ON THE STRUCTURE OF NON-COMMUTATIVE REGULAR LOCAL RINGS OF DIMENSION TWO

MICHEL VAN DEN BERGH AND MARTINE VAN GASTEL

Abstract. In this paper we conjecture that the center of a non-commutative complete regular local ring of global dimension two is a formal power series ring in two variables. We prove this conjecture in the special case of Ore extensions.

1. Introduction

Below k is a field. In this paper we will be concerned with rings of the form $C = k\langle\langle x, y\rangle\rangle/(r)$ where r only has term of total degree ≥ 2 and where the quadratic part of r is non-degenerate. Such rings have global dimension two [7] and it may be argued that they are the non-commutative analogues of two-dimensional regular local rings.

In this paper we propose the following conjecture:

Conjecture 1.1. Let C be as above. Then the center of C is either trivial, or else it is a formal power series ring in two variables. If the quadratic part of r is of the form $yx - xy$ and the characteristic p of k is > 0 then $Z(C)$ is generated by elements of the form $x^{p^n} + \cdots$ and $y^{p^n} + \cdots$ for some $n > 0$.

In this paper we will provide some evidence for this conjecture by proving it in the case that C is given by an Ore extension $C = B[[y; \sigma, \delta]]$ where B is $k[[x]]$, σ is a k-linear automorphism of B and δ is a k-linear σ-derivation of B. Thus δ satisfies $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ and C is obtained from B by adjoining the variable y subject to the commutation rule

$$y\,b = \sigma(b)y + \delta(b) \tag{1.1}$$

In other words $C = k\langle\langle x, y\rangle\rangle/(r)$ where r is given by $yx - \sigma(x)y - \delta(x)$. Thus for r to have only terms of degree ≥ 2 it is necessary that $\delta(x)$ contains only terms of degree ≥ 2. We assume this throughout.

We will prove the following theorem:

Theorem 1.2. *If C is an Ore extension as above then Conjecture 1.1 holds.*

Our treatment of the case where σ is trivial relied originally on the following combinatorial result by G. Baron and A. Schinzel in [1].

Proposition 1.3. *For any prime p and any residues x_i mod p, we have:*

$$\sum_{\sigma \in S_{p-1}} x_{\sigma(1)}(x_{\sigma(1)} + x_{\sigma(2)}) \ldots (x_{\sigma(1)} + \ldots + x_{\sigma(p-1)})$$
$$\equiv (x_1 + \cdots + x_{p-1})^{p-1} \pmod{p}$$

1991 *Mathematics Subject Classification.* Primary 16L30.
Key words and phrases. Ore extensions.

where S_{p-1} is the group of all permutations σ of $\{1,\ldots,p-1\}$.

Afterwards we discovered a new approach which is independent of the above result. It turns out that we can now even give a new proof of the result by G. Baron and A. Schinzel. This proof is produced in the final section of this paper. Whereas the proof in [1] is rather technical, our proof is straightforward and relies on general computations with derivations.

2. Outline

In this section we outline our strategy for proving Theorem 1.2. First we dispense with some trivial cases. If σ is trivial and $\delta = \mathrm{id}$ then there is nothing to prove. In addition it is easy to prove that in the following cases the center of C is trivial.

(1) σ is trivial, δ is not trivial and $p = 0$.
(2) The order of σ is infinite.

In subsequent sections we deal with the remaining cases. In Section 3 we discuss the case where σ is the identity and $p > 0$. In Section 4 we focus on the case where δ is trivial and σ is not trivial but has finite order. Finally in Section 5 we deal with the case where both σ and δ are non-trivial and σ has finite order. In this last case our approach is somewhat indirect and we do not obtain nice expressions for the elements generating the center.

3. The case where σ is the identity and $p > 0$

It follows from (1.1) that in this case the commutation relation between y and x is given by

$$yx = xy + \delta(x) \tag{3.1}$$

In this case we prove that $Z(C)$ equals $k[[z,w]]$, where $z = x^p$ and $w = y^p - c_p(x)\,y$, with $c_p(x) = \frac{\partial}{\partial x}\left(\frac{\partial}{\partial x}\left(\ldots\left(\frac{\partial\,\delta(x)}{\partial x}\cdot\delta(x)\right)\ldots\cdot\delta(x)\right)\cdot\delta(x)\right)$, in which $\frac{\partial}{\partial x}$ and $\delta(x)$ occur $(p-1)$ times.

It is obvious that $[x,z] = 0$, Furthermore from

$$[y,z] = \sum_{a+b=p-1,a,b\geq 0} x^a\delta(x)x^b = p\delta(x)x^{p-1} = 0$$

we deduce that z also commutes with y. Hence z is in the center of C.

To prove that w is in the center of C we use the following key-lemma. This lemma will also be used in the new proof of Proposition 1.3.

