FORMALIZED MATHEMATICS
Vol. 24, No. 3, Pages 227–237, 2016
DOI: 10.1515/forma-2016-0019

DE GRUYTER OPEN
degruyter.com/view/j/forma

Some Algebraic Properties of Polynomial Rings

Christoph Schwarzweller
Institute of Computer Science
University of Gdańsk
Poland

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Agnieszka Rowińska-Schwarzweller
Sopot, Poland

Summary. In this article we extend the algebraic theory of polynomial rings, formalized in Mizar [1], based on [2], [3]. After introducing constant and monic polynomials we present the canonical embedding of R into $R[X]$ and deal with both unit and irreducible elements. We also define polynomial GCDs and show that for fields F and irreducible polynomials p the field $F[X]/\langle p \rangle$ is isomorphic to the field of polynomials with degree smaller than the one of p.

MSC: 12E05 11T55 03B35

Keywords: polynomial; polynomial ring; polynomial GCD

MML identifier: RING_4, version: 8.1.05 5.37.1275

1. Preliminaries

Let R be a non empty double loop structure and a be an element of R. Observe that the functor $\{a\}$ yields a subset of R. Observe that every ring which is almost left invertible and commutative is also almost right invertible and every ring which is almost right invertible and commutative is also almost left invertible and every ring which is almost left cancelable and commutative is also almost right cancelable and every ring which is almost right cancelable and commutative is also almost left cancelable.

Let L be a non empty zero structure and X be a set. We say that X is L-polynomial membered if and only if

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

(Def. 1) for every object p such that $p \in X$ holds p is a polynomial over L.

Let X be a 1-sorted structure. We say that X is L-polynomial membered if and only if

(Def. 2) the carrier of X is L-polynomial membered.

Let us note that there exists a set which is non empty and L-polynomial membered and there exists a 1-sorted structure which is non empty and L-polynomial membered.

Let X be a non empty, L-polynomial membered 1-sorted structure. One can check that the carrier of X is L-polynomial membered.

Let L be an add-associative, right zeroed, right complementable, distributive, non empty double loop structure. Let us observe that Polynom-Ring(L) is L-polynomial membered.

Let L be a non empty zero structure and X be a non empty, L-polynomial membered set.

Observe that an element of X is a polynomial over L. Let R be a ring. One can verify that there exists an element of the carrier of Polynom-Ring(R) which is zero and there exists an element of Polynom-Ring(R) which is zero and there exists a polynomial over R which is zero.

Let R be a non degenerated ring. Let us note that there exists an element of the carrier of Polynom-Ring(R) which is non zero and there exists an element of Polynom-Ring(R) which is non zero.

Let L be an add-associative, right zeroed, right complementable, distributive, non empty double loop structure and p, q be polynomials over L. We say that $p \mid q$ if and only if

(Def. 3) there exist elements a, b of Polynom-Ring(L) such that $a = p$ and $b = q$ and $a \mid b$.

Now we state the proposition:

(1) Let us consider an add-associative, right zeroed, right complementable, distributive, non empty double loop structure L, and polynomials p, q over L. Then $p \mid q$ if and only if there exists a polynomial r over L such that $p * r = q$.

Let us consider a field F and polynomials p, q over F. Now we state the propositions:

(2) If $\deg p < \deg q$, then $p \bmod q = p$.

(3) $p \bmod q = \mathbf{0}.F$ if and only if $q \mid p$. The theorem is a consequence of (1).

(4) $p = (p \operatorname{div} q) * q + (p \bmod q)$.

Let us consider a field F, polynomials p, r over F, and a non zero polynomial q over F. Now we state the propositions:

(5) (i) $p + r \operatorname{div} q = (p \operatorname{div} q) + (r \operatorname{div} q)$, and

(ii) $p + r \bmod q = (p \bmod q) + (r \bmod q)$.

The theorem is a consequence of (4).

