DERIVATIVE OF AN IDEAL IN A NUMBER RING

Raj Kumar Mistri[1]
Department of Mathematics, Indian Institute of Technology, Patna, Bihar, India
itsrajhans@gmail.com

Ram Krishna Pandey[2]
Department of Mathematics, Indian Institute of Technology , Patna, Bihar, India
ram@iitp.ac.in

Received: 9/7/13, Revised: 12/11/13, Accepted: 3/31/14, Published: 5/26/14

Abstract

The derivative of an ideal in a number ring is defined and the relation between the ideal derivative and the arithmetic derivative of a number in $\mathbb{Z}$ is discussed. Some simple ideal differential equations are also studied. Further, the definition of the ideal derivative is extended to the derivative of a fractional ideal in a number ring. Again, the relation between the fractional ideal derivative and the arithmetic derivative of a rational number is discussed.

1. Introduction

Ufnarovski and Åhlander [4] define the arithmetic derivative for the integers and the rational numbers. They further define the arithmetic derivative in a unique factorization domain (UFD). For the sake of convenience, both of the definitions are given below.

1.1. Arithmetic Derivative in $\mathbb{Z}$ and in $\mathbb{Q}$

Let $n \in \mathbb{Z}$. The arithmetic derivative of n, denoted by n', is defined [1, 4] as follows:

(i) $0' = 1' = (-1)' := 0$;

(ii) If $n = up_1p_2 \cdots p_k$, where $u = \pm 1$ and the p_i's are primes (some of them may be equal), then

$$n' := u \sum_{j=1}^{k} p_1 \cdots p_{j-1} \hat{p}_j \cdots p_k,$$

where in each summand the term $\hat{p}_j$ is deleted.

[1]Research fellowship is supported by the University Grants Commission of India
[2]Corresponding author

The arithmetic derivative satisfies the following properties:

(i) $p' = 1$ for all primes p;

(ii) $(-n)' = -n'$ for all $n \in \mathbb{Z}$;

(iii) $(mn)' = mn' + m'n$ for all $m, n \in \mathbb{Z}$ (we will refer to this as "the Leibnitz rule").

The arithmetic derivative of $\frac{m}{n} \in \mathbb{Q}$, denoted by $(\frac{m}{n})'$, is defined [4] by

$$\left(\frac{m}{n}\right)' := \frac{m'n - mn'}{n^2}.$$

1.2. Arithmetic Derivative in a UFD

Let D be a UFD and $\mathcal{P}$ be a set of positive atoms of D (irreducible elements of D) such that each atom of D is an associate of a unique element of $\mathcal{P}$. Further, let $\mathcal{U}$ be the set of units of D. Given $a \in D$, the arithmetic derivative of a, denoted by a', is defined [1, 4] as follows:

(i) $0' := 0$ and $a' := 0$ for all $a \in \mathcal{U}$;

(ii) If $a = up_1p_2 \cdots p_k$, where $p_i \in \mathcal{P}$ for $i = 1, 2 \ldots, k$ and $u \in \mathcal{U}$, then

$$a' := u \sum_{j=1}^{k} p_1 \cdots p_{j-1} \hat{p}_j \cdots p_k,$$

where in each summand the term $\hat{p}_j$ is deleted.

Since the arithmetic derivative in a UFD is defined for a chosen set $\mathcal{P}$ of positive atoms, the arithmetic derivative depends on $\mathcal{P}$. This is illustrated in Example 1. Hence to be precise, we write $a'_{\mathcal{P}}$ to denote the arithmetic derivative of a corresponding to the set $\mathcal{P}$ of positive atoms.

The arithmetic derivative in a UFD satisfies the following properties:

(i) $p' = 1$ for all primes $p \in \mathcal{P}$;

(ii) $(ua)' = ua'$ for all $u \in \mathcal{U}$ and $a \in D$;

(iii) $(ab)' = ab' + a'b$ for all $a, b \in D$.

Example 1. Let $D = \mathbb{Z}$, $\mathcal{P}_1$ be the set of positive primes and $\mathcal{P}_2 = \{2, -3, 5, -7, \ldots\}$. Then

$$6'_{\mathcal{P}_1} = (2 \cdot 3)' = 2 \cdot 3' + 2' \cdot 3 = 2 + 3 = 5,$$

and

$$6'_{\mathcal{P}_2} = \big((-1) \cdot 2 \cdot (-3)\big)' = (-1)\{2 \cdot (-3)' + 2' \cdot (-3)\} = (-1)(2 - 3) = 1.$$

Therefore, $6'_{\mathcal{P}_1} \neq 6'_{\mathcal{P}_2}$.

The authors ([1], Theorem 6) show that it is not possible in general to define an arithmetic derivative in a non-UFD. This can be shown with the help of the following particular example which is a special case of Theorem 6 in [1].

Example 2. Let $D = \mathbb{Z}[\sqrt{-5}]$. Then $\mathcal{U} = \{-1, 1\}$. We can show that $\mathbb{Z}[\sqrt{-5}]$ is a non-UFD by considering the two different prime factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$ given as

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We consider the following cases for the different sets $\mathcal{P}$ of positive atoms.

`Case 1.` Assume that $\mathcal{P}$ is such that $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5} \in \mathcal{P}$. Then

$$6 = 2 \cdot 3 \text{ implies } 6' = 2 + 3 = 5,$$

whereas,

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \text{ implies } 6' = (1 + \sqrt{-5}) + (1 - \sqrt{-5}) = 2.$$

Hence, the derivative is not well defined in this case.

