

# On Roots of Polynomials and Algebraically Closed Fields

Christoph Schwarzweller  
Institute of Informatics  
University of Gdańsk  
Poland

**Summary.** In this article we further extend the algebraic theory of polynomial rings in Mizar [1, 2, 3]. We deal with roots and multiple roots of polynomials and show that both the real numbers and finite domains are not algebraically closed [5, 7]. We also prove the identity theorem for polynomials and that the number of multiple roots is bounded by the polynomial's degree [4, 6].

MSC: 13A05 13B25 03B35

Keywords: commutative algebra; polynomials; algebraic closed fields

MML identifier: RING\_5, version: 8.1.06 5.44.1305

## 1. PRELIMINARIES

From now on  $n$  denotes a natural number.

Note that there exists a natural number which is non trivial and non prime.

Now we state the proposition:

- (1) Let us consider an even natural number  $n$ , and an element  $x$  of  $\mathbb{R}_F$ . Then  $x^n \geq 0_{\mathbb{R}_F}$ .

PROOF: Define  $\mathcal{P}[\text{natural number}] \equiv x^{2 \cdot s_1} \geq 0_{\mathbb{R}_F}$ . For every element  $x$  of  $\mathbb{R}_F$ ,  $x^2 \geq 0_{\mathbb{R}_F}$ . For every natural number  $k$ ,  $\mathcal{P}[k]$ .  $\square$

Let us consider a ring  $R$  and an element  $a$  of  $R$ . Now we state the propositions:

- (2)  $2 \star a = a + a$ .  
(3)  $a^2 = a \cdot a$ .

Let  $F$  be a field and  $a$  be an element of  $F$ . Note that  $\frac{a}{1_F}$  reduces to  $a$ .

One can check that  $\mathbb{Z}/2$  is non trivial and almost left invertible.

Let  $n$  be a non trivial, non prime natural number. Note that  $\mathbb{Z}/n$  is non integral domain-like and  $\mathbb{Z}/6$  is non degenerated.

## 2. SOME MORE PROPERTIES OF POLYNOMIALS

Let  $R$  be a non degenerated ring. Observe that every non zero polynomial over  $R$  is non-zero and every polynomial over  $R$  which is monic is also non zero.

Let  $p$  be a non zero polynomial over  $R$ . One can check that  $\deg p$  is natural.

Let  $R$  be a ring,  $p$  be a zero polynomial over  $R$ , and  $q$  be a polynomial over  $R$ . Let us observe that  $p * q$  is zero and  $q * p$  is zero.

Let us observe that  $p + q$  reduces to  $q$  and  $q + p$  reduces to  $q$ .

Let  $p$  be a polynomial over  $R$ . One can check that  $p * \mathbf{0}.R$  reduces to  $\mathbf{0}.R$  and  $p * \mathbf{1}.R$  reduces to  $p$  and  $\mathbf{0}.R * p$  reduces to  $\mathbf{0}.R$  and  $\mathbf{1}.R * p$  reduces to  $p$ .

One can check that  $1_R \cdot p$  reduces to  $p$ .

Now we state the propositions:

- (4) Let us consider an integral domain  $R$ , a polynomial  $p$  over  $R$ , and a non zero element  $a$  of  $R$ . Then  $\deg(a \cdot p) = \deg p$ .
- (5) Let us consider an integral domain  $R$ , a polynomial  $p$  over  $R$ , and an element  $a$  of  $R$ . Then  $\text{LC}(a \cdot p) = a \cdot \text{LC} p$ .
- (6) Let us consider an integral domain  $R$ , and an element  $a$  of  $R$ . Then  $\text{LC}(a \setminus R) = a$ . The theorem is a consequence of (5).
- (7) Let us consider an integral domain  $R$ , a polynomial  $p$  over  $R$ , and elements  $v, x$  of  $R$ . Then  $\text{eval}(v \cdot p, x) = v \cdot \text{eval}(p, x)$ . The theorem is a consequence of (4).
- (8) Let us consider a ring  $R$ , and elements  $a, b$  of  $R$ . Then  $\text{eval}(a \setminus R, b) = a$ .

Let  $R$  be an integral domain and  $p, q$  be monic polynomials over  $R$ . Let us note that  $p * q$  is monic.

Let  $a$  be an element of  $R$  and  $k$  be a natural number. One can check that  $(\text{rpoly}(1, a))^k$  is non zero and monic.

