COMPOSITIO MATHEMATICA

On the center of the ring of differential operators on a smooth variety over $\mathbb{Z}/p^n\mathbb{Z}$

Allen Stewart and Vadim Vologodsky

Compositio Math. **149** (2013), 63–80.

doi:10.1112/S0010437X12000462

Compositio Math. 149 (2013) 63–80
doi:10.1112/S0010437X12000462

On the center of the ring of differential operators on a smooth variety over $\mathbb{Z}/p^n\mathbb{Z}$

Allen Stewart and Vadim Vologodsky

Abstract

We compute the center of the ring of PD differential operators on a smooth variety over $\mathbb{Z}/p^n\mathbb{Z}$, confirming a conjecture of Kaledin (private communication). More generally, given an associative algebra A_0 over $\mathbb{Z}_p$ and its flat deformation A_n over $\mathbb{Z}/p^{n+1}\mathbb{Z}$, we prove that under a certain non-degeneracy condition, the center of A_n is isomorphic to the ring of length-$(n+1)$ Witt vectors over the center of A_0.

1. Introduction

1.1 Let X_n be a smooth scheme over the spectrum S_n of the ring of length-$(n+1)$ Witt vectors $W_{n+1}(k)$ over a perfect field k of characteristic p, let X_0 be its special fiber over k, and let $D_{X_n} = D_{X_n/S_n}$ be the sheaf of PD differential operators (see [BO78]) on X_n. We prove in Theorem 3 that the center $Z(D_{X_n})$ of D_{X_n} is canonically isomorphic to the ring of Witt vectors $W_{n+1}(S^{\cdot}T_{X_0})$ over the symmetric algebra of the tangent sheaf of X_0. For $n = 0$ we recover the classical isomorphism (see, e.g., [BMR08])

$$Z(D_{X_0}) \simeq S^{\cdot}T_{X_0} \tag{1.1}$$

given by the p-curvature map. The general result was conjectured by Kaledin (private communication). For $p \neq 2$, he even proposed a construction of the map

$$W_{n+1}(S^{\cdot}T_{X_0}) \to Z(D_{X_n}).$$

1.2 In fact, we prove a more general result. Let A_n be a flat associative algebra over $W_{n+1}(k)$, where $n > 0$. Set

$$A_i = A_n \otimes_{W_{n+1}(k)} W_{i+1}(k) \quad \text{for } 0 \leqslant i \leqslant n,$$

and let $Z(A_i)$ be the center of A_i. The first-order deformation A_1 yields a natural biderivation on $Z(A_0)$ (see § 2.1, formula (2.2)),

$$\{\ ,\ \} : Z(A_0) \otimes_k Z(A_0) \to Z(A_0).$$

We shall say that the deformation A_n of A_0 is non-degenerate if Spec $Z(A_0)$ is smooth over k and the biderivation $\{\ ,\ \}$ is associated with a non-degenerate bivector field, $\mu \in \bigwedge^2 T_{Z(A_0)}$, on Spec $Z(A_0)$.

If z is an element of $Z(A_0)$ and $\tilde{z} \in A_n$ is a lifting of z, then for every $0 \leqslant i \leqslant n$ the element $p^i \tilde{z}^{p^{n-i}} \in A_n$ is central and does not depend on the choice of $\tilde{z}$. We prove in Theorem 1 that

Received 14 April 2011, accepted in final form 7 May 2012, published online 31 October 2012.
2010 Mathematics Subject Classification 14F10, 14G17 (primary), 16S34, 16S80 (secondary).
Keywords: deformations of algebras, Poisson algebras, Witt vectors.

for $p \neq 2$, the map

$$\phi_n : W_{n+1}(Z(A_0)) \to Z(A_n) \tag{1.2}$$

defined by the formula

$$\phi_n((z_0, z_1, \dots, z_n)) = \sum_{i=0}^{n} p^i \tilde{z}_i^{p^{n-i}} \tag{1.3}$$

is a homomorphism of rings, and if the deformation A_n of A_0 is non-degenerate, then ϕ_n is an isomorphism. Note that the left-hand side of (1.2) depends only on the algebra A_0 and not on the deformation A_n.

1.3 For $p = 2$, the map ϕ_n given by formula (1.3) is neither additive nor multiplicative[1] and, in fact, even if the deformation A_n is non-degenerate, Z_n need not be isomorphic to $W_{n+1}(Z_0)$ as an abstract ring (see Remark 3.4). However, if A_n is non-degenerate and, in addition, the differential 2-form $\omega = \mu^{-1} \in \Omega^2_{Z(A_0)}$ associated with $\{\ ,\ \}$ is exact, i.e. $\omega = d\eta$, then we can correct our map (1.3) as follows. The Poisson algebra $Z(A_0)$ has a restricted structure in the sense of Bezrukavnikov and Kaledin [BK08]: if $z \in Z(A_0)$ and t_z is the corresponding Hamiltonian vector field on Spec $Z(A_0)$ i.e. $dz = i_{t_z}\omega$, we set

$$z^{[p]} = L_{t_z}^{p-1} i_{t_z}\eta - i_{t_z^{[p]}}\eta \in Z(A_0), \tag{1.4}$$

where $t_z^{[p]} \in T_{Z(A_0)}$ is the pth power in the restricted Lie algebra of vector fields and L_{t_z} is the Lie derivative. For $p = 2$ we define

$$\phi_n((z_0, z_1, \dots, z_{n-1})) = \sum_{i=0}^{n-1} 2^i \big(\tilde{z}_i^2 + 2\widetilde{z_i^{[2]}}\big)^{2^{n-i-1}} + 2^n \tilde{z}_n. \tag{1.5}$$

We prove in Theorem 2 that the map $\phi_n : W_{n+1}(Z(A_0)) \to Z(A_n)$ given by the above formula is an isomorphism of rings.

1.4 According to an observation of Belov-Kanel and Kontsevich [BK05], for every smooth scheme X_n over S_n, the bivector field on $Z(D_{X_0}) \simeq S^{\cdot}T_{X_0}$ induced by the deformation X_n equals, up to sign, the bivector field on $S^{\cdot}T_{X_0}$ induced by the canonical symplectic structure on the cotangent bundle $\mathbf{T}^*_{X_0}$. In particular, the former bivector field is non-degenerate and the associated differential form has a canonical primitive $\eta \in \Omega^1_{\mathbf{T}^*_{X_0}}$. Thus, as a corollary of the above results, we find a canonical isomorphism of sheaves of rings

$$\phi_n : W_{n+1}(S^{\cdot}T_{X_0}) \simeq Z(D_{X_n}). \tag{1.6}$$

2. Main result: odd characteristic case

2.1 Let R_n be a commutative algebra flat over $\mathbb{Z}/p^{n+1}\mathbb{Z}$, with $n > 0$. For $0 \leqslant m \leqslant n$ we set

$$R_m = R_n \otimes_{\mathbb{Z}/p^{n+1}\mathbb{Z}} \mathbb{Z}/p^{m+1}\mathbb{Z}.$$

By a level-n deformation of a flat associative R_0-algebra A_0 we mean a flat associative R_n-algebra A_n together with an isomorphism $A_n \otimes_{R_n} R_0 \cong A_0$. Given such A_n, we denote by A_m

[1] We are grateful to Pierre Berthelot for pointing out this problem.

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

the corresponding algebra over R_m. We will write

$$A_m \xrightarrow{r} A_{m-1}, \quad r(x) = x \bmod p^m$$

for the reduction homomorphism. The preimage of $x \in pA_m \subset A_m$ under the isomorphism

$$A_{m-1} \xrightarrow{p} pA_m$$

is denoted by $(1/p)x$. We will write $Z_m = Z(A_m)$ for the center of A_m. The following lemma is straightforward.

Lemma 2.1. *Let $x \in Z_i$ and $y \in Z_j$, where $0 \leqslant i \leqslant j \leqslant n$, and let $\tilde{x}, \tilde{y} \in A_n$ be liftings of x and y, respectively. Then:*

(1) $[\widetilde{x}, \widetilde{y}\,] \equiv 0 \bmod p^{j+1}$;

(2) $[\widetilde{x}, \widetilde{y}\,] \bmod p^{i+j+2} \in Z_{i+j+1}$;

(3) *the element* $(1/p^{j+1})[\widetilde{x}, \widetilde{y}] \bmod p^{i+1} \in Z_i$ *is independent of the choice of liftings* $\widetilde{x}$ *and* $\widetilde{y}$*;*

(4) *the* R_n*-linear map*

$$Z_i \otimes_{R_n} Z_j \to Z_i, \quad x \otimes y \mapsto \frac{1}{p^{j+1}}[\widetilde{x}, \widetilde{y}] \bmod p^{i+1} \tag{2.1}$$

is a derivation with respect to the first argument;

(5) *the element* $(\widetilde{x})^p \bmod p^{i+2}$ *lies in* Z_{i+1} *and is independent of the choice of the lifting* $\widetilde{x}$.