`Case 2.` Assume that $\mathcal{P}$ is such that $-2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5} \in \mathcal{P}$. Then

$$6 = (-1) \cdot (-2) \cdot 3 \text{ implies } 6' = (-1)\{(-2) + 3\} = -1,$$

whereas,

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \text{ implies } 6' = (1 + \sqrt{-5}) + (1 - \sqrt{-5}) = 2.$$

Hence, in this case also the derivative is not well-defined .

`Case 3.` Assume that $\mathcal{P}$ is such that $2, -3, 1 + \sqrt{-5}, 1 - \sqrt{-5} \in \mathcal{P}$. Then

$$6 = (-1) \cdot 2 \cdot (-3) \text{ implies } 6' = (-1)\{2 + (-3)\} = 1,$$

whereas,

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \text{ implies } 6' = (1 + \sqrt{-5}) + (1 - \sqrt{-5}) = 2.$$

Hence, in this case also the derivative is not well-defined .

`Case 4.` Assume that $\mathcal{P}$ is such that $-2, -3, 1 + \sqrt{-5}, 1 - \sqrt{-5} \in \mathcal{P}$. Then

$$6 = (-2) \cdot (-3) \text{ implies } 6' = \{(-2) + (-3)\} = -5,$$

whereas,

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \text{ implies } 6' = (1 + \sqrt{-5}) + (1 - \sqrt{-5}) = 2.$$

Hence, in this case also the derivative is not well-defined .

Case 5. Assume that $\mathcal{P}$ is such that $2, 3, 1+\sqrt{-5}, -1+\sqrt{-5} \in \mathcal{P}$. Then

$$6 = 2 \cdot 3 \text{ implies } 6' = 2 + 3 = 5,$$

whereas, $6 = (-1) \cdot (1+\sqrt{-5})(-1+\sqrt{-5})$ implies $6' = (-1)\{(1+\sqrt{-5}) + (-1+\sqrt{-5})\} = -2\sqrt{-5}$. Hence, in this case also the derivative is not well-defined . Similarly, we can verify that the derivative is not well-defined in all other cases.

The rings $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{-5}]$ can be viewed as the number rings of the number fields $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-5})$, respectively. Let $m \in \mathbb{Z}$. Instead of considering the arithmetic derivative of m, we consider the derivative of the principal ideal $\langle m \rangle$ generated by m, denoted by $\langle m \rangle'$, which is defined as the principal ideal generated by m' (see the Remark 2.8). This motivates us to define the derivative of an ideal in a general number ring which is defined in Section 2. In this section, we investigate some properties of this ideal derivative and establish a relation between the arithmetic derivative and the ideal derivative in $\mathbb{Z}$. Furthermore, we discuss some differential equations for the ideal derivative. In Section 3, we extend the definition of the ideal derivative to the derivative of a fractional ideal and investigate some similar results as in Section 2.

2. Derivative of an Ideal

Let K be a number field and R be the corresponding number ring. Let I be a nontrivial ideal of R. By the unique factorization theorem, the ideal I can be factorized uniquely as a product of prime ideals and it is known that every nonzero prime ideal contains a unique prime integer ([2], Exercise 4.4.4, pp 49). Consequently, the derivative of an ideal can be defined in such a way that the ideal derivative in $\mathbb{Z}$ gives the usual arithmetic derivative in $\mathbb{Z}$ in the sense of Theorem 2.7.

Before we define the derivative of an ideal, we define a couple of functions and give some properties of these functions.

Definition 1 (Prime Indicator Function). Let R be the number ring of a number field K. Let $\mathcal{S}$ be the set of nonzero prime ideals of R and $\mathbb{N}$ be the set of natural numbers. The *prime indicator function* is a function $\pi : \mathcal{S} \to \mathbb{N}$ which associates each prime ideal P in $\mathcal{S}$ a unique prime integer contained in P.

Definition 2 (Representative Function). Let R be the number ring of a number field K and $\mathcal{I}$ be the set of ideals in R. The *representative function* is a function $\nu : \mathcal{I} \to \mathbb{N} \cup \{0\}$ defined by

$$\nu(\langle 0 \rangle) := 0, \quad \nu(\langle 1 \rangle) = \nu(R) := 1,$$

and if $I \in \mathcal{I}$ is a nontrivial ideal such that $I = P_1P_2 \cdots P_r$ is the factorization of I into prime ideals (some P_i's may be equal), then

$$\nu(I) := \pi(P_1)\pi(P_2) \cdots \pi(P_r),$$

where π is the prime indicator function.

The following properties are satisfied by the representative function.

Theorem 2.1. *(i) Let I and J be ideals in R. Then $\nu(IJ) = \nu(I)\nu(J)$.*

(ii) Let P be a nonzero prime ideal in R. Then $\nu(P) = \pi(P)$.

Proof. For (i), let either $I = \langle 0 \rangle$ or $J = \langle 0 \rangle$. Without loss of generality, assume that $I = \langle 0 \rangle$. Then $IJ = \langle 0 \rangle$. Thus

$$\nu(IJ) = \nu(\langle 0 \rangle) = 0 = \nu(\langle 0 \rangle)\nu(J) = \nu(I)\nu(J).$$

Now, let either $I = R$ or $J = R$. Without loss of generality, assume that $I = R$. Then $IJ = J$. Thus

$$\nu(IJ) = \nu(J) = \nu(R)\nu(J) = \nu(I)\nu(J).$$

Next, let I and J be nontrivial ideals in R. Then $IJ \neq R$. Let $I = P_1P_2 \cdots P_r$ and $J = P_{r+1}P_{r+2} \cdots P_{r+s}$ be the factorizations of I and J into prime ideals. Let $p_i = \pi(P_i)$ for $i = 1, 2, \ldots, r+s$. Then $\nu(I) = p_1p_2 \cdots p_r$ and $\nu(J) = p_{r+1}p_{r+2} \cdots p_{r+s}$. Now, $IJ = P_1P_2 \cdots P_rP_{r+1}P_{r+2} \cdots P_{r+s}$ implies $\nu(IJ) = p_1p_2 \cdots p_rp_{r+1}p_{r+2} \cdots p_{r+s}$. Hence, $\nu(IJ) = (p_1p_2 \cdots p_r)(p_{r+1}p_{r+2} \cdots p_{r+s})$ implies $\nu(IJ) = \nu(I)\nu(J)$.

