FORMALIZED MATHEMATICS
Vol. 29, No. 1, Pages 1–8, 2021
DOI: 10.2478/forma-2021-0001

sciendo
https://sciendo.com/journal/forma

Derivation of Commutative Rings and the Leibniz Formula for Power of Derivation

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

Summary. In this article we formalize in Mizar [1], [2] a derivation of commutative rings, its definition and some properties. The details are to be referred to [5], [7]. A derivation of a ring, say D, is defined generally as a map from a commutative ring A to A-Module M with specific conditions. However we start with simpler case, namely dom $D =$ rng D. This allows to define a derivation in other rings such as a polynomial ring.

A derivation is a map $D : A \longrightarrow A$ satisfying the following conditions:

(i) $D(x + y) = Dx + Dy$,

(ii) $D(xy) = xDy + yDx$, $\forall x, y \in A$.

Typical properties are formalized such as:

$$D(\sum_{i=1}^{n} x_i) = \sum_{i=1}^{n} Dx_i$$

and

$$D(\prod_{i=1}^{n} x_i) = \sum_{i=1}^{n} x_1 x_2 \cdots Dx_i \cdots x_n \ (\forall x_i \in A).$$

We also formalized the Leibniz Formula for power of derivation D :

$$D^n(xy) = \sum_{i=0}^{n} \binom{n}{i} D^i x D^{n-i} y.$$

Lastly applying the definition to the polynomial ring of A and a derivation of polynomial ring was formalized. We mentioned a justification about compatibility of the derivation in this article to the same object that has treated as differentiations of polynomial functions [3].

MSC: 13B25 13N15 68V20

Keywords: derivation; Leibniz Formula; derivation of polynomial ring

MML identifier: RINGDER1, version: 8.1.11 5.65.1394

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

1. Preliminaries

From now on L denotes an Abelian, left zeroed, add-associative, associative, right zeroed, right complementable, distributive, non empty double loop structure, a, b, c denote elements of L, R denotes a non degenerated commutative ring, and n, m, i, j, k denote natural numbers.

Now we state the propositions:

(1) $n \cdot a + n \cdot b = n \cdot (a + b)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv \$_1 \cdot a + \$_1 \cdot b = \$_1 \cdot (a + b)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(2) $(n \cdot a) \cdot b = a \cdot (n \cdot b)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv (\$_1 \cdot a) \cdot b = a \cdot (\$_1 \cdot b)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(3) $n \cdot (0_L) = 0_L$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv \$_1 \cdot (0_L) = 0_L$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$. For every natural number n, $\mathcal{P}[n]$. □

(4) $0_L \cdot n = 0_L$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv 0_L \cdot \$_1 = 0_L$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$. For every natural number n, $\mathcal{P}[n]$. □

2. Definition of Derivation of Rings and its Properties

From now on D denotes a function from R into R and x, y, z denote elements of R.

Definition of derivation of rings.

Let us consider R. Let Δ be a function from R into R. We say that Δ is derivation if and only if

(Def. 1) for every elements x, y of R, $\Delta(x + y) = \Delta(x) + \Delta(y)$ and $\Delta(x \cdot y) = x \cdot \Delta(y) + y \cdot \Delta(x)$.

Observe that every function from R into R which is derivation is also additive and there exists a function from R into R which is derivation.

A derivation of R is derivation function from R into R. The functor $\operatorname{Der} R$ yielding a subset of $(\Omega_R)^{\Omega_R}$ is defined by the term

(Def. 2) $\{f$, where f is a function from R into $R : f$ is derivation$\}$.

Let us observe that Der R is non empty.

From now on D denotes a derivation of R.

Now we state the propositions:

(5) (i) $D(1_R) = 0_R$, and

(ii) $D(0_R) = 0_R$.

(6) $D(n \cdot x) = n \cdot D(x)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv D(\$_1 \cdot x) = \$_1 \cdot D(x)$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(7) $D(x^{m+1}) = (m+1) \cdot (x^m \cdot D(x))$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv D(x^{\$_1+1}) = (\$_1+1) \cdot (x^{\$_1} \cdot D(x))$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(8) (i) $D^{n+1} = D \cdot (D^n)$, and

(ii) $\operatorname{dom} D =$ the carrier of R, and

(iii) $\operatorname{dom}(D^n) =$ the carrier of R, and

(iv) D^n is a (the carrier of R)-valued function.

