Fundamental Theorem of Algebra¹

Robert Milewski University of Białystok

MML Identifier: POLYNOM5.

The papers [18], [22], [19], [4], [16], [5], [12], [1], [3], [26], [24], [6], [7], [25], [13], [2], [20], [15], [14], [21], [9], [29], [27], [8], [10], [23], [28], [11], and [17] provide the terminology and notation for this paper.

1. Preliminaries

The following propositions are true:

- (1) For all natural numbers n, m such that $n \neq 0$ and $m \neq 0$ holds $(n \cdot m n m) + 1 \ge 0$.
- (2) For all real numbers x, y such that y > 0 holds $\frac{\min(x,y)}{\max(x,y)} \leq 1$.
- (3) For all real numbers x, y such that for every real number c such that c > 0 and c < 1 holds $c \cdot x \ge y$ holds $y \le 0$.
- (4) Let p be a finite sequence of elements of \mathbb{R} . Suppose that for every natural number n such that $n \in \text{dom } p$ holds $p(n) \ge 0$. Let i be a natural number. If $i \in \text{dom } p$, then $\sum p \ge p(i)$.
- (5) For all real numbers x, y holds $-(x + yi_{\mathbb{C}_{\mathrm{F}}}) = -x + (-y)i_{\mathbb{C}_{\mathrm{F}}}.$
- (6) For all real numbers x_1, y_1, x_2, y_2 holds $(x_1 + y_1 i_{\mathbb{C}_F}) (x_2 + y_2 i_{\mathbb{C}_F}) = (x_1 x_2) + (y_1 y_2) i_{\mathbb{C}_F}.$
- (7) Let L be a commutative associative left unital distributive field-like non empty double loop structure and f, g, h be elements of the carrier of L. If $h \neq 0_L$, then if $h \cdot g = h \cdot f$ or $g \cdot h = f \cdot h$, then g = f.

C 2001 University of Białystok ISSN 1426-2630

¹This work has been partially supported by TYPES grant IST-1999-29001.

In this article we present several logical schemes. The scheme ExDHGrStrSeq deals with a non empty groupoid \mathcal{A} and a unary functor \mathcal{F} yielding an element of the carrier of \mathcal{A} , and states that:

There exists a sequence S of A such that for every natural number n holds $S(n) = \mathcal{F}(n)$

for all values of the parameters.

The scheme ExDdoubleLoopStrSeq deals with a non empty double loop structure \mathcal{A} and a unary functor \mathcal{F} yielding an element of the carrier of \mathcal{A} , and states that:

There exists a sequence S of A such that for every natural number n holds $S(n) = \mathcal{F}(n)$

for all values of the parameters.

Next we state the proposition

(8) For every element z of the carrier of \mathbb{C}_{F} such that $z \neq 0_{\mathbb{C}_{\mathrm{F}}}$ and for every natural number n holds $|\mathrm{power}_{\mathbb{C}_{\mathrm{F}}}(z, n)| = |z|^n$.

Let p be a finite sequence of elements of the carrier of \mathbb{C}_{F} . The functor |p| yields a finite sequence of elements of \mathbb{R} and is defined by:

(Def. 1) $\operatorname{len} |p| = \operatorname{len} p$ and for every natural number n such that $n \in \operatorname{dom} p$ holds $|p|_n = |p_n|$.

We now state several propositions:

