INSTITUTE OF MATHEMATICS
of the
Polish Academy of Sciences

ul. Śniadeckich 8, P.O.B. 21, 00-956 Warszawa 10, Poland http://www.impan.pl

IM PAN Preprint 723 (2010)

Tomasz Maszczyk

Division with Remainder in Algebras with Valuation

Presented by Piotr M. Hajac

Published as manuscript

Received 05 May 2010

DIVISION WITH REMAINDER IN ALGEBRAS WITH VALUATION

TOMASZ MASZCZYK†

ABSTRACT. To any integral algebra with valuation an abelian group is associated, which measures how much the uniqueness of the division with remainder is violated. The analogy with the divisor class group is discussed. Examples of such groups are computed in cases of formal local rings of some cusps on an algebraic curve.

1. INTRODUCTION

In order to understand complexity of a singularity on an algebraic variety one can search, how much arithmetic properties expected for a local ring of a regular point, fail at a singular point. If one thinks, for instance, of the unique factorization property, one discovers that this failure is captured by an abelian group (the divisor class group), which can be in many cases effectively computed [1]. In this paper we consider the property of the unique division with remainder in local ring of a cusp on an algebraic curve completed with respect to the valuation coming from the unique dominating valuation ring. First, we develop some general theory of division with remainder in algebras with valuation, introduce the property of the unique division with remainder and define an abelian group, which captures its failure. We search carefully the behavior of our construction under completion. We also discuss the analogy and connection between our group and the divisor class group. Finally, we compute it in cases of some simple cusps. The property of strictly unique division with remainder has been already studied by Korotkov [3], whose result specializes for commutative rings to the case of polynomials over a field only. In this paper the uniqueness of division with remainder holds in fact up to the choice of some splitting, which allows applications to local rings, in the spirit of the Weierstrass Division Theorem.

†The author was partially supported by the KBN grant 2P03A 050 22.

Mathematics Subject Classification (2010): Primary 13F30, 13J10, 14H20.

2. Theory of unique division with remainder in algebras with valuation

Let R be a ring with 1, A - an integral R-algebra, K - the field of fractions of a domain A, U - the group of units of A. Let $v : A\backslash\{0\} \to S$ be a surjective valuation with values in a totally ordered non-negative abelian semigroup S, i.e.

1) $v(aa') = v(a) + v(a')$,
2) $v(a + a') \geq \min(v(a), v(a'))$ when $a + a' \neq 0$.

We will use frequently also the following well known property of valuations:

$$v(a + a') = v(a), \text{ if } v(a) < v(a').$$

Definition. Let

$$A_s := \{a \in A \mid v(a) \geq s\}.$$

We have a natural filtration such that:
i) $A_0 = A$,
ii) $A_s \subset A_t$, if $s \geq t$,
iii) $A_s A_t \subset A_{s+t}$.

Let S have the cancellation property. Then the valuation v extends uniquely to the surjective valuation v on K with values in $G(S)$ - the Grothendieck group of S.

Let K^* denote the topological multiplicative group of topological field K equipped with the topology of valuation.

By $\hat{A}$ we denote the completion of A with respect to the valuation. When saying about completion we always assume that $\hat{A}$ is integral.

Definition. We define on $A \setminus \{0\}$ the following relation: $a \sim a'$, if either $a = a'$, or $a \neq a'$ and $v(a' - a) > v(a)$.

Remark. $\sim$ is an equivalence relation and equivalent elements have the same valuation. Moreover $\sim$-equivalence classes are open.

Definition. We call A a *valuation algebra*, if $A\backslash\{0\} = \{a \in K \mid v(a) \geq 0\}$.

Definition. We call a valuation v *semi-discrete* if for every $s \in S$ the set $\{t \in S \mid t < s\}$ is finite.

Example. For $A = R[[x]]$ the order v with respect to x is a semi-discrete valuation.

Definition. Let $W \subset A \setminus \{0\}$ be a subset of elements w such that:

(W1) the canonical short exact sequence of R-modules

$$0 \to (w) \to A \to A/(w) \to 0$$

splits,

(W2) each $a \in A$ has a decomposition

$$a = wq + r,$$

where $v(r) < v(w)$ if $r \neq 0$.