(9) $(D^{n+1})(x) = D((D^n)(x))$. The theorem is a consequence of (8).

(10) If $z \cdot y = 1_R$, then $y^2 \cdot D(x \cdot z) = y \cdot D(x) - x \cdot D(y)$.

In the sequel s denotes a finite sequence of elements of the carrier of R and h denotes a function from R into R.

Let us consider R, s, and h. One can check that the functor $h \cdot s$ yields a finite sequence of elements of the carrier of R. Now we state the proposition:

(11) If h is additive, then $h(\sum s) = \sum(h \cdot s)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every h and s such that $\operatorname{len} s = \$_1$ and h is additive holds $h(\sum s) = \sum(h \cdot s)$. $\mathcal{P}[0]$ by [4, (6)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$. □

(12) FORMULA $(f_1 + f_2 + \cdots + f_n)' = f_1' + f_2' + \cdots + f_n'$:
$D(\sum s) = \sum(D \cdot s)$.

Let us consider R, D, and s. The functor $\operatorname{DProd}(D, s)$ yielding a finite sequence of elements of the carrier of R is defined by

(Def. 3) $\operatorname{len} it = \operatorname{len} s$ and for every i such that $i \in \operatorname{dom} it$ holds $it(i) = \prod \operatorname{Replace}(s, i, D(s_{/i}))$.

Now we state the propositions:

(13) If $\operatorname{len} s = 1$, then $\sum \operatorname{DProd}(D, s) = D(\prod s)$.

(14) Let us consider a finite sequence t of elements of the carrier of R. If $\operatorname{len} t \geqslant 1$, then $\sum \mathrm{DProd}(D, t) = D(\prod t)$.
PROOF: Define $\mathcal{P}[$non zero natural number$] \equiv$ for every s such that $\operatorname{len} s = \$_1$ holds $\sum \mathrm{DProd}(D, s) = D(\prod s)$. $\mathcal{P}[1]$. For every non zero natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every non zero natural number k, $\mathcal{P}[k]$. $\square$

3. Proof of the Leibniz Formula for Power of Derivations

The Leibniz formula for power of a derivation of a commutative ring.

Let us consider R, D, and n. Let x, y be elements of R. The functor $\mathrm{LBZ}(D, n, x, y)$ yielding a finite sequence of elements of the carrier of R is defined by

(Def. 4) $\operatorname{len} it = n + 1$ and for every i such that $i \in \operatorname{dom} it$ holds $it(i) = \binom{n}{i -' 1} \cdot (D^{n+1-' i})(x) \cdot (D^{i -' 1})(y)$.

Now we state the propositions:

(15) $\mathrm{LBZ}(D, 0, x, y) = \langle x \cdot y \rangle$.

(16) $\mathrm{LBZ}(D, 1, x, y) = \langle y \cdot D(x), x \cdot D(y) \rangle$.

Let us consider R, D, and m. Let x, y be elements of R. The functor $\mathrm{LBZ0}(D, m, x, y)$ yielding a finite sequence of elements of the carrier of R is defined by

(Def. 5) $\operatorname{len} it = m$ and for every i such that $i \in \operatorname{dom} it$ holds $it(i) = (\binom{m}{i -' 1} + \binom{m}{i}) \cdot (D^{m+1-' i})(x) \cdot (D^{i})(y)$.

The functor $\mathrm{LBZ1}(D, m, x, y)$ yielding a finite sequence of elements of the carrier of R is defined by

(Def. 6) $\operatorname{len} it = m$ and for every i such that $i \in \operatorname{dom} it$ holds $it(i) = \binom{m}{i -' 1} \cdot (D^{m+1-' i})(x) \cdot (D^{i})(y)$.

