# FOUNDATIONS OF POLYNOMIAL THEORY IN NONCOMMUTATIVE DIVISION RINGS

**Ngo Le Hong Phuc** (1)

*(1) Faculty of Education, Thu Dau Mot University*
*Corresponding author's email: phucnlh@tdmu.edu.vn*

**DOI: 10.37550/tdmu.EJS/2026.01.706**

## Article Info

**Volume:** 8
**Issue:** 1
**March:** 2026
**Received:** Nov. 16th, 2025
**Accepted:** Jan. 20h, 2026
**Page No:** 176-183

## Abstract

This paper develops a systematic framework for polynomials over division algebras, focusing on degree, the Euclidean algorithm, left and right divisibility, greatest common divisors, and minimal polynomials. The relations among these notions are clarified, and conditions ensuring agreement between the left and right constructions are identified. The results extend key features of the commutative theory to the noncommutative setting.

**Keywords:** division algebra; Euclidean algorithm; left and right GCDs; minimal polynomials; noncommutative polynomials; quaternion algebra.

## 1. Introduction

Polynomials are fundamental objects in algebra, playing a central role in many mathematical theories and applications. In the classical setting over commutative fields, polynomial theory is well established, with clear and precise notions of degree, divisibility, the Euclidean algorithm. When these concepts are extended to more general algebraic structures such as division rings, where multiplication is not necessarily commutative, many familiar properties no longer hold and must therefore be examined again and formulated in a suitable non-commutative framework.

In a noncommutative setting, the distinction between left and right operations becomes essential. Concepts such as division, common divisors must be treated separately on the left and on the right. For example, a polynomial may admit different left and right divisors, and the Euclidean algorithm must be modified to account for this asymmetry. A clearer understanding of the structure and behavior of polynomials over division rings is therefore fundamental for the development of noncommutative algebra.

This paper presents a systematic study of fundamental notions concerning polynomials over division rings. We begin by describing the degree of a polynomial in this context, and then examine left and right Euclidean divisions, left and right divisibility, and greatest common divisors. By clarifying these basic concepts, the paper not only extends classical polynomial theory but also provides a conceptual foundation for future work in noncommutative ring theory, particularly in the study of linear operators, and skew polynomial rings.

## 2. Literature Review

Ore (1933) introduced skew polynomial rings in which the indeterminate does not commute with the coefficients but satisfies a twisted commutation rule determined by a ring endomorphism. Subsequent contributions by Jacobson (1956) and Lam (2001) developed and applied this framework to modules and non-commutative ring theory. Cohn's monograph "Free Rings and Their Relations" (1971) further extended the analysis by investigating free ideal rings, factorization algorithms and generalized Euclidean-type conditions in non-commutative settings. Recent surveys, such as Smertnig (2016), provide comprehensive discussions on factorizations in non-commutative rings and highlight the strong structural assumptions involved. Explicit computations in concrete division algebras remain limited, with only a few examples presented in recent work such as Gluesing-Luerssen (2019).

This paper addresses the remaining gap by systematically developing the notions of polynomial degree, left and right division, divisibility, and greatest common divisors in the setting of division algebras. Constructive versions of the left and right Euclidean algorithms are given, together with criteria for existence and uniqueness of quotients and remainders.

## 3. Methods

This paper adopts a constructive and example driven approach to studying polynomial theory over non-commutative division algebras. We begin by defining fundamental notions such as polynomial degree, left and right division, left and right divisors, and greatest common divisors in non-commutative rings.

We then develop explicit versions of the left and right Euclidean algorithms, establishing precise conditions for the existence and uniqueness of quotients and remainders. These algorithms enable the computation of left and right greatest common divisors without relying on the Ore condition.

The remainder of the paper is organized as follows. In Section 4, we state and prove the main result of the paper, and we construct an example to illustrate the applicability of the theoretical result.