Remark. All non-zero remainders r in all such decompositions (provided we fix a and w), are $\sim$ -equivalent, hence they have the same valuation. Given a splitting of the sequence (W1) there exists the unique decomposition with r in the image of $A/(w)$ under this splitting.

Example. Let $A = R[[x]]$, v - an order with respect to x, $w = x^n$. One usually chooses the splitting such that the image of $A/(w)$ consists of polynomials of degree $< n$.

Definition. We call A a *unique division with remainder domain*, if $W = A \setminus \{0\}$.

Theorem 1. *1.0.* $w \in W \Rightarrow A_{v(w)} = (w)$,

1.1. $U \subset W$,

1.2. $\{(w) \mid w \in W\}$ *is linearly ordered by inclusion,*

1.3. $WW \subset W$.

Proof of 1.0. Let $v(a) \geq v(w)$ and $a = wq + r$ be a decomposition as in (W1). If $r \neq 0$ then $v(r) < v(w) \leq v(a)$, so $v(r) = v(a - r)$. Therefore we get the following contradiction:

$$v(w) > v(r) = v(a - r) \geq v(w) + v(q) \geq v(w). \tag{1}$$

Proof of 1.1. We can divide by any $u \in U$ with the remainder $r = 0$.

Proof of 1.2. Let $w, w' \in W$. Dividing mutually with remainder we get

$$w' = wq + r, \tag{2}$$

$$w = w'q' + r'. \tag{3}$$

Therefore

$$w(1 - qq') = rq' + r', \tag{4}$$

$$v(w) \leq v(w) + v(1 - qq') = v(rq' + r'). \tag{5}$$

Let us assume that $r, r' \neq 0$.

If $v(w) \geq v(w')$, then by (5)

$$v(rq' + r') \geq v(w) \geq v(w') > v(r'). \tag{6}$$

Therefore

$$v(rq') = v((rq' + r') - r') = v(r') < v(w'). \tag{7}$$

On the other hand $v(r) \leq v(r) + v(q') = v(rq')$, hence $v(r) < v(w')$. Therefore we get the following contradiction

$$v(w) \leq v(w) + v(q) = v(wq) = v(w' - r) = v(r) < v(w). \tag{8}$$

By symmetry with respect to w and w' we get that the assumption $r, r' \neq 0$ leads to a contradiction. Consequently either $r = 0$ or $r' = 0$, hence either $(w') \subset (w)$ or $(w) \subset (w')$.

Proof of 1.3.

Lemma 1. *Given a non-zero-divisor w of any algebra A over a unital ring R there is a one-to-one correspondence between splittings of the short exact sequence of R-modules*

$$0 \to (w) \to A \to A/(w) \to 0$$

and endomorphisms $\varphi_w \in \mathrm{End}_R(A)$ of the R-module A such that for all $q \in A$ $\varphi_w(wq) = q$.

Proof of Lemma 1. A splitting of the above sequence may be viewed as a morphism of R-modules $\pi_w : A \to (w)$ such that $\pi_w(wq) = wq$. Since w is not a zero divisor, then there exists the unique $\varphi_w \in \mathrm{End}_R(A)$ such that $\pi_w(a) = w\varphi_w(a)$. Then we have

$$w\varphi_w(wq) = \pi_w(wq) = wq. \tag{9}$$

Since w is not a zero-divisor, then this implies that $\varphi_w(wq) = q$. □

Let φ_w and $\varphi_{w'}$ correspond to the two splittings of respective sequences for w and w'. If we put $\varphi_{ww'} := \varphi_{w'} \circ \varphi_w$ then

$$\varphi_{ww'}(ww'q) = \varphi_{w'}(\varphi_{ww}(w(w'q))) = \varphi_{w'}(w'q) = q, \tag{10}$$

so $\varphi_{ww'}$ corresponds to a splitting of the respective sequence for ww'.