In the case where $i = j = 0$, the map (2.1) deserves special notation:

$$\{\ ,\ \} : Z(A_0) \otimes_{R_0} Z(A_0) \to Z(A_0), \quad \{x, y\} = \frac{1}{p}[\widetilde{x}, \widetilde{y}] \bmod p. \tag{2.2}$$

By assertion (4) of the lemma, $\{\ ,\ \}$ is a derivation with respect to each argument. We also remark that if $n > 1$, the map $\{\ ,\ \}$ satisfies the Jacobi identity; this can be seen by dividing the identity

$$[\widetilde{x}, [\widetilde{y}, \widetilde{z}]] + [\widetilde{z}, [\widetilde{x}, \widetilde{y}]] + [\widetilde{y}, [\widetilde{z}, \widetilde{x}]] = 0$$

by p^2 and reducing the result modulo p. Thus, if $n > 1$, the bracket $\{\ ,\ \}$ defines a Poisson structure on Z_0.

We shall say that A_n is a non-degenerate deformation of A_0 if Z_0 is a smooth R_0-algebra and the map $\{\ ,\ \}$ is associated with a non-degenerate bivector field $\mu \in \bigwedge^2 T_{Z_0/R_0}$; that is,

$$\{x, y\} = \langle \mu, dx \wedge dy \rangle$$

for every $x, y \in Z_0$. By viewing μ as Z_0-linear isomorphism $T^*_{Z_0/R_0} \to T_{Z_0/R_0}$ and taking its inverse $T_{Z_0/R_0} \to T^*_{Z_0/R_0}$, we obtain a differential 2-form, $\omega = \mu^{-1} \in \Omega^2_{Z_0/R_0}$. The form ω is closed if and only if the bracket $\{\ ,\ \}$ is Poisson.

We remark that our non-degeneracy condition depends only on the reduction of A_n modulo p^2.

2.2 Let $W_{m+1}(Z_0)$ be the ring of length-$(m+1)$ Witt vectors of Z_0. For $0 \leqslant m \leqslant n$ we define a map

$$\phi_m : W_{m+1}(Z_0) \to A_m$$

by

$$\phi_m(z_0, \ldots, z_m) = \sum_{i=0}^{m} p^i \widetilde{z}_i^{\,p^{m-i}}, \tag{2.3}$$

where $\widetilde{z}_i$ is a lifting of $z_i \in Z_0$ in A_m.

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

CLAIM 2.2. *The map ϕ is well-defined and the image of ϕ is contained in Z_m:*

$$\phi_m : W_{m+1}(Z_0) \to Z_m. \tag{2.4}$$

Proof. If $\widetilde{z}_i$ and $\widetilde{z}'_i$ are liftings of z_i, then by Lemma 2.1(5) we have

$$(\widetilde{z}_i)^{p^{m-i}} \equiv (\widetilde{z}'_i)^{p^{m-i}} \bmod p^{m-i+1} \in Z_{m-i},$$

which implies that

$$p^i(\widetilde{z}_i)^{p^{m-i}} = p^i(\widetilde{z}'_i)^{p^{m-i}} \in Z_m. \qquad \square$$

2.3 In order to state our main theorem, we need to introduce some notation. Let R_n and R_m be as in § 2.1. Then, for any commutative R_0-algebra Z_0 and $0 \leqslant m \leqslant n$, the ring of Witt vectors $W_{m+1}(Z_0)$ has a $W_{m+1}(R_0)$-module structure induced by the homomorphism $R_0 \to Z_0$. Also, since R_m is commutative, the map $\phi_m : W_{m+1}(R_0) \to R_m$ is a homomorphism and thus defines a $W_{m+1}(R_0)$-module structure on R_m. We define the ring of relative Witt vectors $W_{m+1}(Z_0/R_m)$ to be the quotient of the tensor product

$$W_{m+1}(Z_0) \otimes_{W_{m+1}(R_0)} R_m$$

by the ideal generated by elements of the form

$$V^j(x \cdot z) \otimes 1 - V^j z \otimes \phi_{m-j}(x) \quad \text{with } z \in W_{m+1-j}(Z_0),\ x \in W_{m+1-j}(R_0),$$

where V is the Verschiebung operator. Note that for any $z \in W_{m+1-j}(Z_0)$ and $a \in R_{m-j}$, the tensor $V^j z \otimes a$ makes sense as an element of $W_{m+1}(Z_0) \otimes_{W_{m+1}(R_0)} R_m$, since $p^{m+1-j}V^j z = 0$. We remark that if F denotes the Frobenius operator, then we have

$$V^j(F^j(x) \cdot z) \otimes 1 = x \cdot V^j z \otimes 1 = V^j z \otimes \phi_{m-j}(F^j x)$$

in $W_{m+1}(Z_0) \otimes_{W_{m+1}(R_0)} R_m$. In particular, if R_0 is perfect, then

$$W_{m+1}(Z_0) \otimes_{W_{m+1}(R_0)} R_m \xrightarrow{\sim} W_{m+1}(Z_0/R_m).$$

We are now ready to state our main result.

THEOREM 1. *Suppose $p \neq 2$. Then, for every flat associative algebra A_n over R_n and every $0 \leqslant m \leqslant n$, the maps $\phi_m : W_{m+1}(Z_0) \to Z_m$ and*

$$\Phi_m : W_{m+1}(Z_0/R_m) \to Z_m, \quad \Phi_m(z \otimes a) = a\phi_m(z) \tag{2.5}$$

are ring homomorphisms. If, in addition, the deformation A_n is non-degenerate, then Φ_m is an isomorphism.

The proof of this theorem occupies the rest of this section.

2.4 We begin with some general remarks on Witt vectors. It is well known (see, e.g., [Mum66, § 26]) and easy to show that the polynomials

$$\psi_i(x, y) = \frac{(x+y)^{p^{i-1}} - (x^p + y^p)^{p^{i-2}}}{p^{i-1}} \quad \text{for } i > 1, \tag{2.6}$$

$$\psi_1(x, y) = x + y \tag{2.7}$$

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

have integral coefficients and satisfy the recursive formula

$$\psi_{i+1}(x, y) = \sum_{j=1}^{p} \binom{p}{j} p^{j(i-1)-i} \psi_i(x, y)^j (x^p + y^p)^{(p-j)p^{i-2}} \tag{2.8}$$

for $i > 1$. We claim that for every commutative ring Z and all $x, y \in Z$, one has the following equation in $W_n(Z)$:

$$\underline{x+y} = \sum_{i=0}^{n-1} V^i \psi_{i+1}(\underline{x}, \underline{y}). \tag{2.9}$$

Here we write $\underline{x} = (x, 0, \ldots, 0)$ for the Teichmüller representative of x in $W_m(Z)$ and V for the Verschiebung operator $W_m(Z) \to W_{m+1}(Z)$. Indeed, it suffices to check the identity (2.9) for $Z = \mathbb{Z}[x, y]$. In this case, the ghost map $W_n(Z) \to Z^n$ given by the Witt polynomials $\mathcal{W}_m$ is an injective homomorphism. Thus it is enough to check that the ghost coordinates of both sides of (2.9) are equal. We have

$$\begin{aligned}
\mathcal{W}_m(\underline{x+y}) = (x+y)^{p^{m-1}} &= \sum_{i=0}^{m-1} p^i \psi_{i+1}(x^{p^{m-i-1}}, y^{p^{m-i-1}}) \\
&= \sum_{i=0}^{m-1} p^i \psi_{i+1}(\mathcal{W}_{m-i}(\underline{x}), \mathcal{W}_{m-i}(\underline{y})) = \mathcal{W}_m\biggl(\sum_{i=0}^{n-1} V^i \psi_{i+1}(\underline{x}, \underline{y})\biggr),
\end{aligned}$$

where we have used that $\mathcal{W}_i \circ V = p\mathcal{W}_{i-1}$. This proves (2.9).

We are interested in describing ring homomorphisms from $W_n(Z)$ to a given ring.

Lemma 2.3. *Let $Z_0, Z_1, \ldots, Z_{n-1}$ be commutative rings. Suppose that we are given two families of maps $\chi^{(i)} : Z_0 \to Z_i$ and $\pi : Z_i \to Z_{i+1}$, $i = 0, \ldots, n-1$, such that the following conditions hold:*

(a) *$\chi^{(i)}$ is multiplicative and π is additive;*

(b) *for any $x, y \in Z_0$, $p\pi(xy) = \pi(x)\pi(y)$, and if $0 \leqslant i \leqslant m \leqslant n-1$, then*

$$\chi^{(m)}(x)\pi^i\chi^{(m-i)}(y) = \pi^i\chi^{(m-i)}(x^{p^i}y);$$

(c) *for any $x, y \in Z_0$ and $0 \leqslant m \leqslant n-1$,*

$$\chi^{(m)}(x+y) = \sum_{i=0}^{m} \pi^i \psi_{i+1}(\chi^{(m-i)}(x), \chi^{(m-i)}(y)).$$

Then the maps $\varphi_m : W_{m+1}(Z_0) \to Z_m$ defined by

$$\varphi_m(z_0, \ldots, z_m) = \sum_{i=0}^{m} \pi^i \chi^{(m-i)}(z_i) \tag{2.10}$$

are ring homomorphisms, and

$$\pi\varphi_{m-1} = \varphi_m V. \tag{2.11}$$

Proof. Formula (2.11) is clear. We prove that φ_m is a ring homomorphism using induction on m. We have that $\varphi_0(z) = \chi^{(0)}(z)$. By assumption, $\chi^{(0)}$ is multiplicative and, by using property (c), it follows that $\chi^{(0)}$ is additive. Hence φ_0 is a ring homomorphism. Now suppose that φ_l is a ring homomorphism for $l < m$. Let $x = (x_0, \ldots, x_m) \in W_{m+1}(Z_0)$, let $x' = (x_1, \ldots, x_m) \in W_m(Z_0)$,

