbb{R}}})$ holds $((\mathrm{AffineMap}(c, 0))'_{\restriction \Omega_{\mathbb{R}}})(x) = (\mathrm{AffineMap}(0, c))(x)$. $\square$

(2) Let us consider real numbers a, b. Then

(i) $\mathrm{id}_{\mathbb{R}}$ is integrable on $[a, b]$, and

(ii) $\mathrm{id}_{\mathbb{R}} \restriction [a, b]$ is bounded.

(3) (i) $\mathrm{id}_{\mathbb{R}}$ is integrable on A, and

(ii) $\mathrm{id}_{\mathbb{R}} \restriction A$ is bounded.

(4) Let us consider a real number e, and a partial function f from $\mathbb{R}$ to $\mathbb{R}$. Suppose $A \subseteq \mathrm{dom}\, f$ and for every real number x such that $x \in A$ holds $f(x) = e$. Then

(i) f is integrable on A, and

(ii) $f \restriction A$ is bounded, and

(iii) $\int\limits_{\inf A}^{\sup A} f(x) dx = e \cdot (\sup A - \inf A)$.

Let us consider a function f from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(5) If for every real number x such that $x \in A$ holds $f(x) = 0$, then $\int\limits_{A} f(x) dx = 0$. The theorem is a consequence of (4).

(6) Suppose f is integrable on A and $f \restriction A$ is bounded. Then

(i) $\mathrm{id}_{\mathbb{R}} \cdot f$ is integrable on A, and

(ii) $(\mathrm{id}_{\mathbb{R}} \cdot f) \restriction A$ is bounded.

The theorem is a consequence of (3).

(7) Let us consider real numbers a, b, c. Suppose $a < b$. Then

(i) $[a, b] \subseteq \Omega_{\mathbb{R}}$, and

(ii) $\inf [a, b] = a$, and

(iii) $\sup [a, b] = b$.

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

(8) Suppose $a < b \leqslant c$ and f is integrable on $[a, c]$ and $f \restriction [a, c]$ is bounded and for every real number x such that $x \in [b, c]$ holds $f(x) = 0$. Then $\mathrm{centroid}(f, [a, c]) = \mathrm{centroid}(f, [a, b])$. The theorem is a consequence of (3).

(9) Suppose $a \leqslant b < c$ and f is integrable on $[a,c]$ and $f{\restriction}[a,c]$ is bounded and for every real number x such that $x \in [a,b]$ holds $f(x) = 0$. Then $\text{centroid}(f,[a,c]) = \text{centroid}(f,[b,c])$. The theorem is a consequence of (3).

(10) Let us consider a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose f is integrable on A and $f{\restriction}A$ is bounded and $\int\limits_A f(x)dx > 0$. Then there exists a real number c such that

 (i) $c \in A$, and

 (ii) $f(c) > 0$.

PROOF: Set $g = (-1) \cdot f$. There exists a real number r such that for every set y such that $y \in \text{dom}(g{\restriction}A)$ holds $|(g{\restriction}A)(y)| < r$. For every real number x such that $x \in A$ holds $0 \leqslant (g{\restriction}A)(x)$. □

(11) Let us consider a real number r, a fuzzy set f of $\mathbb{R}$, and a function F from $\mathbb{R}$ into $\mathbb{R}$. Suppose $r > 0$ and f is integrable on A and $f{\restriction}A$ is bounded and for every real number x, $F(x) = \min(r, f(x))$. Then $\int\limits_A F(x)dx \geqslant 0$.

PROOF: There exists a real number r such that for every set y such that $y \in \text{dom}(F{\restriction}A)$ holds $|(F{\restriction}A)(y)| < r$. For every real number x such that $x \in A$ holds $0 \leqslant (F{\restriction}A)(x)$. □

Let us consider functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Now we state the propositions:

(12) $\min(f,g) = \frac{1}{2} \cdot (f + g - |f - g|)$.
PROOF: For every object x such that $x \in \text{dom}(\min(f,g))$ holds $(\min(f,g))(x) = (\frac{1}{2} \cdot (f + g - |f - g|))(x)$. □

(13) Suppose f is integrable on A and $f{\restriction}A$ is bounded and g is integrable on A and $g{\restriction}A$ is bounded. Then

 (i) $\min(f,g)$ is integrable on A, and

 (ii) $\min(f,g){\restriction}A$ is bounded, and

 (iii) $\int\limits_A (\min(f,g))(x)dx = \frac{1}{2} \cdot (\int\limits_A f(x)dx + \int\limits_A g(x)dx - \int\limits_A |f - g|(x)dx)$.

The theorem is a consequence of (12).

(14) $\max(f,g) = \frac{1}{2} \cdot (f + g + |f - g|)$.
PROOF: For every object x such that $x \in \text{dom}(\max(f,g))$ holds $(\max(f,g))(x) = (\frac{1}{2} \cdot (f + g + |f - g|))(x)$. □

(15) Suppose f is integrable on A and $f{\restriction}A$ is bounded and g is integrable on A and $g{\restriction}A$ is bounded. Then

 (i) $\max(f,g)$ is integrable on A, and

(ii) $\max(f, g){\restriction}A$ is bounded, and

(iii) $\int\limits_{A}(\max(f, g))(x)dx = \frac{1}{2} \cdot (\int\limits_{A} f(x)dx + \int\limits_{A} g(x)dx + \int\limits_{A} |f - g|(x)dx)$.

The theorem is a consequence of (14).

(16) Let us consider real numbers r_1, r_2, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose f is integrable on A and $f{\restriction}A$ is bounded. Then

(i) $\min(\mathrm{AffineMap}(0, r_1), r_2 \cdot f)$ is integrable on A, and

(ii) $\min(\mathrm{AffineMap}(0, r_1), r_2 \cdot f){\restriction}A$ is bounded.

The theorem is a consequence of (13).

(17) Let us consider real numbers r_1, r_2, and functions f, F from $\mathbb{R}$ into $\mathbb{R}$. Suppose f is integrable on A and $f{\restriction}A$ is bounded and for every real number x, $F(x) = \min(r_1, r_2 \cdot f(x))$. Then

(i) F is integrable on A, and

(ii) $F{\restriction}A$ is bounded.

The theorem is a consequence of (16).

(18) Let us consider a real number s, and functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Then $f{\restriction}]-\infty, s[+\cdot g{\restriction}[s, +\infty[$ is a function from $\mathbb{R}$ into $\mathbb{R}$.

Let us consider real numbers a, b, c and functions f, g, F from $\mathbb{R}$ into $\mathbb{R}$.

(19) If $a \leqslant b \leqslant c$ and $F = f{\restriction}[a, b]+\cdot g{\restriction}[b, c]$, then F is a function from $[a, c]$ into $\mathbb{R}$.

(20) If $a \leqslant b \leqslant c$ and $F = f{\restriction}[a, b]+\cdot g{\restriction}[b, c]$, then $F = F{\restriction}[a, c]$.

Let us consider real numbers a, b, c and functions f, g, h from $\mathbb{R}$ into $\mathbb{R}$.