Now we state the propositions:

- (9) Let us consider a non degenerated ring  $R$ , an element  $a$  of  $R$ , and a non zero element  $k$  of  $\mathbb{N}$ . Then  $\text{LC rpoly}(k, a) = 1_R$ .
- (10) Let us consider a non degenerated, well unital, non empty double loop structure  $R$ , and an element  $a$  of  $R$ . Then  $\langle -a, 1_R \rangle = \text{rpoly}(1, a)$ .
- (11) Let us consider an integral domain  $R$ , a polynomial  $p$  over  $R$ , and an element  $x$  of  $R$ . Then  $\text{eval}(p, x) = 0_R$  if and only if  $\text{rpoly}(1, x) \mid p$ .

(12) Let us consider an integral domain  $F$ , polynomials  $p, q$  over  $F$ , and an element  $a$  of  $F$ . Suppose  $\text{rpoly}(1, a) \mid p * q$ . Then

(i)  $\text{rpoly}(1, a) \mid p$ , or

(ii)  $\text{rpoly}(1, a) \mid q$ .

The theorem is a consequence of (11).

(13) Let us consider an integral domain  $R$ , a polynomial  $p$  over  $R$ , and a non zero polynomial  $q$  over  $R$ . If  $p \mid q$ , then  $\deg p \leq \deg q$ .

(14) Let us consider a non degenerated commutative ring  $R$ , a polynomial  $q$  over  $R$ , a non zero polynomial  $p$  over  $R$ , and a non zero element  $b$  of  $R$ . If  $q \mid p$ , then  $q \mid b \cdot p$ .

(15) Let us consider a field  $F$ , a polynomial  $q$  over  $F$ , a non zero polynomial  $p$  over  $F$ , and a non zero element  $b$  of  $F$ . Then  $q \mid p$  if and only if  $q \mid b \cdot p$ . The theorem is a consequence of (14).

Let us consider an integral domain  $R$ , a non zero polynomial  $p$  over  $R$ , an element  $a$  of  $R$ , and a non zero element  $b$  of  $R$ . Now we state the propositions:

(16)  $\text{rpoly}(1, a) \mid p$  if and only if  $\text{rpoly}(1, a) \mid b \cdot p$ . The theorem is a consequence of (11), (7), and (14).

(17)  $(\text{rpoly}(1, a))^n \mid p$  if and only if  $(\text{rpoly}(1, a))^n \mid b \cdot p$ .

PROOF: Define  $\mathcal{P}[\text{natural number}] \equiv \text{if } (\text{rpoly}(1, a))^{\mathfrak{s}^1} \mid b \cdot p$ , then  $(\text{rpoly}(1, a))^{\mathfrak{s}^1} \mid p$ . For every natural number  $k$ ,  $\mathcal{P}[k]$ .  $\square$

Let  $R$  be an integral domain,  $p$  be a non zero polynomial over  $R$ , and  $b$  be a non zero element of  $R$ . Let us note that  $b \cdot p$  is non zero.

### 3. ON ROOTS OF POLYNOMIALS

Let  $R$  be a non degenerated ring. One can check that  $\mathbf{1} \cdot R$  and has not roots.

Let  $a$  be a non zero element of  $R$ . One can verify that  $a \mid R$  and has not roots and every polynomial over  $R$  which is non zero and has roots is also non constant and every polynomial over  $R$  which and has not roots is also non zero.

Let  $a$  be an element of  $R$ . One can check that  $\text{rpoly}(1, a)$  is non zero and has roots and there exists a polynomial over  $R$  which is non zero and has not roots and there exists a polynomial over  $R$  which is non zero and has roots.

Let  $R$  be an integral domain,  $p$  be a polynomial over  $R$  with non roots, and  $a$  be a non zero element of  $R$ . Let us note that  $a \cdot p$  and has not roots.

Let  $p$  be a polynomial over  $R$  with roots and  $a$  be an element of  $R$ . Note that  $a \cdot p$  has roots.

Let  $R$  be a non degenerated commutative ring and  $q$  be a polynomial over  $R$ . One can verify that  $p * q$  has roots.

Let  $R$  be an integral domain and  $p, q$  be polynomials over  $R$  with non roots. One can check that  $p * q$  and has not roots.

