

Algebraic Numbers

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

Summary. This article provides definitions and examples upon an integral element of unital commutative rings. An algebraic number is also treated as consequence of a concept of “integral”. Definitions for an integral closure, an algebraic integer and a transcendental numbers [14], [1], [10] and [7] are included as well. As an application of an algebraic number, this article includes a formal proof of a ring extension of rational number field \mathbb{Q} induced by substitution of an algebraic number to the polynomial ring of $\mathbb{Q}[x]$ turns to be a field.

MSC: 11R04 13B21 03B35

Keywords: algebraic number; integral dependency

MML identifier: ALGNM.1, version: 8.1.05 5.39.1282

1. PRELIMINARIES

From now on i, j denote natural numbers and A, B denote rings.

Now we state the propositions:

- (1) Let us consider rings L_1, L_2, L_3 . Suppose L_1 is a subring of L_2 and L_2 is a subring of L_3 . Then L_1 is a subring of L_3 .
- (2) $\mathbb{F}_{\mathbb{Q}}$ is a subfield of $\mathbb{C}_{\mathbb{F}}$.
- (3) $\mathbb{F}_{\mathbb{Q}}$ is a subring of $\mathbb{C}_{\mathbb{F}}$.
- (4) $\mathbb{Z}^{\mathbb{R}}$ is a subring of $\mathbb{C}_{\mathbb{F}}$.

Let us consider elements x, y of B and elements x_1, y_1 of A . Now we state the propositions:

- (5) If A is a subring of B and $x = x_1$ and $y = y_1$, then $x + y = x_1 + y_1$.
- (6) If A is a subring of B and $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.

Let c be a complex. Observe that $c(\in \mathbb{C}_{\mathbb{F}})$ reduces to c .

2. EXTENDED EVALUATION FUNCTION

Let A, B be rings, p be a polynomial over A , and x be an element of B . The functor $\text{ExtEval}(p, x)$ yielding an element of B is defined by

- (Def. 1) there exists a finite sequence F of elements of B such that $it = \sum F$ and $\text{len } F = \text{len } p$ and for every element n of \mathbb{N} such that $n \in \text{dom } F$ holds $F(n) = p(n -' 1)(\in B) \cdot \text{power}_B(x, n -' 1)$.

Now we state the proposition:

- (7) Let us consider an element n of \mathbb{N} , rings A, B , and an element z of A . Suppose A is a subring of B . Then $\text{power}_B(z(\in B), n) = \text{power}_A(z, n)(\in B)$. The theorem is a consequence of (6).

Let us consider elements x_1, x_2 of A . Now we state the propositions:

- (8) If A is a subring of B , then $x_1(\in B) + x_2(\in B) = (x_1 + x_2)(\in B)$. The theorem is a consequence of (5).
 (9) If A is a subring of B , then $x_1(\in B) \cdot x_2(\in B) = (x_1 \cdot x_2)(\in B)$. The theorem is a consequence of (6).
 (10) Let us consider a finite sequence F of elements of A , and a finite sequence G of elements of B . If A is a subring of B and $F = G$, then $(\sum F)(\in B) = \sum G$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence F of elements of A for every finite sequence G of elements of B such that $\text{len } F = \text{\$}_1$ and $F = G$ holds $(\sum F)(\in B) = \sum G$. $\mathcal{P}[0]$ by [13, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$ by [4, (4)], [5, (3)], [4, (59)], [3, (11)]. For every natural number n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

- (11) Let us consider a natural number n , an element x of A , and a polynomial p over A . Suppose A is a subring of B . Then $p(n -' 1)(\in B) \cdot \text{power}_B(x(\in B), n -' 1) = (p(n -' 1) \cdot \text{power}_A(x, n -' 1))(\in B)$. The theorem is a consequence of (9) and (7).
 (12) Let us consider an element x of A , and a polynomial p over A . Suppose A is a subring of B . Then $\text{ExtEval}(p, x(\in B)) = (\text{eval}(p, x))(\in B)$.