Let us take $a \in A$ and perform two consequtive divisions with remainder:

$$a = wq + r, \quad v(r) \ < v(w) \quad \text{if } r \neq 0, \tag{11}$$

$$q = w'q' + r', \ v(r') < v(w') \ \text{ if } r' \neq 0. \tag{12}$$

We get

$$a = (ww')q' + (wr' + r). \tag{13}$$

Let $r, r' \neq 0$. Then

$$v(wr') = v(w) + v(r') \geq v(w) > v(r), \tag{14}$$

hence

$$v(wr' + r) = v(r) < v(w) \leq v(w) + v(w') = v(ww'). \tag{15}$$

If were $wr' + r = 0$, we would get the following contradiction

$$v(r) = v(wr') = v(w) + v(r') > v(r) + v(r') \geq v(r). \tag{16}$$

Let $r = 0$, $r' \neq 0$. Then

$$a = (ww')q' + wr', \tag{17}$$

$$v(wr') = v(w) + v(r') < v(w) + v(w') = v(ww'). \tag{18}$$

Since $r' \neq 0$ then $wr' \neq 0$.
Let $r \neq 0$, $r' = 0$. Then

$$a = (ww')q' + r, \tag{19}$$

$$v(r) < v(w) \leq v(w) + v(w') = v(ww'). \tag{20}$$

Let $r, r' = 0$. Then

$$a = (ww')q'. \ \square \tag{21}$$

Definition. The kernel of the endomorphism $\mathrm{id}_A - w\varphi_w$ is equal to the ideal (w), so this endomorphism defines an embedding $A/(w) \hookrightarrow A$.
Let us denote its image by H. Of course $(w) \cap H = 0$.

Corollary 1. *Let* $N := v(W) \subset S$ *and*

$$(W)_n := (w) \quad where \quad w \in W \quad and \quad v(w) = n.$$

By 1.0 $(W)_n$ *does not depend on the choice of* w *provided* $v(w) = n$. *By 1.1, 1.2, 1.3* N *is a linearly ordered sub-semigroup in* S *and we get the natural filtration:*
1.1.1) $(W)_0 = A$,
1.1.2) $(W)_m \subset (W)_n$, *if* $m \geq n$,
1.1.3) $(W)_m(W)_n \subset (W)_{m+n}$.

By 1.0 both filtrations are compatible: for $n \in N$

$$A_n = (W)_n.$$

Definition. We define the following abelian groups

$$@(A) := K^*/G(W),$$
$$@'(A) := G(S)/G(N).$$

Proposition 1. *If A is a valuation algebra, then the canonical epimorphism induced by the valuation*

$$@(A) \to @'(A)$$

is an isomorphism.

Proof. From the short exact sequence

$$0 \to U \to K^* \to G(S) \to 0 \tag{22}$$

by the definition of $@(A)$ we get the short exact sequence

$$0 \to G(W)/U \to G(S) \to @(A) \to 0, \tag{23}$$

which fits into the canonical diagram with exact rows and columns

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & 0 \arrow[d] & 0 \arrow[d] & ker \arrow[d] & \\
0 \arrow[r] & G(W)/U \arrow[r] \arrow[d] & G(S) \arrow[r] \arrow[d] & @(A) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & G(N) \arrow[r] \arrow[d] & G(S) \arrow[r] \arrow[d] & @'(A) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0. &
\end{tikzcd}$$

Therefore, by the snake lemma we get $ker = 0$. □

Theorem 2. *An integral domain A with valuation is unique division with remainder iff $@(A) = 0$.*

Proof. We have to prove that if $@(A) = 0$ then $A \setminus \{0\} \subset W$.

If $@(A) = 0$ then $K^* = G(W)$. Let us take

$$w = \frac{w'}{w''} \in A \setminus \{0\}, \quad \text{where } \ w', w'' \in W. \tag{24}$$

If we put

$$\varphi_w(a) := \varphi_{w'}(w''a), \tag{25}$$

then

$$\varphi_w(wa) = \varphi_{w'}(ww''a) = \varphi_{w'}(w'a) = a. \tag{26}$$

Let us take $a \in A \setminus \{0\}$ and divide $w''a$ with remainder by w':

$$w''a = w'q + r', \tag{27}$$

Then

$$a = wq + r, \tag{28}$$

where $r = r'/w''$. Of course $r = a - wq \in A \subset K$. If $r \neq 0$ then $r' \neq 0$, hence $v(r') < v(w')$ and we get

$$v(r) = v(r') - v(w'') < v(w') - v(w'') = v(w). \tag{29}$$

Therefore $w \in W$. □

Remark. Theorem 2 is an analog of the well known theorem for noetherian normal domains in which the divisor class group plays the role of our group @:

Theorem 2'. *A is a unique factorization domain iff* $\mathrm{Cl}(A) = 0$.