Lemma 3.1. *Let $f \in B$, and let g be the element $\frac{\partial}{\partial x}\left(\frac{\partial}{\partial x}\left(\ldots\left(\frac{\partial f}{\partial x}\cdot f\right)\ldots\cdot f\right)\cdot f\right)$ of B, where both $\frac{\partial}{\partial x}$ and f occur $(p-1)$ times. Then $\frac{\partial g}{\partial x} = 0$.*

Proof. Without loss of generality we may assume that $f \neq 0$. Define the derivation d of B by $d(b) := \frac{\partial b}{\partial x}\cdot f$, and consider the differential operator $e = d^p - g\cdot d$ on B. Since the pth power of a derivation is also a derivation, it follows that e is also a derivation.

If we evaluate e in x, we get $e(x) = d^p(x) - g \cdot d(x) = d^{p-1}(f) - g \cdot f = d^{p-2}\left(\frac{\partial f}{\partial x} \cdot f\right) - g \cdot f = \ldots = f \cdot \frac{\partial}{\partial x}\left(\frac{\partial}{\partial x}\left(\ldots\left(\frac{\partial f}{\partial x} \cdot f\right) \ldots \cdot f\right) \cdot f\right) - g \cdot f = f \cdot g - g \cdot f = 0$ and so e is identically zero on B.

In particular e commutes with d. Computing with operators, we find $0 = [d, e] = [d, d^p - g \cdot d] = dg \cdot d$. Evaluating at x and using the fact that $f \neq 0$, this yields $\frac{\partial g}{\partial x} = 0$. □

Let y_l, respectively y_r be left, respectively right multiplication by y on B. Because y_l and y_r commute, we see that $[y, -]^p = \sum_{i=0}^{p} \binom{p}{i} y_l^i \, (-y_r)^{p-i} = y_l^p - y_r^p = [y^p, -]$. It follows that we have $[y^p, x] = [y, [y, \ldots, [y, \delta(x)] \ldots]]$ ($(p-1)$ times y) and by repeatedly using the fact that $[y, f(x)] = \frac{\partial f(x)}{\partial x}[y, x] = \frac{\partial f(x)}{\partial x} \cdot \delta(x)$, for all $f(x) \in B$, we deduce, for $f(x) = \delta(x)$, $[y^p, x] = c_p(x)\,[y, x]$.

It follows that w commutes with x. Let us prove that it also commutes with y. $[y, w] = [y, c_p(x)]\, y = \frac{\partial c_p(x)}{\partial x}\,[y, x]\, y$ and applying Lemma 3.1 with $f = \delta(x) \in B$, we deduce $[y, w] = 0$. So we obtain $k[[z, w]] \subset Z(C)$.

Let $Q(Z(C))$ and $Q(C)$ be respectively the quotientfields of $Z(C)$ and C. Since $\{x^a y^b \mid 0 \leq a, b \leq p-1\}$ is a basis of C over $k[[z, w]]$, we see that C is free of rank p^2 over $k[[z, w]]$. This implies that $p^2 = \dim_{k((z,w))} Q(Z(C)) \cdot \dim_{Q(Z(C))} Q(C)$, so $\dim_{Q(Z(C))} Q(C) \in \{1, p, p^2\}$. Since C is not commutative and $\dim_{Q(Z(C))} Q(C)$ is a square according to [3], it follows that $\dim_{Q(Z(C))} Q(C) = p^2$ and furthermore that $Z(C)$ and $k[[z, w]]$ have the same quotientfield.

As indicated above C is free of rank p^2 over $k[[z, w]]$. In particular C is finitely generated as a module over $k[[z, w]]$. It follows that $Z(C)$ is also finitely generated as a module over $k[[z, w]]$ and thus $Z(C)$ is integral over $k[[z, w]]$. Since $k[[z, w]]$ is integrally closed, it follows that $Z(C) = k[[z, w]]$.

So in order to complete the proof Conjecture 1.1 in this special case, we have to show that if $v(\delta(x)) \geq 3$ then $v(c_p(x)) > p - 1$, where v is the x-adic valuation on B. Therefore, let $c_r(x)$ be equal to $\frac{\partial}{\partial x}\left(\frac{\partial}{\partial x}\left(\ldots\left(\frac{\partial \delta(x)}{\partial x} \cdot \delta(x)\right) \ldots \cdot \delta(x)\right) \cdot \delta(x)\right)$ in which $\frac{\partial}{\partial x}$ and $\delta(x)$ occur $(r-1)$ times and this for all $r \geq 2$.
We prove by induction that $v(c_r(x)) \geq 2(r-1)$.