Statement (ii) is a consequence of the definition of ν. □

Definition 3 (Derivative of an Ideal). Let I be an ideal in R and let I' denote the *ideal derivative* of I. Define

(i) $I' := \langle 0 \rangle$ if either $I = \langle 0 \rangle$ or $I = \langle 1 \rangle = R$;

(ii)

$$I' := \langle \sum_{j=1}^{k} \pi(P_1) \cdots \pi(P_{j-1})\hat{\pi}(P_j) \cdots \pi(P_k) \rangle,$$

if $I = P_1P_2 \cdots P_r$, where in each summand the term $\hat{\pi}(P_j)$ is deleted. Here, $\langle a \rangle$ denote the principal ideal generated by a in R.

Since the function π is well-defined , the derivative I' is well-defined . Note also that the derivative of an ideal is always a principal ideal by definition.

In the following discussion, the same notation is used for the ideal derivative and for the usual arithmetic derivative. Thus I' denote the ideal derivative of the ideal I and $\langle a' \rangle$ denote the principal ideal generated by the usual arithmetic derivative of a.

2.1. Properties of Ideal Derivative

Theorem 2.2. *Let I be an ideal in R and $\langle \nu(I)' \rangle$ be the principal ideal generated by the usual arithmetic derivative of $\nu(I)$. Then $I' = \langle \nu(I)' \rangle$.*

Proof. Let $I = \langle 0 \rangle$. Then $\nu(I) = 0$ implies $\nu(I)' = 0' = 0$ so $I' = \langle 0 \rangle = \langle \nu(I)' \rangle$. Let $I = R$. Then $\nu(I) = 1$ implies $\nu(I)' = 1' = 0$ so $I' = \langle 0 \rangle = \langle \nu(I)' \rangle$. Now, let I be a nontrivial ideal and $I = P_1 P_2 \cdots P_r$ be the factorization of I into prime ideals. Let $p_i = \pi(P_i)$ for $i = 1, 2, \ldots, r$. Then $\nu(I) = p_1 p_2 \cdots p_r$. Therefore, $I' = \langle \sum_{j=1}^{r} p_1 \cdots p_{j-1} \hat{p}_j \cdots p_r \rangle$. Since $\nu(I)' = \sum_{j=1}^{r} p_1 \cdots p_{j-1} \hat{p}_j \cdots p_r$, it follows that $\langle \nu(I)' \rangle = \langle \sum_{j=1}^{r} p_1 \cdots p_{j-1} \hat{p}_j \cdots p_r \rangle$. Thus $I' = \langle \nu(I)' \rangle$. □

Corollary 2.3. *Let P be a nonzero prime ideal in R. Then $P' = \langle 1 \rangle = R$.*

Proof. We have $P' = \langle \nu(P)' \rangle = \langle \pi(P)' \rangle = \langle p' \rangle = \langle 1 \rangle = R$, where $p = \pi(P)$. □

Corollary 2.4. *Let $I = P^k$, where P is a nonzero prime ideal and $k \in \mathbb{N}$. Then $I' = \langle k\nu(P)^{k-1} \rangle$.*

Proof. Clearly, $I = P^k$ implies $\nu(I) = \nu(P^k) = \nu(P)^k$, which implies $\nu(I)' = k\nu(P)^{k-1}$. Hence, $I' = \langle \nu(I)' \rangle = \langle k\nu(P)^{k-1} \rangle$. □

Corollary 2.5. *Let I be an ideal in R and $k \in \mathbb{N}$. Then $(I^k)' = \langle k\nu(I)^{k-1}\nu(I)' \rangle$.*

Proof. By the Leibnitz rule of the arithmetic derivative, $\nu(I^k) = \nu(I)^k$ implies $\nu(I^k)' = k\nu(I)^{k-1}\nu(I)'$. Therefore, $(I^k)' = \langle \nu(I^k)' \rangle = \langle k\nu(I)^{k-1}\nu(I)' \rangle$. □

Theorem 2.6. *Let I and J be ideals in R. Then $(IJ)' = \langle \nu(I)'\nu(J) + \nu(I)\nu(J)' \rangle$.*

Proof. We have $(IJ)' = \langle \nu(IJ)' \rangle = \langle \big(\nu(I)\nu(J)\big)' \rangle = \langle \nu(I)'\nu(J) + \nu(I)\nu(J)' \rangle$. □

Example 3. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $R = \mathbb{Z}[\sqrt{-5}]$. We have shown in Example 2 that 6 has not well-defined arithmetic derivative in $\mathbb{Z}[\sqrt{-5}]$. Since $\mathbb{Z}[\sqrt{-5}]$ is the number ring of $\mathbb{Q}(\sqrt{-5})$ and $\langle 6 \rangle$ is a principal ideal in $\mathbb{Z}[\sqrt{-5}]$, we can find the derivative of this ideal in $\mathbb{Z}[\sqrt{-5}]$. We can factor the ideal $\langle 6 \rangle$ into prime ideals ([3], pp 214-216) as follows:

$$\langle 6 \rangle = \langle 2, 1 + \sqrt{-5} \rangle^2 \langle 3, 1 + \sqrt{-5} \rangle \langle 3, 1 - \sqrt{-5} \rangle.$$