The functor $\mathrm{LBZ2}(D, m, x, y)$ yielding a finite sequence of elements of the carrier of R is defined by

(Def. 7) $\operatorname{len} it = m$ and for every i such that $i \in \operatorname{dom} it$ holds $it(i) = \binom{m}{i} \cdot (D^{m+1-' i})(x) \cdot (D^{i})(y)$.

Now we state the propositions:

(17) $D(\sum \mathrm{LBZ0}(D, n, x, y)) = \sum D \cdot (\mathrm{LBZ0}(D, n, x, y))$.

(18) $\mathrm{LBZ0}(D, m, x, y) = \mathrm{LBZ1}(D, m, x, y) + \mathrm{LBZ2}(D, m, x, y)$.
PROOF: Set $p = \mathrm{LBZ1}(D, m, x, y)$. Set $q = \mathrm{LBZ2}(D, m, x, y)$. Set $r = \mathrm{LBZ0}(D, m, x, y)$. For every k such that $1 \leqslant k \leqslant \operatorname{len}(p + q)$ holds $(p + q)(k) = r(k)$. $\square$

(19) $\sum \mathrm{LBZ0}(D,n,x,y) = \sum \mathrm{LBZ1}(D,n,x,y) + \sum \mathrm{LBZ2}(D,n,x,y)$. The theorem is a consequence of (18).

(20) $D \cdot (\mathrm{LBZ0}(D,n,x,y)) = (\mathrm{LBZ2}(D,n+1,x,y))_{\restriction n+1} + (\mathrm{LBZ1}(D,n+1,x,y))_{\restriction 1}$.
Proof: Set $p = \mathrm{LBZ2}(D,n+1,x,y)$. Set $q = \mathrm{LBZ1}(D,n+1,x,y)$. Set $r = \mathrm{LBZ0}(D,n,x,y)$. Reconsider $p_1 = p_{\restriction n+1}$ as a finite sequence of elements of the carrier of R. Reconsider $q_1 = q_{\restriction 1}$ as a finite sequence of elements of the carrier of R. For every i such that $1 \leqslant i \leqslant \operatorname{len} D \cdot r$ holds $(D \cdot r)(i) = (p_1 + q_1)(i)$. □

(21) $\sum D \cdot (\mathrm{LBZ0}(D,n,x,y)) = -(\mathrm{LBZ1}(D,n+1,x,y))_{/1} + \sum \mathrm{LBZ0}(D,n+1,x,y) - (\mathrm{LBZ2}(D,n+1,x,y))_{/n+1}$. The theorem is a consequence of (20) and (19).

(22) $\mathrm{LBZ}(D,n+1,x,y) = (\langle (D^{n+1})(x) \cdot y \rangle ^\frown \mathrm{LBZ0}(D,n,x,y)) ^\frown \langle x \cdot (D^{n+1})(y) \rangle$.
Proof: Set $p = \mathrm{LBZ}(D,n+1,x,y)$. Set $q = \mathrm{LBZ0}(D,n,x,y)$. Set $r = (\langle (D^{n+1})(x) \cdot y \rangle ^\frown q) ^\frown \langle x \cdot (D^{n+1})(y) \rangle$. For every k such that $1 \leqslant k \leqslant \operatorname{len} p$ holds $p(k) = r(k)$. □

(23) $\sum((\langle (D^{n+1})(x) \cdot y \rangle ^\frown \mathrm{LBZ0}(D,n,x,y)) ^\frown \langle x \cdot (D^{n+1})(y) \rangle) = (D^{n+1})(x) \cdot y + \sum \mathrm{LBZ0}(D,n,x,y) + x \cdot (D^{n+1})(y)$.

(24) $D(\sum \mathrm{LBZ}(D,n+1,x,y)) = \sum \mathrm{LBZ}(D,n+2,x,y)$. The theorem is a consequence of (9), (21), (11), (22), and (23).

(25) The Leibniz formula for power of derivation:
$(D^n)(x \cdot y) = \sum \mathrm{LBZ}(D,n,x,y)$. The theorem is a consequence of (16), (9), (24), and (15).