PROOF: Consider F_1 being a finite sequence of elements of B such that $\text{ExtEval}(p, x(\in B)) = \sum F_1$ and $\text{len } F_1 = \text{len } p$ and for every element n of \mathbb{N} such that $n \in \text{dom } F_1$ holds $F_1(n) = p(n -' 1)(\in B) \cdot \text{power}_B(x(\in B), n -' 1)$. Consider F_2 being a finite sequence of elements of A such that $\text{eval}(p, x) = \sum F_2$ and $\text{len } F_2 = \text{len } p$ and for every element n of \mathbb{N} such that $n \in \text{dom } F_2$ holds $F_2(n) = p(n -' 1) \cdot \text{power}_A(x, n -' 1)$. $F_1 = F_2$ by [12, (29)], [5, (3)], (19). \square

- (13) Let us consider an element x of B . Then $\text{ExtEval}(\mathbf{0}, A, x) = 0_B$.

- (14) Let us consider non degenerated rings A, B , and an element x of B . If A is a subring of B , then $\text{ExtEval}(\mathbf{1}, A, x) = 1_B$.
- (15) Let us consider an element x of B , and polynomials p, q over A . Suppose A is a subring of B . Then $\text{ExtEval}(p+q, x) = \text{ExtEval}(p, x) + \text{ExtEval}(q, x)$. The theorem is a consequence of (8).
- (16) Let us consider polynomials p, q over A . Suppose A is a subring of B and $\text{len } p > 0$ and $\text{len } q > 0$. Let us consider an element x of B . Then $\text{ExtEval}(\text{Leading-Monomial } p * \text{Leading-Monomial } q, x) = (p(\text{len } p - 1) \cdot q(\text{len } q - 1))(\in B) \cdot \text{power}_B(x, \text{len } p + \text{len } q - 2)$. The theorem is a consequence of (13).
- (17) Let us consider a polynomial p over A , and an element x of B . Suppose A is a subring of B . Then $\text{ExtEval}(\text{Leading-Monomial } p, x) = p(\text{len } p - 1)(\in B) \cdot \text{power}_B(x, \text{len } p - 1)$. The theorem is a consequence of (13).

Let us consider a commutative ring B , polynomials p, q over A , and an element x of B . Now we state the propositions:

- (18) Suppose A is a subring of B . Then $\text{ExtEval}(\text{Leading-Monomial } p * \text{Leading-Monomial } q, x) = \text{ExtEval}(\text{Leading-Monomial } p, x) \cdot \text{ExtEval}(\text{Leading-Monomial } q, x)$. The theorem is a consequence of (16), (9), (17), and (13).
- (19) Suppose A is a subring of B . Then $\text{ExtEval}(\text{Leading-Monomial } p * q, x) = \text{ExtEval}(\text{Leading-Monomial } p, x) \cdot \text{ExtEval}(q, x)$.
 PROOF: Set $p = \text{Leading-Monomial } p_1$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every polynomial q over A such that $\text{len } q = \mathbb{S}_1$ holds $\text{ExtEval}(p * q, x) = \text{ExtEval}(p, x) \cdot \text{ExtEval}(q, x)$. For every natural number k such that for every natural number n such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$ by [9, (16)], [8, (31)], (15), (18). For every natural number n , $\mathcal{P}[n]$ from [3, Sch. 4]. \square
- (20) If A is a subring of B , then $\text{ExtEval}(p * q, x) = \text{ExtEval}(p, x) \cdot \text{ExtEval}(q, x)$.
 PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every polynomial p over A such that $\text{len } p = \mathbb{S}_1$ holds $\text{ExtEval}(p * q, x) = \text{ExtEval}(p, x) \cdot \text{ExtEval}(q, x)$. For every natural number k such that for every natural number n such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$ by [9, (16)], [8, (32)], (15), (19). For every natural number n , $\mathcal{P}[n]$ from [3, Sch. 4]. \square
- (21) Let us consider an element x of B , and an element z_0 of A . Suppose A is a subring of B . Then $\text{ExtEval}(\langle z_0 \rangle, x) = z_0(\in B)$. The theorem is a consequence of (13).
- (22) Let us consider an element x of B , and elements z_0, z_1 of A . Suppose A is a subring of B . Then $\text{ExtEval}(\langle z_0, z_1 \rangle, x) = z_0(\in B) + z_1(\in B) \cdot x$. The theorem is a consequence of (13).