(21) Suppose $a \leqslant b \leqslant c$ and $f{\restriction}[a, c]$ is bounded and $g{\restriction}[a, c]$ is bounded and $h = f{\restriction}[a, b]+\cdot g{\restriction}[b, c]$ and $f(b) = g(b)$. Then $h{\restriction}[a, c]$ is bounded.

PROOF: $f{\restriction}[a, b]$ tolerates $g{\restriction}[b, c]$. There exists a real number r such that for every set y such that $y \in \mathrm{dom}(h{\restriction}[a, c])$ holds $|(h{\restriction}[a, c])(y)| < r$. □

(22) Suppose $a \leqslant b \leqslant c$ and $f{\restriction}[a, c]$ is bounded and $g{\restriction}[a, c]$ is bounded and $h{\restriction}[a, c] = f{\restriction}[a, b]+\cdot g{\restriction}[b, c]$ and $f(b) = g(b)$. Then $h{\restriction}[a, c]$ is bounded.

PROOF: $f{\restriction}[a, b]$ tolerates $g{\restriction}[b, c]$. There exists a real number r such that for every set y such that $y \in \mathrm{dom}(h{\restriction}[a, c])$ holds $|(h{\restriction}[a, c])(y)| < r$. □

Now we state the propositions:

(23) Let us consider a real number c, and functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Suppose $f{\restriction}A$ is bounded and $g{\restriction}A$ is bounded. Then $(f{\restriction}]-\infty, c[+\cdot g{\restriction}[c, +\infty[){\restriction}A$ is bounded.

PROOF: Set $F = f{\restriction}]-\infty, c[+\cdot g{\restriction}[c, +\infty[$. There exists a real number r such that for every set y such that $y \in \mathrm{dom}(F{\restriction}A)$ holds $|(F{\restriction}A)(y)| < r$. □

(24) Let us consider real numbers a, b, c, and functions f, g, h, F from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a \leqslant b \leqslant c$ and f is continuous and g is continuous and $h \upharpoonright [a, c] = f \upharpoonright [a, b] +\cdot g \upharpoonright [b, c]$ and $f(b) = g(b)$ and $F = h \upharpoonright [a, c]$. Then F is continuous.

PROOF: For every real numbers x_0, r such that $x_0 \in [a, c]$ and $0 < r$ there exists a real number s such that $0 < s$ and for every real number x_1 such that $x_1 \in [a, c]$ and $|x_1 - x_0| < s$ holds $|h(x_1) - h(x_0)| < r$. $\square$

(25) Let us consider a non empty, closed interval subset A of $\mathbb{R}$, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose f is continuous. Then

(i) f is integrable on A, and

(ii) $f \upharpoonright A$ is bounded.

(26) Let us consider a real number c, and functions f, g, F from $\mathbb{R}$ into $\mathbb{R}$. Suppose f is Lipschitzian and g is Lipschitzian and $f(c) = g(c)$ and $F = f \upharpoonright]-\infty, c[+\cdot g \upharpoonright [c, +\infty[$. Then F is Lipschitzian.

PROOF: Consider r_3 being a real number such that $0 < r_3$ and for every real numbers x_1, x_2 such that $x_1, x_2 \in \operatorname{dom} f$ holds $|f(x_1) - f(x_2)| \leqslant r_3 \cdot |x_1 - x_2|$. Consider r_4 being a real number such that $0 < r_4$ and for every real numbers x_1, x_2 such that $x_1, x_2 \in \operatorname{dom} g$ holds $|g(x_1) - g(x_2)| \leqslant r_4 \cdot |x_1 - x_2|$. There exists a real number r such that $0 < r$ and for every real numbers x_1, x_2 such that x_1, $x_2 \in \operatorname{dom} F$ holds $|F(x_1) - F(x_2)| \leqslant r \cdot |x_1 - x_2|$. $\square$

(27) Let us consider real numbers a, b. Then $\operatorname{AffineMap}(a, b)$ is Lipschitzian.

PROOF: Set $f = \operatorname{AffineMap}(a, b)$. There exists a real number r such that $0 < r$ and for every real numbers x_1, x_2 such that x_1, $x_2 \in \operatorname{dom} f$ holds $|f(x_1) - f(x_2)| \leqslant r \cdot |x_1 - x_2|$. $\square$

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

(28) Suppose $a \neq p$ and $f = (\operatorname{AffineMap}(a, b)) \upharpoonright]-\infty, \frac{q-b}{a-p}[+\cdot (\operatorname{AffineMap}(p, q)) \upharpoonright [\frac{q-b}{a-p}, +\infty[$. Then f is Lipschitzian. The theorem is a consequence of (27) and (26).

(29) Suppose $a \neq p$ and $f = (\operatorname{AffineMap}(a, b)) \upharpoonright]-\infty, \frac{q-b}{a-p}[+\cdot (\operatorname{AffineMap}(p, q)) \upharpoonright [\frac{q-b}{a-p}, +\infty[$. Then

(i) f is integrable on A, and

(ii) $f \upharpoonright A$ is bounded.

The theorem is a consequence of (28).

(30) Let us consider real numbers a, b, p, q. Suppose $a \neq p$. Then $(\operatorname{AffineMap}(a, b))(\frac{q-b}{a-p}) = (\operatorname{AffineMap}(p, q))(\frac{q-b}{a-p})$.

(31) Every membership function of $\mathbb{R}$ is bounded.

PROOF: There exists a real number r such that for every set x such that $x \in \operatorname{dom} f$ holds $|f(x)| < r$ by [9, (1)]. $\square$

(32) Let us consider a real number r, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $r \neq 0$ and f is integrable on A and $f \restriction A$ is bounded. Then $\operatorname{centroid}(r \cdot f, A) = \operatorname{centroid}(f, A)$. The theorem is a consequence of (6).

Let us consider real numbers a, b, c and functions f, g, h from $\mathbb{R}$ into $\mathbb{R}$.

(33) Suppose $a \leqslant b \leqslant c$ and f is integrable on $[a, c]$ and $f \restriction [a, c]$ is bounded and g is integrable on $[a, c]$ and $g \restriction [a, c]$ is bounded and $h \restriction [a, c] = f \restriction [a, b] {+\cdot} g \restriction [b, c]$ and h is integrable on $[a, c]$ and $f(b) = g(b)$.
Then $\displaystyle\int\limits_{[a,c]} h(x)dx = \int\limits_{[a,b]} f(x)dx + \int\limits_{[b,c]} g(x)dx$.

PROOF: $f \restriction [a, b]$ tolerates $g \restriction [b, c]$. Reconsider $h_1 = h \restriction [a, b]$ as a partial function from $[a, b]$ to $\mathbb{R}$. Reconsider $f_1 = f \restriction [a, b]$ as a partial function from $[a, b]$ to $\mathbb{R}$. Reconsider $H = \text{upper\_sum\_set}\, h_1$ as a function from $\operatorname{divs}[a, b]$ into $\mathbb{R}$. Reconsider $F = \text{upper\_sum\_set}\, f_1$ as a function from $\operatorname{divs}[a, b]$ into $\mathbb{R}$. $H = F$.