Now, $2 \in \langle 2, 1 + \sqrt{-5} \rangle$, $3 \in \langle 3, 1 + \sqrt{-5} \rangle$, and $3 \in \langle 3, 1 - \sqrt{-5} \rangle$. Since 2 and 3 are prime integers, we have $\pi(\langle 2, 1 + \sqrt{-5} \rangle) = 2$, $\pi(\langle 3, 1 + \sqrt{-5} \rangle) = 3$, and $\pi(\langle 3, 1 - \sqrt{-5} \rangle) = 3$ ([2], Exercise 4.4.4, pp 49). Therefore, $\nu(\langle 6 \rangle) = 2^2 \cdot 3 \cdot 3 = 2 \cdot 2 \cdot 3 \cdot 3$ implies $\nu(\langle 6 \rangle)' = 2 \cdot 3 \cdot 3 + 2 \cdot 3 \cdot 3 + 2 \cdot 2 \cdot 3 + 2 \cdot 2 \cdot 3 = 18 + 18 + 12 + 12 = 60$. Thus $\langle 6 \rangle' = \langle \nu(\langle 6 \rangle)' \rangle = \langle 60 \rangle$. Observe that, $\langle 60 \rangle \subseteq \langle 6 \rangle$ implies $\langle 6 \rangle \mid \langle 60 \rangle$. Thus $\langle 6 \rangle \mid \langle 6 \rangle'$, i.e., the ideal $\langle 6 \rangle$ divides its ideal derivative $\langle 6 \rangle'$. Note that this is not

true in general. Take $K = \mathbb{Q}$ and $R = \mathbb{Z}$, $5 \in \mathbb{Z}$, $5' = 1$. Therefore, $\langle 5\rangle' = \langle 5'\rangle = \langle 1\rangle$ but $\langle 5\rangle \nmid \langle 1\rangle$.

The arithmetic derivative and the ideal derivative in $\mathbb{Z}$ have the following relation.

Theorem 2.7. *Let $n \in \mathbb{Z}$ and $\mathcal{P}$ be the set of positive primes. Then $\langle n\rangle' = \langle m\rangle$ if and only if $n' = um$, where $u = \pm 1$.*

Proof. The case $n \in \{0, 1, -1\}$ is trivial. Let $n \in \mathbb{Z}\backslash\{0, 1, -1\}$. Let $n = up_1p_2\cdots p_r$, where $u = \pm 1$ and $p_i \in \mathcal{P}$ for $i = 1, 2, \ldots, r$. Then $\langle n\rangle = \langle up_1p_2\cdots p_r\rangle = \langle p_1p_2\cdots p_r\rangle = \langle p_1\rangle\langle p_2\rangle\cdots\langle p_r\rangle$. Therefore, $\nu(\langle n\rangle) = \pi(\langle p_1\rangle)\pi(\langle p_2\rangle)\cdots\pi(\langle p_r\rangle) = p_1p_2\cdots p_r = un$. Thus $\langle n\rangle' = \langle\nu(\langle n\rangle)'\rangle = \langle(un)'\rangle = \langle un'\rangle = \langle n'\rangle$. Now, let $n' = um$. Then $\langle n\rangle' = \langle n'\rangle = \langle um\rangle = \langle m\rangle$. Conversely, let $\langle n\rangle' = \langle m\rangle$. Then $\langle n'\rangle = \langle m\rangle$ as $\langle n\rangle' = \langle n'\rangle$. This implies either $n' = 0$ (in which case m is also 0) or $n' = um$, where $u = \pm 1$. But $n' = 0$ implies $n = 0, \pm 1$ ([4], Theorem 7), which contradicts our assumption. Hence, $n' = um$. □

Remark 2.8. From the above theorem, it follows that $\langle n\rangle' = \langle n'\rangle$.

Notice that the ideal derivative coincides with the arithmetic derivative in $\mathbb{Z}$ in the sense of Theorem 2.7 for the set $\mathcal{P}$ of positive atoms in $\mathbb{Z}$, which contains only positive primes. For the other set $\mathcal{P}'$ of atoms, we can modify the definition of ideal derivative in $\mathbb{Z}$ by defining $\pi(\langle p\rangle) = up$, where $u \in \{-1, 1\}$ such that $up \in \mathcal{P}'$. Note that this definition of π is also well defined. For, if $p \in \langle p\rangle$, then its associate $up \in \langle p\rangle$. A similar argument is also valid in case of the general number rings.

2.2. Some Differential Equations

Theorem 2.9. *Let I be an ideal in a number ring R. Then $I' = \langle 1\rangle$ if and only if I is a nonzero prime ideal in R.*

Proof. Let I be a nonzero prime ideal of R. Then by Corollary 2.3, $I' = \langle 1\rangle$. Conversely, assume that $I' = \langle 1\rangle$ and I is not a nonzero prime ideal. Let $I = \langle 0\rangle$. Then $I' = \langle 0\rangle' = \langle 0\rangle$. Hence, $I \neq \langle 0\rangle$. Also, $I \neq \langle 1\rangle$ as $\langle 1\rangle' = \langle 0\rangle$. Let $I = P_1P_2\cdots P_r$ be the prime ideal factorization of I. Then we have that $r \geq 2$. Let $\pi(P_i) = p_i$ for $i = 1, 2, \ldots, r$. Then $\nu(I) = p_1p_2\cdots p_r$. Therefore, $\nu(I)' = \sum_{j=1}^{r} p_1\cdots p_{j-1}\hat{p}_j\cdots p_r$. Now $I' = \langle 1\rangle$ implies $\langle\nu(I)'\rangle = \langle 1\rangle$. Thus $\langle\sum_{j=1}^{r} p_1\cdots p_{j-1}\hat{p}_j\cdots p_r\rangle = \langle 1\rangle$. Therefore, for some unit $u \in R$,