- (9) $|\varepsilon_{\text{(the carrier of } \mathbb{C}_{\mathrm{F}})}| = \varepsilon_{\mathbb{R}}.$
- (10) For every element x of the carrier of \mathbb{C}_{F} holds $|\langle x \rangle| = \langle |x| \rangle$.
- (11) For all elements x, y of the carrier of \mathbb{C}_{F} holds $|\langle x, y \rangle| = \langle |x|, |y| \rangle$.
- (12) For all elements x, y, z of the carrier of \mathbb{C}_{F} holds $|\langle x, y, z \rangle| = \langle |x|, |y|, |z| \rangle$.
- (13) For all finite sequences p, q of elements of the carrier of \mathbb{C}_{F} holds $|p^{\uparrow}q| = |p|^{\uparrow} |q|$.
- (14) Let p be a finite sequence of elements of the carrier of \mathbb{C}_{F} and x be an element of the carrier of \mathbb{C}_{F} . Then $|p \cap \langle x \rangle| = |p| \cap \langle |x| \rangle$ and $|\langle x \rangle \cap p| = \langle |x| \rangle \cap |p|$.
- (15) For every finite sequence p of elements of the carrier of \mathbb{C}_{F} holds $|\sum p| \leq \sum |p|$.

2. Operations on Polynomials

Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure, let p be a Polynomial of L, and let n be a natural number. The functor p^n yields a sequence of L and is defined by: (Def. 2) $p^n = \text{power}_{\text{Polynom-Ring }L}(p, n).$

Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure, let p be a Polynomial of L, and let n be a natural number. One can verify that p^n is finite-Support.

One can prove the following propositions:

- (16) Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure and p be a Polynomial of L. Then $p^0 = \mathbf{1}$. L.
- (17) Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure and p be a Polynomial of L. Then $p^1 = p$.
- (18) Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure and p be a Polynomial of L. Then $p^2 = p * p$.
- (19) Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure and p be a Polynomial of L. Then $p^3 = p * p * p$.
- (20) Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure, p be a Polynomial of L, and n be a natural number. Then $p^{n+1} = p^n * p$.
- (21) Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure and n be a natural number. Then $(\mathbf{0}, L)^{n+1} = \mathbf{0}, L$.
- (22) Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure and n be a natural number. Then $(\mathbf{1}, L)^n = \mathbf{1}, L$.
- (23) Let L be a field, p be a Polynomial of L, x be an element of the carrier of L, and n be a natural number. Then $eval(p^n, x) = power_L(eval(p, x), n)$.
- (24) Let L be a field and p be a Polynomial of L. If len $p \neq 0$, then for every natural number n holds len $(p^n) = (n \cdot \text{len } p n) + 1$.

Let L be a non empty groupoid, let p be a sequence of L, and let v be an element of the carrier of L. The functor $v \cdot p$ yields a sequence of L and is defined by:

(Def. 3) For every natural number n holds $(v \cdot p)(n) = v \cdot p(n)$.

Let L be an add-associative right zeroed right complementable right distributive non empty double loop structure, let p be a Polynomial of L, and let v be an element of the carrier of L. Observe that $v \cdot p$ is finite-Support.

We now state several propositions:

- (25) Let L be an add-associative right zeroed right complementable distributive non empty double loop structure and p be a Polynomial of L. Then $len(0_L \cdot p) = 0.$
- (26) Let L be an add-associative right zeroed right complementable left unital commutative associative distributive field-like non empty double loop structure, p be a Polynomial of L, and v be an element of the carrier of L. If $v \neq 0_L$, then $\operatorname{len}(v \cdot p) = \operatorname{len} p$.
- (27) Let L be an add-associative right zeroed right complementable left distributive non empty double loop structure and p be a sequence of L. Then $0_L \cdot p = \mathbf{0}. L.$
- (28) For every left unital non empty multiplicative loop structure L and for every sequence p of L holds $\mathbf{1}_L \cdot p = p$.
- (29) Let L be an add-associative right zeroed right complementable right distributive non empty double loop structure and v be an element of the carrier of L. Then $v \cdot \mathbf{0}$. $L = \mathbf{0}$. L.
- (30) Let L be an add-associative right zeroed right complementable right unital right distributive non empty double loop structure and v be an element of the carrier of L. Then $v \cdot \mathbf{1}$. $L = \langle v \rangle$.
- (31) Let L be an add-associative right zeroed right complementable left unital distributive commutative associative field-like non empty double loop structure, p be a Polynomial of L, and v, x be elements of the carrier of L. Then $eval(v \cdot p, x) = v \cdot eval(p, x)$.
- (32) Let L be an add-associative right zeroed right complementable right distributive unital non empty double loop structure and p be a Polynomial of L. Then $eval(p, 0_L) = p(0)$.