## 4. Results

### *4.1. Polynomials over division rings*

Let $K \subset D$ be a not necessarily commutative division ring and let $t$ be an indeterminate assumed to commute with all elements of $K$. Define

$$K[t] = \left\{ f(t) = \sum_{0 \le i < \infty} a_i t^i \middle| a_i \in K \right\}$$

as the ring of polynomials over $K$ with addition and multiplication defined in the same manner as for polynomials over commutative rings. Since $t$ commutes with elements of $K$, any polynomial in $K[t]$ can be written as $f(t) = \sum_{0 \le i < \infty} a_i t^i$ or equivalently as

$f(t)=\sum_{0\le i<\infty} t^i a_i$, with $a_i \in K$. Now, consider a polynomial $f(t)=\sum_{i=0}^{n} a_i t^i \in K[t]$ and an element $\alpha \in D$. The element $\sum_{i=0}^{n} a_i \alpha^i \in D$ is called the **right value** of $f(t)$ at $\alpha$, denoted by $f(\alpha)$. However, if $f(t)$ is written as $f(t)=\sum_{i=0}^{n} t^i a_i$, the corresponding element $\sum_{i=0}^{n} \alpha^i a_i \in D$ is called the **left value** of $f(t)$ at $\alpha$, and is denoted by $f_l(\alpha)$. We remark that the left and right values of $f(t)$ at $\alpha$ may differ, since $K$ and $D$ are not necessarily commutative rings.

Let $D$ be a division ring and let the polynomial

$$f(t)=a_0+a_1t+\ldots+a_nt^n \in D[t],$$

with $a_n \neq 0$, $n \geq 0$. Then, $n$ is called the *degree* of $f(t)$ and is denoted by $\deg(f)=n$. For convenience, we adopt the following conventions:

$$\deg(0)=-\infty;\ -\infty<n;-\infty+n=-\infty.$$

Remark 4.1.

1. For polynomials over a division ring, the following degree identities hold:

$$\deg(f+g)\le \max\{\deg(f),\deg(g)\},\ \deg(fg)=\deg(f)+\deg(g)$$

2. If $K$ is a division ring, then the polynomial ring $K[t]$ has no zero divisors.

### *4.2. Euclidean Division Algorithm for Polynomials over Division Rings*

Given a pair of division rings $K \subset D$. We say that $\alpha \in D$ is a *right root (resp., left root)* of a polynomial $f(t) \in K[t]$ if $f(\alpha)=0$ (resp., $f_l(\alpha)=0$). We now proceed to prove the theorem on the Euclidean division algorithm in the setting of division rings.

Theorem 4.2**.** (Euclidean Division Algorithm). Let $f(t),g(t) \in D[t]$, where $g(t) \neq 0$. Then, there exist unique polynomials $q(t),r(t),h(t),s(t) \in D[t]$, with $\deg(r)<\deg(g)$ and $\deg(s)<\deg(g)$, such that

$$f(t)=g(t)q(t)+r(t) \quad \text{and} \quad f(t)=h(t)g(t)+s(t).$$

*Proof.* First, we will prove the existence of $q(t)$ and $r(t)$ in $D[t]$ such that

$$f(t)=g(t)q(t)+r(t)$$

with $\deg(r)<\deg(g)$. Indeed, if $f(t)=0$, then the theorem holds with $q(t)=r(t)=0$.

If $0\le \deg(f)<\deg(g)$, then the theorem is satisfied with $q(t)=0$ and $r(t)=f(t)$.

If $\deg(f)\ge \deg(g)$, then we prove the existence of $q(t)$ and $r(t)$ by induction on the degree of $f(t)$. In fact, if $\deg(f)=0$, then $\deg(g)=0$. Hence, $f(t)=a$ and $g(t)=b$ are nonzero elements in the division ring D. Therefore, the theorem holds with $q(t)=b^{-1}a$ and $r(t)=0$.