4. Example of Derivation of Polynomial Ring over a Commutative Ring

Let us consider R. Let f be a function from PolyRing(R) into PolyRing(R) and p be an element of the carrier of PolyRing(R). Observe that the functor $f(p)$ yields an element of the carrier of PolyRing(R). Let R be a ring. The functor Der1(R) yielding a function from PolyRing(R) into PolyRing(R) is defined by

(Def. 8) for every element f of the carrier of PolyRing(R) and for every natural number i, $it(f)(i) = (i+1) \cdot f(i+1)$.

Let us consider R. One can verify that Der1(R) is additive.

In the sequel R denotes an integral domain and f, g denote elements of the carrier of PolyRing(R).

Now we state the proposition:

(26) Let us consider an element f of the carrier of PolyRing(R), and a polynomial f_1 over R. Suppose $f = f_1$ and f_1 is constant. Then $(\mathrm{Der1}(R))(f) = \mathbf{0}.R$.

PROOF: For every element i of $\mathbb{N}$, $(\mathrm{Der1}(R))(f)(i) = (\mathbf{0}.R)(i)$. $\square$

In the sequel a denotes an element of R. Now we state the propositions:

(27) Let us consider a natural number i, and an element p of the carrier of PolyRing(R). Then $((a \restriction R) * p)(i) = a \cdot p(i)$.

(28) Let us consider elements f, g of the carrier of PolyRing(R), and an element a of R. Suppose $f = a \restriction R$. Then $(\mathrm{Der1}(R))(f \cdot g) = (a \restriction R) * (\mathrm{Der1}(R))(g)$.
PROOF: For every natural number n, $(\mathrm{Der1}(R))(f \cdot g)(n) = ((a \restriction R) * (\mathrm{Der1}(R))(g))(n)$. $\square$

Let us consider an element f of the carrier of PolyRing(R) and an element a of R. Now we state the propositions:

(29) If $f = \mathrm{anpoly}(a, 0)$, then $(\mathrm{Der1}(R))(f) = \mathbf{0}.R$.
PROOF: For every element n of $\mathbb{N}$, $(\mathrm{Der1}(R))(f)(n) = (\mathbf{0}.R)(n)$. $\square$

(30) If $f = \mathrm{anpoly}(a, 1)$, then $(\mathrm{Der1}(R))(f) = \mathrm{anpoly}(a, 0)$.
PROOF: For every element n of $\mathbb{N}$, $(\mathrm{Der1}(R))(f)(n) = (\mathrm{anpoly}(a, 0))(n)$. $\square$

(31) Let us consider polynomials p, q over R. Suppose $p = \mathrm{anpoly}(1_R, 1)$. Let us consider an element i of $\mathbb{N}$. Then

(i) $(p * q)(i + 1) = q(i)$, and

(ii) $(p * q)(0) = 0_R$.

PROOF: For every element i of $\mathbb{N}$, $(p * q)(i + 1) = q(i)$. Consider F_1 being a finite sequence of elements of the carrier of R such that $\mathrm{len}\, F_1 = 0 + 1$ and $(p * q)(0) = \sum F_1$ and for every element k of $\mathbb{N}$ such that $k \in \mathrm{dom}\, F_1$ holds $F_1(k) = p(k -' 1) \cdot q(0 + 1 -' k)$. $\square$

(32) Let us consider elements f, g of the carrier of PolyRing(R). Suppose $f = \mathrm{anpoly}(1_R, 1)$. Then $(\mathrm{Der1}(R))(f \cdot g) = (\mathrm{Der1}(R))(f) \cdot g + f \cdot (\mathrm{Der1}(R))(g)$.
PROOF: Reconsider $d_1 = (\mathrm{Der1}(R))(f)$, $d_2 = (\mathrm{Der1}(R))(g)$ as a polynomial over R. Reconsider $f_1 = f$, $g_1 = g$ as a polynomial over R. For every element i of $\mathbb{N}$, $(\mathrm{Der1}(R))(f \cdot g)(i) = (d_1 * g_1 + f_1 * d_2)(i)$. $\square$

(33) Let us consider constant elements f, g of the carrier of PolyRing(R). Then $(\mathrm{Der1}(R))(f \cdot g) = (\mathrm{Der1}(R))(f) \cdot g + f \cdot (\mathrm{Der1}(R))(g)$. The theorem is a consequence of (29).