Reconsider $h_2 = h \restriction [b, c]$ as a partial function from $[b, c]$ to $\mathbb{R}$. Reconsider $g_1 = g \restriction [b, c]$ as a partial function from $[b, c]$ to $\mathbb{R}$. Reconsider $H_1 = \text{upper\_sum\_set}\, h_2$ as a function from $\operatorname{divs}[b, c]$ into $\mathbb{R}$. Reconsider $G = \text{upper\_sum\_set}\, g_1$ as a function from $\operatorname{divs}[b, c]$ into $\mathbb{R}$. $H_1 = G$. $h \restriction [a, c]$ is bounded. $\square$

(34) Suppose $a \leqslant b \leqslant c$ and f is continuous and g is continuous and $h = f \restriction [a, b] {+\cdot} g \restriction [b, c]$ and $f(b) = g(b)$.
Then $\displaystyle\int\limits_{[a,c]} (\mathrm{id}_{\mathbb{R}} \cdot h)(x)dx = \int\limits_{[a,b]} (\mathrm{id}_{\mathbb{R}} \cdot f)(x)dx + \int\limits_{[b,c]} (\mathrm{id}_{\mathbb{R}} \cdot g)(x)dx$.

PROOF: $\mathrm{id}_{\mathbb{R}} \cdot f$ is integrable on $[a, c]$ and $(\mathrm{id}_{\mathbb{R}} \cdot f) \restriction [a, c]$ is bounded and $\mathrm{id}_{\mathbb{R}} \cdot g$ is integrable on $[a, c]$ and $(\mathrm{id}_{\mathbb{R}} \cdot g) \restriction [a, c]$ is bounded. Set $G = (\mathrm{id}_{\mathbb{R}} \cdot f) \restriction [a, b] {+\cdot} (\mathrm{id}_{\mathbb{R}} \cdot g) \restriction [b, c]$. For every object x such that $x \in \operatorname{dom} G$ holds $G(x) = (\mathrm{id}_{\mathbb{R}} \cdot h)(x)$. $\mathrm{id}_{\mathbb{R}} \cdot h$ is integrable on $[a, c]$. $\square$

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

(35) $f \restriction]-\infty, c[{+\cdot} g \restriction [c, +\infty[= f \restriction]-\infty, c] {+\cdot} g \restriction [c, +\infty[$.

PROOF: Set $f_1 = f \restriction]-\infty, c[{+\cdot} g \restriction [c, +\infty[$. Set $f_2 = f \restriction]-\infty, c] {+\cdot} g \restriction [c, +\infty[$. For every object x such that $x \in \operatorname{dom} f_1$ holds $f_1(x) = f_2(x)$. $\square$

(36) Suppose $f \restriction A$ is bounded and $g \restriction A$ is bounded.
Then $(f \restriction]-\infty, c] {+\cdot} g \restriction [c, +\infty[) \restriction A$ is bounded. The theorem is a consequence of (23) and (35).

(37) Let us consider real numbers a, b, c, and functions f, g from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a \leqslant c \leqslant b$. Then $f\restriction[a,c[+\cdot g\restriction[c,b] = f\restriction[a,c] +\cdot g\restriction[c,b]$.
PROOF: Set $f_1 = f\restriction[a,c[+\cdot g\restriction[c,b]$. Set $f_2 = f\restriction[a,c] +\cdot g\restriction[c,b]$. For every object x such that $x \in \operatorname{dom} f_1$ holds $f_1(x) = f_2(x)$. □

(38) Let us consider real numbers a, b, c, and functions f, g, h from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a \leqslant c$ and $h\restriction[a,c] = f\restriction[a,b] +\cdot g\restriction[b,c]$ and $f(b) = g(b)$. Then

(i) if $b \leqslant a$, then $h\restriction[a,c] = g\restriction[a,c]$, and

(ii) if $c \leqslant b$, then $h\restriction[a,c] = f\restriction[a,c]$.

PROOF: If $b \leqslant a$, then $h\restriction[a,c] = g\restriction[a,c]$. If $c \leqslant b$, then $h\restriction[a,c] = f\restriction[a,c]$. □

(39) Let us consider a real number b, and functions f, g, h from $\mathbb{R}$ into $\mathbb{R}$. Suppose $h = f\restriction]-\infty,b[+\cdot g\restriction[b,+\infty[$ and $f(b) = g(b)$. Then

(i) if $b \leqslant \inf A$, then $h\restriction A = g\restriction A$, and

(ii) if $\sup A \leqslant b$, then $h\restriction A = f\restriction A$.

PROOF: If $b \leqslant \inf A$, then $h\restriction A = g\restriction A$ by [3, (4)]. If $\sup A \leqslant b$, then $h\restriction A = f\restriction A$ by [3, (4)]. □

(40) Let us consider real numbers a, b, p, q, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $f = (\text{AffineMap}(a,b))\restriction]-\infty, \frac{q-b}{a-p}[+\cdot (\text{AffineMap}(p,q))\restriction[\frac{q-b}{a-p}, +\infty[$ and $\frac{q-b}{a-p} \in A$.
Then $f\restriction A = (\text{AffineMap}(a,b))\restriction[\inf A, \frac{q-b}{a-p}] +\cdot (\text{AffineMap}(p,q))\restriction[\frac{q-b}{a-p}, \sup A]$.
PROOF: Set $F = (\text{AffineMap}(a,b))\restriction[\inf A, \frac{q-b}{a-p}] +\cdot (\text{AffineMap}(p,q))\restriction[\frac{q-b}{a-p}, \sup A]$. For every object x such that $x \in \operatorname{dom} F$ holds $F(x) = (f\restriction A)(x)$. □

(41) Let us consider real numbers a, b. Then

(i) $(\text{AffineMap}(a,b))\restriction A$ is bounded, and

(ii) $\text{AffineMap}(a,b)$ is integrable on A.

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

(42) Suppose $a \neq p$ and $f = (\text{AffineMap}(a,b))\restriction]-\infty, \frac{q-b}{a-p}[+\cdot (\text{AffineMap}(p,q))\restriction[\frac{q-b}{a-p}, +\infty[$. Then

(i) if $\frac{q-b}{a-p} \in A$, then $\int\limits_A f(x)dx = \int\limits_{[\inf A, \frac{q-b}{a-p}]} (\text{AffineMap}(a,b))(x)dx + \int\limits_{[\frac{q-b}{a-p}, \sup A]} (\text{AffineMap}(p,q))(x)dx$, and

(ii) if $\frac{q-b}{a-p} \leqslant \inf A$, then $\int\limits_A f(x)dx = \int\limits_A (\mathrm{AffineMap}(p,q))(x)dx$, and

(iii) if $\frac{q-b}{a-p} \geqslant \sup A$, then $\int\limits_A f(x)dx = \int\limits_A (\mathrm{AffineMap}(a,b))(x)dx$.