Let  $R$  be a non degenerated commutative ring,  $a$  be an element of  $R$ , and  $k$  be a non zero element of  $\mathbb{N}$ . Let us note that  $\text{rpoly}(k, a)$  is non constant and monic and has roots.

Let  $R$  be a non degenerated ring. Let us observe that there exists a polynomial over  $R$  which is non constant and monic.

Let  $R$  be an integral domain,  $a$  be an element of  $R$ ,  $k$  be a non zero natural number, and  $n$  be a non zero element of  $\mathbb{N}$ . Note that  $(\text{rpoly}(n, a))^k$  is non constant and monic and has roots.

Let  $R$  be a ring and  $p$  be a polynomial over  $R$  with roots. Note that  $\text{Roots}(p)$  is non empty.

Let  $R$  be a non degenerated ring and  $p$  be a polynomial over  $R$  with non roots. Let us observe that  $\text{Roots}(p)$  is empty.

Let  $R$  be an integral domain. One can check that there exists a polynomial over  $R$  which is monic and has roots and there exists a polynomial over  $R$  which is monic and has not roots.

Now we state the propositions:

- (18) Let us consider a non degenerated ring  $R$ , and an element  $a$  of  $R$ . Then  $\text{Roots}(\text{rpoly}(1, a)) = \{a\}$ .
- (19) Let us consider an integral domain  $F$ , a polynomial  $p$  over  $F$ , and a non zero element  $b$  of  $F$ . Then  $\text{Roots}(b \cdot p) = \text{Roots}(p)$ . The theorem is a consequence of (7).
- (20) There exist polynomials  $p, q$  over  $\mathbb{Z}/6$  such that  $\text{Roots}(p * q) \not\subseteq \text{Roots}(p) \cup \text{Roots}(q)$ .
- (21) Let us consider an integral domain  $R$ , and elements  $a, b$  of  $R$ . Then  $\text{rpoly}(1, a) \mid \text{rpoly}(1, b)$  if and only if  $a = b$ . The theorem is a consequence of (18).
- (22) Let us consider an integral domain  $R$ , and a non zero polynomial  $p$  over  $R$ . Then  $\overline{\text{Roots}(p)} \leq \deg p$ .

#### 4. MORE ABOUT BAGS

Let  $X$  be a non empty set and  $B$  be a bag of  $X$ . We introduce the notation  $\overline{B}$  as a synonym of  $\sum B$ .

Observe that there exists a bag of  $X$  which is zero and there exists a bag of  $X$  which is non zero.

Let  $b_1$  be a bag of  $X$  and  $b_2$  be a bag of  $X$ . One can check that  $b_1 + b_2$  is  $X$ -defined and  $b_1 + b_2$  is total.

Let us consider a non empty set  $X$  and a bag  $b$  of  $X$ . Now we state the propositions:

$$(23) \quad \overline{b} = 0 \text{ if and only if support } b = \emptyset.$$

$$(24) \quad b \text{ is zero if and only if support } b = \emptyset.$$

$$(25) \quad b \text{ is zero if and only if } \text{rng } b = \{0\}.$$

Let  $X$  be a non empty set,  $b_1$  be a non zero bag of  $X$ , and  $b_2$  be a bag of  $X$ . One can check that  $b_1 + b_2$  is non zero.

$$(26) \quad \text{Let us consider a non empty set } X, \text{ a bag } b \text{ of } X, \text{ and an element } x \text{ of } X. \text{ Suppose support } b = \{x\}. \text{ Then } b = (\{x\}, b(x))\text{-bag.}$$

$$(27) \quad \text{Let us consider a non empty set } X, \text{ a non empty bag } b \text{ of } X, \text{ and an element } x \text{ of } X. \text{ Then support } b = \{x\} \text{ if and only if } b = (\{x\}, b(x))\text{-bag and } b(x) \neq 0. \text{ The theorem is a consequence of (26).}$$

Let  $X$  be a set and  $S$  be a finite subset of  $X$ . The functor  $\text{Bag}(S)$  yielding a bag of  $X$  is defined by the term

$$(\text{Def. 1}) \quad (S, 1)\text{-bag.}$$

Let  $X$  be a non empty set and  $S$  be a non empty, finite subset of  $X$ . Observe that  $\text{Bag}(S)$  is non zero.