Since $v(\delta(x)) \geq 3$, $v(c_2(x)) = v\left(\frac{\partial \delta(x)}{\partial x}\right) \geq 2$, so we get by induction that $v(c_r(x)) = v\left(\frac{\partial}{\partial x}\,(c_{r-1}(x) \cdot \delta(x))\right) = v(c_{r-1}(x)) + v(\delta(x)) - 1 \geq 2(r-2) + 3 - 1 = 2(r-1)$. So $v(c_p(x)) \geq 2(p-1) > p - 1$.

4. The case where $\delta = 0$ and σ is not trivial but has finite order

In this case the commutation relation between y and x is given by:

$$y\, x = \sigma(x)\, y \tag{4.1}$$

We will denote the order of σ by n and put $A = B^\sigma$. Let K, L be the quotientfields of A, B respectively. We prove that $Z(C) = k[[z, y^n]]$, where $z = x\,\sigma(x)\ldots\sigma^{n-1}(x)$. Let us first discuss the structure of A.

Lemma 4.1. *$A = k[[z]]$, with z as above.*

Proof. It is obvious that A is a complete discrete valuation ring and k is a copy of its residue field. So A is a formal power series ring $k[[u]]$, where u is a uniformizing element. Being a uniformizing element, u must be of the form x^e + higher terms, where e is the ramification index.

Since K is complete under a discrete valuation, L is a finite extension of K and the residue class degree equals 1, we conclude that $e = [L : K] = n$.

It is easy to see that $\sigma(x) = \zeta\, x+$ higher terms, where ζ is an nth root of unity. So $z = x\,\sigma(x)\ldots\sigma^{n-1}(x)$ is of the form $\pm x^n$ + higher terms. Therefore z is also a uniformizing element and furthermore $A = k[[z]]$. $\square$

It is clear that $A \subset Z(C)$ and that y^n belongs to the center of C. We now look at the other inclusion.

Let f be in $Z(C)$. We can write f, in a unique way, in the form $\sum_{i\geq 0} a_i\, y^i$, where $a_i \in B$. Since $f \in Z(C)$, we have (using (4.1)) $0 = [x, f] = \sum_{i\geq 0} a_i\,(x - \sigma^i(x))\, y^i$. Hence, for all $i \in \mathbb{N}$, if $a_i \neq 0$, $x = \sigma^i(x)$, so n divides i. On the other hand we have $0 = [y, f] = \sum_{i\geq 0}(\sigma(a_i) - a_i)\, y^{i+1}$, so $\sigma(a_i) = a_i$, for all i in $\mathbb{N}$, which means that $a_i \in A$, for all i in $\mathbb{N}$. Therefore $f \in k[[z, y^n]]$.

We have now proved that $Z(C)$ is a formal power series ring in the two variables z, w. The remaining claim of Conjecture 1.1 follows from the fact that if $\sigma(x)$ is of the form $x + \cdots$ then

- If $p = 0$ and σ is non-trivial then its order is infinite (easily proved).
- If $p > 0$ and if the order of σ is finite then it is a power of p [6].

5. The case where σ and δ are non trivial and σ has finite order

Here we have the following commutationrelation between y and x :

$$y\,x = \sigma(x)\,y + \delta(x) \tag{5.1}$$

As before we denote the order of σ by n and we assume $n \neq 1$. We put $A = B^\sigma$ and we let K and L be respectevely the quotientfields of A and B. We extend the action of σ and δ to L and we denote these extended maps also by σ and δ.

It was shown in Lemma 4.1, that A is the ring of power series over k in $z = x\,\sigma(x)\ldots\sigma^{n-1}(x) \in B$.

For convenience we will first work in the polynomial Öre extension $S = B[y; \sigma, \delta]$. We prove:

Theorem 5.1. *The center $Z(S)$ of S is the ring of polynomials $A[w]$, where w is a monic (skew) polynomial of degree n in y with coefficients in B. In particular, we find that S is free of rank n^2 over $Z(S)$.*

The proof of this theorem depends on the following lemma:

Lemma 5.2. *Let D, D' be central simple algebras of the same PI-degree with centers Z, Z', respectively. Assume that $D \subseteq D'$. Then $Z \subseteq Z'$ and furthermore the map $\varphi : D \otimes_Z Z' \to D'$, defined by $\varphi(d \otimes z') := dz'$, is an isomorphism.*

Proof. Denote the PI-degree of D and D' by m. The PI-degree of DZ' is equal to m since we have inclusions $D \subseteq DZ' \subseteq D'$. From $Z' \subseteq Z(DZ') \subseteq DZ' \subseteq D'$ (where $Z(DZ')$ is the center of DZ'), we deduce that $m^2 = [DZ' : Z(DZ')] \leq [DZ' : Z'] \leq [D' : Z'] = m^2$,so $[DZ' : Z'] = m^2 = [D' : Z']$. This implies $DZ' = D'$ and in particular $Z \subseteq Z(DZ') = Z(D') = Z'$.