3. INTEGRAL ELEMENT AND ALGEBRAIC NUMBERS

Let A, B be rings and x be an element of B . We say that x is integral over A if and only if

- (Def. 2) there exists a polynomial f over A such that $LC f = 1_A$ and $\text{ExtEval}(f, x) = 0_B$.

Now we state the proposition:

- (23) Let us consider a non degenerated ring A , and an element a of A . If A is a subring of B , then $a(\in B)$ is integral over A . The theorem is a consequence of (12).

Let A be a non degenerated ring and B be a ring. Assume A is a subring of B . The integral closure over A in B yielding a non empty subset of B is defined by the term

- (Def. 3) $\{z, \text{ where } z \text{ is an element of } B : z \text{ is integral over } A\}$.

Let c be a complex. We say that c is algebraic if and only if

- (Def. 4) there exists an element x of \mathbb{C}_F such that $x = c$ and x is integral over \mathbb{F}_Q .

Let x be an element of \mathbb{C}_F . Note that x is algebraic if and only if the condition (Def. 5) is satisfied.

- (Def. 5) x is integral over \mathbb{F}_Q .

Let c be a complex. We say that c is algebraic integer if and only if

- (Def. 6) there exists an element x of \mathbb{C}_F such that $x = c$ and x is integral over \mathbb{Z}^R .

Let x be an element of \mathbb{C}_F . Observe that x is algebraic integer if and only if the condition (Def. 7) is satisfied.

- (Def. 7) x is integral over \mathbb{Z}^R .

Let x be a complex. We introduce the notation x is transcendental as an antonym for x is algebraic.

Note that every complex which is rational is also algebraic and there exists a complex which is algebraic and there exists an element of \mathbb{C}_F which is algebraic and every complex which is integer is also algebraic integer and there exists a complex which is algebraic integer and there exists an element of \mathbb{C}_F which is algebraic integer.

Let A, B be rings and x be an element of B . The functor $\text{AnnPoly}(x, A)$ yielding a non empty subset of $\text{PolyRing}(A)$ is defined by the term

- (Def. 8) $\{p, \text{ where } p \text{ is a polynomial over } A : \text{ExtEval}(p, x) = 0_B\}$.

Now we state the propositions:

- (24) Let us consider rings A, B , an element w of B , and elements x, y of $\text{PolyRing}(A)$. Suppose A is a subring of B and $x, y \in \text{AnnPoly}(w, A)$. Then $x + y \in \text{AnnPoly}(w, A)$. The theorem is a consequence of (15).
- (25) Let us consider a commutative ring B , an element z of B , and elements p, x of $\text{PolyRing}(A)$. Suppose A is a subring of B and $x \in \text{AnnPoly}(z, A)$. Then $p \cdot x \in \text{AnnPoly}(z, A)$. The theorem is a consequence of (20).
- (26) Let us consider a commutative ring B , an element w of B , and elements p, x of $\text{PolyRing}(A)$. Suppose A is a subring of B and $x \in \text{AnnPoly}(w, A)$. Then $x \cdot p \in \text{AnnPoly}(w, A)$. The theorem is a consequence of (20).
- (27) Let us consider a non degenerated ring A , a non degenerated commutative ring B , and an element w of B . Suppose A is a subring of B . Then $\text{AnnPoly}(w, A)$ is a proper ideal of $\text{PolyRing}(A)$.
 PROOF: $\text{AnnPoly}(w, A)$ is closed under addition. $\text{AnnPoly}(w, A)$ is left ideal. $\text{AnnPoly}(w, A)$ is right ideal. $\text{AnnPoly}(w, A)$ is proper by [8, (37)], (14). \square

4. PROPERTIES OF POLYNOMIAL RING OVER PRINCIPAL IDEAL DOMAIN

From now on K, L denote fields.

