A SURPRISING FACT ABOUT $\mathcal{D}$-MODULES IN CHARACTERISTIC $p > 0$

JOSEP ÀLVAREZ MONTANER AND GENNADY LYUBEZNIK

Abstract. Let $R = k[x_1, \ldots, x_d]$ be the polynomial ring in d independent variables, where k is a field of characteristic $p > 0$. Let $\mathcal{D}_R$ be the ring of k-linear differential operators of R and let f be a polynomial in R. In this work we prove that the localization $R[\frac{1}{f}]$ obtained from R by inverting f is generated as a $\mathcal{D}_R$-module by $\frac{1}{f}$. This is an amazing fact considering that the corresponding characteristic zero statement is very false.

1. Introduction

Let k be a field and let $R = k[x_1, \ldots, x_d]$, or $R = k[[x_1, \ldots, x_d]]$ be either a ring of polynomials or formal power series in a finite number of variables over k. Let $\mathcal{D}_R$ be the ring of k-linear differential operators on R. For every $f \in R$, the natural action of $\mathcal{D}_R$ on R extends uniquely to an action on $R[\frac{1}{f}]$ via the standard quotient rule. Hence $R[\frac{1}{f}]$ acquires a natural structure of $\mathcal{D}_R$-module. It is a remarkable fact that $R[\frac{1}{f}]$ has finite length in the category of $\mathcal{D}_R$-modules. This fact has been proven in characteristic 0 by Bernstein [1, Corollary 1.4] in the polynomial case and by Björk [2, Theorems 2.7.12, 3.3.2] in the formal power series case and in characteristic $p > 0$ by Bøgvad [3, Proposition 3.2] in the polynomial case and by Lyubeznik [5, Theorem 5.9] in the formal power series case. Thus the ascending chain of submodules

$$\mathcal{D}_R \cdot \frac{1}{f} \subseteq \mathcal{D}_R \cdot \frac{1}{f^2} \subseteq \cdots \subseteq \mathcal{D}_R \cdot \frac{1}{f^k} \subseteq \cdots \subseteq R[\frac{1}{f}]$$

stabilizes, i.e. $R[\frac{1}{f}]$ is generated by $\frac{1}{f^i}$ for some i. This paper is motivated by the following natural question: *What is the smallest i such that $\frac{1}{f^i}$ generates $R[\frac{1}{f}]$ as a $\mathcal{D}_R$-module?*

2000 *Mathematics Subject Classification.* Primary 13N10, 13B30.

Research of the first author partially supported by a Fulbright grant and the Secretaría de Estado de Educación y Universidades of Spain and the European Social Funding.

The second author greatfully acknowledges NSF support.

When k is a field of characteristic zero and $f \in R$ is a non-zero polynomial it has been proven in [1, Theorem 1'] that there exists of a monic polynomial $b_f(s) \in k[s]$ and a differential operator $Q(s) \in \mathcal{D}_R[s]$ such that

$$Q(s) \cdot f^{s+1} = b_f(s) \cdot f^s$$

for every s. The polynomial $b_f(s)$ is called the Bernstein-Sato polynomial of f and is always a multiple of $(s+1)$. Let $-i$ be the least integer root of $b_f(s)$. Then, $b_f(s) \neq 0$ for any integer $s < -i$ and therefore $f^s \in \mathcal{D}_R \cdot f^{s+1}$. In particular, $R[\frac{1}{f}]$ is generated by $\frac{1}{f^i}$ and, as is shown in [6, Lemma 1.3], it cannot be generated by $\frac{1}{f^j}$ for $j < i$. This gives a complete answer to our question in characteristic zero.

For example, consider the polynomial $f = x_1^2 + \cdots + x_{2n}^2 \in R = k[x_1, \ldots, x_{2n}]$. Then we have the functional equation

$$\frac{1}{4}(\frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_{2n}^2}) \cdot f^{s+1} = (s+1)(s+n) \cdot f^s$$

where the Bernstein-Sato polynomial is $b_f(s) = (s+1)(s+n)$. Hence $R[\frac{1}{f}]$ is generated by $\frac{1}{f^n}$ as a $\mathcal{D}_R$-module but it can not be generated by $\frac{1}{f^i}$ for $i < n$.