Now, suppose the theorem holds for all polynomials $f(t)$ with $\deg(f) < n$. We will prove the theorem for the polynomial $f(t)$ of degree $n$. Assume that $f(t) = a_0 + a_1 t + ... + a_n t^n$, $a_n \neq 0$ and $g(t) = b_0 + b_1 t + ... + b_m t^m, b_m \neq 0$, with m ≤ n. Since $D$ is a division ring and $b_m \neq 0$, the element $b_m$ is invertible. Multiply $g(t)$ on the right by $b_m^{-1} a_n t^{n-m}$, we get $g(t) b_m^{-1} a_n t^{n-m} = a_n t^n + a_n t^{n-1} + ... + b_0 b_m^{-1} a_n t^{n-m}$. Then, the polynomial $h(t) = f(t) - g(t) b_m^{-1} a_n t^{n-m}$ has degree less than $n$. According to the inductive hypothesis for $h(t)$ and $g(t)$, there exist $q_1(t)$ and $r(t)$ such that

$$f(t) - g(t) b_m^{-1} a_n t^{n-m} = g(t) q_1(t) + r(t), \deg(r) < \deg(g).$$

Therefore, $f(t) = g(t)(b_m^{-1} a_n t^{n-m} + q_1(t)) + r(t)$, with $\deg(r) < \deg(g)$. Hence, for all polynomials $f(t), g(t) \in D[t]$, with $g(t) \neq 0$, there always exist $q(t)$ and $r(t)$ such that $f(t) = g(t)q(t) + r(t), \deg(r) < \deg(g)$. Next, we will prove that $q(t)$ and $r(t)$ are unique. Suppose $q'(t)$ and $r'(t)$ are two polynomials satisfying $f(t) = g(t)q'(t) + r'(t)$, with $\deg(r') < \deg(g)$. Then we have $g(t)q(t) + r(t) = g(t)q'(t) + r'(t)$ or equivalently $g(t)(q(t) - q'(t)) = r'(t) - r(t)$. If $r'(t) - r(t) = 0$, then $g(t)(q(t) - q'(t)) = 0$. Since $g \neq 0$, it follows that $q(t) = q'(t)$. Suppose now that $r'(t) \neq r(t)$. Then

$$\deg(r' - r) = \deg(g(q - q')) = \deg(g) + \deg(q - q') \geq \deg(g).$$

On the other hand, $\deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(g)$, which is a contradiction. Hence $r'(t) = r(t)$. If one of the polynomials $r(t)$ or $r'(t)$ is zero, the above argument remains valid, because in that case $\deg(r' - r) = \deg(r) < \deg(g)$ if $r'(t) = 0$, or $\deg(r' - r) = \deg(r') < \deg(g)$ if $r(t) = 0$. Therefore, we have $g(t)(q(t) - q'(t)) = 0$. Since $g \neq 0$, it follows that $q(t) - q'(t) = 0$, and hence $q(t) = q'(t)$.

### *4.3. Left (Right) Greatest Common Divisor*

Let $D$ be a non-commutative division ring and consider the polynomial ring $D[t]$.

Let $h(t), f(t) \in D[t]$. Then $h(t)$ is a *left divisor* (*resp., right divisor*) of $f(t)$ if there exists a polynomial $g(t) \in D[t]$ such that $f(t) = h(t)g(t)$ (*resp.*, $f(t) = g(t)h(t)$). If $d(t) \in D[t]$ is a left (resp., right) divisor of both $f(t)$ and $g(t)$, then $d(t)$ is called a *common left (resp., common right) divisor* of $f(t)$ and $g(t)$. Among all such divisors, a polynomial $d(t)$ is said to be a *left greatest common divisor* (resp., *right greatest common divisor*) of $f(t)$ and $g(t)$ if every left (resp., right) common divisor of $f(t)$ and $g(t)$ is also a left (resp., right) divisor of $d(t)$. This polynomial is denoted by

$$d(t) = (f(t), g(t))_l \ (resp.,\ d(t) = (f(t), g(t))_r).$$

Two polynomials $f(t), g(t) \in D[t]$ are called *left relatively prime* (resp., *right relatively prime*) if their left (resp., right) greatest common divisor equals 1.

Remark 4.3.