PROOF: $(\mathrm{AffineMap}(a,b))(\frac{q-b}{a-p}) = (\mathrm{AffineMap}(p,q))(\frac{q-b}{a-p})$. AffineMap$(a,b)$ is integrable on $[\inf A, \sup A]$ and $(\mathrm{AffineMap}(a,b))\restriction[\inf A, \sup A]$ is bounded. AffineMap(p,q) is integrable on $[\inf A, \sup A]$. AffineMap$(p,q)\restriction[\inf A, \sup A]$ is bounded. f is integrable on $[\inf A, \sup A]$. If $\frac{q-b}{a-p} \in A$, then $\int\limits_A f(x)dx = \int\limits_{[\inf A, \frac{q-b}{a-p}]} (\mathrm{AffineMap}(a,b))(x)dx + \int\limits_{[\frac{q-b}{a-p}, \sup A]} (\mathrm{AffineMap}(p,q))(x)dx$. If $\frac{q-b}{a-p} \leqslant \inf A$, then $\int\limits_A f(x)dx = \int\limits_A (\mathrm{AffineMap}(p,q))(x)dx$. If $\frac{q-b}{a-p} \geqslant \sup A$, then $\int\limits_A f(x)dx = \int\limits_A (\mathrm{AffineMap}(a,b))(x)dx$. □

(43) Suppose $a \neq p$ and $f\restriction A = \mathrm{AffineMap}(a,b)\restriction[\inf A, \frac{q-b}{a-p}] +\cdot \mathrm{AffineMap}(p,q) \restriction[\frac{q-b}{a-p}, \sup A]$ and $\frac{q-b}{a-p} \in A$. Then $\int\limits_A (\mathrm{id}_{\mathbb{R}} \cdot f)(x)dx =$

$$\int\limits_{[\inf A, \frac{q-b}{a-p}]} (\mathrm{id}_{\mathbb{R}} \cdot (\mathrm{AffineMap}(a,b)))(x)dx + \int\limits_{[\frac{q-b}{a-p}, \sup A]} (\mathrm{id}_{\mathbb{R}} \cdot (\mathrm{AffineMap}(p,q)))(x)dx.$$

PROOF: $(\mathrm{id}_{\mathbb{R}} \cdot f)\restriction[\inf A, \sup A] = (\mathrm{id}_{\mathbb{R}} \cdot (\mathrm{AffineMap}(a,b)))\restriction[\inf A, \frac{q-b}{a-p}] +\cdot (\mathrm{id}_{\mathbb{R}} \cdot (\mathrm{AffineMap}(p,q)))\restriction[\frac{q-b}{a-p}, \sup A]$. Set $F = (\mathrm{AffineMap}(a,b))\restriction]-\infty, \frac{q-b}{a-p}[+\cdot \mathrm{AffineMap}(p,q)\restriction[\frac{q-b}{a-p}, +\infty[$. $F\restriction[\inf A, \sup A]$ is integrable. $F\restriction[\inf A, \sup A] = f\restriction A$. f is integrable on $[\inf A, \sup A]$ and $f\restriction[\inf A, \sup A]$ is bounded. $\mathrm{id}_{\mathbb{R}} \cdot f$ is integrable on $[\inf A, \sup A]$. □

(44) Let us consider real numbers a, b. Then $\mathrm{id}_{\mathbb{R}} \cdot \mathrm{AffineMap}(a,b) = a \cdot \square^2 + b \cdot \square^1$.

PROOF: For every object x such that $x \in \mathbb{R}$ holds $\mathrm{id}_{\mathbb{R}} \cdot \mathrm{AffineMap}(a,b)(x) = a \cdot (\square^2 + b \cdot \square^1)(x)$. □

(45) Let us consider real numbers a, b, c, d. Suppose $c \leqslant d$. Then $\int\limits_c^d (\mathrm{id}_{\mathbb{R}} \cdot (\mathrm{AffineMap}(a,b)))(x)dx = \frac{1}{3} \cdot a \cdot (d \cdot d \cdot d - c \cdot c \cdot c) + \frac{1}{2} \cdot b \cdot (d \cdot d - c \cdot c)$.

The theorem is a consequence of (44).

(46) Let us consider real numbers a, b. Then $\mathrm{AffineMap}(a,b) = a \cdot \square^1 + b \cdot \square^0$.
PROOF: For every object x such that $x \in \mathbb{R}$ holds $\mathrm{AffineMap}(a,b)(x) = (a \cdot \square^1 + b \cdot \square^0)(x)$. $\square$

(47) Let us consider real numbers a, b, c, d. Suppose $c \leqslant d$.
Then $\int\limits_c^d (\mathrm{AffineMap}(a,b))(x)dx = \frac{1}{2} \cdot a \cdot (d \cdot d - c \cdot c) + b \cdot (d - c)$. The theorem is a consequence of (46).

(48) Let us consider real numbers a, b, p, q, c, d, e, and a function f from $\mathbb{R}$ into $\mathbb{R}$. Suppose $a \neq p$ and $f \restriction A = \mathrm{AffineMap}(a,b) \restriction [\inf A, \frac{q-b}{a-p}] +\cdot\, \mathrm{AffineMap}(p,q) \restriction [\frac{q-b}{a-p}, \sup A]$ and $\frac{q-b}{a-p} \in A$. Then $\mathrm{centroid}(f,A) =$
$$\frac{\frac{1}{3}\cdot a\cdot((\frac{q-b}{a-p})^{\mathbf{3}}-(\inf A)^{\mathbf{3}})+\frac{1}{2}\cdot b\cdot((\frac{q-b}{a-p})^{\mathbf{2}}-(\inf A)^{\mathbf{2}})+\frac{1}{3}\cdot p\cdot((\sup A)^{\mathbf{3}}-(\frac{q-b}{a-p})^{\mathbf{3}})+\frac{1}{2}\cdot q\cdot((\sup A)^{\mathbf{2}}-(\frac{q-b}{a-p})^{\mathbf{2}})}{\frac{1}{2}\cdot a\cdot((\frac{q-b}{a-p})^{\mathbf{2}}-(\inf A)^{\mathbf{2}})+b\cdot(\frac{q-b}{a-p}-\inf A)+\frac{1}{2}\cdot p\cdot((\sup A)^{\mathbf{2}}-(\frac{q-b}{a-p})^{\mathbf{2}})+q\cdot(\sup A-\frac{q-b}{a-p})}.$$
The theorem is a consequence of (18), (40), (42), (43), (45), and (47).

(49) Let us consider a function f from $\mathbb{R}$ into $\mathbb{R}$.
Then $\max_+(f) = \max(\mathrm{AffineMap}(0,0), f)$.

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] Noboru Endou and Artur Korniłowicz. The definition of the Riemann definite integral and some related lemmas. *Formalized Mathematics*, 8(**1**):93–102, 1999.

[4] Adam Grabowski. Fuzzy implications in the Mizar system. In *30th IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 2021, Luxembourg, July 11–14, 2021*, pages 1–6. IEEE, 2021. doi:10.1109/FUZZ45933.2021.9494593.

[5] Adam Grabowski and Takashi Mitsuishi. *Extending Formal Fuzzy Sets with Triangular Norms and Conorms*, volume 642: *Advances in Intelligent Systems and Computing*, pages 176–187. Springer International Publishing, Cham, 2018. doi:10.1007/978-3-319-66824-6_16.