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

and let w be another element of $W_m(Z_0)$. Then, using the induction assumption and (2.11), we obtain

$$\begin{aligned}\varphi_m(x+Vw) &= \varphi_m(\underline{x_0}+V(x'+w))\\ &= \varphi_m(\underline{x_0})+\varphi_m(V(x'+w))\\ &= \varphi_m(\underline{x_0})+\pi\varphi_{m-1}(x'+w)\\ &= \varphi_m(\underline{x_0})+\varphi_m(Vx')+\varphi_m(Vw)\\ &= \varphi_m(x)+\varphi_m(Vw).\end{aligned}$$

Thus, for any $x\in W_{m+1}(Z_0)$ and $w\in W_m(Z_0)$, we have

$$\varphi_m(x+Vw)=\varphi_m(x)+\varphi_m(Vw). \tag{2.12}$$

This implies that it suffices to check additivity of φ_m on Witt vectors of the form $\underline{z}$. Upon adjusting equation (2.9), we have

$$\underline{z}+\underline{z'}=\underline{z+z'}-\sum_{i=1}^{m}V^i\psi_{i+1}(\underline{z},\underline{z'}). \tag{2.13}$$

Therefore, using (2.11) together with (2.12) and induction, we see that

$$\begin{aligned}\varphi_m(\underline{z}+\underline{z'}) &= \varphi_m\left(\underline{z+z'}-\sum_{i=1}^{m}V^i\psi_{i+1}(\underline{z},\underline{z'})\right)\\ &= \varphi_m(\underline{z+z'})-\varphi_m\left(\sum_{i=1}^{m}V^i\psi_{i+1}(\underline{z},\underline{z'})\right)\\ &= \varphi_m(\underline{z+z'})-\sum_{i=1}^{m}\pi^i\psi_{i+1}(\varphi_{m-i}(\underline{z}),\varphi_{m-i}(\underline{z'}))\\ &= \varphi_m(\underline{z+z'})-\sum_{i=1}^{m}\pi^i\psi_{i+1}(\chi^{(m-i)}(\underline{z}),\chi^{(m-i)}(\underline{z'}))\\ &= \chi^{(m)}(z+z')-\sum_{i=1}^{m}\pi^i\psi_{i+1}(\chi^{(m-i)}(\underline{z}),\chi^{(m-i)}(\underline{z'})).\end{aligned}$$

Hence, by property (c), it follows that $\varphi_m(\underline{z}+\underline{z'})=\chi^{(m)}(z)+\chi^{(m)}(z')$, which implies that φ_m is additive.

Since φ_m is additive, it suffices to check multiplicativity on Witt vectors of the form $V^i\underline{z}$. We have $V^i\underline{z}\cdot V^j\underline{z'}=p^iV^i(\underline{z}\cdot V^{j-i}\underline{z'})$. Notice that $p\pi(xy)=\pi(x)\pi(y)$ implies that $p^i\pi^i(xy)=\pi^i(x)\pi^i(y)$. If $i\neq 0$, then, using this fact along with the facts that φ_m is additive and $\varphi_mV=\pi\varphi_{m-1}$ by induction, it follows that

$$\begin{aligned}\varphi_m(V^i\underline{z}V^j\underline{z'}) &= \varphi_m(p^iV^i(\underline{z}\cdot V^{j-i}\underline{z'}))\\ &= p^i\pi^i(\varphi_{m-i}(\underline{z})\cdot\varphi_{m-i}(V^{j-i}\underline{z'}))\\ &= \pi^i\varphi_{m-i}(\underline{z})\cdot\pi^i\varphi_{m-i}(V^{j-i}\underline{z'})\\ &= \varphi_m(V^i\underline{z})\cdot\varphi_m(V^j\underline{z'}).\end{aligned}$$

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

If $i=0$, then we have $\underline{z}\cdot V^j(\underline{z'}) = V^j(\underline{z^{p^j}z'})$ and, using property (b), it follows that

$$\begin{aligned}\varphi_m(\underline{z}\cdot V^j\underline{z'}) &= \varphi_m(V^j(\underline{z^{p^j}z'}))\\ &= \pi^j\varphi_{m-j}(\underline{z^{p^j}z'})\\ &= \pi^j\chi^{(m-j)}(z^{p^j}z')\\ &= \chi^{(m)}(z)\cdot\pi^j\chi^{(m-j)}(z')\\ &= \varphi_m(\underline{z})\cdot\varphi_m(V^j\underline{z'}).\end{aligned}$$

□

2.5 To show that the map ϕ_m in Theorem 1 is a ring homomorphism, we check that for $Z_i = Z(A_i)$ the maps $\chi^{(i)}: Z_0\to Z_i$ and $\pi: Z_i\to Z_{i+1}$ defined by $\chi^{(i)}(z)=\widetilde{z}^{p^i}$ and $\pi(z)=pz$ satisfy the conditions of Lemma 2.3. The only assertions that merit proof here are the multiplicativity of $\chi^{(m)}$ and property (c), which is implied by the following identity:[2]

$$p^i\psi_{i+1}(\widetilde{x}^{p^j},\widetilde{y}^{p^j}) = (\widetilde{x}^{p^j}+\widetilde{y}^{p^j})^{p^i} - (\widetilde{x}^{p^{j+1}}+\widetilde{y}^{p^{j+1}})^{p^{i-1}} \tag{2.14}$$

for all $\widetilde{x},\widetilde{y}\in A_m$ that are central modulo p and every pair i,j with $i+j=m$.

Suppose that elements $\widetilde{x},\widetilde{y}\in A_{m+1}$ are central modulo p^{m+1}, i.e. their reductions in A_m lie in Z_m. Then, by Lemma 2.1, we have that $[\widetilde{x},\widetilde{y}]\in Z_{m+1}\cap p^{m+1}A_{m+1}$. Using this property, one proves inductively that for all $n\geqslant 1$,

$$\begin{gathered}(\widetilde{x}\widetilde{y})^n = \widetilde{x}^n\widetilde{y}^n - \binom{n}{2}\widetilde{x}^{n-1}\widetilde{y}^{n-1}[\widetilde{x},\widetilde{y}],\\ (\widetilde{x}+\widetilde{y})^n = \sum_{i=0}^{n}\binom{n}{i}\widetilde{x}^i\widetilde{y}^{n-i} - \binom{n}{2}(\widetilde{x}+\widetilde{y})^{n-2}[\widetilde{x},\widetilde{y}].\end{gathered}$$

As $\binom{p}{2}$ is divisible by p (here we use that $p\neq 2$), it follows that

$$(\widetilde{x}\widetilde{y})^p = \widetilde{x}^p\widetilde{y}^p, \tag{2.15}$$

$$(\widetilde{x}+\widetilde{y})^p = \sum_{i=0}^{p}\binom{p}{i}\widetilde{x}^i\widetilde{y}^{p-i}. \tag{2.16}$$

The multiplicativity of $\chi^{(m)}$ is derived from (2.15) by induction. Let us check (2.14). When $i=1$, formula (2.14) follows directly from (2.16). For $i>1$, by using induction on i we get

$$\begin{aligned}(\widetilde{x}^{p^j}+\widetilde{y}^{p^j})^{p^i} &= ((\widetilde{x}^{p^{j+1}}+\widetilde{y}^{p^{j+1}})^{p^{i-2}} + p^{i-1}\psi_i(\widetilde{x}^{p^j},\widetilde{y}^{p^j}))^p\\ &= (\widetilde{x}^{p^{j+1}}+\widetilde{y}^{p^{j+1}})^{p^{i-1}} + p^i\sum_{l=1}^{p}\binom{p}{l}p^{l(i-1)-i}\psi_i(\widetilde{x}^{p^j},\widetilde{y}^{p^j})^l(\widetilde{x}^{p^{j+1}}+\widetilde{y}^{p^{j+1}})^{(p-l)p^{i-2}},\end{aligned}$$

and (2.14) follows from the recursive formula (2.8).

Thus ϕ_m is a homomorphism. Let us check that the homomorphism

$$W_{m+1}(Z_0)\otimes_{W_{m+1}(R_0)} R_m \to Z_m, \quad z\otimes a\mapsto a\phi_m(z)$$

[2] Although formula (2.14) may seem to be the definition of the polynomial ψ_{i+1}, it is in fact false when $p=2$. Because $\widetilde{x}^{p^j}$ and $\widetilde{y}^{p^j}$ are not central in A_m, one cannot evaluate ψ_{i+1} on these elements in A_m. Instead, one evaluates ψ_{i+1} on $\widetilde{x}^{p^j}$ and $\widetilde{y}^{p^j}$ in A_j, where they are central, and one gets a well-defined element of A_m upon multiplying by p^j.

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

descends to a homomorphism from the quotient ring $W_{m+1}(Z_0/R_m)$. Indeed, for $z \in W_{m+1-j}(Z_0)$ and $x \in W_{m+1-j}(R_0)$, we have

$$\phi_m(V^j\,(x \cdot z)) = p^j \phi_{m-j}\,(x \cdot z) = \phi_{m-j}(x)\phi_m(V^j z).$$

This shows that the homomorphism Φ_m is well-defined.