Let  $b$  be a bag of  $X$  and  $a$  be an element of  $X$ . The functor  $b \setminus a$  yielding a bag of  $X$  is defined by the term

$$(\text{Def. 2}) \quad b + \cdot (a, 0).$$

Let us consider a non empty set  $X$ , a bag  $b$  of  $X$ , and an element  $a$  of  $X$ . Now we state the propositions:

$$(28) \quad b \setminus a = b \text{ if and only if } a \notin \text{support } b.$$

$$(29) \quad \text{support}(b \setminus a) = \text{support } b \setminus \{a\}.$$

$$(30) \quad (b \setminus a) + (\{a\}, b(a))\text{-bag} = b.$$

$$(31) \quad \text{Let us consider a non empty set } X, \text{ an element } a \text{ of } X, \text{ and an element } n \text{ of } \mathbb{N}. \text{ Then } \overline{(\{a\}, n)}\text{-bag} = n. \text{ The theorem is a consequence of (23).}$$

## 5. ON MULTIPLE ROOTS OF POLYNOMIALS

Let  $R$  be an integral domain and  $p$  be a non zero polynomial over  $R$  with roots. One can verify that  $\text{BRoots}(p)$  is non zero.

Now we state the propositions:

$$(32) \quad \text{Let us consider a non degenerated commutative ring } R, \text{ a non zero polynomial } p \text{ over } R, \text{ and an element } a \text{ of } R. \text{ Then multiplicity}(p, a) = 0 \text{ if and only if } \text{rpoly}(1, a) \nmid p.$$

- (33) Let us consider an integral domain  $R$ , a non zero polynomial  $p$  over  $R$ , and an element  $a$  of  $R$ . Then  $\text{multiplicity}(p, a) = n$  if and only if  $(\text{rpoly}(1, a))^n \mid p$  and  $(\text{rpoly}(1, a))^{n+1} \nmid p$ . The theorem is a consequence of (10).
- (34) Let us consider an integral domain  $R$ , and an element  $a$  of  $R$ . Then  $\text{multiplicity}(\text{rpoly}(1, a), a) = 1$ . The theorem is a consequence of (13) and (33).
- (35) Let us consider an integral domain  $R$ , and elements  $a, b$  of  $R$ . If  $b \neq a$ , then  $\text{multiplicity}(\text{rpoly}(1, a), b) = 0$ . The theorem is a consequence of (21) and (32).
- (36) Let us consider an integral domain  $R$ , a non zero polynomial  $p$  over  $R$ , a non zero element  $b$  of  $R$ , and an element  $a$  of  $R$ . Then  $\text{multiplicity}(p, a) = \text{multiplicity}(b \cdot p, a)$ . The theorem is a consequence of (33), (14), and (17).
- (37) Let us consider an integral domain  $R$ , a non zero polynomial  $p$  over  $R$ , and a non zero element  $b$  of  $R$ . Then  $\text{BRoots}(b \cdot p) = \text{BRoots}(p)$ . The theorem is a consequence of (36).
- (38) Let us consider an integral domain  $R$ , and a non zero polynomial  $p$  over  $R$  without roots. Then  $\text{BRoots}(p) = \text{EmptyBag}(\text{the carrier of } R)$ .
- (39) Let us consider an integral domain  $R$ , and a non zero element  $a$  of  $R$ . Then  $\overline{\text{BRoots}(a \mid R)} = 0$ . The theorem is a consequence of (23).
- (40) Let us consider an integral domain  $R$ , and an element  $a$  of  $R$ . Then  $\overline{\text{BRoots}(\text{rpoly}(1, a))} = 1$ . The theorem is a consequence of (10).
- (41) Let us consider an integral domain  $R$ , and non zero polynomials  $p, q$  over  $R$ . Then  $\overline{\text{BRoots}(p * q)} = \overline{\text{BRoots}(p)} + \overline{\text{BRoots}(q)}$ .
- (42) Let us consider an integral domain  $R$ , and a non zero polynomial  $p$  over  $R$ . Then  $\overline{\text{BRoots}(p)} \leq \deg p$ .

PROOF: Define  $\mathcal{P}[\text{natural number}] \equiv$  for every non zero polynomial  $p$  over  $R$  such that  $\deg p = \mathbb{S}_1$  holds  $\overline{\text{BRoots}(p)} \leq \deg p$ .  $\mathcal{P}[0]$ . For every natural number  $k$ ,  $\mathcal{P}[k]$ .  $\square$

6. THE POLYNOMIAL  $X^n + 1$

Let  $R$  be a unital, non empty double loop structure and  $n$  be a natural number. The functor  $\text{npoly}(R, n)$  yielding a sequence of  $R$  is defined by the term

(Def. 3)  $\mathbf{0.R} + \cdot [0 \mapsto 1_R, n \mapsto 1_R]$ .