1. If $g(t) \in D[t]$ is a left divisor of $f(t) \in D[t]$, then it does not necessarily follow that $g(t)$ is a right divisor of $f(t)$. For example, in the quaternion algebra H, consider

$$f(t) = (t-i)j,\ g(t) = t-i.$$

Since $f(t) = g(t)j,$ the polynomial $g(t)$ is a left divisor of $f(t).$ Assume that $g(t)$ is also a right divisor of $f(t)$. Then, there exists $k(t) \in \mathrm{H}[t]$ such that $f(t) = k(t)g(t)$. We compute

$$f(t) = (t-i)j = tj - ij = jt - k.$$

Because $\deg(f) = \deg(g) = 1,$ we must have $\deg(k) = 0.$ Hence, $k(t) = c \in \mathrm{H}.$ Substituting gives

$$(t-i)j = c(t-i),$$

that is,

$$jt - k = ct - ci.$$

Comparing coefficients yields $c = j$ and $-ci = -k.$ Substituting $c = j$ into the second equality gives $k = -k,$ which is impossible. Therefore $g(t)$ is **not** a right divisor of $f(t)$.

2. Two left greatest common divisors of $f(t)$ and $g(t)$ differ by a left invertible element. Indeed, if $d(t)$ and $d'(t)$ are two left greatest common divisors of $f(t)$ and $g(t)$, then $d(t)$ is a left divisor of $d'(t)$ and $d'(t)$ is a left divisor of $d(t)$. Hence, $d'(t) = d(t)\ k(t)$ and $d(t) = d'(t)h(t).$ It follows that $d'(t) = d'(t)h(t)k(t)$, that is, $d'(t)(h(t)k(t) - 1) = 0.$ Since $d'(t) \neq 0$, by Remark 4.1, we have $h(t)k(t) = 1.$ Thus, $k(t)$ is left invertible. The argument for the right greatest common divisor is analogous.

Proposition 4.4**.** Let $D$ be a division ring and $f(t) \in D[t]$. Then,

$$(f(t), 0)_l = f(t) \text{ (resp., } (f(t), 0)_r = f(t).$$

*Proof.* It is clear that $f(t)$ is a left common divisor of $f(t)$ and 0. Suppose $d(t)$ is any left common divisor of $f(t)$ and 0. Then, $d(t)$ divides $f(t)$. Hence, $f(t)$ is the left greatest common divisor of $f(t)$ and 0. The proof for the second case is similar.

Lemma 4.5. Let $D$ be a division ring, and $f(t), g(t), q(t), r(t), q'(t), r'(t) \in D[t]$ satisfy

$$f(t) = g(t)q(t) + r(t)\ (resp.,\ f(t) = q'(t)g(t) + r'(t)).$$

Then,

$$(f(t), g(t))_l = (g(t), r(t))_l\ (resp.(f(t), g(t))_r = (g(t), r'(t))_r).$$

*Proof.* We prove the first case. The other one can be shown in a completely similar way. Assume that $(f(t), g(t))_l = d(t)$ and $(g(t), r(t))_l = d'(t).$ It follows that $d(t)$ is a left

divisor of both $f(t)$ and $g(t)$. Hence, there exist $f_1(t), g_1(t) \in D[t]$ such that $f(t) = d(t) f_1(t)$ and $g(t) = d(t) g_1(t)$. Then,

$$r(t) = f(t) - g(t)q(t) = d(t) f_1(t) - d(t) g_1(t) q(t) = d(t)(f_1(t) - g_1(t)q(t)).$$

Thus, $d(t)$ is also a left divisor of $r(t)$, which means that $d(t)$ is a common left divisor of $g(t)$ and $r(t)$. Consequently, $d(t)$ divides $d'(t)$ on the left. By a similar argument, $d'(t)$ divides $d(t)$ on the left as well. By Remark 4.3, $d(t)$ and $d'(t)$ differ by an invertible element. Therefore, if $d'(t)$ is the greatest common left divisor of $g(t)$ and $r(t)$, then $d(t)$ is also, and hence $(f(t), g(t))_l = (g(t), r(t))_l$.