2.6 It remains to prove that if the deformation A_n is non-degenerate, then the homomorphism $\Phi_m : W_{m+1}(Z_0/R_m) \to Z_m$ is an isomorphism. When $m = 0$, Φ_0 is clearly an isomorphism. Now assume that Φ_l is an isomorphism for all $0 \leqslant l < m+1$. For a positive integer i, we denote by

$$F^i_{Z_0/R_0} : Z_0^{(i)} = Z_0 \otimes_{F^i_{R_0}} R_0 \to Z_0$$

the ith iterate of the relative Frobenius map.

In order to show that Φ_{m+1} is an isomorphism, we need the following result.

Proposition 2.4. *Let $r(Z_{m+1}) \subset Z_0$ be the image of the reduction map; then $r(Z_{m+1}) = \mathrm{Im}(F^{m+1}_{Z_0/R_0})$.*

Proof. We retain the assumption that Φ_l is an isomorphism for all $0 \leqslant l < m+1$. The containment $r(Z_{m+1}) \supset \mathrm{Im}(F^{m+1}_{Z_0/R_0})$ is clear by Lemma 2.1(5).

Let $y \in Z_m$ and $x \in Z_0$, and let $\widetilde{x}, \widetilde{y} \in A_n$ be liftings of x and y. Then the element $[\widetilde{y}, \widetilde{x}]/p^{m+1} \bmod p \in Z_0$ is independent of the liftings. Moreover, by Lemma 2.1(4), the map

$$\Pi_y : Z_0 \to Z_0, \quad x \mapsto [\widetilde{y}, \widetilde{x}]/p^{m+1} \bmod p \tag{2.17}$$

is a R_0-linear derivation, $\Pi_y \in T_{Z_0/R_0}$. Identifying T_{Z_0/R_0} with $\Omega^1_{Z_0/R_0}$, we get a linear map

$$\Pi : Z_m \to \Omega^1_{Z_0/R_0}, \quad y \mapsto i_{\Pi_y}\mu^{-1}. \tag{2.18}$$

Note that if $y \in Z_m$ is the reduction mod p^{m+1} of some element $\widetilde{y} \in Z_{m+1}$, then $\Pi(y) = 0$.

Lemma 2.5. *The image of an element $(z_0, \ldots, z_m) \otimes a \in W_{m+1}(Z_0/R_m)$ under the composition*

$$S = \Pi \circ \Phi_m : W_{m+1}(Z_0/R_m) \xrightarrow{\sim} Z_m \longrightarrow \Omega^1_{Z_0/R_0}$$

is given by the formula

$$S((z_0, \ldots, z_m) \otimes a) = \overline{a} \sum_{i=0}^{m} z_i^{p^{m-i}-1}\, dz_i, \tag{2.19}$$

where $\overline{a} \in R_0$ is the reduction of a modulo p.

Proof. We start with the following claim.

Claim 2.6. *If $x \in Z_0$, $z \in Z_i$ and $\widetilde{x}, \widetilde{z} \in A_n$ are any liftings, then we have*

$$[\widetilde{z}^p, \widetilde{x}] \equiv p\widetilde{z}^{p-1}[\widetilde{z}, \widetilde{x}] \mod p^{i+3}. \tag{2.20}$$

Indeed,

$$\begin{aligned}[\widetilde{z}^p, \widetilde{x}] &= \sum_{j=0}^{p-1} \widetilde{z}^{p-j-1}[\widetilde{z}, \widetilde{x}]\widetilde{z}^j \\ &= \sum_{j=0}^{p-1} (\widetilde{z}^{p-1}[\widetilde{z}, \widetilde{x}] - \widetilde{z}^{p-j-1}[\widetilde{z}^j, [\widetilde{z}, \widetilde{x}]]).\end{aligned}$$

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

Since $z \in Z_i$, we have $[\widetilde{z}, [\widetilde{z}, \widetilde{x}]] \bmod p^{i+3} \in Z_{i+2}$. Thus $\widetilde{z}^{p-j-1}[\widetilde{z}^j, [\widetilde{z}, \widetilde{x}]] \equiv j\widetilde{z}^{p-2}[\widetilde{z}, [\widetilde{z}, \widetilde{x}]] \bmod p^{i+3}$ and

$$\begin{aligned}\sum_{j=0}^{p-1}(\widetilde{z}^{p-1}[\widetilde{z}, \widetilde{x}] - \widetilde{z}^{p-j-1}[\widetilde{z}^j, [\widetilde{z}, \widetilde{x}]]) &\equiv \sum_{j=0}^{p-1}(\widetilde{z}^{p-1}[\widetilde{z}, \widetilde{x}] - j\widetilde{z}^{p-2}[\widetilde{z}, [\widetilde{z}, \widetilde{x}]]) \\ &\equiv p\widetilde{z}^{p-1}[\widetilde{z}, \widetilde{x}] - \binom{p}{2}\widetilde{z}^{p-2}[\widetilde{z}, [\widetilde{z}, \widetilde{x}]] \mod p^{i+3}.\end{aligned}$$

Since $p \neq 2$, we have $\binom{p}{2} \equiv 0 \bmod p$ and thus $\binom{p}{2}[\widetilde{z}, [\widetilde{z}, \widetilde{x}]] \equiv 0 \bmod p^{i+3}$, which gives (2.20).

The claim above implies, by induction, that for every $i \geqslant 0$ and $x, z \in Z_0$ we have

$$[\widetilde{z}^{p^i}, \widetilde{x}] \equiv p^i \widetilde{z}^{p^i-1}[\widetilde{z}, \widetilde{x}] \mod p^{i+2}.$$

Thus, we conclude that

$$\left[\sum_{i=0}^{m} p^i \widetilde{z}_i^{p^{m-i}}, \widetilde{x}\right] \equiv p^m \sum_{i=0}^{m} \widetilde{z}_i^{p^{m-i}-1}[\widetilde{z}_i, \widetilde{x}] \mod p^{m+2},$$

which implies the desired result. □

The following result will also be used in the next section.

Lemma 2.7. *Let p be a prime number (not necessarily odd), let Z_0 be a smooth R_0-algebra, and let $S : W_{m+1}(Z_0/R_m) \longrightarrow \Omega^1_{Z_0/R_0}$ be the morphism (the 'Serre morphism') defined by formula (2.19). If $z \in \operatorname{Ker} S$, then the image of z under the map*

$$\alpha : W_{m+1}(Z_0/R_m) \to Z_0^{(m)}, \quad (z_0, \dots, z_m) \otimes a \mapsto z_0 \otimes \overline{a}$$

is contained in the image of the relative Frobenius map $F_{Z_0^{(m)}/R_0} : Z_0^{(m+1)} \to Z_0^{(m)}$, so that we have the following diagram.

$$\begin{tikzcd} \operatorname{Ker} S \arrow[r, hook] \arrow[d] & W_{m+1}(Z_0/R_m) \arrow[d, "\alpha"] \\ Z_0^{(m+1)} \arrow[r, hook, "F_{Z_0^{(m)}/R_0}"'] & Z_0^{(m)} \end{tikzcd}$$

Proof. Recall (see, e.g., [Ill79]) that for every smooth R_0-algebra Z_0 we have the Cartier isomorphism

$$C^{-1} : \Omega^1_{Z_0^{(1)}/R_0} = \Omega^1_{Z_0/R_0} \otimes_{F_{R_0}} R_0 \xrightarrow{\sim} H^1(\Omega^{\cdot}_{Z_0/R_0}) \subset \Omega^1_{Z_0/R_0}/d(Z_0),$$
$$x\, dy \otimes \overline{a} \mapsto \overline{a} x^p y^{p-1} dy \quad \text{for } x\, dy \in \Omega^1_{Z_0/R_0},\ \overline{a} \in R_0.$$

More generally, for each positive integer i we shall define a R_0-module D_i together with a R_0-linear map

$$C^{-i} : \Omega^1_{Z_0^{(i)}/R_0} \to D_i.$$

The first R_0-module D_1 is just the quotient of $\Omega^1_{Z_0/R_0}$ by the subspace $d(Z_0)$ of exact forms. Assuming that D_i and C^{-i} are already defined, we define D_{i+1} to be the quotient of D_i by $C^{-i}(d(Z_0^{(i)}))$ and C^{-i-1} to be the composition

$$\Omega^1_{Z_0^{(i+1)}/R_0} \xrightarrow{C^{-1}} \Omega^1_{Z_0^{(i)}/R_0}/d(Z_0^{(i)}) \xrightarrow{C^{-i}} D_{i+1}.$$

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

As C^{-1} is injective, C^{-i} is injective as well. By construction, D_i is a quotient of $\Omega^1_{Z_0/R_0}$; we denote by $\beta : \Omega^1_{Z_0/R_0} \to D_i$ the projection. Then we have the following commutative diagram.

$$\begin{tikzcd} W_{m+1}(Z_0/R_m) \arrow[r, "S"] \arrow[d, "\alpha"'] & \Omega^1_{Z_0/R_0} \arrow[d, "\beta"'] \\ Z_0^{(m)} \arrow[r, "C^{-m}d"'] & D_m \end{tikzcd}$$

If $z \in \operatorname{Ker} S$, then $C^{-m}d(\alpha(z)) = 0$ and thus $d(\alpha(z)) = 0$. Therefore $\alpha(z)$ lies in the image of the relative Frobenius map. $\square$

Now we can finish the proof of Proposition 2.4. As we have observed above, if $y \in Z_m$ is the reduction mod p^{m+1} of an element $\widetilde{y} \in Z_{m+1}$, then $\Pi(y) = 0$. Consider the following commutative diagram.

$$\begin{tikzcd} Z_{m+1} \arrow[r] \arrow[d] & Z_m \arrow[r, "r"] \arrow[d, "\Phi_m^{-1}"'] & Z_0 & \\ \operatorname{Ker} S \arrow[r, hook] & W_{m+1}(Z_0/R_m) \arrow[r, "\alpha"] & Z_0^{(m)} \arrow[u, "F^m_{Z_0/R_0}"'] & Z_0^{(m+1)} \arrow[l, hook', "F_{Z_0^{(m)}/R_0}"'] \end{tikzcd} \tag{2.21}$$

By Lemma 2.7, the map $\alpha : \operatorname{Ker} S \xrightarrow{\alpha} Z_0^{(m)}$ factors through $Z_0^{(m+1)} \xrightarrow{F_{Z_0^{(m)}/R_0}} Z_0^{(m)}$. Thus, the reduction map r factors through $Z_0^{(m+1)} \xrightarrow{F^{m+1}_{Z_0/R_0}} Z_0$. $\square$

To finish the proof of Theorem 1, we need the following general property of relative Witt vectors.