$$1 = u\sum_{j=1}^{r} p_1\cdots p_{j-1}\hat{p}_j\cdots p_r$$

so

$$\mathrm{N}_K(1) = \mathrm{N}_K(u)\mathrm{N}_K(\sum_{j=1}^{r} p_1\cdots p_{j-1}\hat{p}_j\cdots p_r),$$

which implies

$$\mathrm{N}_K(\sum_{j=1}^{r} p_1 \cdots p_{j-1}\hat{p}_j \cdots p_r) = \pm 1.$$

Hence, $|\mathrm{N}_K(\sum_{j=1}^{r} p_1 \cdots p_{j-1}\hat{p}_j \cdots p_r)| = 1$ (here $\mathrm{N}_K(\alpha)$ denote the norm of the algebraic integer α with respect to the number field K). Thus

$$(\sum_{j=1}^{r} p_1 \cdots p_{j-1}\hat{p}_j \cdots p_r)^d = 1,$$

where $d = [K : \mathbb{Q}]$. On the other hand, we have that $\sum_{j=1}^{r} p_1 \cdots p_{j-1}\hat{p}_j \cdots p_r = p_1p_3p_4 \cdots p_r + \sum_{j=1, j\neq 2}^{r} p_1 \cdots p_{j-1}\hat{p}_j \cdots p_r > p_1p_3p_4 \cdots p_r > p_1 \geq 2$. Therefore, $1 = (\sum_{j=1}^{r} p_1 \cdots p_{j-1}\hat{p}_j \cdots p_r)^d \geq 2^d$, a contradiction, as $d \geq 1$. This proves that I must be a nonzero prime ideal in R. □

Theorem 2.10. *Let I be an ideal in a number ring R. Then $I' = \langle 0\rangle$ if and only if either $I = \langle 0\rangle$ or $I = \langle 1\rangle$.*

Proof. Let either $I = \langle 0\rangle$ or $I = \langle 1\rangle$. Then by definition, $I' = \langle 0\rangle$. Conversely, assume that $I' = \langle 0\rangle$. Let $I \neq \langle 0\rangle$ and $I \neq \langle 1\rangle$. Then I is a nontrivial ideal in R. Let $I = P_1P_2 \cdots P_r$ be the prime ideal factorization. If $r = 1$, then $I = P_1$ is a prime ideal and hence $I' = \langle 1\rangle$, a contradiction. Therefore, $r \geq 2$. Let $\pi(P_i) = p_i$ for $i = 1, 2, \ldots, r$. Then $\nu(I) = p_1p_2 \cdots p_r$. This implies $\nu(I)' = \sum_{j=1}^{r} p_1 \cdots p_{j-1}\hat{p}_j \cdots p_r$. Hence, $I' = \langle \nu(I)'\rangle = \langle \sum_{j=1}^{r} p_1 \cdots p_{j-1}\hat{p}_j \cdots p_r\rangle$. Now, $I' = \langle 0\rangle$ implies $\langle \sum_{j=1}^{r} p_1 \cdots p_{j-1}\hat{p}_j \cdots p_r\rangle = \langle 0\rangle$. Therefore, $\sum_{j=1}^{r} p_1 \cdots \hat{p}_j \cdots p_r = 0$, which is not possible as $\sum_{j=1}^{r} p_1 \cdots p_{j-1}\hat{p}_j \cdots p_r \geq 2$. Hence, $I' \neq \langle 0\rangle$. This completes the proof. □

Theorem 2.11. *The number of solutions in a number ring R of the differential equation $I' = \langle m\rangle$, where $m \in \mathbb{Z} \setminus \{-1, 1\}$, is finite.*

Proof. Let $m = 0$. Then the result follows from the previous theorem. So let $m \neq 0$. Without loss of generality, we may consider the equation $I' = \langle m\rangle$ for positive integers m, because $\langle m\rangle = \langle -m\rangle$ for all $m \in \mathbb{Z}$. If there is no solution, we are done. So assume that there is at least one solution. Let I be a solution. Then $I \neq \langle 0\rangle$, $\langle 1\rangle$ and also I is not a prime ideal because if I happens to be prime, then $I' = \langle 1\rangle = R \neq \langle m\rangle$ (since the only units in R which are also in $\mathbb{Z}$ are ± 1). Hence, I is a nontrivial ideal. Next, assume that $\nu(I) = n$. Then $I' = \langle \nu(I)'\rangle = \langle n'\rangle$. Therefore, $\langle n'\rangle = \langle m\rangle$ implies either $n' = 0$ or $n' = um$ for some unit u in R. If $n' = 0$, then $\langle m\rangle = \langle 0\rangle$. This implies $m = 0$, which contradicts our assumption that m is positive. So $n' = um$. Since n' is a positive integer, um is also a positive integer. Now, as $um \in \mathbb{Z}$, $u \in R$, and $m > 0$, it follows that $u = 1$. Therefore, $n' = m$, which has a finite number of solutions for n ([4], Corollary 3, pp. 6). Hence

it suffices to show that there are a finite number of ideals I such that $\nu(I)$ is a solution of $n' = m$. So let n be a solution of the equation $n' = m$. We show that there are only finitely many ideals I such that $\nu(I) = n$. Notice that $n > 0$ as I is a nontrivial ideal. Let $n = p_1 p_2 \cdots p_r$ be the prime factorization of n. Then there must be r nonzero prime ideals $P_1, P_2, \ldots, P_r$ in the prime factorization of I such that $\pi(P_i) = p_i$ for $i = 1, 2, \ldots, r$. Hence it suffices to show that for each prime p_i there are only finitely many nonzero prime ideals P such that $\pi(P) = p_i$. Observe that, $p_i \in P$ implies $\langle p_i \rangle \subseteq P$, so $\mathcal{N}(P) \leq \mathcal{N}(\langle p_i \rangle)$ (here $\mathcal{N}(P)$ denote the norm of the ideal P). Thus $\mathcal{N}(P) \leq |\mathrm{N}_K(p_i)|$ ([2], Exercise 5.3.15, pp 61). It follows that there are only a finite number of such prime ideals ([2], Exercise 6.2.4, pp 72). Hence, there are only finitely many solutions of the differential equation $I' = \langle m \rangle$, where $m \in \mathbb{Z} \setminus \{-1, 1\}$. This completes the proof. □