Theorem 4.6**.** Let $D$ be a division ring and $f(t), g(t) \in D[t]$. If $d(t) \in D[t]$ is a greatest common left divisor (resp., greatest common right divisor) of $f(t)$ and $g(t)$, then there exist polynomials $u(t), v(t), z(t), w(t) \in D[t]$ such that

$$f(t)u(t) + g(t)v(t) = d(t) (resp., z(t) f(t) + w(t) g(t) = d(t)).$$

*Proof.* By the Euclidean division algorithm, for any two polynomials $f(t), g(t) \in D[t]$ with $g(t) \neq 0$, there exist unique $q_1(t), r_1(t) \in D[t]$ such that $f(t) = g(t)q_1(t) + r_1(t)$, where $\deg(r_1) < \deg(g)$. If $r_1(t) \neq 0$, then applying the Euclidean division to $g(t)$ and $r_1(t)$, we obtain

$$g(t) = r_1(t)q_2(t) + r_2(t),$$

with $\deg(r_2) < \deg(r_1)$.

If $r_2(t) \neq 0$, then we continue by dividing $r_1(t)$ by $r_2(t)$, that is,

$$r_1(t) = r_2(t)q_3(t) + r_3(t),$$

with $\deg(r_3) < \deg(r_2)$. Proceeding in this manner, we obtain

$$r_{k-2}(t) = r_{k-1}(t)q_k(t) + r_k(t),$$

with $\deg(r_k) < \deg(r_{k-1})$. Since the sequence of natural numbers

$$\deg(g) > \deg(r_1) > \deg(r_2) > ...$$

cannot decrease indefinitely, the process must terminate after finitely many steps. Thus, at some step we reach a remainder equal to zero. If $r_n(t)$ is the last nonzero remainder, then

$$r_{n-2}(t) = r_{n-1}(t)q_n(t) + r_n(t),$$
$$r_{n-1}(t) = r_n(t)q_{n+1}$$

By Lemmas 4.5 and Proposition **4.4**, we have

$$(f(t), g(t))_l = (g(t), r_1(t))_l = (r_1(t), r_2(t))_l = ... = (r_{n-1}(t), r_n(t))_l = (r_n(t), 0)_l = r_n(t).$$

Hence, $r_n(t) = d(t).$ Now consider the chain of left Euclidean divisions:

$$f(t) = g(t)q_1(t) + r_1(t),\ \deg(r_1) < \deg(g)$$
$$g(t) = r_1(t)q_2(t) + r_2(t), \deg(r_2) < \deg(r_1),$$
$$r_1(t) = r_2(t)q_3(t) + r_3(t), \deg(r_3) < \deg(r_2),$$
$$\ldots$$
$$r_{n-1}(t) = r_n(t)q_n(t) + r_n(t), \deg(r_n) < \deg(r_{n-1})$$
$$r_{n-1}(t) = r_n(t)q_{n+1}(t)$$

We shall now show that there exist polynomials $u_k(t), v_k(t)$ such that $r_k(t) = f(t)u_k(t) + g(t)v_k(t),$ for each integer $k,$ with $1 \le k \le n.$ Indeed, from the first equation we have $r_1(t) = f(t).1 + g(t)(-q_1(t)),$ so $u_1(t) = 1$ and $v_1(t) = -q_1(t).$ Similarly, from the second equation, we have

$$r_2(t) = g(t) - r_1(t)q_2(t) = f(t)(-q_2(t)) + g(t)(1 + q_1(t)q_2(t)),$$

hence $u_2(t) = -q_2(t)$ and $v_2(t) = 1 + q_1(t)q_2(t).$ Assume inductively that $u_i(t)$ and $v_i(t)$ satisfy $r_i(t) = f(t)u_i(t) + g(t)v_i(t),$ for $i = 1,2,\ldots,k-1.$ Then,

$$r_k(t) = r_{k-2}(t) - r_{k-1}(t)q_k(t) = f(t)(u_{k-2}(t) - u_{k-1}(t)q_k(t))) + g(t)(v_{k-2}(t) - v_{k-1}(t)q_k(t)).$$