Lemma 2.8. *For every R_0-algebra Z_0, we have a right exact sequence of R_{m+1}-modules*

$$W_{m+1}(Z_0/R_m) \to W_{m+2}(Z_0/R_{m+1}) \to Z_0 \otimes_{F^{m+1}_{R_0}} R_0 \to 0,$$

where the first morphism takes $z \otimes a \in W_{m+1}(Z_0/R_m)$ to $Vz \otimes a$ and the second morphism is induced by the projection $W_{m+2}(Z_0) \to Z_0$ onto the first coordinate.

Proof. Consider the exact sequence of $W_{m+2}(R_0)$-modules

$$0 \longrightarrow W_{m+1}(Z_0) \xrightarrow{V} W_{m+2}(Z_0) \longrightarrow Z_0 \longrightarrow 0. \tag{2.22}$$

We remark that the action of $W_{m+2}(R_0)$ on $W_{m+1}(Z_0)$, viewed as a submodule of $W_{m+2}(Z_0)$, is given by the homomorphism

$$W_{m+2}(R_0) \xrightarrow{F} W_{m+1}(R_0) \to W_{m+1}(Z_0).$$

Thus, the tensor product of (2.22) with R_{m+1} can be identified with the sequence

$$W_{m+1}(Z_0) \otimes_{W_{m+1}(R_0^p)} R_m \xrightarrow{V \otimes \mathrm{Id}} W_{m+2}(Z_0) \otimes_{W_{m+2}(R_0)} R_{m+1} \to Z_0 \otimes_{F^{m+1}_{R_0}} R_0 \to 0,$$

which is right exact. Here R_0^p denotes the image of the Frobenius morphism $R_0 \to R_0$. One checks that the composition of $V \otimes \mathrm{Id}$ with the projection

$$W_{m+2}(Z_0) \otimes_{W_{m+2}(R_0)} R_{m+1} \longrightarrow W_{m+2}(Z_0/R_{m+1})$$

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

factors through the surjection

$$W_{m+1}(Z_0) \otimes_{W_{m+1}(R_0^p)} R_m \twoheadrightarrow W_{m+1}(Z_0) \otimes_{W_{m+1}(R_0)} R_m \twoheadrightarrow W_{m+1}(Z_0/R_m).$$

This gives the sequence displayed in the lemma. □

Now we finish the proof that Φ_{m+1} is an isomorphism. Consider the following commutative diagram.

$$\begin{tikzcd}
& W_{m+1}(Z_0/R_m) \arrow[r] \arrow[d, "f"] & W_{m+2}(Z_0/R_{m+1}) \arrow[r] \arrow[d, "\Phi_{m+1}"] & Z_0 \otimes_{F^{m+1}_{R_0}} R_0 \arrow[r] \arrow[d, "\overline{\Phi_{m+1}}"] & 0 \\
0 \arrow[r] & Z_{m+1} \cap pA_{m+1} \arrow[r] & Z_{m+1} \arrow[r] \arrow[dr, "r"'] & \dfrac{Z_{m+1}}{Z_{m+1} \cap pA_{m+1}} \arrow[r] \arrow[d, hook] & 0 \\
& & & Z_0 &
\end{tikzcd}$$

Here the top row is the right exact sequence from Lemma 2.8, $f : W_{m+1}(Z_0/R_m) \to Z_{m+1} \cap pA_{m+1}$ equals $p\Phi_m$, which is an isomorphism by the induction assumption, and, finally, the morphism $\overline{\Phi_{m+1}} : Z_0 \otimes R_{m+1} \simeq Z_0^{(m+1)} \to Z_{m+1}/(Z_{m+1} \cap pA_{m+1}) \subset Z_0$ is equal to $F^{m+1}_{Z_0/R_0}$. By Proposition 2.4, $\overline{\Phi_{m+1}}$ is an isomorphism. It follows that Φ_{m+1} is an isomorphism as well.

3. Main result: characteristic 2 case

3.1 Throughout this section, R_n is a commutative algebra flat over $\mathbb{Z}/2^{n+1}\mathbb{Z}$, where $n > 0$, and A_n is a flat associative R_n-algebra. We will also assume that the deformation A_n of A_0 is non-degenerate and denote by $\omega \in \Omega^2_{Z_0/R_0}$ the corresponding non-degenerate 2-form. Although the map $W_{n+1}(Z_0) \to Z_n$ defined by equation (2.3) is neither additive nor multiplicative, we explain in this section that if ω is exact, formula (2.3) can be corrected to yield an isomorphism of R_n-algebras,

$$W_{n+1}(Z_0/R_n) \xrightarrow{\sim} Z_n.$$

Our construction depends on the choice of a primitive $\eta \in \Omega^1_{Z_0/R_0}$, $\omega = d\eta$. Define a map

$$Z_0 \to Z_0, \quad z \mapsto z^{[2]} \tag{3.1}$$

by the formula

$$z^{[2]} = L_{t_z} i_{t_z} \eta - i_{t_z^{[2]}} \eta \in Z(A_0), \tag{3.2}$$

where $t_z \in T_{Z_0/R_0}$ is the Hamiltonian vector field corresponding to z, i.e. $dz = i_{t_z}\omega$, $t_z^{[2]} \in T_{Z_0/R_0}$ is its square in the restricted Lie algebra of vector fields, and L_{t_z} is the Lie derivative. We remark that the map $z \mapsto z^{[2]}$ depends only on the class of η in the quotient $\Omega^1_{Z_0/R_0}/d(Z_0)$.

Lemma 3.1. *For every $x, y \in Z_0$, we have*

$$(x+y)^{[2]} - x^{[2]} - y^{[2]} = \{x, y\}, \tag{3.3}$$

$$\{x^{[2]}, y\} = \{x, \{x, y\}\}, \tag{3.4}$$

$$(xy)^{[2]} = y^2 x^{[2]} + x^2 y^{[2]} + xy\{x, y\}. \tag{3.5}$$

Proof. Define a map $\mathcal{Q}: T_{Z_0/R_0} \to Z_0$ by the formula

$$\mathcal{Q}(\theta) = L_\theta i_\theta \eta - i_{\theta^{[2]}} \eta \quad \text{for } \theta \in T_{Z_0/R_0}. \tag{3.6}$$

Then, for every $\theta_1, \theta_2 \in T_{Z_0/R_0}$, by using the identity $(\theta_1+\theta_2)^{[2]} = \theta_1^{[2]} + \theta_2^{[2]} + [\theta_1, \theta_2]$ and Cartan's formula we find that

$$\mathcal{Q}(\theta_1+\theta_2) - \mathcal{Q}(\theta_1) - \mathcal{Q}(\theta_2) = L_{\theta_1} i_{\theta_2} \eta + L_{\theta_2} i_{\theta_1} \eta - i_{[\theta_1,\theta_2]} \eta = i_{\theta_1} i_{\theta_2} \omega. \tag{3.7}$$

Using $i_{t_x} i_{t_y} \omega = \{x, y\}$, equation (3.3) follows. Next, for every $z \in Z_0$, by using the identity $(z\theta)^{[2]} = z^2 \theta^{[2]} + z(L_\theta z)\theta$ one obtains

$$\mathcal{Q}(z\theta) = z L_\theta (z i_\theta \eta) - z^2 i_{\theta^{[2]}} \eta - z(L_\theta z) i_\theta \eta = z^2 \mathcal{Q}(\theta). \tag{3.8}$$

Thus, we conclude that

$$(xy)^{[2]} = \mathcal{Q}(x t_y + y t_x) = x^2 \mathcal{Q}(t_y) + y^2 \mathcal{Q}(t_x) + xy i_{t_x} i_{t_y} \omega,$$

which proves (3.5). Finally, for (3.4) it suffices to check that $t_x^{[2]} = t_{x^{[2]}}$ or, equivalently, that $i_{t_x^{[2]}} \omega = i_{t_{x^{[2]}}} \omega$. We have

$$i_{t_{x^{[2]}}} \omega = dx^{[2]} = d(L_{t_x} i_{t_x} \eta - i_{t_x^{[2]}} \eta) = -L_{t_x} i_{t_x} \omega + L_{t_x}^2 \eta + i_{t_x^{[2]}} \omega - L_{t_x^{[2]}} \eta. \tag{3.9}$$