We conclude that the $\varphi : D \otimes_Z Z' \to D'$ is an epimorphism. Since D is a central simple algebra, the same holds for $D \otimes_Z Z'$. Thus $D \otimes_Z Z'$ is simple and it follows that φ must be an isomorphism. □

Proof of Theorem 5.1. Working out the identity $\delta(x \cdot f) = \delta(f \cdot x)$, for all $f \in B$, we deduce:

$$\delta(f) = \frac{\sigma(f) - f}{\sigma(x) - x} \cdot \delta(x) \tag{5.2}$$

This implies immediately that, if $f \in A$, then $\delta(f) = 0$, in other words, the polynomial ring $R = A[y]$ is a commutative subring of S.
Now consider S as right R-module. The rank of S over R is n, since $B = k[[x]]$ is free of rank n over $A = k[[z]] = k[[x^n + \text{higher terms}]]$.
Left multiplication yields an injective ringhomomorphism:

$$S \hookrightarrow \operatorname{End}_R(S_R) \tag{5.3}$$

So S satisfies a polynomial identity because S is isomorphic to a subring of the matrix ring $M_n(R)$, which is a PI-ring since R is commutative. This implies also that the PI-degree of S is less or equal to the PI-degree of $M_n(R)$ which is n. We claim that it is exactly n. To see this, filter S by y degree and denote the associated graded ring by $\operatorname{gr} S$. Since $\operatorname{gr} S = B[\overline{y}; \sigma]$, we see that $\operatorname{gr} S$ is a domain and furthermore $Z(\operatorname{gr} S) = A[\overline{y}^n]$ by Section 3. So $\operatorname{gr} S$ is a prime ring of rank n^2 over its center which implies that its PI-degree is equal to n. Since the PI-degree of $S \geq$ PI-degree of $\operatorname{gr} S$, it now follows that the PI-degree of S is exactly n.

Let E be the quotientfield of S. As in (5.3) we have an inclusion:

$$i : E \hookrightarrow \operatorname{End}_{K(y)}(E_{K(y)}) \tag{5.4}$$

E is a central simple algebra of PI-degree n and so is $\operatorname{End}_{K(y)}(E_{K(y)})$. Hence (5.4) induces, by Lemma 5.2, an isomorphism

$$\varphi : E \otimes_{Z(E)} K(y) \hookrightarrow \operatorname{End}_{K(y)}(E_{K(y)}) \tag{5.5}$$

defined by $\varphi(e \otimes f) = i(e) \cdot f$. This means that we can compute the characteristic polynomial of each $e \in E$, in $\operatorname{End}_{K(y)}(E_{K(y)})$.

Since S is an Öre extension, it is also a maximal order by [4] and so it is closed under taking coefficients of reduced characteristic polynomials. Using this observation we can now explicitly construct central elements in the center of S and the one we are interested in, is the reduced norm of y.

By definition this reduced norm may be computed by taking the image of y in $\operatorname{End}_{K(y)}(E_{K(y)})$ under (5.5), i.e. $\varphi(y \otimes 1) = i(y)$, where $i(y)$ is left multiplication by y, and then computing the determinant of $i(y)$ in $\operatorname{End}_{K(y)}(E_{K(y)})$.

To perform this computation we need a suitable basis for $E\,/\,K(y)$. We pick a normal basis $\{f,\sigma(f),\ldots,\sigma^{n-1}(f)\}$ for $L\,/\,K$, for some $f\in L$ in [3]. This is still a basis for $E\,/\,K(y)$.

We now compute the matrix of $i(y)$ explicitly. By (5.1) we get, for all $0\le j\le n-1$, $i(y)(\sigma^j(f)) = \sigma^{j+1}(f)\cdot y + \delta(\sigma^j(f))$, and since $\{f,\sigma(f),\ldots,\sigma^{n-1}(f)\}$ is a basis for $L\,/\,K$, $i(y)(\sigma^j(f)) = \sigma^{j+1}(f)\cdot y + \sum_{i=0}^{n-1}\sigma^i(f)\cdot a_{ji}$, for certain $a_{ji}\in K$.

This means that the matrix of $i(y) = D + Cy$, where $D = (a_{ji})\in M_n(K)$ and

$$C=\begin{pmatrix} 0 & 1 & 0 & \ldots & 0\\ 0 & 0 & 1 & \ldots & 0\\ \vdots & \vdots & \vdots & & \vdots\\ 0 & 0 & 0 & \ldots & 1\\ 1 & 0 & 0 & \ldots & 0\end{pmatrix}$$

the matrix of a cyclic permutation. Hence $\operatorname{Nrd}(y) = \det(D+Cy) = (-1)^{n+1}y^n +$ lower terms in y.

