Journal of Integer Sequences, Vol. 16 (2013),
Article 13.1.2

Can the Arithmetic Derivative be Defined on a Non-Unique Factorization Domain?

Pentti Haukkanen, Mika Mattila, and Jorma K. Merikoski
School of Information Sciences
FI-33014 University of Tampere
Finland
pentti.haukkanen@uta.fi
mika.mattila@uta.fi
jorma.merikoski@uta.fi

Timo Tossavainen
School of Applied Educational Science and Teacher Education
University of Eastern Finland
P.O. Box 86
FI-57101 Savonlinna
Finland
timo.tossavainen@uef.fi

Abstract

Given $n \in \mathbb{Z}$, its arithmetic derivative n' is defined as follows: (i) $0' = 1' = (-1)' = 0$. (ii) If $n = up_1 \cdots p_k$, where $u = \pm 1$ and $p_1, \ldots, p_k$ are primes (some of them possibly equal), then

$$n' = n \sum_{j=1}^{k} \frac{1}{p_j} = u \sum_{j=1}^{k} p_1 \cdots p_{j-1} p_{j+1} \cdots p_k.$$

An analogous definition can be given in any unique factorization domain. What about the converse? Can the arithmetic derivative be (well-)defined on a non-unique factorization domain? In the general case, this remains to be seen, but we answer the question negatively for the integers of certain quadratic fields. We also give a sufficient condition under which the answer is negative.

1 The arithmetic derivative

Let $n \in \mathbb{Z}$. Its arithmetic derivative n' (A003415 in [4]) is defined [1, 6] as follows:

(i) $0' = 1' = (-1)' = 0$.

(ii) If $n = up_1 \cdots p_k$, where $u = \pm 1$ and $p_1, \ldots, p_k \in \mathbb{P}$, the set of primes, (some of them possibly equal), then

$$n' = n \sum_{j=1}^{k} \frac{1}{p_j} = u \sum_{j=1}^{k} p_1 \cdots p_{j-1} p_{j+1} \cdots p_k. \tag{1}$$

If $k = 1$, we set $p_1 \cdots p_{k-1} p_{k+1} \cdots p_k = 1$ in the last expression.

A few basic properties of n' follow:

$$\forall p \in \mathbb{P} : p' = 1,$$
$$\forall n \in \mathbb{Z} : (-n)' = -n',$$
$$\forall m, n \in \mathbb{Z} : (mn)' = m'n + mn'.$$

The third equality is called the Leibniz rule. Moreover, $f(n) = n'$ is the only mapping $\mathbb{Z} \to \mathbb{Z}$ having these properties. For details, see [6, Theorems 1 and 13].

Kovič [3, Proposition 1] studied how to extend f to $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. Ufnarovski and Åhlander [6, Section 10] outlined how to define the arithmetic derivative on a unique factorization domain (UFD from now on). We begin by performing this task in detail. To that end, we follow the terminology of [2, Section 6.5].

Let D be a UFD. First, we must decide what atoms (irreducible elements) are "positive". Write $\mathcal{P}$ for a set of atoms of D such that every atom of D is associated with one and only one element of $\mathcal{P}$. Call $\mathcal{P}$ the set of positive atoms. Further, denote by $\mathcal{U}$ the set of units of D.

Given $a \in D$, we define its arithmetic derivative a' as follows: If $a = 0$ or $a \in \mathcal{U}$, then $a' = 0$. Otherwise, there are unique (up to the ordering) $p_1, \ldots, p_k \in \mathcal{P}$ (some of them possibly equal) and $u \in \mathcal{U}$ such that

$$a = up_1 \cdots p_k.$$

Then

$$a' = u \sum_{j=1}^{k} p_1 \cdots p_{j-1} p_{j+1} \cdots p_k. \tag{2}$$

To be precise, we should actually write $a'_{\mathcal{P}}$ (or something like that) for the derivative of a, since a' depends on $\mathcal{P}$. However, for the simplicity of notation, we will omit this practice if there is no need to emphasize $\mathcal{P}$.

The given definition implies the analogous equalities as above:

$$\forall p \in \mathcal{P} : p' = 1,$$
$$\forall v \in \mathcal{U}, a \in D : (va)' = va',$$
$$\forall a, b \in D : (ab)' = a'b + ab'.$$

Again, $f(x) = x'$ is the only mapping $D \to D$ with these properties.