But in characteristic $p > 0$ a differential operator of a fixed order annihilates the powers $\frac{1}{f^{p^s}}$ for s large enough, so a functional equation such as above even if it exists does not imply that $\frac{1}{f^{p^{s+1}}} \in \mathcal{D}_R \cdot \frac{1}{f^{p^s}}$ for all s.

The goal of this paper is to prove the following amazing result.

Theorem 1.1. *Let $R = k[x_1, \ldots, x_d]$ where k is a field of characteristic $p > 0$ and let $f \in R$ be a non-zero polynomial. Then $R[\frac{1}{f}]$ is generated by $\frac{1}{f}$ as $\mathcal{D}_R$-module.*

Our proof does not extend to the case of formal power series; some new idea seems to be needed in this case (see Remark 3.6).

Acknowledgement The first author would like to thank the Department of Mathematics at the University of Minnesota for the warm welcome he received during his postdoctoral stay.

2. Differential operators in positive characteristic

Let $\mathbb{N}$ be the set of non-negative integers. Throughout, we will use multi-index notation in the polynomial ring $R = k[x_1, \ldots, x_d]$, where k is a field of characteristic $p > 0$. So, given $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{N}^d$ we will denote the sum of its components by $|\alpha|$ and $\underline{x}^\alpha$ will stand for the monomial $\underline{x}^\alpha = x_1^{\alpha_1} \cdots x_d^{\alpha_d}$.

A pair of multi-indices α and β are ordered as usual: $\alpha < \beta$ if and only if $\alpha_i < \beta_i$ for $i = 1, \dots, d$.

For a general description of the ring of differential operators we refer to [4, §16.8]. For the case we are considering in this work we refer to [4, Théorème 16.11.2]. The ring of differential operators $\mathcal{D}_R = D(R,k)$ associated to the polynomial ring R is the ring extension of R generated by the set of differential operators

$$\{ \ D_{t,i} = \frac{1}{t!}\frac{\partial^t}{\partial x_i^t} \ \mid \ t \in \mathbb{N} \ , \ i = 1, \dots, d \ \}$$

Given $\beta \in \mathbb{N}^d$, D_β will denote the differential operator $D_\beta := D_{\beta_1,1} \cdots D_{\beta_d,d}$. We can extend the multi-index notation to $\mathcal{D}_R$ considering the k-basis formed by the monomials $\underline{x}^\alpha D_\beta$. In the sequel, a differential operator $Q \in \mathcal{D}_R$ will be written in right normal form, i.e.

$$Q = \sum_{\alpha,\beta \in \mathbb{N}^d} a_{\alpha\beta} \, \underline{x}^\alpha \, D_\beta,$$

where all but finitely many $a_{\alpha\beta} \in k$ are zero.

Let $k[R^{p^n}]$ be the k-algebra generated by p^n-th powers of elements of R. Let $\mathcal{D}_R^{(n)}$ be the ring extension of R generated by the set of differential operators up to order p^n, i.e. $\{ \ D_\alpha \mid \alpha < \underline{p}^n \ \}$ where $\underline{p}^n = (p^n, \dots, p^n) \in \mathbb{N}^d$. Then we have an increasing chain of finitely generated ring extensions of R

$$\mathcal{D}_R^{(0)} \subseteq \mathcal{D}_R^{(1)} \subseteq \mathcal{D}_R^{(2)} \subseteq \cdots \subseteq \mathcal{D}_R$$

whose union is $\mathcal{D}_R$.