We now take $w = (-1)^{n+1}\operatorname{Nrd}(y)$. Clearly $A[w]\subset Z(S)$. Since B is free of rank n over A and $w = y^n +$ lower terms in y, S is free of rank n^2 over $A[w]$. In particular, $Z(S)$ is integral over $A[w]$. Now because $A[w]\subset Z(S)\subset S$, we know that $K(w)\subset Q(Z(S))\subset E$, where $Q(Z(S))$ is the quotientfield of $Z(S)$. Since S is free of rank n^2 over $A[w]$ and E is a central simple algebra of PI-degree n, the dimension of $Q(Z(S))$ over $K(w)$ must be 1, so $A[w]$ and $Z(S)$ have the same quotientfield.

The fact that $A[w]$ is integrally closed and that $Z(S)$ is integral over $A[w]$ now implies that $A[w] = Z(S)$. $\square$

In the next proposition we will obtain more information on the element w constructed in the above theorem. Let v be the x-adic valuation on B.

Proposition 5.3. *Assume that $v(\delta(x)) = a$.*
If $w = y^n + \sum_{i=0}^{n-1} f_i(x)\,y^i$, then for $i>0$ we have $v(f_i)\ge (a-1)(n-i)$. Furthermore there exists an element $q_0(z)\in k[[z]]$ such that $v(f_0+q_0(z))\ge (a-1)n$.

In the proof of this proposition we need the result of the following lemma:

Lemma 5.4. *If $f\in B$, then $v\left(\dfrac{\sigma(f)-f}{\sigma(x)-x}\right)\ge v(f)-1$.*

Proof. Put $r=v(f)$.

Case 1. $r\ge 1$
Put $h = \sigma(x)-x$, then we get $\dfrac{\sigma(f)-f}{\sigma(x)-x} = \dfrac{f(\sigma(x))-f(x)}{\sigma(x)-x} = \dfrac{f(x+h)-f(x)}{h}$.

Since $f(x) = \sum_{i=r}^{+\infty} a_i x^i$, for certain $a_i\in k$ with $a_r\ne 0$, it is easy to see that

$$\frac{f(x+h)-f(x)}{h} = \sum_{i=0}^{+\infty}\left(\sum_{j=r}^{+\infty} a_j\psi_{i,j}h^{j-i-1}\right)x^i$$

where $\psi_{ij} = \begin{cases} 0 & \text{if } i \geq j \\ \frac{j!}{i!(j-i)!} & \text{if } i < j \end{cases}$.

So $v\left(\dfrac{\sigma(f) - f}{\sigma(x) - x}\right) = v\left(\dfrac{f(x+h) - f(x)}{h}\right) \geq \min_i((r-i-1)v(h)+i) \geq r-1$ since $v(h) \geq v(x) \geq 1$.

Case 2. $r = 0$.

In this case we get that $f(x) = \sum_{i=0}^{+\infty} a_i x^i$, for certain $a_i \in k$ with $a_0 \neq 0$. Since σ is an automorphism which is also k-linear, it follows that $v\left(\dfrac{\sigma(f) - f}{\sigma(x) - x}\right) = v\left(\dfrac{\sigma(g) - g}{\sigma(x) - x}\right)$, where $g = \sum_{i=1}^{+\infty} a_i x^i$. Since $v(g) \geq 1$, we get by applying Case 1, $v\left(\dfrac{\sigma(f) - f}{\sigma(x) - x}\right) \geq v(g) - 1 \geq 0 \geq v(f) - 1$. $\square$

We return now to the proof of Proposition 5.3.

Proof of Proposition 5.3. Put $\overline{y} = x^{-a+1}y$. If we multiply (5.1) on the left with x^{-a+1}, we obtain

$$\overline{y}\, x = \sigma(x)\, \overline{y} + x^{-a+1}\, \delta(x) \tag{5.6}$$

Consider the ring $\overline{S} = B[\overline{y}; \sigma, \overline{\delta}]$, where $\overline{\delta}$ is the σ-derivation of B defined by $\overline{\delta}(b) = x^{-a+1}\,\delta(b)$. We clearly have inclusions $S \subset \overline{S} \subset L[y; \sigma, \delta]$.

Applying Theorem 5.1 to $\overline{S}$, we find that $\overline{S}$ has a central element $\overline{w}$ of the form

$$\overline{w} = \overline{y}^n + \sum_{i=0}^{n-1} g_i(x)\overline{y}^i \tag{5.7}$$

with $g_i(x) \in B$. Verifying the commutationrelation of x^{-a+1} and y, we find

$$y\, x^{-a+1} = \sigma(x^{-a+1})\, y + \delta(x^{-a+1}) \tag{5.8}$$

For all $f \in B$, we get by (5.2) and Lemma 5.4 that $v(\delta(f)) = v\left(\dfrac{\sigma(f) - f}{\sigma(x) - x} \cdot \delta(x)\right)$
$= v\left(\dfrac{\sigma(f) - f}{\sigma(x) - x}\right) + v(\delta(x)) \geq v(f) - 1 + a$.
In particular, it follows that $\delta(x^{-a+1}) \in B$.