(6) $p * r \bmod q = (p \bmod q) * (r \bmod q) \bmod q$. The theorem is a consequence of (4), (5), (3), and (1).

Now we state the propositions:

(7) Let us consider a field F, polynomials r, q, u over F, and a non zero polynomial p over F. Then $(r * q \bmod p) * u \bmod p = (r * q) * u \bmod p$. The theorem is a consequence of (5), (3), and (1).

(8) Let us consider an add-associative, right zeroed, right complementable, left distributive, non empty double loop structure L, and a sequence p of L. Then $0_L \cdot p = \mathbf{0}.L$.

(9) Let us consider a left unital, non empty double loop structure L, and a sequence p of L. Then $1_L \cdot p = p$.

(10) Let us consider an add-associative, right zeroed, right complementable, right unital, distributive, associative, commutative, non empty double loop structure L, sequences p, q of L, and an element a of L. Then $a \cdot (p * q) = p * (a \cdot q)$.

(11) Let us consider an associative, non empty multiplicative magma L, a sequence p of L, and elements a, b of L. Then $(a \cdot b) \cdot p = a \cdot (b \cdot p)$.

(12) Let us consider an add-associative, right zeroed, right complementable, left distributive, left unital, non empty double loop structure L, and a sequence p of L. Then $\mathbf{1}.L * p = p$.

Let L be an add-associative, right zeroed, right complementable, well unital, distributive, non empty double loop structure. Let us observe that Polynom-Ring(L) is well unital.

2. Constant Polynomials

Let R be an add-associative, right zeroed, right complementable, distributive, non empty double loop structure and x be an element of the carrier of Polynom-Ring(R). We say that x is constant if and only if

(Def. 4) $\deg x \leqslant 0$.

Let R be a non degenerated ring. Observe that there exists an element of Polynom-Ring(R) which is non zero and constant and there exists an element of the carrier of Polynom-Ring(R) which is non zero and constant.

Let R be an integral domain. Let us observe that there exists an element of Polynom-Ring(R) which is non constant and there exists an element of the carrier of Polynom-Ring(R) which is non constant.

Let L be a non empty zero structure and a be an element of L. The functor $a\restriction L$ yielding a sequence of L is defined by the term

(Def. 5) $\mathbf{0}.\,L +\cdot (0, a)$.

Note that $a\restriction L$ is finite-Support and $a\restriction L$ is constant.

Let a be a non zero element of L. Let us note that $a\restriction L$ is non zero and there exists a polynomial over L which is non zero and constant.

Now we state the propositions:

(13) Let us consider a non empty zero structure L. Then $0_L\restriction L = \mathbf{0}.\,L$.

(14) Let us consider a non empty multiplicative loop with zero structure L. Then $1_L\restriction L = \mathbf{1}.\,L$.

Let L be a non empty zero structure. Observe that $0_L\restriction L$ is zero.

Let L be a non degenerated multiplicative loop with zero structure. Let us note that $1_L\restriction L$ is non zero.

Now we state the propositions:

(15) Let us consider an add-associative, right zeroed, right complementable, distributive, non empty double loop structure L, and an element p of the carrier of Polynom-Ring(L). Then p is non zero and constant if and only if $\deg p = 0$.

(16) Let us consider an add-associative, right zeroed, right complementable, right distributive, right unital, non empty double loop structure L, and an element a of L. Then $a\restriction L = a \cdot \mathbf{1}.\,L$.

Let us consider a ring R and elements a, b of R. Now we state the propositions:

(17) $a\restriction R + b\restriction R = (a + b)\restriction R$.

(18) $(a\restriction R) * (b\restriction R) = a \cdot b\restriction R$.

(19) $a\restriction R = b\restriction R$ if and only if $a = b$.

(20) Let us consider a ring R, and an element p of the carrier of Polynom-Ring-(R). Then p is constant if and only if there exists an element a of R such that $p = a\restriction R$.