Since $L_{t_x} i_{t_x} \omega = d\{x, x\} = 0$ and $L_{t_x}^2 \eta = L_{t_x^{[2]}} \eta$, the right-hand side of (3.9) equals $i_{t_x^{[2]}} \omega$ as required. $\square$

Remark 3.2. Equations (3.7) and (3.8) show that the quadratic form $\mathcal{Q}$ on the Z_0-module T_{Z_0/R_0} is a quadratic refinement of the symmetric form ω. In fact, for every smooth R_0-algebra Z_0 in characteristic 2, one can define a refined de Rham complex

$$(S^{\cdot}\Omega^1_{Z_0/R_0}, \tilde{d}) = Z_0 \to \Omega^1_{Z_0/R_0} \to S^2 \Omega^1_{Z_0/R_0} \to \cdots$$

to be the initial object in the category of commutative DG algebras $\mathcal{A}$ over R_0 equipped with a homomorphism $Z_0 \to \mathcal{A}$. By the universal property, the DG algebra $(S^{\cdot}\Omega^1_{Z_0/R_0}, \tilde{d})$ maps to the de Rham DG algebra $(\bigwedge^{\cdot} \Omega^1_{Z_0/R_0}, \tilde{d})$. The quadratic form $\mathcal{Q} \in S^2 \Omega^1_{Z_0/R_0}$ is identified with $\tilde{d}\eta$.

Remark 3.3. In [BK08, Definition 1.8], Bezrukavnikov and Kaledin introduced the notion of a restricted Poisson algebra in characteristic p. If $p = 2$, a restricted Poisson algebra is just a Poisson algebra Z_0 over R_0 together with a map $Z_0 \to Z_0$, $z \mapsto z^{[2]}$, satisfying equations (3.3), (3.4) and (3.5). According to [BK08, Theorem 1.11], a smooth Poisson algebra Z_0 with a non-degenerate Poisson bracket admits a restricted structure if and only if the associated symplectic form ω is exact. If $\omega = d\eta$, then the formula

$$z^{[p]} = L_{t_z}^{p-1} i_{t_z} \eta - i_{t_z^{[p]}} \eta$$

defines a restricted structure on Z_0 (cf. [BK08, Theorem 1.12]).

The main result of this section is the following theorem.

Theorem 2. *Let R_n be a flat commutative algebra over $\mathbb{Z}/2^{n+1}\mathbb{Z}$, and let A_n be a flat associative algebra over R_n such that the center Z_0 is smooth over R_0 and the bracket $\{\,,\}: Z_0 \otimes Z_0 \to Z_0$ is associated with an exact symplectic form $\omega = d\eta$. Then, for every $0 \leqslant m \leqslant n$, the map*

$$\phi_m : W_{m+1}(Z_0) \to Z_m$$

given by

$$\phi_m(z_0, \ldots, z_m) = \sum_{i=0}^{m-1} 2^i \big(\tilde{z}_i^2 + 2\widetilde{z_i^{[2]}}\big)^{2^{m-i-1}} + 2^m \tilde{z}_m$$

is a ring homomorphism. Moreover, the induced homomorphism

$$\Phi_m : W_{m+1}(Z_0/R_m) \to Z_m, \quad \Phi_m(z \otimes a) = a\phi_m(z) \tag{3.10}$$

is an isomorphism.

The proof of this theorem occupies the next two subsections.

Remark 3.4. The construction in Theorem 2 can be partially generalized to the case where ω is not exact. To indicate this generalization, let A_n be a non-degenerate deformation over R_n, and let $\mu = \omega^{-1} \in \bigwedge^2 T_{Z_0/R_0}$ be the corresponding bivector field. Let $\mathcal{P}$ be a quadratic refinement of μ, which is a preimage of μ under the canonical projection

$$S^2 T_{Z_0/R_0} \to \bigwedge^2 T_{Z_0/R_0}.$$

Then the map

$$h_{\mathcal{P}} : Z_0 \to Z_0, \quad h_{\mathcal{P}}(z) = \langle \mathcal{P}, dz \otimes dz \rangle$$

satisfies the following properties (cf. (3.3) and (3.5)):

$$h_{\mathcal{P}}(x+y) - h_{\mathcal{P}}(x) - h_{\mathcal{P}}(y) = \{x, y\},$$
$$h_{\mathcal{P}}(xy) = y^2 h_{\mathcal{P}}(x) + x^2 h_{\mathcal{P}}(y) + xy\{x, y\}.$$

We note that if ω is exact, then the choice of a primitive η, with $d\eta = \omega$, specifies a quadratic refinement $\mathcal{Q} = \tilde{d}\eta \in S^2\Omega^1_{Z_0/R_0}$ of ω (Remark 3.2), which in turn gives rise to a quadratic refinement $\mathcal{P}$ of μ. In this convention we have that $z^{[2]} = h_{\mathcal{P}}(z)$.

Coming back to the general case, the proof of Theorem 2 given below extends directly and shows that the map

$$\Phi_{\mathcal{P},m} : W_{m+1}(Z_0/R_0) \to Z_m$$

given by

$$\Phi_{\mathcal{P},m}((z_0, \ldots, z_m) \otimes a) = a\left(\sum_{i=0}^{m-1} 2^i \big(\tilde{z}_i^2 + 2\widetilde{h_{\mathcal{P}}(z_i)}\big)^{2^{m-i-1}} + 2^m \tilde{z}_m\right)$$

is a ring homomorphism for every m and an isomorphism for $m = 1$. However, for $m > 1$, the morphism $\Phi_{\mathcal{P},m}$ need not be surjective.

In fact, in general, the center Z_m of a non-degenerate deformation need not be isomorphic to the Witt vectors $W_{m+1}(Z_0/R_0)$. For example, let A_2 be the quotient of the free algebra over $\mathbb{Z}/8\mathbb{Z}$ on generators x, y by the ideal $(xy + yx)$. We have that $Z_0 = A_0 = \mathbb{F}_2[x, y]$ and $Z_2 = \mathbb{Z}/8\mathbb{Z}[x^2, y^2] + 4A_2$. Therefore, it follows that $W_3(Z_0)/2\text{-torsion} \cong W_2(\mathbb{F}_2[x, y])$ and $Z_2/2\text{-torsion} \cong \mathbb{Z}/4\mathbb{Z}[x^2, y^2]$. In particular, $Z_2/2$-torsion is flat over $\mathbb{Z}/4\mathbb{Z}$, whereas $W_3(Z_0)/2$-torsion is not flat. Therefore $W_3(Z_0)$ and Z_2 cannot be isomorphic. Notice that the associated symplectic form of this deformation is $xy\, dx\, dy$, which is closed but not exact.

3.2 Now we give a proof of Theorem 2. We will show that ϕ_{m+1} is a homomorphism and that Φ_{m+1} is an isomorphism simultaneously. It is clear that $\phi_0 = \Phi_0$ are isomorphisms.

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

Consider the general case. In everything that follows we will assume that ϕ_l is a homomorphism and Φ_l is an isomorphism for all $0 \leqslant l \leqslant m$. We will need the following result.

LEMMA 3.5. *If $x \in Z_1$, $y \in Z_i$ with $1 \leqslant i \leqslant m$, and $\widetilde{x}, \widetilde{y} \in A_n$ are any liftings, then*

$$[\widetilde{x}, \widetilde{y}] \equiv 0 \mod 2^{i+2}.$$

Proof. We may assume that $m \geqslant 1$ (otherwise, the statement is empty). Then, by our induction hypothesis, the map $\Phi_1 : W_2(Z_0/R_1) \to Z_1$ is surjective. Thus, it suffices to check the lemma for $\widetilde{x}$ of the form $\widetilde{x} = \widetilde{w}^2 + 2\widetilde{v}$ with $\widetilde{w}, \widetilde{v} \in A_n$ central modulo 2. We have

$$\begin{aligned}[\widetilde{x}, \widetilde{y}] &= [\widetilde{w}^2 + 2\widetilde{v}, \widetilde{y}] \\ &= \widetilde{w}[\widetilde{w}, \widetilde{y}] + [\widetilde{w}, \widetilde{y}]\widetilde{w} + 2[\widetilde{v}, \widetilde{y}] \equiv 0 \mod 2^{i+2},\end{aligned}$$

since the elements $[\widetilde{w}, \widetilde{y}]$ and y are central modulo 2^{i+1}. □

COROLLARY 3.6. *If $x, y \in Z_i$ with $1 \leqslant i \leqslant m$ and $\widetilde{x}, \widetilde{y} \in A_{i+1}$ are any liftings, then we have*

$$\begin{aligned}(\widetilde{x}\widetilde{y})^2 &= \widetilde{x}^2\widetilde{y}^2, \\ (\widetilde{x} + \widetilde{y})^2 &\equiv \widetilde{x}^2 + 2\widetilde{x}\widetilde{y} + \widetilde{y}^2.\end{aligned}$$

Let $\pi : Z_i \to Z_{i+1}$ be given by $\pi(z) = 2z$ and $\chi^{(i)} : Z_0 \to Z_i$ be defined by $\chi^{(i)}(z) = (\widetilde{z}^2 + 2\widetilde{z^{[2]}})^{2^{i-1}}$ for $0 < i \leqslant m+1$ with $\chi^{(0)}(z) = z$. We will use Lemma 2.3 to show that ϕ_{m+1} is a homomorphism. Let us check that $\chi^{(i)}$ is multiplicative. For $i = 1$, using the formula (3.5) we have that

$$\begin{aligned}\chi^{(1)}(xy) &= \widetilde{x}^2\widetilde{y}^2 - \widetilde{x}[\widetilde{x}, \widetilde{y}]\widetilde{y} + 2(xy)^{[2]} \\ &= \widetilde{x}^2\widetilde{y}^2 - 2xy\{x, y\} + 2(x^2y^{[2]} + y^2x^{[2]} + xy\{x, y\}) \\ &= \chi^{(1)}(x)\chi^{(1)}(y).\end{aligned}$$

The general case now follows from Corollary 3.6.