Remark. If v is semi-discrete and A is a unique division with remainder domain then we have the Euclid algorithm for A. Therefore if A is also noetherian then it is a principal ideal domain, hence a unique factorization domain. This shows, that in this particular case the following implication holds

$$@(A) = 0 \;\Rightarrow\; \mathrm{Cl}(A) = 0. \tag{30}$$

In general, however, the relationship between our @ and other arithmetical invariants is not clear.

An analog of the Weierstrass Division Theorem looks as follows:

Theorem 3. *Let in addition S satisfy Archimedes' axiom and let A be complete with respect to the valuation. Then W is a union of $\sim$-equivalence classes.*

Proof. We have to prove that if $w \in W$ and $w' \sim w$ then $w' \in W$ as well. Let us choose a splitting $\varphi_w \in \mathrm{End}_R(A)$ according to Lemma 1.

Let $v(w' - w) > v(w)$. Let us divide any $a \in A$ with remainder by w

$$a = wq + r, \tag{31}$$

where $q = \varphi_w(a)$, $r = a - w\varphi_w(a)$. We have

$$v((w' - w)q) = v(w' - w) - v(w) + v(wq). \tag{32}$$

If $r = 0$ then

$$v(wq) = v(a). \tag{33}$$

If $r \neq 0$ then

$$v(wq) = v(w) + v(q) \geq v(w) > v(r) = v(wq + r) = v(a). \tag{34}$$

Then in both cases

$$v(wq) \geq v(a), \tag{35}$$

hence by (32)

$$v((w' - w)\varphi_w(a)) \geq v(w' - w) - v(w) + v(a). \tag{36}$$

Lemma 2. *φ_w is automatically continuous.*

Proof of Lemma 2. Let us divide any $a \in A$ with remainder by w

$$a = wq + r, \tag{37}$$

where $q = \varphi_w(a)$, $r = a - w\varphi_w(a)$.

If $r = 0$ then

$$v(\varphi_w(a)) = v(a) - v(w). \tag{38}$$

If $r \neq 0$ then $v(r) < v(w)$. Since $v(q) \geq 0$ then

$$v(wq) = v(w) + v(q) \geq v(w) > v(r), \tag{39}$$

hence

$$v(wq) > \min(v(wq), v(r)) = v(wq + r) = v(a), \tag{40}$$

so

$$v(\varphi_w(a)) > v(a) - v(w). \tag{41}$$

In both cases

$$v(\varphi_w(a)) \geq v(a) - v(w), \tag{42}$$

hence φ_w is continuous in the topology of v. □

Let $I_k := A_{ks}$, where $k = 0, 1, ...,$ and $s := v(w' - w) - v(w)$. Then

$$I_0 = A,\ I_k \to 0,$$
$$(w' - w)\varphi_w(I_k) \subset I_{k+1},$$

hence by Theorem 2.2 of [4] we have the unique decomposition

$$a = w'q' + r' \tag{43}$$

with $r' \in H$, and the respective short exact sequence for w' is split with the same H. Moreover we have

$$r' - r = (w - w')q + w'(q' - q). \tag{44}$$

Let $r \neq 0$. Then

$$v((w - w')q) = v(w - w') + v(q) > v(w) + v(q) \geq v(w) > v(r), \tag{45}$$

$$v(w'(q' - q)) = v(w') + v(q' - q) = v(w) + v(q' - q) \geq v(w) > v(r). \tag{46}$$

So,

$$v(r'-r) \geq \min(v((w-w')q), v(w'(q'-q))) > v(r), \tag{47}$$

hence $r' \neq 0$, $r' \sim r$ and therefore

$$v(r') = v(r) < v(w) = v(w'). \tag{48}$$

Let $r = 0$. By 1.0 there exists $p \in A$ such that $w' = wp$. Therefore from (44)

$$r' = wq - w'q' = w(q - pq') \in (w). \tag{49}$$

But $r' \in H$ and $H \cap (w) = 0$, hence $r' = 0$. Consequently, $w' \in W$. □

Example. $A = R[[x]]$, v - an order with respect to x, $w = c_n x^n$ with c_n invertible in R. Of course $w \in W$ and we can choose the respective splitting such that H is the R-submodule in $R[[x]]$ consisting of polynomials of degree $< n$. Let

$$w' = c_n x^n + c_{n+1}x^{n+1} + ...,$$

with arbitrary c_m for $m > n$. Since $w \sim w'$, then $w' \in W$ as well. Therefore, if R is a field A is a unique division with remainder domain.