[6] Adam Grabowski and Takashi Mitsuishi. Initial comparison of formal approaches to fuzzy and rough sets. In Leszek Rutkowski, Marcin Korytkowski, Rafal Scherer, Ryszard Tadeusiewicz, Lotfi A. Zadeh, and Jacek M. Zurada, editors, *Artificial Intelligence and Soft Computing – 14th International Conference, ICAISC 2015, Zakopane, Poland, June 14-18, 2015, Proceedings, Part I*, volume 9119 of *Lecture Notes in Computer Science*, pages 160–171. Springer, 2015. doi:10.1007/978-3-319-19324-3_15.

[7] Tetsuro Katafuchi, Kiyoji Asai, and Hiroshi Fujita. Investigation of deffuzification in fuzzy inference: Proposal of a new defuzzification method (in Japanese). *Medical Imaging and Information Sciences*, 18(1):19–30, 2001. doi:10.11318/mii1984.18.19.

[8] Ebrahim H. Mamdani. Application of fuzzy algorithms for control of simple dynamic plant. *IEE Proceedings*, 121:1585–1588, 1974.

[9] Takashi Mitsuishi, Katsumi Wasaki, and Yasunari Shidama. Basic properties of fuzzy set operation and membership function. *Formalized Mathematics*, 9(**2**):357–362, 2001.

[10] Masaharu Mizumoto. Improvement of fuzzy control (IV)-case by product-sum-gravity method. In *Proc. 6th Fuzzy System Symposium, 1990*, pages 9–13, 1990.

[11] Timothy J. Ross. *Fuzzy Logic with Engineering Applications*. John Wiley and Sons Ltd, 2010.

[12] Yasunari Shidama. The Taylor expansions. *Formalized Mathematics*, 12(**2**):195–200, 2004.

[13] Werner Van Leekwijck and Etienne E. Kerre. Defuzzification: Criteria and classification. *Fuzzy Sets and Systems*, 108(2):159–178, 1999.

Accepted July 23, 2022

FORMALIZED MATHEMATICS
Vol. 30, No. 2, Pages 135–158, 2022
ISSN: 1426–2630, e-ISSN: 1898–9934
DOI: 10.2478/forma-2022-0011

sciendo
sciendo.com/journal/forma

Elementary Number Theory Problems. Part III

Artur Korniłowicz
Institute of Computer Science
University of Białystok
Poland

Summary. In this paper problems 11, 16, 19–24, 39, 44, 46, 74, 75, 77, 82, and 176 from [10] are formalized as described in [6], using the Mizar formalism [1], [2], [4]. Problems 11 and 16 from the book are formulated as several independent theorems. Problem 46 is formulated with a given example of required properties. Problem 77 is not formulated using triangles as in the book is.

MSC: 11A41 03B35 68V20

Keywords: number theory; divisibility; primes

MML identifier: `NUMBER03`, version: `8.1.12 5.71.1431`

1. Preliminaries

One can verify that every set which is natural is also natural-membered.

From now on a, b, i, k, m, n denote natural numbers, s, z denote non zero natural numbers, r denotes a real number, c denotes a complex number, and e_1, e_2, e_3, e_4, e_5 denote extended reals.

Now we state the propositions:

(1) If $e_1 \leqslant e_2 \leqslant e_3 \leqslant e_4$, then $e_1 \leqslant e_4$.

(2) If $e_1 \leqslant e_2 \leqslant e_3 \leqslant e_4 \leqslant e_5$, then $e_1 \leqslant e_5$. The theorem is a consequence of (1).

(3) $2^{10} + 1 = 1025$.

(4) $3^{10} + 1 = 5905 \cdot 10$.

(5) $4^{10} + 1 = 1048 \cdot 1000 + 577$.

(6) $5^{10} + 1 = 9765 \cdot 1000 + 626$.

(7) $6^{10} + 1 = 6046 \cdot 10000 + 6177$.

(8) $7^{10} + 1 = (2824 \cdot 10000 + 7525) \cdot 10$.

(9) $8^{10} + 1 = (1073 \cdot 100 + 74) \cdot 10000 + 1825$.

(10) $9^{10} + 1 = (3486 \cdot 100 + 78) \cdot 10000 + 4402$.

(11) $n \bmod (m+1) = 0$ or ... or $n \bmod (m+1) = m$.

(12) If $n \mid 8$, then $n \in \{1, 2, 4, 8\}$.

(13) If $0 < m$, then $\gcd(m, n) \leqslant m$.

(14) Let us consider integers i, j. If i and j are relatively prime, then $i \neq j$ or $i = j = 1$ or $i = j = -1$.

(15) Let us consider natural numbers i, j. If i and j are relatively prime, then $i \neq j$ or $i = j = 1$.

(16) If $a < n$ and $b < n$ and $n \mid a - b$, then $a = b$.

(17) Let us consider integers a, b, m. Suppose $a < b$. Then there exists k such that

 (i) $m < (b - a) \cdot k + 1 - a$, and

 (ii) $k = |\lceil \frac{m+a-1}{b-a} + 1 \rceil|$.

Let i be an integer. Let us observe that $(i^{\kappa})_{\kappa \in \mathbb{N}}$ is $\mathbb{Z}$-valued.

Let us consider n. Note that $(n^{\kappa})_{\kappa \in \mathbb{N}}$ is $\mathbb{N}$-valued.

Let f be a non-negative yielding, real-valued many sorted set indexed by $\mathbb{N}$. Let us observe that $(\sum_{\alpha=0}^{\kappa} f(\alpha))_{\kappa \in \mathbb{N}}$ is non-decreasing.

Now we state the propositions:

(18) Suppose $a \neq 0$ or $b \neq 0$. Then there exist natural numbers A, B such that

 (i) $a = (\gcd(a, b)) \cdot A$, and

 (ii) $b = (\gcd(a, b)) \cdot B$, and

 (iii) A and B are relatively prime.

(19) If $n \neq 0$, then for every integers p, m such that $p \mid m$ holds $p \mid ((m^{\kappa})_{\kappa \in \mathbb{N}})(n)$.

PROOF: Set $G = (m^{\kappa})_{\kappa \in \mathbb{N}}$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \neq 0$, then $p \mid G(\$_1)$. For every non zero natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every non zero natural number k, $\mathcal{P}[k]$. $\square$

(20) $((r^{\kappa})_{\kappa \in \mathbb{N}})(a + b) = ((r^{\kappa})_{\kappa \in \mathbb{N}})(a) \cdot (r^{b})$.

PROOF: Set $S = (r^{\kappa})_{\kappa \in \mathbb{N}}$. Define $\mathcal{P}$[natural number] $\equiv S(a + \$_1) = S(a) \cdot (r^{\$_1})$. $\mathcal{P}[0]$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every k, $\mathcal{P}[k]$. $\square$

(21) Let us consider integers p, m. Suppose $p \mid m$.
Then $p \mid ((\sum_{\alpha=0}^{\kappa}((m^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(n) - 1$.
PROOF: Set $G = (m^{\kappa})_{\kappa\in\mathbb{N}}$. Set $P = (\sum_{\alpha=0}^{\kappa} G(\alpha))_{\kappa\in\mathbb{N}}$. Define $\mathcal{P}$[natural number] $\equiv p \mid P(\$_1) - 1$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every k, $\mathcal{P}[k]$. □

(22) $((\sum_{\alpha=0}^{\kappa}((m^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(n)$ and m^{n+1} are relatively prime. The theorem is a consequence of (21).