Now we state the propositions:

- (28) Let us consider fields K, L , and an element w of L . Suppose K is a subring of L . Then there exists an element g of $\text{PolyRing}(K)$ such that $\{g\}$ -ideal = $\text{AnnPoly}(w, K)$. The theorem is a consequence of (27).
- (29) Let us consider fields K, L , and an element z of L . Suppose z is integral over K . Then $\text{AnnPoly}(z, K) \neq \{0_{\text{PolyRing}(K)}\}$.
 PROOF: Consider f being a polynomial over K such that $\text{LC} f = 1_K$ and $\text{ExtEval}(f, z) = 0_L$. $f \notin \{0_{\text{PolyRing}(K)}\}$ by [2, (47), (64)], [11, (7)]. \square
- (30) Let us consider a field K , and an element p of $\text{PolyRing}(K)$. Suppose $p \neq \mathbf{0}_K$. Then p is a non zero element of the carrier of $\text{PolyRing}(K)$.

Let us consider fields K, L and an element w of L . Now we state the propositions:

- (31) If K is a subring of L , then $\text{AnnPoly}(w, K)$ is quasi-prime. The theorem is a consequence of (20).
- (32) If K is a subring of L and w is integral over K , then $\text{AnnPoly}(w, K)$ is prime. The theorem is a consequence of (31) and (27).
- (33) Let us consider fields K, L , and an element z of L . Suppose K is a subring of L and z is integral over K . Then there exists an element f of $\text{PolyRing}(K)$ such that

- (i) $f \neq \mathbf{0}.K$, and
- (ii) $\{f\}$ -ideal = $\text{AnnPoly}(z, K)$, and
- (iii) $f = \text{NormPoly } f$.

The theorem is a consequence of (28), (29), and (30).

- (34) Let us consider fields K, L , an element z of L , and elements f, g of $\text{PolyRing}(K)$. Suppose z is integral over K and $\{f\}$ -ideal = $\text{AnnPoly}(z, K)$ and $f = \text{NormPoly } f$ and $\{g\}$ -ideal = $\text{AnnPoly}(z, K)$ and $g = \text{NormPoly } g$. Then $f = g$. The theorem is a consequence of (29) and (30).

Let K, L be fields and z be an element of L . Assume K is a subring of L and z is integral over K . The minimal polynomial of z over K yielding an element of the carrier of $\text{PolyRing}(K)$ is defined by

- (Def. 9) $it \neq \mathbf{0}.K$ and $\{it\}$ -ideal = $\text{AnnPoly}(z, K)$ and $it = \text{NormPoly } it$.

Assume K is a subring of L and z is integral over K . The degree of algebraic number z over K yielding an element of \mathbb{N} is defined by the term

- (Def. 10) $\text{deg}(\text{the minimal polynomial of } z \text{ over } K)$.

Let A, B be rings and x be an element of B . The functor $\text{HomExtEval}(x, A)$ yielding a function from $\text{PolyRing}(A)$ into B is defined by

- (Def. 11) for every polynomial p over A , $it(p) = \text{ExtEval}(p, x)$.

Let x be an element of \mathbb{C}_F . Note that $\text{HomExtEval}(x, \mathbb{F}_Q)$ is unity-preserving, additive, and multiplicative.

Now we state the propositions:

- (35) Let us consider an element x of \mathbb{C}_F .

Then \mathbb{C}_F is $(\text{PolyRing}(\mathbb{F}_Q))$ -homomorphic.

- (36) Let us consider an element x of B , and an object z .

If $z \in \text{rng HomExtEval}(x, A)$, then $z \in B$.

Let x be an element of \mathbb{C}_F . The functor $\text{FQ}(x)$ yielding a subset of \mathbb{C}_F is defined by the term

- (Def. 12) $\text{rng HomExtEval}(x, \mathbb{F}_Q)$.

Let us note that $\text{FQ}(x)$ is non empty.

Let us consider elements x, z_1, z_2 of \mathbb{C}_F . Now we state the propositions:

- (37) If $z_1, z_2 \in \text{FQ}(x)$, then $z_1 + z_2 \in \text{FQ}(x)$. The theorem is a consequence of (3) and (15).

- (38) If $z_1, z_2 \in \text{FQ}(x)$, then $z_1 \cdot z_2 \in \text{FQ}(x)$. The theorem is a consequence of (3) and (20).