Corollary 2. *Under assumptions of Theorem 3 the group* $@(A)$ *with the quotient topology is a discrete group.*

Proof. We have to prove that the subgroup $G(W)$ is open in K^*. For that it is enough to show that if for any given $x \in K^*$

$$v(x - \frac{w}{w'}) \gg 0 \ \text{ for some } w, w' \in W, \tag{50}$$

there exist $w'', w''' \in W$ such that

$$x = \frac{w''}{w'''}. \tag{51}$$

Let

$$v(x - \frac{w}{w'}) > \max(v(w) - v(w'), 0). \tag{52}$$

Then

$$v(xw' - w) > v(w), \tag{53}$$

hence $xw' \sim w$ and by Theorem 3 $w'' := xw'$ belongs to W. Then indeed

$$x = \frac{w''}{w'}, \tag{54}$$

and one can take $w''' := w'$. □

The following theorem describes the behaviour of @ groups under completion.

Theorem 4. *Let in addition S satisfy Archimedes' axiom and let*

$$A \hookrightarrow A' \tag{55}$$

be a dense valuation preserving embedding into a complete A'. Then W embeds into W' and this induces the epimorphism of groups

$$@(A) \twoheadrightarrow @(A'). \tag{56}$$

If in addition W is dense in W' the above homomorphism is an isomorphism.

Proof. Let $w \in W \subset A$ and φ_w be a respective splitting. We have the implication

$$a - w\varphi_w(a) \neq 0 \quad \Rightarrow \quad v(a - w\varphi_w(a)) < v(w). \tag{57}$$

Let $a_n \to a'$. Then $a_n - w\varphi_w(a_n) \to a' - w\varphi_w(a')$, where

$$\varphi_w(a') := \lim_n \varphi_w(a_n) \tag{58}$$

is well defined independently of the choice of the sequence $a_n \to a'$ because by Lemma 2 φ_w is continuous R-linear and A' is complete.

Lemma 3. *For every R-algebra A with valuation $v : A \setminus \{0\} \to S$ as in the beginning, we have the following implication*

$$a_n \to a, \ v(a_n) < s \ \Rightarrow \ v(a) < s. \tag{59}$$

Proof of Lemma 3. Let us suppose that $v(a) \geq s$. For almost all n $v(a_n - a) \geq s$, hence for almost all n

$$v(a_n) = v((a_n - a) + a) \geq \min(v(a_n - a), v(a)) \geq s. \tag{60}$$

Contradiction. □

Therefore, by continuity of φ_w, we get the following sequence of implications

$$a' - w\varphi_w(a') \neq 0 \ \Rightarrow \ a_n - w\varphi_w(a_n) \neq 0 \text{ for almost all } n \tag{61}$$

$$\Rightarrow v(a_n - w\varphi_w(a_n)) < v(w) \ \Rightarrow \ v(a' - w\varphi_w(a')) < v(w) \text{ for almost all } n, \tag{62}$$

hence $W \hookrightarrow W'$ and consequently $G(W) \hookrightarrow G(W')$. Thus the dense embedding $K^* \hookrightarrow K'^*$ induces a continuous homomorphism of topological groups $@(A) \to @(A')$ with dense image. Since the right-hand side group is discrete, then it is an epimorphism. Now we are to show that if W is dense in W' then it is also a monomorphism.

Lemma 4. *$G(W)$ is closed in K^*.*

Proof of Lemma 4. Let us take a sequence

$$G(W) \ni \frac{w_n'}{w_n} \to \frac{a'}{a} \in K^*. \tag{63}$$

Then for almost all $n \in \mathbb{N}$

$$v(\frac{w_n'}{w_n} - \frac{a'}{a}) > -v(a), \tag{64}$$

or equivalently

$$v(w_n'a - w_na') > v(w_n). \tag{65}$$

But the equality

$$w_n'a = w_na' + (w_n'a - w_na') \tag{66}$$

is a division of $w_n'a$ by w_n with the remainder $w_n'a - w_na'$, so if were $w_n'a - w_na' \neq 0$, then would be $v(w_n'a - w_na') < v(w_n)$, because all non-zero remainders in division by w_n have the same valuation $< v(w_n)$. Contradiction.