(23) $\gcd(((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k), ((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k+i)) = \gcd(((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k), ((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k+i) - ((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k))$.

(24) $((\sum_{\alpha=0}^{\kappa}((r^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k+i+1) - ((\sum_{\alpha=0}^{\kappa}((r^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(k) = r^{k+1} \cdot ((\sum_{\alpha=0}^{\kappa}((r^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(i)$.
PROOF: Set $S = (r^{\kappa})_{\kappa\in\mathbb{N}}$. Set $P = (\sum_{\alpha=0}^{\kappa} S(\alpha))_{\kappa\in\mathbb{N}}$. Define $\mathcal{P}$[natural number] $\equiv P(k + \$_1 + 1) - P(k) = r^{k+1} \cdot P(\$_1)$. $\mathcal{P}[0]$. For every a such that $\mathcal{P}[a]$ holds $\mathcal{P}[a+1]$. For every k, $\mathcal{P}[k]$. □

(25) Suppose $n+1$ and $m+1$ are relatively prime.
Then $((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(n)$ and $((\sum_{\alpha=0}^{\kappa}((a^{\kappa})_{\kappa\in\mathbb{N}})(\alpha))_{\kappa\in\mathbb{N}})(m)$ are relatively prime. The theorem is a consequence of (14).

(26) If $a \neq 0$ and $b \neq 0$ and $i \neq 0$, then $\gcd(i^a - 1, i^b - 1) = i^{\gcd(a,b)} - 1$. The theorem is a consequence of (18) and (25).

Let us consider integers a, b, k. Now we state the propositions:

(27) Suppose $a+b > 0$ and $(a \bmod k)+(b \bmod k) > 0$. Then $(a+b)^n \bmod k = ((a \bmod k) + (b \bmod k))^n \bmod k$.
PROOF: Set $a_1 = a \bmod k$. Set $b_1 = b \bmod k$. Define $\mathcal{P}$[natural number] $\equiv (a+b)^{\$_1} \bmod k = (a_1 + b_1)^{\$_1} \bmod k$. $\mathcal{P}[0]$. For every natural number x such that $\mathcal{P}[x]$ holds $\mathcal{P}[x+1]$. For every natural number x, $\mathcal{P}[x]$. □

(28) $(a+b)^n \bmod k = ((a \bmod k) + (b \bmod k))^n \bmod k$.
PROOF: Set $a_1 = a \bmod k$. Set $b_1 = b \bmod k$. Define $\mathcal{P}$[natural number] $\equiv (a+b)^{\$_1} \bmod k = (a_1 + b_1)^{\$_1} \bmod k$. $\mathcal{P}[0]$. For every natural number x such that $\mathcal{P}[x]$ holds $\mathcal{P}[x+1]$. For every natural number x, $\mathcal{P}[x]$. □

(29) If $1 < m$, then $m \mid a^b + 1$ iff $m \mid (a \bmod m)^b + 1$.
PROOF: Set $r = a \bmod m$. If $m \mid a^b + 1$, then $m \mid r^b + 1$ by [8, (7)], (28). □

(30) $10 \mid a^{10} + 1$ if and only if there exist natural numbers r, k such that $a = 10 \cdot k + r$ and $10 \mid r^{10} + 1$ and $r = 0$ or ... or $r = 9$.
PROOF: If $10 \mid a^{10} + 1$, then there exist natural numbers r, k such that $a = 10 \cdot k + r$ and $10 \mid r^{10} + 1$ and $r = 0$ or ... or $r = 9$ by (29), [3, (8)]. □

(31) Let us consider odd natural numbers a, b. If $a - b = 2$, then a and b are relatively prime.

(32) Let us consider odd natural numbers a, b, c. If $c - b = 2$ and $b - a = 2$, then $3 \mid a$ or $3 \mid b$ or $3 \mid c$.

(33) Let us consider odd prime numbers a, b, c. If $c - b = 2$ and $b - a = 2$, then $a = 3$ and $b = 5$ and $c = 7$. The theorem is a consequence of (32).

(34) If a^n is prime, then $n = 1$.

(35) If $1 < a$, then there exists k such that $1 < k$ and $n < a^k$.

(36) (i) $2^n \bmod 3 = 1$, or

(ii) $2^n \bmod 3 = 2$.

Proof: Define $\mathcal{P}$[natural number] $\equiv 2^{\$_1} \bmod 3 = 1$ or $2^{\$_1} \bmod 3 = 2$. For every k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every k, $\mathcal{P}[k]$. □

(37) $3^m \mid 2^{3^m} + 1$.

Proof: Define $\mathcal{P}$[natural number] $\equiv 3^{\$_1} \mid 2^{3^{\$_1}} + 1$. $\mathcal{P}[0]$. For every m such that $\mathcal{P}[m]$ holds $\mathcal{P}[m+1]$ by [7, (2),(1)]. For every m, $\mathcal{P}[m]$. □

(38) $\mathrm{Euler}\,0 = 0$.

Let us note that Euler 0 is zero.

Let n be a positive natural number. One can check that Euler n is positive.

2. Main Problems

Now we state the propositions:

(39) $5 \mid 2^{2 \cdot n+1} - 2^{n+1} + 1$ if and only if $n \bmod 4 = 1$ or $n \bmod 4 = 2$.

Proof: Define $\mathcal{F}$(natural number) $= 2^{2 \cdot \$_1 + 1} - 2^{\$_1 + 1} + 1$. Consider k such that $n = 4 \cdot k$ or $n = 4 \cdot k + 1$ or $n = 4 \cdot k + 2$ or $n = 4 \cdot k + 3$. If $5 \mid \mathcal{F}(n)$, then $n \bmod 4 = 1$ or $n \bmod 4 = 2$. □

(40) $5 \mid 2^{2 \cdot n+1} + 2^{n+1} + 1$ if and only if $n \bmod 4 = 0$ or $n \bmod 4 = 3$.

Proof: Define $\mathcal{G}$(natural number) $= 2^{2 \cdot \$_1 + 1} + 2^{\$_1 + 1} + 1$. Consider k such that $n = 4 \cdot k$ or $n = 4 \cdot k + 1$ or $n = 4 \cdot k + 2$ or $n = 4 \cdot k + 3$. If $5 \mid \mathcal{G}(n)$, then $n \bmod 4 = 0$ or $n \bmod 4 = 3$. □

(41) $5 \mid 2^{2 \cdot n+1} - 2^{n+1} + 1$ if and only if $5 \nmid 2^{2 \cdot n+1} + 2^{n+1} + 1$. The theorem is a consequence of (11), (39), and (40).