Example 1. Let $D = \mathbb{Z}$. If $\mathcal{P}_1 = \mathbb{P}$, we obtain the ordinary arithmetic derivative defined above. For example, because $30 = 2 \cdot 3 \cdot 5$, we have $30'_{\mathcal{P}_1} = 30' = 3 \cdot 5 + 2 \cdot 5 + 2 \cdot 3 = 31$. Obviously, another selection of positive atoms results in a different derivative function. For instance, if $\mathcal{P}_2 = \{2, -3, 5, -7, 11, \dots\}$, then $30 = (-1) \cdot 2 \cdot (-3) \cdot 5$ and $30'_{\mathcal{P}_2} = (-1) \cdot [(-3) \cdot 5 + 2 \cdot 5 + 2 \cdot (-3)] = 11$.

Example 2. Let D be an arbitrary field F. Since all nonzero elements of F are units, then $\mathcal{P} = \emptyset$ and, hence, $a' = 0$ for all $a \in F$.

Example 3. To give an example of a nontrivial derivative on the field $\mathbb{Q}$, we define [6, Theorem 14]

$$\left(\frac{m}{n}\right)' = \frac{m'n - mn'}{n^2}. \tag{3}$$

Here $m, n \in \mathbb{Z}$, $n \neq 0$, and m' and n' are ordinary arithmetic derivatives on $\mathbb{Z}$. An analogous definition can be given in the division field of any UFD.

Let us summarize the above discussion.

Proposition 4.

(i) *Let D be a* UFD. *The mapping $f(a) = a'_{\mathcal{P}}$ defined on D by (2) is an arithmetic derivative. It depends on the chosen set $\mathcal{P}$ of positive atoms.*

(ii) *The mapping $g(a) = a'$ defined on $\mathbb{Q}$ by (3) is an extension of the mapping $f(a) = a'$ defined on $\mathbb{Z}$ by (1). Similarly, (2) can be extended to the division field of D.*

2 A problem and its partial answers

If a factorization domain (FD in the sequel) is not a UFD, we call it a non-unique factorization domain (NUFD in the sequel). We saw above that the arithmetic derivative can be defined on any UFD. What about the converse?

Problem 5. *Is it possible to define an arithmetic derivative on some* NUFD*?*

The next theorem gives a partial answer which is negative. In the following, we mostly apply the same terminology and notation as in [5, Chapter 4].

Theorem 6. *Let D_m be the integral domain of integers of $\mathbb{Q}(\sqrt{m})$, where $m \in \mathbb{Z}\backslash\{1\}$ is squarefree (A005117 in [4]). If m satisfies*

$$m \not\equiv 1 \pmod 4 \text{ and } m < -2, \tag{4}$$

then either $1 - m$ or $4 - m$ does not have a well-defined derivative as an element of D_m.

Proof. Clearly, D_m is an FD, yet it is not a UFD, see [5, p. 93] or [7, Theorem (actually, in Finnish: Lause) 4.23]. We modify and enhance the argument used in the latter reference.

Case 1. $m \equiv 3 \pmod 4$. Then m is odd and $m \leq -5$. Since $1 - m$ is even and greater than five, it is a composite number (when considered as a positive integer) and expressible as

$$1 - m = p_1 \cdots p_k, \tag{5}$$

where $k \geq 2$ and $p_1, \ldots, p_k \in \mathbb{P}$ with $2 = p_1 \leq \cdots \leq p_k$. On the other hand,

$$1 - m = (1 - \sqrt{m})(1 + \sqrt{m}). \tag{6}$$

We will see later that the factors of the right-hand sides of both (5) and (6) are atoms in D_m.

Next, if some of the p_j's in (5) are equal, we omit their repetition; let $\{p_{j_1}, \ldots, p_{j_h}\}$ be the set obtained so. Since the only units of D_m are ± 1, see [5, Proposition 4.2] or [7, Lause 4.8], the atoms $p_{j_1}, \ldots, p_{j_h}$, $1 - \sqrt{m}$, $1 + \sqrt{m}$ are pairwise non-associated.