Thus, we need

$$u_k(t) = u_{k-2}(t) - u_{k-1}(t)q_k(t) \qquad (4.1)$$

$$v_k(t) = v_{k-2}(t) - v_{k-1}(t)q_k(t) \qquad (4.2)$$

for all $k > 2.$ Now, if we define $u_1(t), v_1(t), u_2(t), v_2(t)$ as above, then we may use (4.1) and (4.2) to define $u_k(t)$ and $v_k(t)$ for larger values of $k.$ Moreover, if we set $u_{-1}(t) = 1, u_0(t) = 0, v_{-1}(t) = 0$ and $v_0(t) = 1,$ then (4.1) and (4.2) hold for every $k \ge 1$ and $r_k(t) = f(t)u_k(t) + g(t)v_k(t)$ for all $k > 2.$ Hence, there exist $u(t) = u_n(t)$ and $v(t) = v_n(t)$ such that $d(t) = f(t)u_n(t) + g(t)v_n(t).$ The proof is entirely analogous in the case when $d(t) \in D[t]$ is a right greatest common divisor of $f(t)$ and $g(t).$ There exist polynomials $z(t), w(t) \in D[t]$ with $z(t)f(t) + w(t)g(t) = d(t),$ with the understanding that all divisions involved are right divisions.

### *4.4. Example*

In this section, we illustrate the Euclidean algorithm in a non-commutative division ring by computing the left greatest common divisor of two polynomials in the quaternion polynomial ring $H[t]$.

Consider

$$f(t) = t^3 + (i + j)t + k,\ \ g(t) = t^2 + jt + i$$

Performing left division of $f(t)$ by $g(t)$ yields

$$f(t) = g(t)q_1(t) + r_1(t),\ \ q_1(t) = t - j \text{ and } r_1(t) = (j-1)t + 2k,$$

With $\deg(r_1) < \deg(g).$ Next, dividing $g(t)$ on the left by $r_1(t)$ produces

$$g(t) = r_1(t)q_2(t) + r_2(t),\ q_2(t) = -\frac{1}{2}(1+j)t + \left(\frac{1}{2} - \frac{1}{2}j - k\right),\ r_2 = -2 - k,$$

Where $r_2$ is a nonzero constant quaternion. Finally, dividing $r_1(t)$ on the left by $r_2$ gives

$$r_1(t) = r_2 q_3(t) + 0,\ q_3(t) = \frac{2 - i - 2j - k}{5}t + \frac{-2 - 4k}{5}.$$

Since the last nonzero remainder $r_2$ is invertible in $H,$ the algorithm terminates. Therefore, the left greatest common divisor of $f(t)$ and $g(t)$ is a unit in $H.$ Hence, $(f(t), g(t))_l$ is trivial up to left multiplication by a unit.

## 5. Conclusions

This paper has developed the fundamental concepts and results concerning polynomials over division rings, with particular emphasis on the distinction between left and right operations in division, divisibility. The discussion clarifies how these non-commutative aspects influence the structure and properties of polynomials, and provides a rigorous framework for further study of algebraic elements, factorization, and coprimality in division rings.

## References

Cohn, P. M. (1971). *Free rings and their relations*. Academic Press.

Gluesing-Luerssen, H. (2019). *On skew polynomials over division rings*. *Journal of Algebra and Its Applications*, 18(10), 1–36.

Giesbrecht, M. (1998). *Factoring in skew-polynomial rings over finite fields*. *Journal of Symbolic Computation*, 26(4), 463–486.

Jacobson, N. (1956). *Structure of rings* (2nd ed.). American Mathematical Society.

Lam, T. Y. (2001). *A first course in noncommutative rings* (2nd ed.). Springer.

Lam, T. Y., & Leroy, A. (2007). *Wedderburn polynomials over division rings*. In S. Caenepeel & F. Van Oystaeyen (Eds.), *Hopf algebras and generalizations* (pp. 125–146). American Mathematical Society.

Ore, Ø. (1933). *Theory of noncommutative polynomials*. *Annals of Mathematics*, 34(3), 480–508.

Smertnig, D. (2016). *Factorizations of elements in noncommutative rings: A survey*. https://math.smertnig.at/paper/survey.pdf