Let L be a non empty zero structure and let z_0 , z_1 be elements of the carrier of L. The functor $\langle z_0, z_1 \rangle$ yields a sequence of L and is defined by:

(Def. 4) $\langle z_0, z_1 \rangle = \mathbf{0}. L + (0, z_0) + (1, z_1).$

The following propositions are true:

- (33) Let L be a non empty zero structure and z_0 be an element of the carrier of L. Then $\langle z_0 \rangle(0) = z_0$ and for every natural number n such that $n \ge 1$ holds $\langle z_0 \rangle(n) = 0_L$.
- (34) For every non empty zero structure L and for every element z_0 of the carrier of L such that $z_0 \neq 0_L$ holds $\ln \langle z_0 \rangle = 1$.
- (35) For every non empty zero structure L holds $\langle 0_L \rangle = 0. L$.
- (36) Let L be an add-associative right zeroed right complementable distributive commutative associative left unital field-like non empty double loop structure and x, y be elements of the carrier of L. Then $\langle x \rangle * \langle y \rangle = \langle x \cdot y \rangle$.
- (37) Let L be an Abelian add-associative right zeroed right complementable right unital associative commutative distributive field-like non empty do-

464

uble loop structure, x be an element of the carrier of L, and n be a natural number. Then $\langle x \rangle^n = \langle \text{power}_L(x, n) \rangle$.

- (38) Let L be an add-associative right zeroed right complementable unital non empty double loop structure and z_0 , x be elements of the carrier of L. Then $eval(\langle z_0 \rangle, x) = z_0$.
- (39) Let L be a non empty zero structure and z_0, z_1 be elements of the carrier of L. Then $\langle z_0, z_1 \rangle(0) = z_0$ and $\langle z_0, z_1 \rangle(1) = z_1$ and for every natural number n such that $n \ge 2$ holds $\langle z_0, z_1 \rangle(n) = 0_L$.

Let L be a non empty zero structure and let z_0 , z_1 be elements of the carrier of L. One can verify that $\langle z_0, z_1 \rangle$ is finite-Support.

The following propositions are true:

- (40) For every non empty zero structure L and for all elements z_0 , z_1 of the carrier of L holds $\operatorname{len}\langle z_0, z_1 \rangle \leq 2$.
- (41) For every non empty zero structure L and for all elements z_0 , z_1 of the carrier of L such that $z_1 \neq 0_L$ holds $\operatorname{len}\langle z_0, z_1 \rangle = 2$.
- (42) For every non empty zero structure L and for every element z_0 of the carrier of L such that $z_0 \neq 0_L$ holds $\operatorname{len}\langle z_0, 0_L \rangle = 1$.
- (43) For every non empty zero structure L holds $\langle 0_L, 0_L \rangle = 0. L$.
- (44) For every non empty zero structure L and for every element z_0 of the carrier of L holds $\langle z_0, 0_L \rangle = \langle z_0 \rangle$.
- (45) Let L be an add-associative right zeroed right complementable left distributive unital non empty double loop structure and z_0, z_1, x be elements of the carrier of L. Then $eval(\langle z_0, z_1 \rangle, x) = z_0 + z_1 \cdot x$.
- (46) Let L be an add-associative right zeroed right complementable left distributive unital non empty double loop structure and z_0, z_1, x be elements of the carrier of L. Then $eval(\langle z_0, 0_L \rangle, x) = z_0$.
- (47) Let L be an add-associative right zeroed right complementable left distributive unital non empty double loop structure and z_0, z_1, x be elements of the carrier of L. Then $eval(\langle 0_L, z_1 \rangle, x) = z_1 \cdot x$.
- (48) Let L be an add-associative right zeroed right complementable left distributive well unital non empty double loop structure and z_0 , z_1 , x be elements of the carrier of L. Then $eval(\langle z_0, \mathbf{1}_L \rangle, x) = z_0 + x$.
- (49) Let L be an add-associative right zeroed right complementable left distributive well unital non empty double loop structure and z_0 , z_1 , x be elements of the carrier of L. Then $eval(\langle 0_L, \mathbf{1}_L \rangle, x) = x$.