Lema 2.1. *Let $Q \in \mathcal{D}_R^{(n)}$ and $f \in k[R^{p^n}]$. Then Q commutes with f, i.e. $Q(f \cdot g) = f \cdot Q(g)$ for all $g \in R$.*

Proof. Writing out Q, f and g as sums of monomials and considering that $D_{t,i}$ commutes with $D_{t',j}$ and x_j^s for $j \neq i$, one sees that it is enough to prove the statement for $Q = D_{t,i}$, $f = x_i^{p^n}$ and $g = x_i^s$, where $t < p^n$, s is an integer and $i = 1, \dots, d$. In this case we have

$$D_{t,i}(x_i^{p^n+s}) = x_i^{p^n} \cdot D_{t,i}(x_i^s)$$

just comparing the coefficient at $x_i^{p^n+s-t}$ on both sides modulo p. □

3. Proof of Theorem 1.1

We notice first that it is enough to show that if $f \in R$ is a non-zero polynomial, then $\frac{1}{f^p}$ belongs to the $\mathcal{D}_R$-module generated by $\frac{1}{f}$. Once this is proved we can apply this result to $f^{p^{s-1}}$ to get $\frac{1}{f^{p^s}} \in \mathcal{D}_R \cdot \frac{1}{f^{p^{s-1}}}$ for every $s > 1$. Since the set $\frac{1}{f}, \frac{1}{f^p}, \frac{1}{f^{p^2}}, \dots$ generates $R[\frac{1}{f}]$ as R-module, we are done.

We can also reduce to the case of k being a perfect field. If k is not perfect, let K be the perfect closure of k. Assume there is a differential operator $Q = \sum a_{\alpha\beta} \underline{x}^{\alpha} D_{\beta}$ with coefficients $a_{\alpha\beta} \in K$ such that $Q(\frac{1}{f}) = \frac{1}{f^p}$. This is equivalent to the fact that a system of finitely many linear equations with coefficients in k has solutions in K, where the non-zero coefficients $a_{\alpha\beta}$ of Q are thought of as the unknowns of the system. For example, if $f = x_1$, we may be looking for a solution in the form $Q = aD_{p-1,1}$, so we get an equation $Q(\frac{1}{x}) = \frac{1}{x^p}$. Since $Q(\frac{1}{x}) = a\frac{1}{x^p}$, the corresponding linear system is just one equation $a = 1$. The system has a solution in K, namely, the coefficients of Q. Hence it is consistent, so it must have a solution in k because the coefficients of the linear system are in k (in fact the coefficients are in the prime field $\mathbb{Z}/p\mathbb{Z}$). So there is a differential operator Q' with coefficients in k such that $Q'(\frac{1}{f}) = \frac{1}{f^p}$.

Henceforth we will assume that the base field k of our polynomial ring is perfect. It is enough to show that under this assumption $\frac{1}{f^p}$ belongs to the $\mathcal{D}_R$-submodule generated by $\frac{1}{f}$, for all $f \in R$.

Given a polynomial $f \in R$ and an integer $n \geq 1$, we can write in a unique way

$$f(\underline{x}) = \sum_{0 \leq \alpha < \underline{p}^n} f_{\alpha}(\underline{x}^{\underline{p}^n}) \ \underline{x}^{\alpha}$$

where $f_{\alpha}(\underline{z}) \in k[\underline{z}]$ are polynomials in d variables. Consider the ideal $J_n(f)$ generated by the polynomials $f_{\alpha}(\underline{x}^{\underline{p}^n})$ in the decomposition of f with respect to $\underline{x}^{\underline{p}^n}$.

Lema 3.1. *Let $f, g, h \in R$ be polynomials such that $f = g \cdot h$. Then $J_n(f) \subseteq J_n(g)$.*

Proof. Consider the decomposition of g with respect to $\underline{x}^{\underline{p}^n}$

$$g(\underline{x}) = \sum_{0 \leq \alpha < \underline{p}^n} g_{\alpha}(\underline{x}^{\underline{p}^n}) \ \underline{x}^{\alpha}$$