- (39) Let us consider an element x of \mathbb{C}_F , and an element a of \mathbb{F}_Q . Then $a \in \text{FQ}(x)$. The theorem is a consequence of (3) and (21).

Let x be an element of \mathbb{C}_F . The functor $\text{FQ-add}(x)$ yielding a binary operation on $\text{FQ}(x)$ is defined by the term

(Def. 13) $+_{\mathbb{C}} \upharpoonright \text{FQ}(x)$.

The functor $\text{FQ-mult}(x)$ yielding a binary operation on $\text{FQ}(x)$ is defined by the term

(Def. 14) $\cdot_{\mathbb{C}} \upharpoonright \text{FQ}(x)$.

Let us consider an element x of \mathbb{C}_F and elements z, w of $\text{FQ}(x)$. Now we state the propositions:

(40) $(\text{FQ-add}(x))(z, w) = z + w$.

(41) $(\text{FQ-mult}(x))(z, w) = z \cdot w$.

(42) Let us consider an element x of \mathbb{C}_F . Then $1_{\mathbb{C}_F}(\in \text{FQ}(x)) = 1_{\mathbb{C}_F}$. The theorem is a consequence of (3) and (39).

(43) $(-1_{\mathbb{F}_Q})(\in \mathbb{C}_F) = -1_{\mathbb{C}_F}$. The theorem is a consequence of (3).

Let x be an element of \mathbb{C}_F . The functor $\mathbb{Q}[x]$ yielding a strict, non empty double loop structure is defined by the term

(Def. 15) $\langle \text{FQ}(x), \text{FQ-add}(x), \text{FQ-mult}(x), 1_{\mathbb{C}_F}(\in \text{FQ}(x)), 0_{\mathbb{C}_F}(\in \text{FQ}(x)) \rangle$.

Now we state the proposition:

(44) Let us consider an element x of \mathbb{C}_F . Then $\mathbb{Q}[x]$ is a ring.

PROOF: Reconsider $Z = \langle \text{FQ}(x), \text{FQ-add}(x), \text{FQ-mult}(x), 1_{\mathbb{C}_F}(\in \text{FQ}(x)), 0_{\mathbb{C}_F}(\in \text{FQ}(x)) \rangle$ as a non empty double loop structure. For every elements v, w of Z , $v + w = w + v$. For every elements u, v, w of Z , $(u + v) + w = u + (v + w)$. For every element v of Z , $v + 0_Z = v$. Every element of Z is right complementable by (36), [6, (9)], (39), (43). For every elements a, b, v of Z , $(a + b) \cdot v = a \cdot v + b \cdot v$. For every elements a, v, w of Z , $a \cdot (v + w) = a \cdot v + a \cdot w$ and $(v + w) \cdot a = v \cdot a + w \cdot a$. For every elements a, b, v of Z , $(a \cdot b) \cdot v = a \cdot (b \cdot v)$. For every element v of Z , $v \cdot 1_Z = v$ and $1_Z \cdot v = v$. \square

Let x be an element of \mathbb{C}_F . One can verify that $\mathbb{Q}[x]$ is Abelian, add-associative, right zeroed, right complementable, associative, well unital, and distributive.

Let z be an element of \mathbb{C}_F . One can verify that $\mathbb{Q}[z]$ is integral domain-like, commutative, and non degenerated.

Now we state the proposition:

(45) Let us consider an element x of \mathbb{C}_F . Then $\mathbb{Q} \times \mathbb{Q} \subseteq \text{FQ}(x) \times \text{FQ}(x) \subseteq \mathbb{C} \times \mathbb{C}$. The theorem is a consequence of (39).

Let us consider an element x of \mathbb{C}_F . Now we state the propositions:

(46) The addition of $\mathbb{F}_Q = (\text{the addition of } \mathbb{Q}[x]) \upharpoonright \mathbb{Q}$. The theorem is a consequence of (45).

- (47) The multiplication of $\mathbb{F}_{\mathbb{Q}} = (\text{the multiplication of } \mathbb{Q}[x]) \upharpoonright \mathbb{Q}$. The theorem is a consequence of (45).
- (48) $\mathbb{F}_{\mathbb{Q}}$ is a subring of $\mathbb{Q}[x]$. The theorem is a consequence of (46), (47), (42), (3), and (39).