3. Derivative of a Fractional Ideal

The definition of the ideal derivative can be extended to the derivative of a fractional ideal in K in such a way that the ideal derivative in $\mathbb{Q}$ gives the usual arithmetic derivative in $\mathbb{Q}$ in the sense of Theorem 3.6. Due to the different notation used in this paper we mention the following already known definitions and results from [2].

Definition (Fractional Ideal). Let K be a number field and R be the corresponding number ring. A *fractional ideal* $\mathcal{A}$ of R is an R-module contained in K such that there exists a nonzero integer m such that $m\mathcal{A} \subseteq R$.

Any ideal of R is a fractional ideal by taking $m = 1$. Let P be a prime ideal of R. Define $P^{-1} := \{x \in K : xP \subseteq R\}$. Then P^{-1} is a fractional ideal and $PP^{-1} = R$. Note that the sum and the product of two fractional ideals are again fractional ideals. Let P and Q be prime ideals. We shall write $\frac{P}{Q}$ for $Q^{-1}P$. We shall also write $\frac{P_1 P_2 \cdots P_r}{Q_1 Q_2 \cdots Q_s}$ to mean $Q_1^{-1} Q_2^{-1} \cdots Q_s^{-1} P_1 P_2 \cdots P_r$, where the P_i's and the Q_j's are prime ideals.

Theorem 3.1. *([2], Exercise 5.3.7, p. 59) Any fractional ideal $\mathcal{A}$ can be written uniquely in the form $\frac{P_1 P_2 \cdots P_r}{Q_1 Q_2 \cdots Q_s}$, where the P_i's and the Q_j's may be repeated, but no $P_i = Q_j$.*

Theorem 3.2. *([2], Exercise 5.3.8, p. 59) Given any nonzero fractional ideal $\mathcal{A}$ in K, there exists a fractional ideal $\mathcal{A}^{-1}$ such that $\mathcal{A}\mathcal{A}^{-1} = R$.*

3.1. Fractional Ideals of $\mathbb{Q}$

Set $K = \mathbb{Q}$ and $R = \mathbb{Z}$. Let P be a prime ideal in $\mathbb{Z}$. Then $P = \langle p \rangle = p\mathbb{Z}$ for some prime p and $P^{-1} = \{x \in \mathbb{Q} : xp\mathbb{Z} \subseteq \mathbb{Z}\} = \{x \in \mathbb{Q} : px \in \mathbb{Z}\} = \frac{1}{p}\mathbb{Z}$ is a fractional ideal. Now, let $\frac{a}{b} \in \mathbb{Q} \setminus \{0, 1, -1\}$. Then $\frac{a}{b}\mathbb{Z} = \{\frac{ax}{b} \in \mathbb{Q} : x \in \mathbb{Z}\}$ is a

fractional ideal which can be written as $\frac{a}{b}\mathbb{Z} = \frac{p_1p_2\cdots p_r}{q_1q_2\cdots q_s}\mathbb{Z}$, where the p_i's and the q_j's are primes and $p_i \neq q_j$ for all i and j. Hence, $\frac{a}{b}\mathbb{Z} = \frac{1}{q_1}\mathbb{Z}\frac{1}{q_2}\mathbb{Z}\cdots\frac{1}{q_s}\mathbb{Z}p_1\mathbb{Z}p_2\mathbb{Z}\cdots p_r\mathbb{Z} = Q_1^{-1}Q_2^{-1}\cdots Q_s^{-1}P_1P_2\cdots P_r$, where $P_i = p_i\mathbb{Z} = \langle p_i\rangle$ and $Q_j = q_j\mathbb{Z} = \langle q_j\rangle$ are prime ideals and $P_i \neq Q_j$ for $i = 1, 2, \ldots, r$ and $j = 1, 2, \ldots, s$. By Theorem 3.1, this representation of $\frac{a}{b}\mathbb{Z}$ is unique. We shall also write $\langle\frac{a}{b}\rangle$ for $\frac{a}{b}\mathbb{Z}$.

Definition 4 (Fractional Representative Function). Let R be the number ring of a number field K. Let $\mathcal{I}^*$ be the set of fractional ideals in K. The *fractional representative function* is a function $\nu^* : \mathcal{I}^* \to \mathbb{Q}$ defined by

$$\nu^*(\mathcal{A}) := \begin{cases} 0, & \text{if } \mathcal{A} = \langle 0\rangle; \\ 1, & \text{if } \mathcal{A} = \langle 1\rangle; \\ \pi(Q_1)^{-1}\cdots\pi(Q_s)^{-1}\pi(P_1)\cdots\pi(P_r), & \text{if } \mathcal{A} = Q_1^{-1}\cdots Q_s^{-1}P_1\cdots P_r, \end{cases}$$

where $\mathcal{A} \in \mathcal{I}^*$.