Therefore for almost all $n \in \mathbb{N}$ $w_n'a - w_na' = 0$, hence

$$\frac{a'}{a} = \frac{w_n'}{w_n} \in G(W). \ \Box \tag{67}$$

Lemma 5. *If in the following commutative diagram of subspaces of a topological space Y'*

$$\begin{tikzcd}
X \arrow[r, phantom, "\subset"] \arrow[d, phantom, "\cap"] & X' \arrow[d, phantom, "\cap"] \\
Y \arrow[r, phantom, "\subset"] & Y'
\end{tikzcd}$$

X is dense in X' and closed in Y , then $Y \cap X' = X$.

Proof of Lemma 5. Of course $X \subset Y \cap X'$. Let $\overline{X}$ be the closure of X in Y'.

Since X is dense in X', then $X' \subset \overline{X}$.

Since X is closed in Y , then $Y \cap \overline{X} \subset X$. Therefore we get

$$Y \cap X' \subset Y \cap \overline{X} \subset X. \ \Box \tag{68}$$

Taking the diagram

$$\begin{tikzcd}
G(W) \arrow[r] \arrow[d] & G(W') \arrow[d] \\
K^* \arrow[r] & K'^*,
\end{tikzcd}$$

assuming that W is dense in W', hence $G(W)$ is dense in $G(W')$, and applying Lemma 4 and Lemma 5 we get

$$K^* \cap G(W') = G(W), \tag{69}$$

hence the homomorphism (56) is indeed an embedding. □

Remark. By Lemma 4 @(A) with the canonical quotient topology is always Hausdorff.

Finally, we will show that the situation of our Example arises in a canonical way in the process of some completion.

Theorem 5. *Let $t \in A$ be not a zero divisor of a commutative R-algebra A over a commutative ring R, such that the following canonical homomorphism*

$$R \to A/(t) \tag{70}$$

is an isomorphism. Then t is transcendental over R and we have the canonical isomorphism of R-algebras

$$\lim_{n} A/(t)^n = R[[t]]. \tag{71}$$

Proof. First of all, under the assumption the canonical homomorphism $R \to A$ is injective. Let us assume now that t is algebraic over R, i.e. there are $r_0, ..., r_n \in R$ not all equal to zero, such that

$$r_n t^n + r_{n-1} t^{n-1} + ... + r_0 = 0. \tag{72}$$

Then reducing by (t) we get $r_0 = 0$, hence

$$r_n t^{n-1} + r_{n-1} t^{n-2} + ... + r_1 = 0, \tag{73}$$

because t is not a zero divisor. Repeating this procedure we get that all r_i's are zero. Contradiction shows that t is transcendental over R.

Now we are to show that for every $n = 0, 1, 2, ...$ the isomorphism $R \to A/(t)$ induces canonical splittings of the following canonical short exact sequences

$$0 \to (t)^n \to A \to A/(t)^n \to 0 \tag{74}$$

such that the image $H_n \subset A$ of $A/(t)^n$ consists of elements of the form

$$a = a_0 + a_1 t + ... + a_{n-1} t^{n-1}, \tag{75}$$

where $a_i \in R$. We will prove it by induction.

To start the induction we compose the canonical homomorphism $R \to A$ with the inverse to the isomorphism $R \to A/(t)$ to get a splitting $A \leftarrow A/(t)$ of the short exact sequence (74) for $n = 1$ as follows

$$\begin{tikzcd} 0 \arrow[r] & (t) \arrow[r] & A \arrow[r] & A/(t) \arrow[r] & 0. \\ & & R \arrow[u] \arrow[ur] & & \end{tikzcd} \tag{76}$$

Let $\varphi_t \in \mathrm{End}_R(A)$ be the respective endomorphism, as in Lemma 1.

Since the projection $A \to A/(t)$ and the splitting $A \leftarrow A/(t)$ are unit preserving, the endomorphism $\varphi_t \in \mathrm{End}_R(A)$ annihilates the unit $1 \in A$, hence $H_1 = R$, as it should be. Then, according to (10), the endomorphism

$$\varphi_{t^n} := \varphi_t^n = \varphi_t \circ ... \circ \varphi_t \tag{77}$$

defines the splitting of the respective sequence for t^n and $H_n = \mathrm{ker}\varphi_{t^n}$.