Assume first that $\mathcal{P}$ is such that

$$p_{j_1}, \ldots, p_{j_h}, 1 - \sqrt{m}, 1 + \sqrt{m} \in \mathcal{P}. \tag{7}$$

If $(1 - m)'$ exists, then, by (6),

$$(1 - m)' = 1 + \sqrt{m} + 1 - \sqrt{m} = 2.$$

On the other hand, (5) implies that

$$(1 - m)' = p_2 \cdots p_k + \cdots + p_1 \cdots p_{k-1} \geq p_2 + p_1 \geq 2 + 2 = 4$$

which contradicts the previous conclusion. So, $(1 - m)'$ is not well-defined under (7).

Second, if (7) does not hold, we anyway have

$$\pm p_{j_1}, \ldots, \pm p_{j_h}, \pm(1 - \sqrt{m}), \pm(1 + \sqrt{m}) \in \mathcal{P}$$

with an appropriate selection of signs. Hence a simple modification of the above argument is sufficient to show that the derivative of $1 - m$ is not well-definable.

Case 2. $m \equiv 2 \pmod 4$. Now m is even and $m \leq -6$. Thus, $4 - m$ is also an even composite number such that $4 - m \geq 10$. So, again

$$4 - m = p_1 \cdots p_k, \tag{8}$$

where k and $p_1, \ldots, p_k$ are as described above. On the other hand,

$$4 - m = (2 - \sqrt{m})(2 + \sqrt{m}). \tag{9}$$

The factors of the right-hand sides of (8) and (9) are atoms in D_m, see below.

We continue similarly as in Case 1 only replacing $1 \pm \sqrt{m}$ with $2 \pm \sqrt{m}$. So, assume first that

$$p_{j_1}, \ldots, p_{j_h}, 2 - \sqrt{m}, 2 + \sqrt{m} \in \mathcal{P}. \tag{10}$$

If $(4-m)'$ exists, then $(4-m)' = 2+\sqrt{m}+2-\sqrt{m} = 4$ by (9). However, we have $k > 2$ or $p_k > 2$, since otherwise $4-m = 2\cdot 2 = 4$ contradicting the assumption $m \leq -6$. By (8), we encounter a dilemma in both cases; if $k > 2$, then

$$(4-m)' \geq p_2p_3 + p_1p_3 + p_1p_2 \geq 4+4+4 = 12,$$

and

$$(4-m)' \geq p_{k-1} + p_k \geq 2+3 = 5$$

if $p_k > 2$. Consequently, $(1-m)'$ is not well-defined under (10). If $\mathcal{P}$ does not satisfy this condition, an analogous argument as at the end of Case 1 applies again.

To complete the proof, we still have to verify that the factors of the right-hand sides of (5), (6), (8) and (9) are atoms. We do so by using the norm function. We begin by noticing that $D_m = \mathbb{Z}(\sqrt{m}) = \{x + y\sqrt{m} \,|\, x, y \in \mathbb{Z}\}$, see [5, Theorem 3.2] or [7, Theorem 4.2]. An element $a = x + y\sqrt{m} \in D_m$ is rational if $y = 0$ and irrational if $y \neq 0$. If a is irrational, then, recalling that m is negative, we have

$$N(a) = x^2 - my^2 = x^2 + |m|y^2 \geq |m|.$$

If also $b \in D_m$ is irrational, then

$$N(ab) = N(a)N(b) \geq m^2. \tag{11}$$

Let $c \in D_m$ so that $c \neq 0, \pm 1$. If $c = ab$ where a and b are irrational, then $N(c) \geq m^2$ by (11). Therefore, c is an atom if the following two conditions are satisfied: (i) c has no rational atom divisor (except possibly $\pm c$) and (ii) $N(c) < m^2$.

Now choose any p_j from (5) or (8). It clearly satisfies the condition (i). Since $|m| \geq 5$, we have

$$p_j \leq p_k = \frac{1}{2}\cdot 2p_k \leq \frac{1}{2}p_1\cdots p_k \leq \frac{1}{2}(4-m) < \frac{1}{2}(5+|m|) \leq \frac{1}{2}\cdot 2|m| = |m|.$$

Hence $N(p_j) = p_j^2 < m^2$ and, consequently, also (ii) is satisfied. In other words, p_j is an atom in D_m.

Next, consider the factors of the right-hand sides of (6) and (9), i.e., $q = t \pm \sqrt{m}$, where $t \in \{1, 2\}$. If $r, x, y \in \mathbb{Z}$ so that $t \pm \sqrt{m} = r(x + y\sqrt{m})$, then $ry = \pm 1$ implying also that $r = \pm 1$. Consequently, q satisfies (i). Also the condition (ii) is now satisfied because

$$N(1 \pm \sqrt{m}) < N(2 \pm \sqrt{m}) = 4 - m < 5 + |m| \leq 2|m| < m^2.$$

So, these numbers are atoms also. □

We conclude this section by stating a sufficient condition under which the answer to Problem 5 is negative.