(21) Let us consider a ring R, and an element a of R. Then $\deg(a\restriction R) = 0$ if and only if $a \neq 0_R$. The theorem is a consequence of (19).

3. MONIC POLYNOMIALS

Let L be a non empty double loop structure and p be a polynomial over L. We introduce the notation p is monic as a synonym of p is normalized.

Let L be an add-associative, right zeroed, right complementable, distributive, non degenerated double loop structure. Let us observe that $\mathbf{1}_L$ is monic and $\mathbf{0}_L$ is non monic and there exists a polynomial over L which is monic and there exists a polynomial over L which is non monic and there exists an element of the carrier of Polynom-Ring(L) which is monic and there exists an element of the carrier of Polynom-Ring(L) which is non monic.

Let L be a well unital, non degenerated double loop structure and x be an element of L. One can verify that $\mathrm{rpoly}(1, x)$ is monic.

Let L be a field and p be an element of the carrier of Polynom-Ring(L). Let us observe that the functor NormPolynomial p yields an element of the carrier of Polynom-Ring(L). Let F be a field and p be a non zero polynomial over F. Observe that NormPolynomial p is monic.

Let L be a field and p be a non zero element of the carrier of Polynom-Ring(L). Observe that NormPolynomial p is monic.

Now we state the proposition:

(22) Let us consider a field F. Then NormPolynomial $\mathbf{0}_F = \mathbf{0}_F$.

Let us consider a field F and a non zero element p of the carrier of Polynom-Ring(F). Now we state the propositions:

(23) NormPolynomial $p = (\mathrm{LC}\, p)^{-1} \cdot p$.

(24) p is monic if and only if NormPolynomial $p = p$. The theorem is a consequence of (23) and (9).

Let us consider a field F and elements p, q of the carrier of Polynom-Ring(F). Now we state the propositions:

(25) $q \mid p$ if and only if NormPolynomial $q \mid p$. The theorem is a consequence of (22), (1), (9), (11), (10), and (23).

(26) $q \mid p$ if and only if $q \mid$ NormPolynomial p. The theorem is a consequence of (22), (1), (23), (10), (9), and (11).

Let us consider a field F and an element p of the carrier of Polynom-Ring(F). Now we state the propositions:

(27) NormPolynomial p is associated to p. The theorem is a consequence of (1), (26), and (25).

(28) NormPolynomial p is irreducible if and only if p is irreducible. The theorem is a consequence of (27).

Now we state the propositions:

(29) Let us consider an integral domain R, and elements p, q of the carrier of Polynom-Ring(R). If p is associated to q, then $\deg p = \deg q$.

(30) Let us consider an integral domain R, and monic elements p, q of the carrier of Polynom-Ring(R). Then p is associated to q if and only if $p = q$.

The theorem is a consequence of (29), (20), (16), (10), and (12).

4. The Canonical Homomorphism from R into $R[X]$

Let R be a ring. The canonical homomorphism of R into quotient field yielding a function from R into Polynom-Ring(R) is defined by

(Def. 6) for every element x of R, $it(x) = x\restriction R$.

Note that the canonical homomorphism of R into quotient field is additive, multiplicative, and unity-preserving and the canonical homomorphism of R into quotient field is monomorphic and Polynom-Ring(R) is R-homomorphic and R-monomorphic.

Now we state the proposition:

(31) Let us consider a ring R. Then char(Polynom-Ring(R)) = char(R).

Let R be a non degenerated ring. Let us note that Polynom-Ring(R) is infinite and every ring with characteristic 0 is infinite.

Now we state the proposition:

(32) Let us consider a ring R. If char(R) = 0, then R is infinite.

Let n be a non trivial natural number.

One can verify that Polynom-Ring($\mathbb{Z}/n$) is infinite. Now we state the proposition:

(33) Let us consider a non trivial natural number n.

Then char(Polynom-Ring($\mathbb{Z}/n$)) $\neq 0$.