3. Substitution in Polynomials

Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure and let p, qbe Polynomials of L. The functor p[q] yielding a Polynomial of L is defined by the condition (Def. 5).

(Def. 5) There exists a finite sequence F of elements of the carrier of Polynom-Ring L such that $p[q] = \sum F$ and len F = len p and for every natural number n such that $n \in \text{dom } F$ holds $F(n) = p(n - 1) \cdot q^{n-1}$.

One can prove the following propositions:

- (50) Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure and p be a Polynomial of L. Then $(\mathbf{0}, L)[p] = \mathbf{0}, L$.
- (51) Let L be an Abelian add-associative right zeroed right complementable right unital commutative distributive non empty double loop structure and p be a Polynomial of L. Then $p[\mathbf{0}, L] = \langle p(0) \rangle$.
- (52) Let L be an Abelian add-associative right zeroed right complementable right unital associative commutative distributive field-like non empty double loop structure, p be a Polynomial of L, and x be an element of the carrier of L. Then $\operatorname{len}(p[\langle x \rangle]) \leq 1$.
- (53) For every field L and for all Polynomials p, q of L such that $\ln p \neq 0$ and $\ln q > 1$ holds $\ln(p[q]) = (\ln p \cdot \ln q - \ln p - \ln q) + 2$.
- (54) Let L be a field, p, q be Polynomials of L, and x be an element of the carrier of L. Then eval(p[q], x) = eval(p, eval(q, x)).

4. Fundamental Theorem of Algebra

Let L be a unital non empty double loop structure, let p be a Polynomial of L, and let x be an element of the carrier of L. We say that x is a root of p if and only if:

(Def. 6) $eval(p, x) = 0_L.$

Let L be a unital non empty double loop structure and let p be a Polynomial of L. We say that p has roots if and only if:

- (Def. 7) There exists an element x of the carrier of L such that x is a root of p. The following proposition is true
 - (55) For every unital non empty double loop structure L holds **0**. L has roots.

Let L be a unital non empty double loop structure. One can verify that **0**. L has roots.

The following proposition is true

(56) Let L be a unital non empty double loop structure and x be an element of the carrier of L. Then x is a root of $\mathbf{0}$. L.

Let L be a unital non empty double loop structure. One can verify that there exists a Polynomial of L which has roots.

Let L be a unital non empty double loop structure. We say that L is algebraic-closed if and only if:

(Def. 8) For every Polynomial p of L such that len p > 1 holds p has roots.

Let L be a unital non empty double loop structure and let p be a Polynomial of L. The functor Roots p yields a subset of L and is defined by:

(Def. 9) For every element x of the carrier of L holds $x \in \text{Roots } p$ iff x is a root of p.

Let L be a commutative associative left unital distributive field-like non empty double loop structure and let p be a Polynomial of L. The functor NormPolynomial p yielding a sequence of L is defined as follows:

(Def. 10) For every natural number n holds $(\text{NormPolynomial } p)(n) = \frac{p(n)}{p(\ln p - '1)}$. Let L be an add-associative right zeroed right complementable commutative associative left unital distributive field-like non empty double loop structure and let p be a Polynomial of L. Note that NormPolynomial p is finite-Support.