One can check that  $\text{npoly}(R, n)$  is finite-Support and  $\text{npoly}(R, n)$  is non zero.

Let us consider a unital, non degenerated double loop structure  $R$ . Now we state the propositions:

(43)  $\text{deg npoly}(R, n) = n$ .

(44)  $\text{LC npoly}(R, n) = 1_R$ .

(45) Let us consider a non degenerated ring  $R$ , and an element  $x$  of  $R$ . Then  $\text{eval}(\text{npoly}(R, 0), x) = 1_R$ .

(46) Let us consider a non degenerated ring  $R$ , a non zero natural number  $n$ , and an element  $x$  of  $R$ . Then  $\text{eval}(\text{npoly}(R, n), x) = x^n + 1_R$ .

PROOF: Set  $q = \text{npoly}(R, n)$ . Consider  $F$  being a finite sequence of elements of  $R$  such that  $\text{eval}(q, x) = \sum F$  and  $\text{len } F = \text{len } q$  and for every element  $j$  of  $\mathbb{N}$  such that  $j \in \text{dom } F$  holds  $F(j) = q(j-1) \cdot \text{power}_R(x, j-1)$ . Consider  $f_1$  being a sequence of the carrier of  $R$  such that  $\sum F = f_1(\text{len } F)$  and  $f_1(0) = 0_R$  and for every natural number  $j$  and for every element  $v$  of  $R$  such that  $j < \text{len } F$  and  $v = F(j+1)$  holds  $f_1(j+1) = f_1(j) + v$ . Define  $\mathcal{P}[\text{element of } \mathbb{N}] \equiv \$1 = 0$  and  $f_1(\$1) = 0_R$  or  $0 < \$1 < \text{len } F$  and  $f_1(\$1) = 1_R$  or  $\$1 = \text{len } F$  and  $f_1(\$1) = x^n + 1_R$ . For every element  $j$  of  $\mathbb{N}$  such that  $0 \leq j \leq \text{len } F$  holds  $\mathcal{P}[j]$ .  $\square$

(47) Let us consider an even natural number  $n$ , and an element  $x$  of  $\mathbb{R}_F$ . Then  $\text{eval}(\text{npoly}(\mathbb{R}_F, n), x) > 0_{\mathbb{R}_F}$ . The theorem is a consequence of (45), (1), and (46).

(48) Let us consider an odd natural number  $n$ . Then  $\text{eval}(\text{npoly}(\mathbb{R}_F, n), -1_{\mathbb{R}_F}) = 0_{\mathbb{R}_F}$ . The theorem is a consequence of (46).

(49)  $\text{eval}(\text{npoly}(\mathbb{Z}/2, 2), 1_{\mathbb{Z}/2}) = 0_{\mathbb{Z}/2}$ . The theorem is a consequence of (46) and (2).

Let  $n$  be an even natural number. Let us note that  $\text{npoly}(\mathbb{R}_F, n)$  and has not roots.

Let  $n$  be an odd natural number. Observe that  $\text{npoly}(\mathbb{R}_F, n)$  has roots and  $\text{npoly}(\mathbb{Z}/2, 2)$  has roots.

7. THE POLYNOMIALS  $(x - a_1) * (x - a_2) * \dots * (x - a_n)$

Let  $R$  be a ring.

A product of linear polynomials of  $R$  is a polynomial over  $R$  and is defined by

(Def. 4) there exists a non empty finite sequence  $F$  of elements of  $\text{PolyRing}(R)$  such that  $it = \prod F$  and for every natural number  $i$  such that  $i \in \text{dom } F$  there exists an element  $a$  of  $R$  such that  $F(i) = \text{rpoly}(1, a)$ .

Let  $R$  be an integral domain. One can verify that every product of linear polynomials of  $R$  is non constant and monic and has roots.

Now we state the propositions:

- (50) Let us consider an integral domain  $R$ , and a product of linear polynomials  $p$  of  $R$ . Then  $\text{LC } p = 1_R$ .
- (51) Let us consider an integral domain  $R$ , and an element  $a$  of  $R$ . Then  $\text{rpoly}(1, a)$  is a product of linear polynomials of  $R$ .
- (52) Let us consider an integral domain  $R$ , and products of linear polynomials  $p, q$  of  $R$ . Then  $p * q$  is a product of linear polynomials of  $R$ .