Set $h(\underline{x}) = \sum a_{\beta} \ \underline{x}^{\beta}$, then

$$f(\underline{x}) = g(\underline{x}) \cdot h(\underline{x}) = \sum_{0 \leq \alpha < \underline{p}^n} g_{\alpha}(\underline{x}^{\underline{p}^n}) \ (\sum a_{\beta} \ \underline{x}^{\alpha+\beta})$$

Rewriting in the form

$$f(\underline{x}) = \sum_{0 \leq \gamma < \underline{p}^n} f_\gamma(\underline{x}^{\underline{p}^n})\ \underline{x}^\gamma$$

we get

$$f_\gamma(\underline{x}^{\underline{p}^n}) = \sum a_\beta\ \ g_\alpha(\underline{x}^{\underline{p}^n})\ \ \underline{x}^{j\underline{p}^n}$$

where the sum is taken over the multi-indices α and β such that $\underline{x}^{\alpha+\beta} = \underline{x}^{j\underline{p}^n}\underline{x}^\gamma$ for a given $j \in \mathbb{N}$. In particular $f_\gamma(\underline{x}^{\underline{p}^n}) \in J_n(g)$. $\square$

Lema 3.2. *Let $f, g \in R$ be polynomials such that $f = g^p$. Then $J_n(f) = J_{n-1}(g)^{[p]}$*

Proof. It is enough to raise to the $p-$th power the decomposition of g with respect to $\underline{x}^{\underline{p}^{n-1}}$. $\square$

Notice that $\mathcal{D}_R^{(n)} \cdot f$ is an ideal of R. This ideal can be also described as follows:

Lema 3.3. $J_n(f) = \mathcal{D}_R^{(n)} \cdot f$.

Proof. By Lemma 2.1 every $Q \in \mathcal{D}_R^{(n)}$ commutes with every $f_\alpha(\underline{x}^{\underline{p}^n})$ in the decomposition of f with respect to $\underline{x}^{\underline{p}^n}$. Hence

$$Q(f) = \sum_{0 \leq \alpha < \underline{p}^n} f_\alpha(\underline{x}^{\underline{p}^n})\ \ Q(\underline{x}^\alpha)$$

In particular, $Q(f) \in J_n(f)$, i.e. $\mathcal{D}_R^{(n)} \cdot f \subseteq J_n(f)$. To prove the opposite containment it is enough to show that every $f_\alpha(\underline{x}^{\underline{p}^n})$ belongs to the ideal $\mathcal{D}_R^{(n)} \cdot f$.

Consider the multi-index $\beta = (p^n - 1, \ldots, p^n - 1) \in \mathbb{N}^d$. Then we have

$$D_\beta(f) = f_\beta(\underline{x}^{\underline{p}^n}) \in \mathcal{D}_R^{(n)} \cdot f$$

Now we proceed by induction on $\sigma_\beta = \Sigma_{i=1}^d (p^n - 1 - \beta_i)$, the case $\sigma_\beta = 0$ being just proved. Let $\beta \in \mathbb{N}^d$ be a multi-index such that $D_\beta \in \mathcal{D}_R^{(n)}$. Then we have

$$D_\beta(f) = f_\beta(\underline{x}^{\underline{p}^n}) + \sum_{\beta' > \beta} f_{\beta'}(\underline{x}^{\underline{p}^n})\ (a_{\beta'\beta}\ \underline{x}^{\beta' - \beta})$$

where $a_{\beta'\beta} = \begin{pmatrix} \beta_1' \\ \beta_1 \end{pmatrix} \cdots \begin{pmatrix} \beta_d' \\ \beta_d \end{pmatrix}$. By induction $f_{\beta'}(\underline{x}^{\underline{p}^n}) \in \mathcal{D}_R^{(n)} \cdot f$ for any $\beta' > \beta$, so we are done. $\square$

Since k is a perfect field, the coefficients of $f_\alpha(\underline{x}^{\underline{p}^n})$ in the decomposition of f with respect to $\underline{x}^{\underline{p}^n}$ are p^n-th powers, hence $f_\alpha(\underline{x}^{\underline{p}^n}) = (\widetilde{f}_\alpha(\underline{x}))^{p^n}$, where $\widetilde{f}_\alpha(\underline{x})$ are polynomials in R. Consider the ideal $I_n(f)$ generated by the polynomials $\widetilde{f}_\alpha(\underline{x})$. Notice that $J_n(f)$ is the n-th Frobenius powers of the ideal $I_n(f)$, i.e. $J_n(f) = I_n(f)^{[p^n]}$.