The following propositions are true:

- (57) Let *L* be a commutative associative left unital distributive field-like non empty double loop structure and *p* be a Polynomial of *L*. If len $p \neq 0$, then (NormPolynomial *p*)(len $p 1 = \mathbf{1}_L$.
- (58) For every field L and for every Polynomial p of L such that $len p \neq 0$ holds len NormPolynomial p = len p.
- (59) Let *L* be a field and *p* be a Polynomial of *L*. Suppose len $p \neq 0$. Let x be an element of the carrier of *L*. Then eval(NormPolynomial p, x) = $\frac{\operatorname{eval}(p,x)}{p(\operatorname{len} p '1)}$.
- (60) Let L be a field and p be a Polynomial of L. Suppose $\text{len } p \neq 0$. Let x be an element of the carrier of L. Then x is a root of p if and only if x is a root of NormPolynomial p.
- (61) For every field L and for every Polynomial p of L such that $\text{len } p \neq 0$ holds p has roots iff NormPolynomial p has roots.
- (62) For every field L and for every Polynomial p of L such that $len p \neq 0$ holds Roots p = Roots NormPolynomial p.
- (63) $\operatorname{id}_{\mathbb{C}}$ is continuous on \mathbb{C} .
- (64) For every element x of \mathbb{C} holds $\mathbb{C} \mapsto x$ is continuous on \mathbb{C} .

Let L be a unital non empty groupoid, let x be an element of the carrier of L, and let n be a natural number. The functor FPower(x, n) yields a map from L into L and is defined as follows:

(Def. 11) For every element y of the carrier of L holds $(\text{FPower}(x, n))(y) = x \cdot \text{power}_L(y, n)$.

The following propositions are true:

- (65) For every unital non empty groupoid L holds $FPower(1_L, 1) = id_{the \ carrier \ of \ L}$.
- (66) FPower $(\mathbf{1}_{\mathbb{C}_{\mathrm{F}}}, 2) = \mathrm{id}_{\mathbb{C}} \mathrm{id}_{\mathbb{C}}.$
- (67) For every unital non empty groupoid L and for every element x of the carrier of L holds FPower $(x, 0) = (\text{the carrier of } L) \longmapsto x.$
- (68) For every element x of the carrier of \mathbb{C}_{F} there exists an element x_1 of \mathbb{C} such that $x = x_1$ and $\mathrm{FPower}(x, 1) = x_1 \operatorname{id}_{\mathbb{C}}$.
- (69) For every element x of the carrier of \mathbb{C}_{F} there exists an element x_1 of \mathbb{C} such that $x = x_1$ and $\mathrm{FPower}(x, 2) = x_1 (\mathrm{id}_{\mathbb{C}} \mathrm{id}_{\mathbb{C}}).$
- (70) Let x be an element of the carrier of \mathbb{C}_{F} and n be a natural number. Then there exists a function f from \mathbb{C} into \mathbb{C} such that $f = \mathrm{FPower}(x, n)$ and $\mathrm{FPower}(x, n+1) = f \operatorname{id}_{\mathbb{C}}$.
- (71) Let x be an element of the carrier of \mathbb{C}_{F} and n be a natural number. Then there exists a function f from \mathbb{C} into \mathbb{C} such that $f = \mathrm{FPower}(x, n)$ and f is continuous on \mathbb{C} .

Let L be a unital non empty double loop structure and let p be a Polynomial of L. The functor Polynomial-Function(L, p) yields a map from L into L and is defined as follows:

(Def. 12) For every element x of the carrier of L holds

(Polynomial-Function(L, p))(x) = eval(p, x).

The following propositions are true:

- (72) For every Polynomial p of \mathbb{C}_{F} there exists a function f from \mathbb{C} into \mathbb{C} such that $f = \operatorname{Polynomial-Function}(\mathbb{C}_{\mathrm{F}}, p)$ and f is continuous on \mathbb{C} .
- (73) Let p be a Polynomial of \mathbb{C}_{F} . Suppose len p > 2 and $|p(\operatorname{len} p '1)| = 1$. Let F be a finite sequence of elements of \mathbb{R} . Suppose len $F = \operatorname{len} p$ and for every natural number n such that $n \in \operatorname{dom} F$ holds F(n) = |p(n - '1)|. Let z be an element of the carrier of \mathbb{C}_{F} . If $|z| > \sum F$, then $|\operatorname{eval}(p, z)| > |p(0)| + 1$.
- (74) Let p be a Polynomial of \mathbb{C}_{F} . Suppose len p > 2. Then there exists an element z_0 of the carrier of \mathbb{C}_{F} such that for every element z of the carrier of \mathbb{C}_{F} holds $|\operatorname{eval}(p, z)| \ge |\operatorname{eval}(p, z_0)|$.
- (75) For every Polynomial p of \mathbb{C}_{F} such that $\operatorname{len} p > 1$ holds p has roots.