Using (5.8), we can rewrite $\overline{w}$ in the following form

$$\overline{w} = z^{-a+1}y^n + h_0(x) + \sum_{i=1}^{n-1}(x \cdot \sigma(x) \cdot \ldots \cdot \sigma^{i-1}(x))^{-a+1} h_i(x) y^i$$

where, for all $0 \leq i \leq n-1$, we have $h_i(x) \in B$ and with z the element of A defined in Section 4.

Multiplying $\overline{w}$ with z^{a-1}, we get the element

$$y^n + z^{a-1}h_0(x) + \sum_{i=1}^{n-1}(\sigma^i(x) \cdot \ldots \cdot \sigma^{n-1}(x))^{a-1} h_i(x) y^i$$

which we will denote by w'.

Let us write $p_0(x)$ for $z^{a-1}h_0(x)$ and $p_i(x)$ for $(\sigma^i(x) \cdot \ldots \cdot \sigma^{n-1}(x))^{a-1}h_i(x)$, for all $1 \leq i \leq n-1$. Since $v(p_0(x)) = (a-1)\, v(z) + v(h_0(x)) \geq (a-1)n \geq 0$ and, for all $1 \leq i \leq n-1$, $v(p_i(x)) = (a-1)\left(\sum_{j=i}^{n-1} v(\sigma^j(x))\right) + v(h_i(x)) \geq (a-1)(n-i) \geq 0$, we see that w' belongs to S. w' is also a central element of $\overline{S}$, so it follows that w' is a central element of S. This means that w' has to be of the form

$$w' = \sum q_i(z)w^i \tag{5.9}$$

since by Theorem 5.1, we know that $Z(S) = A[w] = k[[z]][w]$.

By looking at the degree of y, we can reduce (5.9) to $w' = q_0(z) + q_1(z)\,w$ and if we look at the coefficient of y^n, we see that $q_1(z) = 1$. Hence $f_i(x) = p_i(x)$, for all $1 \leq i \leq n-1$, which implies that $v(f_i(x)) \geq (a-1)(n-i)$. Furthermore $p_0(x) = q_0(z) + f_0(x)$ which implies $v(q_0(z) + f_0(x)) \geq (a-1)n$. □

Corollary 5.5. *Let C be the formal power series ring $k[[x]][[y;\sigma,\delta]]$, where $v(\delta(x)) \geq 3$. Let n be the order of σ. Then the center of C is equal to $k[[z,w]]$, where $z = x^n + \varphi(x)$ and $w = y^n + \theta(x,y)$ with φ, θ containing only terms in x, y of total degree $> n$.*

Proof. Let $M \subset S$ be the twosided ideal generated by x, y. Clearly C is equal to the M-adic completion of S. Let m be the maximal ideal of $Z(S)$ generated by z, w. It is easy to see that

$$M^{2N} \subset mS \subset M$$
$$m^a S \cap Z(S) = m^a$$

Thus the completion of $Z(S)$ at the induced topology coincides with the completion at the m-adic topology, which is $k[[z,w]]$. Since $S \subset C$ the PI-degree of C is $\geq n$. On the other hand, using the properties of completion every identity in S vanishes in C. So the PI-degree of C is exactly n. Since $Z(C) \supset k[[z,w]]$, $\mathrm{rk}_{Z(C)}\, C = n^2$ and $k[[z,w]]$ is integrally closed, we prove exactly as before that $Z(C) = k[[z,w]]$. □

To complete the proof of Theorem 1.2 we use the fact that in characteristic $p > 0$ the order of σ is a power of p [5].

6. A new proof of Proposition 1.3

Let k be a field of characteristic $p > 1$ and consider the field $k(t_1, \ldots, t_{p-1})$, where $t_1, \ldots, t_{p-1}$ are variables. Let $f = \sum_{i=1}^{p-1} f_i\, t_i \in k(t_1, \ldots, t_{p-1})[x]$ be arbitrary.

Since $k(t_1, \ldots, t_{p-1})$ is also a field of characteristic p it follows from Lemma 3.1 that f satisfies

$$\frac{\partial^2}{\partial x^2}\left(\frac{\partial}{\partial x}\left(\cdots\left(\frac{\partial f}{\partial x}\cdot f\right)\cdots f\right)\cdot f\right) = 0 \tag{6.1}$$

where $\frac{\partial}{\partial x}$ occurs p times and f occurs $(p-1)$ times.