Lema 3.4. *Let $f \in R$ be a polynomial. For any integer $n \geq 1$ there is an inclusion of ideals*

$$I_n(f^{p^n-1}) \subseteq I_{n-1}(f^{p^{n-1}-1})$$

Proof. The equality $J_n(f^{p^n-p}) = J_{n-1}(f^{p^{n-1}-1})^{[p]}$ given by Lemma 3.2 translates to

$$I_n(f^{p^n-p})^{[p^n]} = (I_{n-1}(f^{p^{n-1}-1})^{[p^{n-1}]})^{[p]} = I_{n-1}(f^{p^{n-1}-1})^{[p^n]}$$

This implies

$$I_n(f^{p^n-p}) = I_{n-1}(f^{p^{n-1}-1})$$

due to the fact that the polynomial ring R is regular. On the other hand, the inclusion $J_n(f^{p^n-1}) = J_n(f^{p^n-p} \cdot f^{p-1}) \subseteq J_n(f^{p^n-p})$ given by Lemma 3.1 implies

$$I_n(f^{p^n-1}) \subseteq I_n(f^{p^n-p})$$

again because R is regular so we get the desired inclusion. $\square$

Lema 3.5. *The descending chain of ideals*

$$I_1(f^{p-1}) \supseteq I_2(f^{p^2-1}) \supseteq \cdots \supseteq I_{n-1}(f^{p^{n-1}-1}) \supseteq I_n(f^{p^n-1}) \supseteq \cdots$$

stabilizes.

Proof. Assume that $\deg f = e$. Let

$$f^{p^n-1}(\underline{x}) = \sum_{0 \leq \alpha < \underline{p}^n} f_\alpha(\underline{x}^{\underline{p}^n}) \ \underline{x}^\alpha$$

be the decomposition of f^{p^n-1} with respect to $\underline{x}^{\underline{p}^n}$. Since $\deg f^{p^n-1} = e(p^n-1)$, the polynomials in the decomposition satisfy $\deg f_\alpha(\underline{x}^{\underline{p}^n}) \leq e(p^n-1) < ep^n$. On the other hand, $\deg f_\alpha(\underline{x}^{\underline{p}^n}) = p^n \deg \widetilde{f}_\alpha(\underline{x})$ implies $\deg \widetilde{f}_\alpha(\underline{x}) < e$.

Let W_e be the k-vector space of polynomials of degree strictly smaller than e. For every n, the ideal $I_n(f^{p^n-1})$ is generated by $I_n(f^{p^n-1}) \cap W_e$. Thus we have a descending sequence of k-vector subspaces of W_e

$$(I_1(f^{p-1}) \cap W_e) \supseteq (I_2(f^{p^2-1}) \cap W_e) \supseteq \cdots \supseteq (I_n(f^{p^n-1}) \cap W_e) \supseteq \cdots$$

that must stabilize because W_e is a finite-dimensional k-vector space. $\square$

Now we can complete the proof of Theorem 1.1 as follows. Assume that the chain of ideals given in Lemma 3.5 stabilize at the level $s-1$, i.e. $I := I_{s-1}(f^{p^{s-1}-1}) = I_s(f^{p^s-1})$. From the equalities $J_s(f^{p^s-1}) = I^{[p^s]}$ and $J_{s-1}(f^{p^{s-1}-1}) = I^{[p^{s-1}]}$ we deduce

$$J_s(f^{p^s-p}) = J_{s-1}(f^{p^{s-1}-1})^{[p]} = (I^{[p^{s-1}]})^{[p]} = I^{[p^s]} = J_s(f^{p^s-1})$$