Let  $R$  be an integral domain and  $B$  be a non zero bag of the carrier of  $R$ .

A product of linear polynomials of  $R$  and  $B$  is a product of linear polynomials of  $R$  and is defined by

(Def. 5)  $\text{deg } it = \overline{B}$  and for every element  $a$  of  $R$ ,  $\text{multiplicity}(it, a) = B(a)$ .

Let us consider an integral domain  $R$ , a non zero bag  $B$  of the carrier of  $R$ , a product of linear polynomials  $p$  of  $R$  and  $B$ , and an element  $a$  of  $R$ . Now we state the propositions:

- (53) If  $a \in \text{support } B$ , then  $\text{eval}(p, a) = 0_R$ . The theorem is a consequence of (11).
- (54) (i)  $(\text{rpoly}(1, a))^{B(a)} \mid p$ , and  
 (ii)  $(\text{rpoly}(1, a))^{B(a)+1} \nmid p$ .

The theorem is a consequence of (33).

Let us consider an integral domain  $R$ , a non zero bag  $B$  of the carrier of  $R$ , and a product of linear polynomials  $p$  of  $R$  and  $B$ . Now we state the propositions:

- (55)  $\text{BRoots}(p) = B$ .
- (56)  $\text{deg } p = \overline{\text{BRoots}(p)}$ . The theorem is a consequence of (55).
- (57) Let us consider an integral domain  $R$ , and an element  $a$  of  $R$ . Then  $\text{rpoly}(1, a)$  is a product of linear polynomials of  $R$  and  $\text{Bag}(\{a\})$ . The theorem is a consequence of (51), (34), and (35).
- (58) Let us consider an integral domain  $R$ , non zero bags  $B_1, B_2$  of the carrier of  $R$ , a product of linear polynomials  $p$  of  $R$  and  $B_1$ , and a product of linear



polynomials  $q$  of  $R$  and  $B_2$ . Then  $p * q$  is a product of linear polynomials of  $R$  and  $B_1 + B_2$ . The theorem is a consequence of (52), (56), and (55).

- (59) Let us consider an integral domain  $R$ . Then every product of linear polynomials of  $R$  is a product of linear polynomials of  $R$  and  $\text{BRoots}(p)$ .  
 PROOF: Define  $\mathcal{P}[\text{natural number}] \equiv$  for every product of linear polynomials  $p$  of  $R$  such that  $\deg p = \$_1$  holds  $p$  is a product of linear polynomials of  $R$  and  $\text{BRoots}(p)$ .  $\mathcal{P}[1]$ . For every natural number  $k$  such that  $k \geq 1$  holds  $\mathcal{P}[k]$ .  $\square$

Let  $R$  be an integral domain and  $S$  be a non empty, finite subset of  $R$ .

A product of linear polynomials of  $R$  and  $S$  is a product of linear polynomials of  $R$  and  $\text{Bag}(S)$ . Now we state the proposition:

- (60) Let us consider an integral domain  $R$ , a non empty, finite subset  $S$  of  $R$ , and a product of linear polynomials  $p$  of  $R$  and  $S$ . Then  $\deg p = \overline{S}$ .

Let us consider an integral domain  $R$ , a non empty, finite subset  $S$  of  $R$ , a product of linear polynomials  $p$  of  $R$  and  $S$ , and an element  $a$  of  $R$ . Now we state the propositions:

- (61) If  $a \in S$ , then  $\text{rpoly}(1, a) \mid p$  and  $(\text{rpoly}(1, a))^2 \nmid p$ . The theorem is a consequence of (54).  
 (62) If  $a \in S$ , then  $\text{eval}(p, a) = 0_R$ . The theorem is a consequence of (61).  
 (63) Let us consider an integral domain  $R$ , a non empty, finite subset  $S$  of  $R$ , and a product of linear polynomials  $p$  of  $R$  and  $S$ . Then  $\text{Roots}(p) = S$ . The theorem is a consequence of (62), (22), and (60).