Next, we show property (b) of Lemma 2.3, which is the following identity:

$$(\widetilde{x}^2 + 2\widetilde{x^{[2]}})^{2^j}(\widetilde{y}^2 + 2\widetilde{y^{[2]}})^{2^{j-i}} \equiv \big((\widetilde{x}^{2^i}\widetilde{y})^2 + 2\widetilde{(x^{2^i}y)^{[2]}}\big)^{2^{j-i}} \mod 2^{j-i+2}$$

for every $0 \leqslant i \leqslant j \leqslant m$. If $i = 0$, then this is equivalent to $\chi^{(j)}$ being multiplicative. Assume that $i > 0$. By Corollary 3.6, it follows that

$$(\widetilde{x}^2 + 2\widetilde{x^{[2]}})^{2^j}(\widetilde{y}^2 + 2\widetilde{y^{[2]}})^{2^{j-i}} \equiv \big((\widetilde{x}^2 + 2\widetilde{x^{[2]}})^{2^i}(\widetilde{y}^2 + 2\widetilde{y^{[2]}})\big)^{2^{j-i}} \mod 2^{j-i+2};$$

thus, to show the desired result, it suffices to check that

$$(\widetilde{x}^2 + 2x^{[2]})^{2^i}(\widetilde{y}^2 + 2y^{[2]}) \equiv (\widetilde{x}^{2^i}\widetilde{y})^2 + 2(x^{2^i}y)^{[2]} \mod 4.$$

Now $(\widetilde{x}^2 + 2x^{[2]})^{2^i} \equiv \widetilde{x}^{2^{i+1}} \mod 4$. Hence we have

$$\begin{aligned}(\widetilde{x}^2 + 2x^{[2]})^{2^i}(\widetilde{y}^2 + 2y^{[2]}) &\equiv \widetilde{x}^{2^{i+1}}(\widetilde{y}^2 + 2y^{[2]}) \\ &\equiv (\widetilde{x}^{2^i}\widetilde{y})^2 + 2x^{2^{i+1}}y^{[2]} \\ &\equiv (\widetilde{x}^{2^i}\widetilde{y})^2 + 2(x^{2^i}y)^{[2]} \mod 4,\end{aligned}$$

where the last congruence is implied by (3.5).

Let us check property (c) of Lemma 2.3. It suffices to prove the following claim.

CLAIM 3.7. (a) *If $x, y \in Z_{m+2-j}$ with $1 < j < m+2$ and $\widetilde{x}, \widetilde{y} \in A_{m+1}$ are any liftings, then*

$$2^{j-1}\psi_j(x, y) = (\widetilde{x} + \widetilde{y})^{2^{j-1}} - (\widetilde{x}^2 + \widetilde{y}^2)^{2^{j-2}} \mod 2^{m+2}.$$

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

(b) *If $x, y \in Z_0$, then for $1 < j \leqslant m+1$ we have*

$$2^{j-1}\psi_j(x,y) = \chi^{(j-1)}(x+y) - (\widetilde{\chi^{(1)}(x)} + \widetilde{\chi^{(1)}(y)})^{2^{j-2}} \mod 2^j.$$

If $j = 2$, then part (a) follows from Corollary 3.6. Now assume that property (a) holds for $2 \leqslant l < j$; then the recursive definition of ψ, equation (2.8), and the induction hypothesis imply that

$$2^{j-1}\psi_j(x,y) \equiv 2((\widetilde{x}+\widetilde{y})^{2^{j-2}} - (\widetilde{x}^2+\widetilde{y}^2)^{2^{j-3}})(\widetilde{x}^2+\widetilde{y}^2)^{2^{j-3}} + ((\widetilde{x}+\widetilde{y})^{2^{j-2}} - (\widetilde{x}^2+\widetilde{y}^2)^{2^{j-3}})^2$$

modulo 2^{m+2}. Applying Corollary 3.6 to the right-hand side, we obtain the desired result. Now let us consider property (b). If $j = 2$, then by using (3.3) we get

$$\chi^{(1)}(x+y) - (\chi^{(1)}(x) + \chi^{(1)}(y)) \equiv 2xy \mod 4,$$

which is the desired result. Now, assuming that property (b) holds for $2 \leqslant l < j$, we find that

$$\begin{aligned}\chi^{(j-1)}(x+y) &= (\widetilde{\chi^{(j-2)}(x+y)})^2 = ((\widetilde{\chi^{(1)}(x)} + \widetilde{\chi^{(1)}(y)})^{2^{j-3}} + 2^{j-2}\widetilde{\psi_{j-1}(x,y)})^2 \\ &= (\widetilde{\chi^{(1)}(x)} + \widetilde{\chi^{(1)}(y)})^{2^{j-2}} + 2^{j-1}(x^2+y^2)^{2^{j-3}}\psi_{j-1}(x,y).\end{aligned}$$

The result then follows from the congruence $\psi_j(x,y) \equiv \psi_{j-1}(x,y)(x^2+y^2)^{2^{j-3}} \mod 2$.

We have shown that π^i and $\chi^{(i)}$ for $0 \leqslant i \leqslant m+1$ satisfy the conditions of Lemma 2.3; hence ϕ_{m+1} is a homomorphism.

3.3 It remains to show that Φ_{m+1} is an isomorphism. As in the odd characteristic case, it suffices to check that

$$r(Z_{m+1}) = \mathrm{Im}(F^{m+1}_{Z_0/R_0}), \tag{3.11}$$

where $r : Z_{m+1} \to Z_0$ is the reduction map and $F^{m+1}_{Z_0/R_0} : Z_0^{(m+1)} \to Z_0$ is the $(m+1)$th iterate of the relative Frobenius map. Let $\Pi : Z_m \to \Omega^1_{Z_0/R_0}$ be the map defined by formulas (2.17) and (2.18).

LEMMA 3.8. *The image of an element $(z_0, \ldots, z_m) \otimes a \in W_{m+1}(Z_0/R_m)$ under the composition*

$$S = \Pi \circ \Phi_m : W_{m+1}(Z_0/R_m) \xrightarrow{\sim} Z_m \to \Omega^1_{Z_0/R_0}$$

is given by the formula

$$S((z_0, \ldots, z_m) \otimes a) = \overline{a} \sum_{i=0}^{m} z_i^{2^{m-i}-1}\, dz_i \tag{3.12}$$

where $\overline{a} \in R_0$ is the reduction of a modulo 2.

Proof. We start with the following fact.

CLAIM 3.9. *If $x \in Z_0$, $z \in Z_i$ with $0 < i \leqslant m$, and $\widetilde{x}, \widetilde{z} \in A_n$ are any liftings, then we have*

$$[\widetilde{z}^2, \widetilde{x}] \equiv 2\widetilde{z}[\widetilde{z}, \widetilde{x}] \mod 2^{i+3}. \tag{3.13}$$

Indeed, we have

$$\begin{aligned}[\widetilde{z}^2, \widetilde{x}] &= \widetilde{z}[\widetilde{z}, \widetilde{x}] + [\widetilde{z}, \widetilde{x}]\widetilde{z} \\ &= 2\widetilde{z}[\widetilde{z}, \widetilde{x}] - [\widetilde{z}, [\widetilde{z}, \widetilde{x}]].\end{aligned}$$

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

Since $[\widetilde{z},\widetilde{x}] \bmod 2^{i+2} \in Z_{i+1}$, Lemma 3.5 implies that $[\widetilde{z},[\widetilde{z},\widetilde{x}]] \equiv 0 \bmod 2^{i+3}$, and the result follows.

Formula (3.13) implies, by induction, that for $z \in Z_1$ and $i > 1$, we have

$$[\widetilde{z}^{2^{i-1}},\widetilde{x}] \equiv 2^{i-1}\widetilde{z}^{2^{i-1}-1}[\widetilde{z},\widetilde{x}] \mod 2^{i+2}. \tag{3.14}$$

On the other hand, for $x, z \in Z_0$, by using (3.4) we obtain[3]

$$\begin{aligned}[\widetilde{z}^2 + 2\widetilde{z^{[2]}},\widetilde{x}] &= [\widetilde{z}^2,\widetilde{x}] + 2[\widetilde{z^{[2]}},\widetilde{x}]\\ &= 2\widetilde{z}[\widetilde{z},\widetilde{x}] + [\widetilde{z},[\widetilde{z},\widetilde{x}]] + 2[\widetilde{z^{[2]}},\widetilde{x}]\\ &\equiv 2\widetilde{z}[\widetilde{z},\widetilde{x}] + [\widetilde{z},[\widetilde{z},\widetilde{x}]] + [\widetilde{z},[\widetilde{z},\widetilde{x}]]\\ &\equiv 2\widetilde{z}[\widetilde{z},\widetilde{x}] \mod 8.\end{aligned}$$

This fact, along with (3.14), implies that for every $x, z \in Z_0$ one has

$$[(\widetilde{z}^2 + 2\widetilde{z^{[2]}})^{2^{i-1}},\widetilde{x}] \equiv 2^i(\widetilde{z}^2 + 2\widetilde{z^{[2]}})^{2^{i-1}-1}\widetilde{z}[\widetilde{z},\widetilde{x}] = 2^{i+1}z^{2^i-1}\{z,x\} \mod 2^{i+2},$$

which proves the result. □

The above lemma and Lemma 2.7 together imply (3.11). Thus Theorem 2 is proven.