Let us consider elements f, g of $\text{PolyRing}(K)$. Now we state the propositions:

- (49) Suppose $f \neq 0_{\text{PolyRing}(K)}$ and $\{f\}$ -ideal is prime and $g \notin \{f\}$ -ideal. Then $\{f, g\}$ -ideal = the carrier of $\text{PolyRing}(K)$.
- (50) Suppose $f \neq 0_{\text{PolyRing}(K)}$ and $\{f\}$ -ideal is prime and $g \notin \{f\}$ -ideal. Then $\{f\}$ -ideal and $\{g\}$ -ideal are co-prime. The theorem is a consequence of (49).
- (51) Let us consider an element x of \mathbb{C}_F , and an element a of $\mathbb{Q}[x]$. Then there exists an element g of $\text{PolyRing}(\mathbb{F}_{\mathbb{Q}})$ such that $a = (\text{HomExtEval}(x, \mathbb{F}_{\mathbb{Q}}))(g)$.

Let us consider elements x, a of \mathbb{C}_F . Now we state the propositions:

- (52) Suppose $a \neq 0_{\mathbb{C}_F}$ and $a \in$ the carrier of $\mathbb{Q}[x]$. Then there exists an element g of $\text{PolyRing}(\mathbb{F}_{\mathbb{Q}})$ such that
 - (i) $g \notin \text{AnnPoly}(x, \mathbb{F}_{\mathbb{Q}})$, and
 - (ii) $a = (\text{HomExtEval}(x, \mathbb{F}_{\mathbb{Q}}))(g)$.

The theorem is a consequence of (51).

- (53) Suppose x is algebraic and $a \neq 0_{\mathbb{C}_F}$ and $a \in$ the carrier of $\mathbb{Q}[x]$. Then there exist elements f, g of $\text{PolyRing}(\mathbb{F}_{\mathbb{Q}})$ such that
 - (i) $\{f\}$ -ideal = $\text{AnnPoly}(x, \mathbb{F}_{\mathbb{Q}})$, and
 - (ii) $g \notin \text{AnnPoly}(x, \mathbb{F}_{\mathbb{Q}})$, and
 - (iii) $a = (\text{HomExtEval}(x, \mathbb{F}_{\mathbb{Q}}))(g)$, and
 - (iv) $\{f\}$ -ideal and $\{g\}$ -ideal are co-prime.

The theorem is a consequence of (28), (3), (52), (32), (29), and (50).

- (54) Suppose x is algebraic and $a \neq 0_{\mathbb{C}_F}$ and $a \in$ the carrier of $\mathbb{Q}[x]$. Then there exists an element b of \mathbb{C}_F such that
 - (i) $b \in$ the carrier of $\mathbb{Q}[x]$, and
 - (ii) $a \cdot b = 1_{\mathbb{C}_F}$.

The theorem is a consequence of (53), (3), (14), (15), and (20).

- (55) Let us consider an element x of \mathbb{C}_F . If x is algebraic, then $\mathbb{Q}[x]$ is a field. The theorem is a consequence of (54), (41), and (42).

REFERENCES

- [1] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to Commutative Algebra*, volume 2. Addison-Wesley Reading, 1969.
- [2] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweiler. Ring ideals. *Formalized Mathematics*, 9(3):565–582, 2001.
- [3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(1):41–46, 1990.
- [4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(1):107–114, 1990.
- [5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [6] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(2):335–342, 1990.
- [7] Hideyuki Matsumura. *Commutative Ring Theory*. Cambridge University Press, 2nd edition, 1989. Cambridge Studies in Advanced Mathematics.
- [8] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(2):339–346, 2001.
- [9] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(2):391–395, 2001.
- [10] Masayoshi Nagata. *Theory of Commutative Fields*, volume 125. American Mathematical Society, 1985. Translations of Mathematical Monographs.
- [11] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(2):329–334, 1990.
- [12] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(3):569–573, 1990.
- [13] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(2):291–296, 1990.
- [14] Oscar Zariski and Pierre Samuel. *Commutative Algebra I*. Springer, 2nd edition, 1975.

Received December 15, 2016