(34) Let us consider elements f, g of the carrier of PolyRing(R). Suppose f is constant. Then $(\mathrm{Der1}(R))(f \cdot g) = (\mathrm{Der1}(R))(f) \cdot g + f \cdot (\mathrm{Der1}(R))(g)$. The theorem is a consequence of (29) and (28).

(35) Let us consider elements x, y of the carrier of PolyRing(R). Suppose x is not constant. Then $(\mathrm{Der1}(R))(x \cdot y) = (\mathrm{Der1}(R))(x) \cdot y + x \cdot (\mathrm{Der1}(R))(y)$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every elements f, g of the carrier of PolyRing(R) for every elements f_0, g_0 of the carrier of PolyRing(R) such

that $f_0 = f$ and $g_0 = g$ and $\deg f_0 - 1 = \$_1$ holds $(\mathrm{Der1}(R))(f_0 \cdot g_0) = (\mathrm{Der1}(R))(f_0) \cdot g_0 + f_0 \cdot (\mathrm{Der1}(R))(g_0)$. 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 [8, (4)]. For every natural number n, $\mathcal{P}[n]$. □

(36) $(\mathrm{Der1}(R))(f \cdot g) = (\mathrm{Der1}(R))(f) \cdot g + f \cdot (\mathrm{Der1}(R))(g)$. The theorem is a consequence of (35) and (34).

Let us consider R. Let us observe that $\mathrm{Der1}(R)$ is derivation.

Now we state the propositions:

(37) Let us consider an element x of $\mathrm{PolyRing}(R)$, and a polynomial f over R. If $x = f$, then for every natural number n, $x^n = f^n$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv x^{\$_1} = f^{\$_1}$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [6, (19)]. For every natural number n, $\mathcal{P}[n]$. □

(38) Let us consider an element x of $\mathrm{PolyRing}(R)$. Suppose $x = \mathrm{anpoly}(1_R, 1)$. Then there exists an element y of $\mathrm{PolyRing}(R)$ such that

(i) $y = \mathrm{anpoly}(1_R, n)$, and

(ii) $(\mathrm{Der1}(R))(x^{n+1}) = (n+1) \cdot y$.

The theorem is a consequence of (30), (37), and (7).

From now on p denotes a polynomial over $\mathbb{R}_{\mathrm{F}}$.

Let us consider p. The functor p' yielding a sequence of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 9) for every natural number n, $it(n) = p(n+1) \cdot (n+1)$.

Now we state the proposition:

(39) Let us consider an element p_0 of $\mathrm{PolyRing}(\mathbb{R}_{\mathrm{F}})$, and a polynomial p over $\mathbb{R}_{\mathrm{F}}$. If $p_0 = p$, then $p' = (\mathrm{Der1}(\mathbb{R}_{\mathrm{F}}))(p_0)$.

Proof: For every n, $(p')(n) = (\mathrm{Der1}(\mathbb{R}_{\mathrm{F}}))(p_0)(n)$. □

References

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

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

[3] Artur Korniłowicz. Differentiability of polynomials over reals. *Formalized Mathematics*, 25(**1**):31–37, 2017. doi:10.1515/forma-2017-0002.

[4] Artur Korniłowicz and Christoph Schwarzweller. The first isomorphism theorem and other properties of rings. *Formalized Mathematics*, 22(**4**):291–301, 2014. doi:10.2478/forma-2014-0029.

[5] Hideyuki Matsumura. *Commutative Ring Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2nd edition, 1989.

[6] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.

[7] Masayoshi Nagata. *Theory of Commutative Fields*, volume 125 of *Translations of Mathematical Monographs*. American Mathematical Society, 1985.

[8] Christoph Schwarzweller. On roots of polynomials and algebraically closed fields. *Formalized Mathematics*, 25(**3**):185–195, 2017. doi:10.1515/forma-2017-0018.

Accepted March 30, 2021