Let us note that \mathbb{C}_{F} is algebraic-closed.

Let us mention that there exists a left unital right unital non empty double loop structure which is algebraic-closed, add-associative, right zeroed, right complementable, Abelian, commutative, associative, distributive, field-like, and non degenerated.

References

- Agnieszka Banachowicz and Anna Winnicka. Complex sequences. Formalized Mathematics, 4(1):121–124, 1993.
- [2] Grzegorz Bancerek. The fundamental properties of natural numbers. Formalized Mathematics, 1(1):41-46, 1990.
- [3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. Formalized Mathematics, 1(1):107–114, 1990.
- [4] Czesław Byliński. Binary operations. Formalized Mathematics, 1(1):175–180, 1990.
- [5] Czesław Byliński. The complex numbers. Formalized Mathematics, 1(3):507–513, 1990.
- [6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [7] Czesław Byliński. Functions from a set to a set. Formalized Mathematics, 1(1):153–164, 1990.
- [8] Czesław Byliński. The sum and product of finite sequences of real numbers. Formalized Mathematics, 1(4):661–668, 1990.
- [9] Krzysztof Hryniewiecki. Basic properties of real numbers. Formalized Mathematics, 1(1):35–40, 1990.
- [10] Jarosław Kotowicz. Real sequences and basic operations on them. Formalized Mathematics, 1(2):269–272, 1990.
- [11] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(2):335–342, 1990.
- [12] Anna Justyna Milewska. The field of complex numbers. Formalized Mathematics, 9(2):265–269, 2001.
- [13] Anna Justyna Milewska. The Hahn Banach theorem in the vector space over the field of complex numbers. Formalized Mathematics, 9(2):363–371, 2001.
- [14] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(2):391–395, 2001.
- [15] Robert Milewski. The ring of polynomials. Formalized Mathematics, 9(2):339–346, 2001.
- [16] Takashi Mitsuishi, Katsumi Wasaki, and Yasunari Shidama. Property of complex sequence and continuity of complex function. *Formalized Mathematics*, 9(1):185–190, 2001.
- [17] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. Formalized Mathematics, 2(1):3–11, 1991.
- [18] Michał Muzalewski and Lesław W. Szczerba. Construction of finite sequences over ring and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(1):97–104, 1991.
- [19] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. Formalized Mathematics, 4(1):83–86, 1993.
- [20] Jan Popiołek. Real normed space. Formalized Mathematics, 2(1):111–115, 1991.
- [21] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. Formalized Mathematics, 2(2):213–216, 1991.
- [22] Wojciech Skaba and Michał Muzalewski. From double loops to fields. Formalized Mathematics, 2(1):185–191, 1991.
- [23] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. Formalized Mathematics, 1(3):445–449, 1990.
- [24] Wojciech A. Trybulec. Binary operations on finite sequences. Formalized Mathematics, 1(5):979–981, 1990.
- [25] Wojciech A. Trybulec. Groups. Formalized Mathematics, 1(5):821-827, 1990.
- [26] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(3):575–579, 1990.
- [27] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(2):291–296, 1990.
- [28] Zinaida Trybulec. Properties of subsets. Formalized Mathematics, 1(1):67–71, 1990.

[29] Edmund Woronowicz. Relations defined on sets. Formalized Mathematics, 1(1):181–186, 1990.

Received August 21, 2000

470