Theorem 7. *Let D be an* NUFD. *Assume that $a \in D$ can be factorized so that*

$$a = p_1p_2 = q_1q_2,$$

where p_1, p_2, q_1, q_2 are atoms with $\{p_1, p_2\} \neq \{q_1, q_2\}$. Then a does not have a well-defined derivative.

Proof. If a' exists, then, by the Leibniz rule,

$$a' = p_1 + p_2 = q_1 + q_2.$$

But two elements are uniquely defined by their sum and product. To show this, simply note that

$$\begin{aligned}\{p_1, p_2\} = \{q_1, q_2\} &\iff \forall x \in D : (x - p_1)(x - p_2) = (x - q_1)(x - q_2) \\ &\iff \forall x \in D : x^2 - (p_1 + p_2)x + p_1p_2 = x^2 - (q_1 + q_2)x + q_1q_2 \\ &\iff p_1 + p_2 = q_1 + q_2 \wedge p_1p_2 = q_1q_2.\end{aligned}$$

(To show the forward implication in the last equivalence, substitute $x = 0$ and $x = 1$.) Therefore $p_1 + p_2 \neq q_1 + q_2$ and our claim follows. □

Now we encounter another problem arising from Theorem 7.

Problem 8. *Does every* NUFD *contain an element a satisfying the assumption of Theorem 7?*

If the answer to this question is positive, then the answer to Problem 5 is negative.

3 Concluding remarks

We defined an arithmetic derivative on a UFD and asked in Problem 5 about the possibility to do so also in some NUFD. If $m \not\equiv 1 \pmod 4$ and $m < -2$, the FD of integers of $\mathbb{Q}(\sqrt{m})$ is an NUFD. We proved in Theorem 6 that the answer is negative in this case. If $m \equiv 1 \pmod 4$ and $m < 0$, then this FD is an NUFD if and only if $m \neq -3, -7, -11, -19, -43, -67, -163$, see [5, p. 93].

Surveying these m's might be the next step. However, it is an essentially more laborious task. Namely, assuming $m \equiv 1 \pmod 4$ implies ([5, Theorem 3.2] or [7, Theorem 4.2]) that $D_m = \{x + y(1 + \sqrt{m})/2 \mid x, y \in \mathbb{Z}\}$ which already complicates the situation compared to that in the proof of Theorem 6. More difficulties arise as the simple condition $m < -2$ is replaced with the condition excluding the mentioned values of m. Studying the integers of $\mathbb{Q}(\sqrt{m})$ for $m > 1$ may be even more difficult since, according to our knowledge, it is not completely understood which m's yield a UFD and which do not.

Obviously, an alternative way to try to advance is to study NUFD's different from those described above.

4 Acknowledgment

We thank the referee for valuable remarks, in particular for those that led us to formulate Theorem 7 and Problem 8.

References

[1] E. J. Barbeau, Remark on an arithmetic derivative, *Canad. Math. Bull.* **4** (1961), 117–122.

[2] P. M. Cohn, *Algebra, Volume 1*, John Wiley, 1974.

[3] J. Kovič, The arithmetic derivative and antiderivative, *J. Integer Seq.* **15** (2012), Article 12.3.8.

[4] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, http://oeis.org.

[5] I. N. Stewart and D. O. Tall, *Algebraic Number Theory*, Second Edition, Chapman and Hall, 1987.

[6] V. Ufnarovski and B. Åhlander, How to differentiate a number, *J. Integer Seq.* **6** (2003), Article 03.3.4.

[7] K. Väisälä, *Lukuteorian ja korkeamman algebran alkeet* [in Finnish], Otava, 1950.

2010 *Mathematics Subject Classification:* Primary 11A25; Secondary 11A51, 11R27.
Keywords: arithmetic derivative, unique factorization, non-unique factorization, quadratic field.

(Concerned with sequences A000040, A003415 and A005117.)

Received October 30 2012; revised version received January 1 2013. Published in *Journal of Integer Sequences*, January 1 2013.

Return to Journal of Integer Sequences home page.