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

Proof: Set $S = \{n$, where n is a natural number $: n \mid 2^n + 1\}$. Define $\mathcal{F}$(natural number) $= 3^{\$_1}$. Consider f being a many sorted set indexed by $\mathbb{N}$ such that for every element i of $\mathbb{N}$, $f(i) = \mathcal{F}(i)$. Set $R = \operatorname{rng} f$. $R \subseteq S$. For every natural number m, there exists a natural number N such that $N \geqslant m$ and $N \in R$ by [9, (1)]. □

(43) $\{n$, where n is a natural number : $n \mid 2^n + 1$ and n is prime$\} = \{3\}$.
PROOF: Set $S = \{n$, where n is a natural number : $n \mid 2^n + 1$ and n is prime$\}$. $S \subseteq \{3\}$. $3^1 \mid 2^{3^1} + 1$. $\square$

(44) $10 \mid a^{10} + 1$ if and only if there exists k such that $a = 10 \cdot k + 3$ or $a = 10 \cdot k + 7$.
PROOF: If $10 \mid a^{10} + 1$, then there exists k such that $a = 10 \cdot k + 3$ or $a = 10 \cdot k + 7$. $\square$

(45) If ($a \neq 0$ or $b \neq 0$) and $n > 0$ and $a \mid b^n - 1$, then a and b are relatively prime.

(46) There exists no natural number n such that $1 < n$ and $n \mid 2^n - 1$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv 1 < \$_1$ and $\$_1 \mid 2^{\$_1} - 1$. Consider N being a natural number such that $\mathcal{P}[N]$ and for every natural number n such that $\mathcal{P}[n]$ holds $N \leqslant n$. Set $E = \operatorname{Euler} N$. Set $d = \gcd(N, E)$. 2 and N are relatively prime. $\gcd(2^N - 1, 2^E - 1) = 2^d - 1$. $d \leqslant E$. $\square$

(47) $\{n$, where n is an odd natural number : $n \mid 3^n + 1\} = \{1\}$.
PROOF: Set $A = \{n$, where n is an odd natural number : $n \mid 3^n + 1\}$. $A \subseteq \{1\}$. $\square$

(48) $\{n$, where n is a positive natural number : $3 \mid n\cdot(2^n)+1\}$ = the set of all $6\cdot k+1$ where k is a natural number$\cup$the set of all $6\cdot k+2$ where k is a natural number.
PROOF: Set $A = \{n$, where n is a positive natural number : $3 \mid n\cdot(2^n)+1\}$. Set B = the set of all $6 \cdot k + 1$ where k is a natural number. Set C = the set of all $6 \cdot k+2$ where k is a natural number. $A \subseteq B \cup C$ by [5, (26)]. $\square$

Let us consider an odd prime number p. Now we state the propositions:

(49) If $n = (p-1) \cdot (k \cdot p + 1)$, then $2^n \bmod p = 1$.

(50) If $n = (p-1) \cdot (k \cdot p + 1)$, then $p \mid$ the Cullen number of n. The theorem is a consequence of (49).

(51) $\{n$, where n is a natural number : $p \mid$ the Cullen number of $n\}$ is infinite.
PROOF: Set $S = \{n$, where n is a natural number : $p \mid$ the Cullen number of $n\}$. Define $\mathcal{F}$(natural number) $= (p-1) \cdot (\$_1 \cdot p + 1)$. Consider f being a many sorted set indexed by $\mathbb{N}$ such that for every element i of $\mathbb{N}$, $f(i) = \mathcal{F}(i)$. Set $R = \operatorname{rng} f$. $R \subseteq S$. For every natural number m, there exists a natural number N such that $N \geqslant m$ and $N \in R$. $\square$

(52) There exist natural numbers x, y such that

(i) $x > n$, and

(ii) $x \nmid y$, and

(iii) $x^x \mid y^y$.

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

(53) Let us consider integers a, b, c, n. Suppose $3 < n$. Then there exists an integer k such that

(i) $n \nmid k + a$, and

(ii) $n \nmid k + b$, and

(iii) $n \nmid k + c$.

(54) Let us consider integers a, b. Suppose $a \neq b$. Then $\{n$, where n is a natural number : $a + n$ and $b + n$ are relatively prime$\}$ is infinite.

Let a, b, c be integers. We say that a, b, c are mutually coprime if and only if

(Def. 1) a and b are relatively prime and a and c are relatively prime and b and c are relatively prime.

Let d be an integer. We say that a, b, c, d are mutually coprime if and only if

(Def. 2) a and b are relatively prime and a and c are relatively prime and a and d are relatively prime and b and c are relatively prime and b and d are relatively prime and c and d are relatively prime.

Now we state the propositions:

(55) Let us consider prime numbers a, b, c. If a, b, c are mutually different, then a, b, c are mutually coprime.

(56) Let us consider prime numbers a, b, c, d. If a, b, c, d are mutually different, then a, b, c, d are mutually coprime.

(57) (i) 1, 2, 3, 4 are mutually different, and

(ii) there exists no positive natural number n such that $1+n$, $2+n$, $3+n$, $4+n$ are mutually coprime.

(58) Let us consider an even natural number n. Suppose $n > 6$. Then there exist prime numbers p, q such that

(i) $n - p$ and $n - q$ are relatively prime, and

(ii) $p = 3$, and

(iii) $q = 5$.

The theorem is a consequence of (31).

(59) $\{p$, where p is a prime number : there exist prime numbers a, b such that $p = a + b$ and there exist prime numbers c, d such that $p = c - d\} = \{5\}$.
Proof: Set $A = \{p$, where p is a prime number : there exist prime numbers a, b such that $p = a + b$ and there exist prime numbers c, d such that $p = c - d\}$. $A \subseteq \{5\}$. $\square$

Let us consider a prime number p. Now we state the propositions:

(60) A corollary from the Fermat Theorem:
If $p = 4 \cdot k + 1$, then there exist positive natural numbers a, b such that $a > b$ and $p = a^{\mathbf{2}} + b^{\mathbf{2}}$.

(61) If $p = 4 \cdot k + 1$, then there exist positive natural numbers a, b such that $p^{\mathbf{2}} = a^{\mathbf{2}} + b^{\mathbf{2}}$. The theorem is a consequence of (60).

(62) (i) $5 \mid n + 1$, or
(ii) $5 \mid n + 7$, or
(iii) $5 \mid n + 9$, or
(iv) $5 \mid n + 13$, or
(v) $5 \mid n + 15$.

(63) $\{n$, where n is a natural number : $n+1$ is prime and $n+3$ is prime and $n+7$ is prime and $n+9$ is prime and $n+13$ is prime and $n+15$ is prime$\} = \{4\}$.
Proof: Set $A = \{n$, where n is a natural number : $n+1$ is prime and $n+3$ is prime and $n+7$ is prime and $n+9$ is prime and $n+13$ is prime and $n+15$ is prime$\}$. $A \subseteq \{4\}$. $\square$

(64) $r^3 + (r+1)^3 + (r+2)^3 = (r+3)^3$ if and only if $r = 3$.
Proof: If $r^3 + (r+1)^3 + (r+2)^3 = (r+3)^3$, then $r = 3$. $\square$

3. Tools for Computing Prime Numbers

In the sequel p denotes a prime number. Now we state the propositions:

(65) If $p < 3$, then $p = 2$.

(66) If $k < 9$ and $p \cdot p \leqslant k$, then $p = 2$. The theorem is a consequence of (65).

(67) If $p < 5$, then $p = 2$ or $p = 3$. The theorem is a consequence of (65).