It is clear that $\dfrac{\partial f}{\partial x} = \displaystyle\sum_{i=1}^{p-1} \dfrac{\partial f_i}{\partial x} \cdot t_i$. Taking the coefficient of $t_1 \cdot \ldots \cdot t_{p-1}$ in (6.1) we get

$$\sum_{\sigma \in S_{p-1}} \frac{\partial^2}{\partial x^2} \left(\frac{\partial}{\partial x} \left(\ldots \left(\frac{\partial f_{\sigma(1)}}{\partial x} \cdot f_{\sigma(2)} \right) \ldots \cdot f_{\sigma(p-2)} \right) \cdot f_{\sigma(p-1} \right) = 0$$

for all polynomials f_i over a field k of characteristic $p > 0$.

Consider the following expression in the variables $f_1, \ldots, f_{p-1}$:

$$\sum_{\sigma \in S_{p-1}} \left[\frac{\partial^2}{\partial x^2} \left(\frac{\partial}{\partial x} \left(\ldots \left(\frac{\partial f_{\sigma(1)}}{\partial x} \cdot f_{\sigma(2)} \right) \ldots \cdot f_{\sigma(p-2)} \right) \cdot f_{\sigma(p-1)} \right) - \frac{\partial^p f_{\sigma(1)}}{\partial x^p} \cdot f_{\sigma(2)} \cdot \ldots \cdot f_{\sigma(p-1)} \right] \tag{6.2}$$

(6.2) has the following properties:

(a) (6.2) $=$ 0, if $f_1, \ldots, f_{p-1}$ are polynomials over a field k of characteristic $p > 0$.

(b) Over any field, we may rewrite (6.2) in the form

$$\sum_{0 \leq u_1, \ldots, u_{p-1} \leq p-1} a_{u_1 \ldots u_{p-1}} \frac{\partial^{u_1} f_1}{\partial x^{u_1}} \cdot \ldots \cdot \frac{\partial^{u_{p-1}} f_{p-1}}{\partial x^{u_{p-1}}} \tag{6.3}$$

such that $a_{u_1 \ldots u_{p-1}} \in \mathbb{Z}$.

Using these properties we will prove that the coefficients of (6.3) are multiples of p.

Define for q, $n \in \mathbb{N}$ the symbolic nth power $q^{(n)}$ of q as follows:

$$q^{(n)} = \begin{cases} 1 & \text{if } n = 0 \\ q\,(q-1) \ldots (q-n+1) & \text{if } n \geq 1 \end{cases}$$

Now let $(q_i)_{i=1,\ldots,p-1} \in \mathbb{N}$ be arbitrary and put $f_i = x^{q_i}$. Then it is easy to see that (6.3) equals

$$\sum_{u_1, \ldots, u_{p-1}} a_{u_1 \ldots u_{p-1}}\, q_1^{(u_1)} \ldots q_{p-1}^{(u_{p-1})}\, x^{q_1 - u_1} \ldots x^{q_{p-1} - u_{p-1}}$$

Since (6.3) is zero in k by property (a) we deduce:

$$\sum_{u_1, \ldots, u_{p-1}} a_{u_1 \ldots u_{p-1}}\, q_1^{(u_1)} \ldots q_{p-1}^{(u_{p-1})} = 0 \tag{6.4}$$

in k.

Let X be the k-vectorspace of all functions $h : k^{p-1} \to k$. By [2]

$$\left\{ x_1^{u_1} \ldots x_{p-1}^{u_{p-1}} \mid \text{for all } 1 \leq i \leq p-1,\ u_i \leq p-1 \right\}$$

is a basis for X. We may transform these 'normal' monomials into 'symbolic' monomials by a triangular matrix whose determinant is equal to 1. It follows that

$$\left\{ x_1^{(u_1)} \ldots x_{p-1}^{(u_{p-1})} \mid \text{for all } 1 \leq i \leq p-1,\ u_i \leq p-1 \right\}$$

is also a basis for X.

Since (6.4) holds for all $q_1, \ldots, q_{p-1} \in \mathbb{N}$, this implies that

$$\sum_{u_1,\ldots,u_{p-1}} a_{u_1\ldots u_{p-1}}\, x_1^{(u_1)} \ldots x_{p-1}^{(u_{p-1})} \;=\; 0$$

in k. We conclude that the coefficients $a_{u_1\ldots u_{p-1}}$ are zero in k and hence they are divisible by p, as elements of $\mathbb{Z}$.