Thus we have $f^{p^s-p} \in J_s(f^{p^s-1})$. By Lemma 3.3 there is a differential operator $Q \in \mathcal{D}_R^{(s)}$ such that $Q(f^{p^s-1}) = f^{p^s-p}$. Since Q commutes with f^{p^s}, we see that

$$Q(\frac{f^{p^s-1}}{f^{p^s}}) = \frac{f^{p^s-p}}{f^{p^s}}$$

so we get $Q(\frac{1}{f}) = \frac{1}{f^p}$ as we desired. □

Remark 3.6. In the case of formal power series all parts of our proof go through except the proof of Lemma 3.5. Most likely, the statement of Lemma 3.5 is still true in the case of formal power series but a very different proof is needed.

Example 3.7. Let $R = k[x_1, x_2, x_3, x_4]$ where k is a field of characteristic $p > 0$. Consider the polynomial $f = x_1^2 + x_2^2 + x_3^2 + x_4^2$. We are going to find a differential operator $Q \in \mathcal{D}_R$ such that $Q(\frac{1}{f}) = \frac{1}{f^p}$ just checking out the monomials in f^{p-1}. Let $S(f, p, n)$ be the set of terms $a_\alpha \underline{x}^\alpha$ in f^{p-1} such that $\alpha < \underline{p}^n$.

The set $S(f, p, 1)$ is non-empty. Namely we have:

- If 4 divides $p-1$, then $a_\alpha \underline{x}^\alpha \in S(f, p, 1)$ where

  $\alpha = (\frac{p-1}{2}, \frac{p-1}{2}, \frac{p-1}{2}, \frac{p-1}{2})$

  $a_\alpha = \frac{(p-1)!}{(\frac{p-1}{4}!)^4}$

- If 4 does not divide $p-1$, then $a_\alpha \underline{x}^\alpha \in S(f, p, 1)$ where

  $\alpha = (\frac{p+1}{2}, \frac{p+1}{2}, \frac{p-3}{2}, \frac{p-3}{2})$

  $a_\alpha = \frac{(p-1)!}{(\frac{p+1}{4}!)^2(\frac{p-3}{4}!)^2}$

Let $a_\alpha \underline{x}^\alpha$ be a leading term of $S(f, p, 1)$ with respect to the usual order. Notice that $\frac{1}{a_\alpha} D_\alpha(f^{p-1}) = 1$. The differential operator $Q = \frac{1}{a_\alpha} D_\alpha$ commutes with f^p by Lemma 2.1 so we get the desired result.

References

[1] I. N. Bernšteĭn, Analytic continuation of generalized functions with respect to a parameter, Funkcional. Anal. i Priložen., 6 (4) (1972) 26–40.

[2] J. E. Björk, Rings of differential operators, North Holland Mathematics Library, Amsterdam, 1979.
[3] R. Bøgvad, Some results on D-modules on Borel varieties in characteristic $p > 0$, J. Algebra, 173 (3) (1995) 638–667.
[4] A. Grothendieck and J. Dieudonné, Éléments de géométrie algébrique IV. Étude locale des schémas et des morphismes de schémas, Publications Mathématiques I.H.E.S. 32 (1967).
[5] G. Lyubeznik, F-modules: applications to local cohomology and D-modules in characteristic $p > 0$, J. Reine Angew. Math. 491 (1997), 65–130.
[6] U. Walther, Bernstein-Sato polynomials versus cohomology of the Milnor fiber for generic hyperplane arrangements, to appear in Compositio Math.

Departament de Matemàtica Aplicada I, Universitat Politècnica de Catalunya, Avinguda Diagonal 647, Barcelona 08028, SPAIN

E-mail address: Josep.Alvarez@upc.es

Department of Mathematics, University of Minnesota, 206 Church St. S.E., Minneapolis, MN 55455, USA

E-mail address: gennady@math.umn.edu