(68) If $k < 25$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$. The theorem is a consequence of (67).

(69) If $p < 7$, then $p = 2$ or $p = 3$ or $p = 5$. The theorem is a consequence of (67).

(70) If $k < 49$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$. The theorem is a consequence of (69).

(71) If $p < 11$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$. The theorem is a consequence of (69).

(72) If $k < 121$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$. The theorem is a consequence of (71).

(73) If $p < 13$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$. The theorem is a consequence of (71).

(74) If $k < 169$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$. The theorem is a consequence of (73).

(75) If $p < 17$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$. The theorem is a consequence of (73).

(76) If $k < 289$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$. The theorem is a consequence of (75).

(77) If $p < 19$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$. The theorem is a consequence of (75).

(78) If $k < 361$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$. The theorem is a consequence of (77).

(79) If $p < 23$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$. The theorem is a consequence of (77).

(80) If $k < 529$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$. The theorem is a consequence of (79).

(81) If $p < 29$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$. The theorem is a consequence of (79).

(82) If $k < 841$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$. The theorem is a consequence of (81).

(83) If $p < 31$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$. The theorem is a consequence of (81).

(84) If $k < 961$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$. The theorem is a consequence of (83).

(85) If $p < 37$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$. The theorem is a consequence of (83).

(86) If $k < 1369$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$. The theorem is a consequence of (85).

(87) If $p < 41$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$. The theorem is a consequence of (85).

(88) If $k < 1681$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$. The theorem is a consequence of (87).

(89) If $p < 43$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or

$p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$ or $p = 41$. The theorem is a consequence of (87).

(90) If $k < 1849$ and $p \cdot p \leqslant k$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$ or $p = 41$. The theorem is a consequence of (89).

(91) If $p < 47$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$ or $p = 41$ or $p = 43$. The theorem is a consequence of (89).

(92) Suppose $k < 2209$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$.

The theorem is a consequence of (91).

(93) If $p < 53$, then $p = 2$ or $p = 3$ or $p = 5$ or $p = 7$ or $p = 11$ or $p = 13$ or $p = 17$ or $p = 19$ or $p = 23$ or $p = 29$ or $p = 31$ or $p = 37$ or $p = 41$ or $p = 43$ or $p = 47$. The theorem is a consequence of (91).

(94) Suppose $k < 2809$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$.

The theorem is a consequence of (93).

(95) Suppose $p < 59$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$.

The theorem is a consequence of (93).

(96) Suppose $k < 3481$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$.

The theorem is a consequence of (95).

(97) Suppose $p < 61$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$.

The theorem is a consequence of (95).

(98) Suppose $k < 3721$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or
(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or
(x) $p = 29$, or
(xi) $p = 31$, or
(xii) $p = 37$, or
(xiii) $p = 41$, or
(xiv) $p = 43$, or
(xv) $p = 47$, or
(xvi) $p = 53$, or
(xvii) $p = 59$.

The theorem is a consequence of (97).

(99) Suppose $p < 67$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or
(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or
(x) $p = 29$, or
(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$.

The theorem is a consequence of (97).

(100) Suppose $k < 4489$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$.

The theorem is a consequence of (99).

(101) Suppose $p < 71$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or
(x) $p = 29$, or
(xi) $p = 31$, or
(xii) $p = 37$, or
(xiii) $p = 41$, or
(xiv) $p = 43$, or
(xv) $p = 47$, or
(xvi) $p = 53$, or
(xvii) $p = 59$, or
(xviii) $p = 61$, or
(xix) $p = 67$.

The theorem is a consequence of (99).

(102) Suppose $k < 5041$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or
(ii) $p = 3$, or
(iii) $p = 5$, or
(iv) $p = 7$, or
(v) $p = 11$, or
(vi) $p = 13$, or
(vii) $p = 17$, or
(viii) $p = 19$, or
(ix) $p = 23$, or
(x) $p = 29$, or
(xi) $p = 31$, or
(xii) $p = 37$, or
(xiii) $p = 41$, or
(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$.

The theorem is a consequence of (101).

(103) Suppose $p < 73$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$.

The theorem is a consequence of (101).

(104) Suppose $k < 5329$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$.

The theorem is a consequence of (103).

(105) Suppose $p < 79$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$.

The theorem is a consequence of (103).

(106) Suppose $k < 6241$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$.

The theorem is a consequence of (105).

(107) Suppose $p < 83$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$.

The theorem is a consequence of (105).

(108) Suppose $k < 6889$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$.

The theorem is a consequence of (107).

(109) Suppose $p < 89$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$, or

(xxiii) $p = 83$.

The theorem is a consequence of (107).

(110) Suppose $k < 7921$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$, or

(xxiii) $p = 83$.

The theorem is a consequence of (109).

(111) Suppose $p < 97$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$, or

(xxiii) $p = 83$, or

(xxiv) $p = 89$.

The theorem is a consequence of (109).

(112) Suppose $k < 9409$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$, or

(xxiii) $p = 83$, or

(xxiv) $p = 89$.

The theorem is a consequence of (111).

(113) Suppose $p < 101$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$, or

(xxiii) $p = 83$, or

(xxiv) $p = 89$, or

(xxv) $p = 97$.

The theorem is a consequence of (111).

(114) Suppose $k < 10201$ and $p \cdot p \leqslant k$. Then

(i) $p = 2$, or

(ii) $p = 3$, or

(iii) $p = 5$, or

(iv) $p = 7$, or

(v) $p = 11$, or

(vi) $p = 13$, or

(vii) $p = 17$, or

(viii) $p = 19$, or

(ix) $p = 23$, or

(x) $p = 29$, or

(xi) $p = 31$, or

(xii) $p = 37$, or

(xiii) $p = 41$, or

(xiv) $p = 43$, or

(xv) $p = 47$, or

(xvi) $p = 53$, or

(xvii) $p = 59$, or

(xviii) $p = 61$, or

(xix) $p = 67$, or

(xx) $p = 71$, or

(xxi) $p = 73$, or

(xxii) $p = 79$, or

(xxiii) $p = 83$, or

(xxiv) $p = 89$, or

(xxv) $p = 97$.

The theorem is a consequence of (113).

References

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

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

[3] Adam Grabowski. Polygonal numbers. *Formalized Mathematics*, 21(**2**):103–113, 2013. doi:10.2478/forma-2013-0012.

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

[5] Artur Korniłowicz and Dariusz Surowik. Elementary number theory problems. Part II. *Formalized Mathematics*, 29(**1**):63–68, 2021. doi:10.2478/forma-2021-0006.

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

[7] Marco Riccardi. Solution of cubic and quartic equations. *Formalized Mathematics*, 17(**2**):117–122, 2009. doi:10.2478/v10037-009-0012-z.

[8] Christoph Schwarzweller. Modular integer arithmetic. *Formalized Mathematics*, 16(**3**):247–252, 2008. doi:10.2478/v10037-008-0029-8.

[9] Christoph Schwarzweller. Proth numbers. *Formalized Mathematics*, 22(**2**):111–118, 2014. doi:10.2478/forma-2014-0013.

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

Accepted July 23, 2022