It is clear that $\nu^*(I) = \nu(I)$ if I is an ideal of R. By Theorem 3.1, any fractional ideal $\mathcal{A}$ in K can be uniquely written in the form IJ^{-1}, where I and J are ideals of R. Therefore, by the definition of ν^*, it is clear that

$$\nu^*(\mathcal{A}) = \nu^*(IJ^{-1}) = \nu(I)\nu(J)^{-1}.$$

The following properties are satisfied by the fractional representative function.

Theorem 3.3. *(i) Let $\mathcal{A}$ and $\mathcal{B}$ be fractional ideals in K. Then $\nu^*(\mathcal{AB}) = \nu^*(\mathcal{A})\nu^*(\mathcal{B})$.*

(ii) Let $\mathcal{A}$ be a nonzero fractional ideal in K. Then $\nu^*(\mathcal{A}^{-1}) = \nu^*(\mathcal{A})^{-1}$.

Proof. (i) Let $\mathcal{A}$ and $\mathcal{B}$ be fractional ideals in K. Then there exist ideals I_1, I_2, J_1 and J_2 in R such that $\mathcal{A} = I_1J_1^{-1}$ and $\mathcal{B} = I_2J_2^{-1}$. Therefore, $\mathcal{AB} = (I_1J_1^{-1})(I_2J_2^{-1}) = (I_1I_2)(J_1J_2)^{-1}$. We have

$$\begin{aligned} \nu^*(\mathcal{AB}) &= \nu^*\big((I_1I_2)(J_1J_2)^{-1}\big) \\ &= \nu(I_1I_2)\nu(J_1J_2)^{-1} \\ &= \nu(I_1)\nu(I_2)\big(\nu(J_1)\nu(J_2)\big)^{-1} \\ &= \nu(I_1)\nu(J_1)^{-1}\nu(I_2)\nu(J_2)^{-1} \\ &= \nu^*(I_1J_1^{-1})\nu^*(I_2J_2^{-1}) \\ &= \nu^*(\mathcal{A})\nu^*(\mathcal{B}). \end{aligned}$$

(ii) Let $\mathcal{A}$ be a nonzero fractional ideal in K. Then by Theorem 3.2, there exists a fractional ideal $\mathcal{A}^{-1}$ such that $\mathcal{A}\mathcal{A}^{-1} = R$. Therefore, $\nu^*(\mathcal{A}\mathcal{A}^{-1}) = \nu^*(R) = \nu^*(<1>)$ implies $\nu^*(\mathcal{A})\nu^*(\mathcal{A}^{-1}) = 1$ (by (i)). Thus $\nu^*(\mathcal{A}^{-1}) = \nu^*(\mathcal{A})^{-1}$.

□

Definition 5 (Derivative of a Fractional Ideal). Let $\mathcal{A}$ be a fractional ideal in K and let $\nu^*(\mathcal{A})'$ denote the arithmetic derivative of the rational number $\nu^*(\mathcal{A})$. Then the *fractional ideal derivative* of $\mathcal{A}$, denoted by $\mathcal{A}'$, is defined by $\mathcal{A}' := \langle \nu^*(\mathcal{A})' \rangle$. Here, $\langle \nu^*(\mathcal{A})' \rangle$ is the cyclic R-module generated by the rational number $\nu^*(\mathcal{A})'$ in K.

Theorem 3.4. *Let $\mathcal{A}$ and $\mathcal{B}$ be fractional ideals in K. Then $(\mathcal{AB})' = \langle \nu^*(\mathcal{A})'\nu^*(\mathcal{B}) + \nu^*(\mathcal{A})\nu^*(\mathcal{B})' \rangle$.*

Proof. By the Leibnitz rule, $(\mathcal{AB})' = \langle \nu^*(\mathcal{AB})' \rangle = \langle (\nu^*(\mathcal{A})\nu^*(\mathcal{B}))' \rangle = \langle \nu^*(\mathcal{A})'\nu^*(\mathcal{B}) + \nu^*(\mathcal{A})\nu^*(\mathcal{B})' \rangle$. □

Lemma 3.5. *Let $\langle q_1 \rangle = q_1\mathbb{Z}$ and $\langle q_2 \rangle = q_2\mathbb{Z}$ be cyclic $\mathbb{Z}$-modules generated by the nonzero rational numbers q_1 and q_2, respectively. Then $\langle q_1 \rangle = \langle q_2 \rangle$ if and only if $q_1 = uq_2$, where $u = \pm 1$.*

Proof. Let $\langle q_1 \rangle = \langle q_2 \rangle$. Then $q_1 \in \langle q_2 \rangle$ implies $q_1 = q_2 m$ for some $m \in \mathbb{Z}$. Similarly, $q_2 = q_1 n$ for some $n \in \mathbb{Z}$. Therefore, $q_1 = q_2 m = q_1 nm = mnq_1$ implies $m = n = 1$ or $m = n = -1$. Thus $q_1 = uq_2$, where $u = \pm 1$. Conversely, let $q_1 = uq_2$. Then $q_1\mathbb{Z} = uq_2\mathbb{Z} = q_2\mathbb{Z}$ implies $\langle q_1 \rangle = \langle q_2 \rangle$ as $\mathbb{Z}$-modules. □

Theorem 3.6. *Let $\frac{a}{b} \in \mathbb{Q}$ and $\langle \frac{a}{b} \rangle'$ denote the derivative of the fractional ideal generated by $\frac{a}{b} \in \mathbb{Q}$. Let $(\frac{a}{b})'$ denote the usual arithmetic derivative of $\frac{a}{b}$. Then $\langle \frac{a}{b} \rangle' = \langle q \rangle$ if and only if $(\frac{a}{b})' = uq$, where $u = \pm 1$.*

Proof. Let $\frac{a}{b} = 0$. Then $\langle \frac{a}{b} \rangle = \frac{a}{b}\mathbb{Z} = \langle 0 \rangle$ and $(\frac{a}{b})' = 0' = 0$. We have $\nu^*(\langle 0 \rangle) = 0$. Therefore, $\langle 0 \rangle' = \langle \nu^*(\langle 0 \rangle)' \rangle = \langle 0' \rangle = \langle 0 \rangle$. Conversely, let $\langle 0 \rangle' = \langle q \rangle$. Then $\langle q \rangle = \langle 0 \rangle' = \langle \nu^*(\langle 0 \rangle)' \rangle = \langle 0' \rangle = \langle 0 \rangle$. This gives $q = 0$. Therefore, $0' = 0 = q$. Thus the theorem is true in the case $\frac{a}{b} = 0$.