Let n be a non trivial natural number. Observe that there exists a ring which is infinite and has characteristic n.

5. Units and Irreducible Polynomials

Let us note that there exists an integral domain which is non almost left invertible.

Let R be a non almost left invertible integral domain. One can verify that there exists a non-unit of R which is non zero and $\mathbb{Z}^{\mathrm{R}}$ is non almost left invertible.

Let R be an integral domain. Observe that Polynom-Ring(R) is non almost left invertible.

Now we state the propositions:

(34) Let us consider an integral domain R. Then R is a field if and only if for every non-unit a of R, $a = 0_R$.

(35) Let us consider an integral domain R, and an element a of R. Then $a\restriction R$ is a unit of Polynom-Ring(R) if and only if a is a unit of R. The theorem is a consequence of (1), (20), (18), and (19).

(36) Let us consider an integral domain F, and an element p of the carrier of Polynom-Ring(F). If p is a unit of Polynom-Ring(F), then $\deg p = 0$. The theorem is a consequence of (1).

(37) Let us consider a field F, and an element p of the carrier of Polynom-Ring (F). Then p is a unit of Polynom-Ring(F) if and only if $\deg p = 0$. The theorem is a consequence of (1), (20), and (18).

(38) Let us consider an integral domain R, and an element p of the carrier of Polynom-Ring(R). Suppose p is a unit of Polynom-Ring(R). Then p is non zero and constant. The theorem is a consequence of (36) and (15).

(39) Let us consider a field F, and an element p of the carrier of Polynom-Ring (F). Then p is a unit of Polynom-Ring(F) if and only if p is non zero and constant. The theorem is a consequence of (37) and (15).

Let R be an integral domain. One can check that every element of Polynom-Ring(R) which is non constant is also non zero and non unital.

Let F be an integral domain. Let us observe that every element of the carrier of Polynom-Ring(F) which is non constant is also non zero and non unital.

Let F be a field. Observe that every element of Polynom-Ring(F) which is non zero and constant is also unital and every element of Polynom-Ring(F) which is unital is also non zero and constant and every element of the carrier of Polynom-Ring(F) which is non zero and constant is also unital and every element of the carrier of Polynom-Ring(F) which is unital is also non zero and constant.

Now we state the propositions:

(40) Let us consider an integral domain R, and an element p of the carrier of Polynom-Ring(R). Suppose there exists an element q of the carrier of Polynom-Ring(R) such that $q \mid p$ and $1 \leqslant \deg q < \deg p$. Then p is reducible. The theorem is a consequence of (36).

(41) Let us consider a field F, and an element p of the carrier of Polynom-Ring (F). Then p is reducible if and only if $p = \mathbf{0}.F$ or p is a unit of Polynom-Ring (F) or there exists an element q of the carrier of Polynom-Ring(F) such that $q \mid p$ and $1 \leqslant \deg q < \deg p$. The theorem is a consequence of (1), (37), and (40).

(42) Let us consider an integral domain R, and a monic element p of the carrier of Polynom-Ring(R). If $\deg p = 1$, then p is irreducible. The theorem

is a consequence of (36), (20), (16), (10), (12), and (35).

(43) There exists a non monic element p of the carrier of Polynom-Ring($\mathbb{Z}^{\mathrm{R}}$) such that

(i) $\deg p = 1$, and

(ii) p is reducible.

The theorem is a consequence of (16), (10), (12), (15), (35), and (36).

(44) Let us consider a field F, and an element p of the carrier of Polynom-Ring (F). If $\deg p = 1$, then p is irreducible. The theorem is a consequence of (36), (20), (21), and (35).

(45) Let us consider an algebraic closed field F, and an element p of the carrier of Polynom-Ring(F). Then p is irreducible if and only if $\deg p = 1$. The theorem is a consequence of (36) and (44).