We have

$$\varphi_t^n(a) = \varphi_t(\varphi_t^{n-1}(a)). \tag{78}$$

Therefore, for every $a \in H_n$, putting $a_n := \varphi_t^n(a) \in H_1 = R$, we have

$$\varphi_t^n(a - a_n t^n) = 0, \tag{79}$$

since by (77) $\varphi_t^n(t^n) = \varphi_{t^n}(t^n) = 1$, so $(a - a_n t^n) \in H_n$. If H_n consists already of elements of the desired form, then there exist $a_0, ..., a_{n-1} \in R$ such that

$$a - a_n t^n = a_0 + a_1 t + ... + a_{n-1} t^{n-1}, \tag{80}$$

hence a is also of that form.

Now it is clear that the canonical homomorphism of R-algebras

$$R[t] \to A \tag{81}$$

induces a compatible system of isomorphisms

$$R[t]/(t)^n \to A/(t)^n, \tag{82}$$

which gives the desired canonical isomorphism of limits. □

The above theorem has the following immediate consequence in algebraic geometry.

Corollary 3. *The formal neighborhood of any Cartier divisorial section of a fibration of an integral scheme is locally canonically isomorphic to the formal neighborhood of the zero section in the trivial line bundle.*

The Cartier hypothesis for the divisor in the above theorem is necessary as the following example shows.

Example. Take $R := k[X]$, the ring of polynomial functions on the affine line over a field k, $A := k[X, Y, Z]/(Z^2 - XY)$, the ring of polynomial functions on the quadratic cone fibred over the affine line by the ring homomorphism $k[X] \to k[X, Y, Z]/(Z^2 - XY)$, $X \mapsto X$. The (non-principal) ideal $I := (Y, Z) \subset A$ cuts out a Weil divisorial section of this fibration. Since the conormal module $I/I^2 = (k[X]/(X))Y \oplus k[X]Z$ is not locally free, the formal neighborhood of that divisorial section can not be locally trivial.

3. Application to singularities of algebraic curves

In this paragraph we will give examples of computing $@(A)$, when A is a formal local ring of a point on an algebraic curve over a field R, being formally irreducible at this point. The valuation comes from the discrete valuation ring of a point on the normalization dominating a given point. Then @ of that is an invariant of formal equivalence [5], in particular points with different @ cannot be formally equivalent.

Example. *Smooth point.* The formal local ring of a smooth point is isomorphic to $R[[x]]$. Therefore by the last example

$$@(A) = 0. \tag{83}$$

Example. *One-branch singularity.* Let us recall that a singular point on an algebraic curve over a field R is called *one-branch singularity* (or *generalized cusp*) if its local ring is contained in one and only one valuation ring of the field of rational functions of a given curve. The following theorem (Thm. 1 of [2]) describes all formal local rings of such singularities.

Theorem. *The complete local ring of a one-branch singularity is isomorphic to a proper R-subalgebra of R[[t]] which contains its conductor. Every such subalgebra is isomorphic to a formal local ring of some one-branch singularity.*

Let us consider, for example, a singular point of a curve over a field R, formally equivalent at this point to the cusp $y^2 = x^d$ for $d = 3,\ 5$. We claim that

$$@(A) \cong R \oplus \mathbb{Z};\ \text{for } d = 3, \tag{84}$$

$$@(A) \cong R^2 \oplus \mathbb{Z};\ \text{for } d = 5,\ \text{char}(R) \neq 3. \tag{85}$$

Let us compute this. The formal local ring $A = R[[x, y]]/(y^2 - x^d)$ is integral. The normalization has the form

$$R[[x, y]]/(y^2 - x^d) \hookrightarrow R[[t]], \tag{86}$$

$$x \mapsto t^2,\ y \mapsto t^d. \tag{87}$$

The image of that consists of formal series of the form:

$$a \ = \ a_0 + a_2t^2 + a_3t^3 + a_4t^4 + ...,\quad \text{for } d = 3, \tag{88}$$

$$a \ = \ a_0 + a_2t^2 + a_4t^4 + a_5t^5 + ...,\quad \text{for } d = 5 \tag{89}$$

(for $d = 3$ without a summand of degree 1, for $d = 5$ without summands of degree 1 and 3). The valuation is an order with respect to t. Using the above representation one can easily see that for $d = 2 : W =$