Let us look now at the difference of (6.2) and (6.3), i.e.

$$\sum_{\sigma\in S_{p-1}} \left[\frac{\partial^2}{\partial x^2}\left(\frac{\partial}{\partial x}\left(\ldots\left(\frac{\partial\, f_{\sigma(1)}}{\partial x}\cdot f_{\sigma(2)}\right)\cdots\cdot f_{\sigma(p-2)}\right)\cdot f_{\sigma(p-1)}\right)\right. \tag{6.5}$$

$$\left. -\;\frac{\partial^p\, f_{\sigma(1)}}{\partial x^p}\cdot f_{\sigma(2)}\cdot\ldots\cdot f_{\sigma(p-1)}\right] - \sum_{u_1,\ldots,u_{p-1}} a_{u_1\ldots u_{p-1}}\,\frac{\partial^{u_1}\, f_1}{\partial x^{u_1}}\cdot\ldots\cdot\frac{\partial^{u_{p-1}}\, f_{p-1}}{\partial x^{u_{p-1}}}$$

By definition (6.5) is equal to zero over any field with a derivation. We will consider (6.5) over the complex numbers $\mathbb{C}$. Let $(v_i)_{i=1,\ldots,p-1} \in \mathbb{C}$ and put $f_i = e^{v_i x}$. We deduce that

$$\sum_{\sigma\in S_{p-1}} \Big[v_{\sigma(1)}\,(v_{\sigma(1)} + v_{\sigma(2)})\ldots(v_{\sigma(1)} + \ldots + v_{\sigma(p-1)})^2\, e^{(v_{\sigma(1)}+\ldots+v_{\sigma(p-1)})\,x}$$

$$-\, v^p_{\sigma(1)}\, e^{(v_{\sigma(1)}+\ldots+v_{\sigma(p-1)})\,x}\Big] - \sum_{u_1,\ldots,u_{p-1}} a_{u_1\ldots u_{p-1}}\, v_1^{u_1}\ldots v_{p-1}^{u_{p-1}}\, e^{(v_1+\ldots+v_{p-1})\,x} \;=\; 0$$

If we divide this by $e^{(v_1+\ldots+v_{p-1})\,x}$, we get, for all $v_1, \ldots, v_{p-1} \in \mathbb{C}$

$$\sum_{\sigma\in S_{p-1}} (\, v_{\sigma(1)}\,(v_{\sigma(1)} + v_{\sigma(2)})\ldots(v_{\sigma(1)} + \ldots + v_{\sigma(p-1)})^2 \;-\; v^p_{\sigma(1)}\,)$$

$$-\sum_{u_1,\ldots,u_{p-1}} a_{u_1\ldots u_{p-1}}\, v_1^{u_1}\ldots v_{p-1}^{u_{p-1}} \;=\; 0$$

So the polynomial

$$\sum_{\sigma\in S_{p-1}} (\, x_{\sigma(1)}\,(x_{\sigma(1)} + x_{\sigma(2)})\ldots(x_{\sigma(1)} + \ldots + x_{\sigma(p-1)})^2 \;-\; x^p_{\sigma(1)}\,)$$

$$-\sum_{u_1,\ldots,u_{p-1}} a_{u_1\ldots u_{p-1}}\, x_1^{u_1}\ldots x_{p-1}^{u_{p-1}}$$

is identically zero.

If we reduce this modulo p, we deduce that

$$\left[\sum_{\sigma\in S_{p-1}} x_{\sigma(1)}\,(x_{\sigma(1)} + x_{\sigma(2)})\ldots(x_{\sigma(1)} + \ldots + x_{\sigma(p-1)})\right](x_1 + \ldots + x_{p-1})$$

$$\equiv\; x_1^p + \ldots + x_{p-1}^p \;\equiv\; (x_1 + \ldots + x_{p-1})^p \qquad (\mathrm{mod}\ p)$$

Hence Proposition 1.3 is proved.

References

[1] G. Baron and A. Schinzel, *An extension of Wilson's theorem*, C. R. Math. Rep. Acad. Sci. Canada **1** (1978/79), no. 2, 115–118.
[2] Z. I. Borevitch and I. R. Shafarevitch, *Number theory*, Academic Press, 1966.
[3] P. M. Cohn, *Algebra*, John Wiley & Sons, 1982.
[4] G. Maury and J. Raynaud, *Ordres maximaux au sens de K. Asano*, Springer, Berlin, 1980.
[5] S. Sen, *On automorphisms of local fields*, Ann. of Math. (2) **90** (1969), 33–46.
[6] S. P. Smith and J. T. Stafford, *Regularity of the 4-dimensional Sklyanin algebra*, Compositio Math. **83** (1992), 259–289.
[7] M. Van den Bergh and M. Van Gastel, *Graded modules of Gelfand-Kirillov dimension one over three-dimensional Artin-Schelter regular algebras*, J. Algebra **196** (1997), 251–282.

Departement WNI, Limburgs Universitair Centrum, Universitaire Campus, Building D, 3590 Diepenbeek, Belgium
E-mail address, M. Van Gastel: martine.vangastel@luc.ac.be
E-mail address, M. Van den Bergh: michel.vandenbergh@luc.ac.be