(46) Let us consider a field F. Then F is algebraic closed if and only if for every monic element p of the carrier of Polynom-Ring(F), p is irreducible iff $\deg p = 1$. The theorem is a consequence of (37), (41), (28), and (45).

Let R be an integral domain. Note that there exists an element of Polynom-Ring(R) which is irreducible and there exists an element of the carrier of Polynom-Ring(R) which is irreducible.

Let R be a ring. Let us observe that there exists an element of Polynom-Ring (R) which is reducible and there exists an element of the carrier of Polynom-Ring(R) which is reducible. Let R be an integral domain.

Note that IRR(Polynom-Ring(R)) is non empty.

Let F be a field. Observe that every element of Polynom-Ring(F) which is constant is also reducible and every element of the carrier of Polynom-Ring(F) which is constant is also reducible and every element of Polynom-Ring(F) which is irreducible is also non constant and every element of the carrier of Polynom-Ring(F) which is irreducible is also non constant.

6. The Field $F[X]/<p>$

Let F be a field and p be an element of the carrier of Polynom-Ring(F). Let us note that $\frac{\text{Polynom-Ring}(F)}{\{p\}\text{-ideal}}$ is Abelian, add-associative, right zeroed, right complementable, commutative, associative, well unital, and distributive.

Let p be an irreducible element of the carrier of Polynom-Ring(F). Observe that $\frac{\text{Polynom-Ring}(F)}{\{p\}\text{-ideal}}$ is non degenerated and almost left invertible.

Let p be a polynomial over F. The functor PolyMultMod(p) yielding a binary operation on Polynom-Ring(F) is defined by

(Def. 7) for every polynomials r, q over F, $it(r, q) = r * q \bmod p$.

Let p be a non constant element of the carrier of Polynom-Ring(F). The functor Polynom-Ring(p) yielding a strict double loop structure is defined by

(Def. 8) the carrier of it = $\{q$, where q is a polynomial over $F : \deg q < \deg p\}$ and the addition of it = (the addition of Polynom-Ring(F)) $\restriction$ (the carrier of it) and the multiplication of it = PolyMultMod(p) $\restriction$ (the carrier of it) and the one of $it = \mathbf{1}.F$ and the zero of $it = \mathbf{0}.F$.

Observe that Polynom-Ring(p) is non degenerated and Polynom-Ring(p) is Abelian, add-associative, right zeroed, and right complementable and Polynom-Ring(p) is associative, well unital, and distributive.

The functor PolyMod(p) yielding a function from Polynom-Ring(F) into Polynom-Ring(p) is defined by

(Def. 9) for every polynomial q over F, $it(q) = q \bmod p$.

Observe that PolyMod(p) is additive, multiplicative, and unity-preserving and Polynom-Ring(p) is (Polynom-Ring(F))-homomorphic and PolyMod(p) is onto.

Let us consider a field F and a non constant element p of the carrier of Polynom-Ring(F). Now we state the propositions:

(47) $\ker \mathrm{PolyMod}(p) = \{p\}$–ideal. The theorem is a consequence of (1) and (3).

(48) $\frac{\text{Polynom-Ring}(F)}{\{p\}\text{–ideal}}$ and Polynom-Ring(p) are isomorphic. The theorem is a consequence of (47).

Let F be a field and p be a non constant element of the carrier of Polynom-Ring (F). Observe that Polynom-Ring(p) is commutative.

Let p be an irreducible element of the carrier of Polynom-Ring(F). Observe that Polynom-Ring(p) is almost left invertible.

7. Polynomial GCDs

Let L be a non empty multiplicative magma, x, y be elements of L, and z be an element of L. We say that z is x,y-GCD if and only if

(Def. 10) $z \mid x$ and $z \mid y$ and for every element r of L such that $r \mid x$ and $r \mid y$ holds $r \mid z$.

Let L be a GCD domain. Note that there exists an element of L which is x,y-GCD.