$R^* + (t)^2$ and for $d = 5 : W = R^* + R \cdot t^2 + (t)^4$, where (t) is the maximal ideal in the dominating discrete valuation ring $R[[t]]$. Indeed, by Theorem 4 it is enough to show that if $t^n \in W$ then $n = 0$. By definition $w \in W$ iff for every $a \in A$ there exists $q \in A$ such that

$$v(a - wq) \geq v(w) \;\Rightarrow\; a - wq = 0. \tag{90}$$

When $n \geq 2$ let us take

$$w = t^n, \; a = t^{n+1}, \tag{91}$$

Then, in both cases $d = 3, \; 5$, for all $q = q_0 + q_2 t^2 + ...$ we have $a - wq = -q_0 t^n + t^{n+1} - ...$, and of course $a - wq \neq 0$ but $v(a - wq) \geq v(w)$. Therefore in both cases $G(W)$ coincides with the group of units U of A and is contained in the group of units $R^* + (t)$ of $R[[t]]$. The field K of fractions of A coincides with the field of fractions of its normalization, which is a field of Laurent series

$$a = a_{-n} t^{-n} + ... + a_0 + a_1 t + ... \tag{92}$$

Therefore the short exact sequence of multiplicative abelian groups, for $d = 3$ or $d = 5$ respectively,

(93)
$$1 \to (R^* + (t))/(R^* + (t)^2) \to K^*/(R^* + (t)^2) \to K^*/(R^* + (t)) \to 1,$$

(94)
$$1 \to (R^* + (t))/(R^* + R \cdot t^2 + (t)^4) \to K^*/(R^* + R \cdot t^2 + (t)^4) \to K^*/(R^* + (t)) \to 1$$

is isomorphic to the split short exact sequence of abelian groups

$$1 \to G_d \to @(A) \to \mathbb{Z} \to 1, \tag{95}$$

where G_d is a multiplicative quotient group. For $d = 3$ the latter abelian group is isomorphic to the additive quotient group

$$G_3 \cong (t)/(t)^2 \cong R. \tag{96}$$

For to understand the structure of the group G_5 let us use the following factorization.

(97)
$$a_0 + a_1 t + a_2 t^2 + a_3 t^3 + ... = (1 + b_1 t + b_3 t^3)(c_0 + c_2 t^2 + c_4 t^4 + ...).$$

Provided a_0 is invertible in R this factorization is unique. Therefore G_5 can be identified with the set of pairs (b_1, b_3) with the group law coming from the following unique decomposition

$$(1 + b_1 t + b_3 t^3)(1 + b'_1 t + b'_3 t^3) \tag{98}$$

$$= (1 + b''_1 t + b''_3 t^3)(c_0 + c_2 t^2 + c_4 t^4 + ...), \tag{99}$$

i.e.

$$(b_1, b_3)(b'_1, b'_3) = (b_1 + b'_1, b_3 + b'_3 - (b_1 + b'_1)b_1 b'_1). \tag{100}$$

It is easy to see that if $\mathrm{char}(R) \neq 3$ then we have the following isomorphism onto the additive group

$$\begin{gathered} G_5 \to R^2, \\ (b_1, b_3) \mapsto (b_1, b_3 + \frac{1}{3}b_1^3). \end{gathered} \tag{101}$$

References

[1] Bingener, J.; Storch, U.: *On the computation of the divisor class group of complete local rings* (German), Nova Acta Leopoldina (N.F.) **52** no. 240 (1981), 7–63.

[2] Ebey, S.: *The classification of singular points of algebraic curves.* Trans. Am. Math. Soc. **118** (1965), 454-471.

[3] Korotkov, M. V.: *Description of rings with single-valued division with remainder.* (Russian) Uspehi Mat. Nauk **31** (1976), no.1(187), 253-254.

[4] Łojasiewicz, S.; Maszczyk, T.; Rusek, K.: *On the Weierstrass division.* Univ. Iagell. Acta Math., Fasc. **XXXIX** (2001), 49-58.

[5] Rosenlicht, M.: *Equivalence relations on algebraic curves.* Amer. J. Math. (2) **56** (1952), 169-191.

Institute of Mathematics, Polish Academy of Sciences,
Sniadeckich 8, 00–956 Warszawa, Poland

Institute of Mathematics, University of Warsaw,
Banacha 2, 02–097 Warszawa, Poland
E-mail address: `maszczyk@mimuw.edu.pl`