## 8. MAIN THEOREMS

Now we state the proposition:

- (64) Let us consider an integral domain  $R$ , and a non zero polynomial  $p$  over  $R$  with roots. Then there exists a product of linear polynomials  $q$  of  $R$  and  $\text{BRoots}(p)$  and there exists a polynomial  $r$  over  $R$  with non roots such that  $p = q * r$  and  $\text{Roots}(q) = \text{Roots}(p)$ .

PROOF: Define  $\mathcal{P}[\text{natural number}] \equiv$  for every non zero polynomial  $p$  over  $R$  with roots such that  $\deg p = \$_1$  there exists a product of linear polynomials  $q$  of  $R$  and  $\text{BRoots}(p)$  and there exists a polynomial  $r$  over  $R$  with non roots such that  $p = q * r$  and  $\text{Roots}(q) = \text{Roots}(p)$ .  $\mathcal{P}[1]$  by (11), [9, (1)], (51), [8, (23), (27), (24)]. For every natural number  $k$  such that  $1 \leq k$  holds  $\mathcal{P}[k]$ . Consider  $d$  being a natural number such that  $\deg p = d$ .  
 $\square$

Let us consider an integral domain  $R$  and a non zero polynomial  $p$  over  $R$ .

- (65)  $\overline{\overline{\text{Roots}(p)}} \leq \overline{\overline{\text{BRoots}(p)}}$ . The theorem is a consequence of (64), (56), (55), (22), and (38).
- (66)  $\overline{\overline{\text{BRoots}(p)}} = \deg p$  if and only if there exists an element  $a$  of  $R$  and there exists a product of linear polynomials  $q$  of  $R$  such that  $p = a \cdot q$ . The theorem is a consequence of (64), (56), (55), (59), (4), (37), and (38).

Now we state the proposition:

- (67) Let us consider an integral domain  $R$ , and polynomials  $p, q$  over  $R$ . Suppose there exists a subset  $S$  of  $R$  such that  $\overline{S} = \max(\deg p, \deg q) + 1$  and for every element  $a$  of  $R$  such that  $a \in S$  holds  $\text{eval}(p, a) = \text{eval}(q, a)$ . Then  $p = q$ . The theorem is a consequence of (22).

Let  $F$  be an algebraic closed field. Note that every non constant polynomial over  $F$  has roots and  $\mathbb{R}_F$  is non algebraic closed and every finite integral domain is non algebraic closed and every ring which is algebraic closed is also almost right invertible.

Now we state the propositions:

- (68) Let us consider an algebraic closed field  $F$ , and a non constant polynomial  $p$  over  $F$ . Then there exists an element  $a$  of  $F$  and there exists a product of linear polynomials  $q$  of  $F$  and  $\text{BRoots}(p)$  such that  $a \cdot q = p$ . The theorem is a consequence of (64).
- (69) Let us consider an algebraic closed field  $F$ . Then every non constant, monic polynomial over  $F$  is a product of linear polynomials of  $F$  and  $\text{BRoots}(p)$ . The theorem is a consequence of (68).
- (70) Let us consider a field  $F$ . Then  $F$  is algebraic closed if and only if every non constant, monic polynomial over  $F$  is a product of linear polynomials of  $F$ . The theorem is a consequence of (69).

## REFERENCES

- [1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pał, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8\_17.
- [2] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.
- [3] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. On algebraic hierarchies in mathematical repository of Mizar. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371, 2016. doi:10.15439/2016F520.
- [4] H. Heuser. *Lehrbuch der Analysis*. B.G. Teubner Stuttgart, 1990.
- [5] Nathan Jacobson. *Basic Algebra I*. 2nd edition. Dover Publications Inc., 2009.

- [6] Heinz Lüneburg. *Gruppen, Ringe, Körper: Die grundlegenden Strukturen der Algebra*. Oldenbourg Verlag, 1990.
- [7] Knut Radbruch. *Algebra I*. Lecture Notes, University of Kaiserslautern, Germany, 1991.
- [8] Christoph Schwarzweiler and Agnieszka Rowińska-Schwarzweiler. Schur's theorem on the stability of networks. *Formalized Mathematics*, 14(4):135–142, 2006. doi:10.2478/v10037-006-0017-9.
- [9] Christoph Schwarzweiler, Artur Korniłowicz, and Agnieszka Rowińska-Schwarzweiler. Some algebraic properties of polynomial rings. *Formalized Mathematics*, 24(3):227–237, 2016. doi:10.1515/forma-2016-0019.

*Received August 30, 2017*

---



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