4. Applications

Let S_n be a flat scheme over $\mathbb{Z}/p^{n+1}\mathbb{Z}$, and let $X_n \xrightarrow{f_n} S_n$ be a smooth scheme over S_n. For $0 \leqslant m \leqslant n$ we set $X_m = X_n \times \operatorname{Spec} \mathbb{Z}/p^{m+1}\mathbb{Z} \xrightarrow{f_m} S_n \times \operatorname{Spec} \mathbb{Z}/p^{m+1}\mathbb{Z} = S_m$. One has the following relative Frobenius diagram.

$$\begin{tikzcd} X_0 \arrow[r, "F_{X_0/S_0}"] \arrow[dr, "f_0"'] & X_0^{(1)} \arrow[r, "\pi_{X_0/S_0}"] \arrow[d, "f_0'"] & X_0 \arrow[d, "f_0"] \\ & S_0 \arrow[r, "F_S"] & S_0 \end{tikzcd} \tag{4.1}$$

Since the relative Frobenius morphism $F_{X_0/S_0} : X_0 \to X_0^{(1)}$ is a homeomorphism, the functor F_{X_0/S_0*} induces an equivalence between the category of Zariski sheaves on X_0 and that on $X_0^{(1)}$. We shall also identify the categories of Zariski sheaves on X_n and on X_0.

We will write D_{X_m/S_m} for the sheaf of PD differential operators on X_m (see [BO78, § 2]) and Z_m for its center. One has a canonical isomorphism of $f_0'^{-1}\mathcal{O}_{S_0}$-algebras on $X_0^{(1)}$,

$$F_{X_0/S_0*}(Z_0) \simeq S^{\cdot}T_{X_0^{(1)}/S_0} \tag{4.2}$$

given by the p-curvature map (see, e.g., [OV07, Theorem 2.1]). If $n > 0$, the construction from § 2.1 applied to affine charts of $f_n : X_n \to S_n$ yields a biderivation

$$\{\ ,\ \} : Z_0 \otimes_{f_0^{-1}\mathcal{O}_{S_0}} Z_0 \to Z_0,$$

[3] This is the only place in the proof of Theorem 2 which depends on formula (3.4) and, thus, does not extend to a more general setup such as that of Remark 3.4.

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

which can be interpreted via isomorphism (4.2) as a bivector field

$$\mu \in \Gamma\left(\mathbf{T}^*_{X_0^{(1)}/S_0}, \bigwedge^2 T_{\mathbf{T}^*_{X_0^{(1)}/S_0}/S_0}\right)$$

on the cotangent space, $\mathbf{T}^*_{X_0^{(1)}/S_0}$. On the other hand, the cotangent space to any smooth scheme has a canonical 1-form (the 'contact form')

$$\eta_{\mathrm{can}} \in \Gamma\big(\mathbf{T}^*_{X_0^{(1)}/S_0}, \Omega^1_{\mathbf{T}^*_{X_0^{(1)}/S_0}/S_0}\big),$$

whose differential $\omega_{\mathrm{can}} = d\eta_{\mathrm{can}}$ is a symplectic form.

LEMMA 4.1. *We have that* $\mu^{-1} = -\omega_{\mathrm{can}}$.

Proof. This is proven in [BK05, Lemma 2] for $X_n = \mathbb{A}^m_{S_n}$. The general case follows since the statement is local for étale topology.

If $\mathcal{Z}$ is a sheaf of commutative algebras on a site Y, the presheaf $U \mapsto W_{n+1}(\mathcal{Z}(U))$ is a sheaf denoted by $W_{n+1}(\mathcal{Z})$. More generally, using the construction from § 2.3, for a sheaf $\mathcal{R}_n$ of commutative algebras flat over $\mathbb{Z}/p^{n+1}\mathbb{Z}$ and a sheaf $\mathcal{Z}$ of commutative $\mathcal{R}_0$-algebras, one defines the sheaf of relative Witt vectors $W_{n+1}(\mathcal{Z}/\mathcal{R}_n)$ together with a surjection

$$W_{n+1}(\mathcal{Z}) \otimes_{W_{n+1}(\mathcal{R}_0)} \mathcal{R}_n \twoheadrightarrow W_{n+1}(\mathcal{Z}/\mathcal{R}_n).$$

THEOREM 3. *There is a canonical isomorphism of sheaves of $f_0'^{-1}\mathcal{O}_{S_n}$-algebras on $X_0^{(1)}$,*

$$W_{n+1}(F_{X_0/S_0*}(Z_0)/f_0'^{-1}\mathcal{O}_{S_n}) \xrightarrow{\sim} F_{X_0/S_0*}(Z_n). \tag{4.3}$$

Proof. Let $U \subset X_n$ be an affine open subset lying over an open affine subset $W = \operatorname{Spec} R_n \subset S_n$. Then R_n is a flat algebra over $\mathbb{Z}/p^{n+1}\mathbb{Z}$ and $A_n = \Gamma(U, D_{X_n/S_n})$ is a flat algebra over R_n. By (4.2), the center $Z(A_0)$ of its reduction modulo p is isomorphic to

$$S^{\cdot}T_{\mathcal{O}(U)/R_0} \otimes_{F_{R_0}} R_0,$$

which is smooth over R_0. Moreover, Lemma 4.1 shows that the deformation A_n is non-degenerate and the associated 2-form is the differential of a canonical 1-form, $-\eta_{\mathrm{can}}$. Thus, by Theorems 1 and 2, we get a canonical isomorphism

$$\Phi_n : W_{n+1}(Z(A_0/R_n)) \xrightarrow{\sim} Z(A_n).$$

There exists a unique isomorphism of sheaves of algebras (4.3) that induces Φ_n for each pair U, W as above. □

Combining (4.3) with (4.2), we find an isomorphism

$$W_{n+1}(S^{\cdot}T_{X_0^{(1)}/S_0}/f_0'^{-1}\mathcal{O}_{S_n}) \xrightarrow{\sim} F_{X_0/S_0*}(Z_n).$$

Remark 4.2. The fact that the center of D_{X_m/S_m} depends only on $X_0 \to S_n$ and not on the deformation $X_n \to S_n$ is not surprising: the category of quasi-coherent D_{X_m/S_m}-modules on X_m is equivalent to the category of quasi-coherent crystals on X_0/S_n (see [BO78]). In particular, its categorical center,[4] which is just Z_n, is isomorphic to the center of the category of crystals.

[4] Recall that the center of a category $\mathcal{A}$ is the ring of endomorphisms of the identity functor $\mathrm{Id}_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}$.

https://doi.org/10.1112/S0010437X12000462 Published online by Cambridge University Press

Acknowledgements

This paper owes its existence to Dima Kaledin, who explained to the second author his conjecture on the center of the ring of differential operators. We are grateful to Pierre Berthelot, Arthur Ogus, and Victor Ostrik for helpful conversations related to the subject of this paper. Finally, our deep thanks are due to the referees, who pointed out a gap in an early draft and suggested a simplification of our argument in § 2.5.

References

BK05 A. Belov-Kanel and M. Kontsevich, *Automorphisms of the Weyl algebra*, Lett. Math. Phys. **74** (2005), 181–199.

BO78 P. Berthelot and A. Ogus, *Notes on crystalline cohomology* (Princeton University Press, Princeton, NJ and University of Tokyo Press, Tokyo, 1978).

BK08 R. Bezrukavnikov and D. Kaledin, *Fedosov quantization in positive characteristic*, J. Amer. Math. Soc. **21** (2008), 409–438.

BMR08 R. Bezrukavnikov, I. Mirkovic and D. Rumynin, *Localization of modules for a semisimple Lie algebra in prime characteristic*, Ann. of Math. (2) **167** (2008), 945–991.

Ill79 L. Illusie, *Complexe de de Rham–Witt et cohomologie cristalline*, Ann. Sci. Éc. Norm. Sup. (4) **12** (1979), 501–661.

Mum66 D. Mumford, *Lectures on curves on an algebraic surface*, Annals of Mathematics Studies, vol. 59 (Princeton University Press, Princeton, NJ, 1966).

OV07 A. Ogus and V. Vologodsky, *Nonabelian Hodge theory in characteristic p*, Publ. Math. Inst. Hautes Études Sci. **106**, 2007, 1–138.

Allen Stewart allens@uoregon.edu
Department of Mathematics, University of Oregon, Eugene, OR 97403, USA

Vadim Vologodsky vvologod@uoregon.edu
Department of Mathematics, University of Oregon, Eugene, OR 97403, USA