A GCD of x and y is an x,y-GCD element of L. Now we state the proposition:

(49) Let us consider a GCD domain L, elements x, y of L, and GCDs u, v of x and y. Then u is associated to v.

Let L be a GCD domain and x, y be elements of L. One can verify that every element of L which is x,y-GCD is also y,x-GCD.

Let F be a field and p, q be elements of the carrier of Polynom-Ring(F). The functor $\gcd(p, q)$ yielding an element of the carrier of Polynom-Ring(F) is defined by

(Def. 11) (i) *it* $= \mathbf{0}.F$, **if** $p = \mathbf{0}.F$ and $q = \mathbf{0}.F$,

(ii) *it* is GCD of p and q and monic, **otherwise**.

One can check that the functor $\gcd(p, q)$ is commutative.

Let p, q be elements of Polynom-Ring(F). Let us note that the functor $\gcd(p, q)$ is commutative.

Let p, q be elements of the carrier of Polynom-Ring(F). Let us observe that $\gcd(p, q)$ is p,q-GCD.

Let p, q be elements of Polynom-Ring(F). Observe that $\gcd(p, q)$ is p,q-GCD.

Let p be an element of the carrier of Polynom-Ring(F) and q be a non zero element of the carrier of Polynom-Ring(F). Note that $\gcd(p, q)$ is non zero and monic.

Let p be an element of Polynom-Ring(F) and q be a non zero element of Polynom-Ring(F). Let us observe that $\gcd(p, q)$ is non zero and monic.

Let p, q be zero elements of the carrier of Polynom-Ring(F). Let us note that $\gcd(p, q)$ is zero.

Let p, q be zero elements of Polynom-Ring(F). One can verify that $\gcd(p, q)$ is zero.

Now we state the propositions:

(50) Let us consider a field F, and elements p, q of the carrier of Polynom-Ring (F). Then

(i) $\gcd(p, q) \mid p$, and

(ii) $\gcd(p, q) \mid q$, and

(iii) for every element r of the carrier of Polynom-Ring(F) such that $r \mid p$ and $r \mid q$ holds $r \mid \gcd(p, q)$.

(51) Let us consider a field F, and elements p, q of Polynom-Ring(F). Then

(i) $\gcd(p, q) \mid p$, and

(ii) $\gcd(p, q) \mid q$, and

(iii) for every element r of Polynom-Ring(F) such that $r \mid p$ and $r \mid q$ holds $r \mid \gcd(p, q)$.

Let F be a field and p, q be polynomials over F. The functor $\gcd(p, q)$ yielding a polynomial over F is defined by

(Def. 12) there exist elements a, b of Polynom-Ring(F) such that $a = p$ and $b = q$ and $it = \gcd(a, b)$.

Observe that the functor $\gcd(p, q)$ is commutative.

Let p be a polynomial over F and q be a non zero polynomial over F. Let us note that $\gcd(p, q)$ is non zero and monic.

Let p, q be zero polynomials over F. One can verify that $\gcd(p, q)$ is zero.

Now we state the propositions:

(52) Let us consider a field F, and polynomials p, q over F. Then

(i) $\gcd(p, q) \mid p$, and

(ii) $\gcd(p, q) \mid q$, and

(iii) for every polynomial r over F such that $r \mid p$ and $r \mid q$ holds $r \mid \gcd(p, q)$.

The theorem is a consequence of (1).

(53) Let us consider a field F, a polynomial p over F, a non zero polynomial q over F, and a monic polynomial s over F. Then $s = \gcd(p, q)$ if and only if $s \mid p$ and $s \mid q$ and for every polynomial r over F such that $r \mid p$ and $r \mid q$ holds $r \mid s$. The theorem is a consequence of (52).

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] H. Heuser. *Lehrbuch der Analysis*. B.G. Teubner Stuttgart, 1990.

[3] Steven H. Weintraub. *Galois Theory*. Springer Verlag, 2 edition, 2009.

Received June 30, 2016