Now, let $\frac{a}{b} = 1$. Then $\langle \frac{a}{b} \rangle = \langle 1 \rangle = \mathbb{Z}$ and $(\frac{a}{b})' = 1' = 0$. We have $\nu^*(\langle 1 \rangle) = 1$. Therefore, $\langle 1 \rangle' = \langle \nu^*(\langle 1 \rangle)' \rangle = \langle 1' \rangle = \langle 0 \rangle$. Conversely, let $\langle 1 \rangle' = \langle q \rangle$. Then $\langle q \rangle = \langle 1 \rangle' = \langle \nu^*(\langle 1 \rangle)' \rangle = \langle 1' \rangle = \langle 0 \rangle$. This gives $q = 0$. Therefore, $1' = 0 = q$. Thus the theorem is true in the case $\frac{a}{b} = 1$ as well.

Similar argument holds for the case $\frac{a}{b} = -1$. Now, assume that $\frac{a}{b} \in \mathbb{Q} \backslash \{0, 1, -1\}$. Let $\frac{a}{b} = u\frac{p_1 p_2 \cdots p_r}{q_1 q_2 \cdots q_s}$, where the p_i's and the q_j's are primes such that $p_i \neq q_j$ for all i, j and $u = \pm 1$. We have $\langle \frac{a}{b} \rangle = \frac{a}{b}\mathbb{Z} = \frac{p_1 p_2 \cdots p_r}{q_1 q_2 \cdots q_s}\mathbb{Z}$. Therefore, $\langle \frac{a}{b} \rangle = Q_1^{-1}Q_2^{-1} \cdots Q_s^{-1}P_1P_2 \cdots P_r$, where $P_i = \langle p_i \rangle = p_i\mathbb{Z}$ and $Q_j = \langle q_j \rangle = q_j\mathbb{Z}$ are prime ideals and $P_i \neq Q_j$ for $i = 1, 2, \ldots, r$ and $j = 1, 2, \ldots, s$. Thus $\nu^*(\langle \frac{a}{b} \rangle) = q_1^{-1}q_2^{-1} \cdots q_s^{-1}p_1p_2 \cdots p_r = u\frac{a}{b}$. Now, let $(\frac{a}{b})' = uq$. Then $\langle \frac{a}{b} \rangle' = \langle \nu^*(\langle \frac{a}{b} \rangle)' \rangle = \langle (u\frac{a}{b})' \rangle = \langle u(\frac{a}{b})' \rangle = \langle (\frac{a}{b})' \rangle$. This implies $\langle \frac{a}{b} \rangle' = \langle uq \rangle = \langle q \rangle$.

Conversely, let $\langle \frac{a}{b} \rangle' = \langle q \rangle$. Then $\langle \nu^*(\langle \frac{a}{b} \rangle)' \rangle = \langle q \rangle$ implies $\langle (u\frac{a}{b})' \rangle = \langle q \rangle$. Hence, $\langle u(\frac{a}{b})' \rangle = \langle q \rangle$. This gives $\langle (\frac{a}{b})' \rangle = \langle q \rangle$. If $q = 0$, then $(\frac{a}{b})' = 0 = uq$. If $q \neq 0$, we claim that $(\frac{a}{b})' = uq$ for some unit u. Let $(\frac{a}{b})' = 0$. Then $\langle (\frac{a}{b})' \rangle = \langle q \rangle$ implies

$\langle q\rangle = \langle 0\rangle$. Hence, $q = 0$, which contradicts our assumption. Therefore, $(\frac{a}{b})' \neq 0$. Thus by Lemma 3.5, $\langle(\frac{a}{b})'\rangle = \langle q\rangle$ implies $(\frac{a}{b})' = uq$, where $u = \pm 1$. This completes the proof. □

4. Concluding Remarks

We defined the ideal derivative in a number ring, where we used the facts that every ideal in a number ring is uniquely representable as a product of prime ideals and that every nonzero prime ideal in a number ring contains exactly one prime integer. Because of the latter fact, we could define the prime indicator function which played an important role in defining the concept of ideal derivative in a number ring.

The computation of ideal derivative may be difficult because its computation depends on the factorization of an ideal in a number ring into prime ideals which is not an easy task. Further, finding the unique prime integer in a prime ideal is also challenging.

Acknowledgement The authors are very much thankful to the anonymous referee and to Professor Bruce Landman for their comments to present the paper in a better form.

References

[1] P. Haukkanen, M. Mattila , J. K. Merikoski, T. Tossavainen, *Can the arithmetic derivative be defined on a non-unique factorization domain*, J. Integer Seq., **16** (2013), Article 13.1.2.

[2] M. R. Murty, J. Esmonde, Problems in Algebraic Number Theory, 2nd edition, Springer, 2005.

[3] J. Stillwell, Elements of Number Theory, Springer, 2003.

[4] V. Ufnarovski, B. Åhlander, *How to Differentiate a Number*, J. Integer Seq., **6**(2003), Article 03.3.4.