ON THE RING OF UNIPOTENT VECTOR BUNDLES ON ELLIPTIC CURVES IN POSITIVE CHARACTERISTICS

STEFAN SCHRÖER

Revised version, 8 February 2010

ABSTRACT. Using Fourier–Mukai transforms, we prove some results about the ring of unipotent vector bundles on elliptic curves in positive characteristics. This ring was determined by Atiyah in characteristic zero, who showed that it is a polynomial ring in one variable. It turns out that the situation in characteristic $p > 0$ is completely different and rather bizarre: the ring is nonnoetherian and contains a subring whose spectrum contains infinitely many copies of $\mathrm{Spec}(\mathbb{Z})$, which are glued with successively higher and higher infinitesimal identification at the point corresponding to the prime p.

CONTENTS

INTRODUCTION

Using sheaf theoretic methods, Atiyah [2] described the category of locally free sheaves on elliptic curves. In particular, he determined all *irreducible* locally free sheaves. Later, Oda [19] gave another approach based on isogenies. More recently, Polishchuk [20] as well as Hein and Ploog [10] used to this end Fourier–Mukai transforms, which were introduced by Mukai [16].

Given two irreducible sheaves $\mathcal{F}, \mathcal{F}'$ on an elliptic curve E, their tensor product is usually no longer irreducible, and one has a decomposition $\mathcal{F} \otimes \mathcal{F}' = \bigoplus_i \mathcal{F}_i^{\oplus \lambda_i}$ into irreducible summands. To understand this decomposition, it essentially suffices to consider sheaves $\mathcal{F}$ having a filtration $0 = \mathcal{F}_0 \subset \ldots \subset \mathcal{F}_n = \mathcal{F}$ with $\mathcal{F}_i/\mathcal{F}_{i-1} = \mathcal{O}_E$. Such sheaves are called *unipotent*. The classification of unipotent sheaves neither depends on the elliptic curve nor the ground field: For each integer $n \geq 1$, there is, up to isomorphism, precisely one irreducible unipotent sheaf $\mathcal{F}_n$ of rank n. For

2000 *Mathematics Subject Classification.* 14H60, 14L05.

example, the extensions of $\mathcal{O}_E$ by itself coming from the nontrivial classes in the 1-dimensional $H^1(E, \mathcal{O}_E) = \mathrm{Ext}^1(\mathcal{O}_E, \mathcal{O}_E)$ yield $\mathcal{F}_2$.

The decomposition of tensor products of unipotent sheaves, however, does depend on the characteristic. For characteristic zero, Atiyah was able to determine the ring structure on the free abelian group R generated by the isomorphism classes of indecomposable unipotent sheaves: It turns out that it is nothing but the polynomial ring $\mathbb{Z}[\mathcal{F}_2]$.

The goal of this paper is to analyze the ring R in positive characteristics. The idea is to use *Fourier–Mukai transforms*, which induce an equivalence between the category of unipotent sheaves and the category of sheaves supported by the origin $0 \in E$, according to a result of Mukai [15]. Under this equivalence, tensor products of unipotent sheaves corresponds to *convolution products* of sheaves supported by the origin, which is defined in terms of the formal group attached to the elliptic curve. The latter has not much to do with geometry, and is basically a matter of linear or commutative algebra. We shall see that this links our original problem to the behavior of Jordan normal forms under tensor products, and to the modular representation ring of the additive group of the p-adic integers.

Our main results in characteristic $p > 0$ are the following: First, we show that the ring structure of R depends only on p, and not on the elliptic curve. In particular, there is no difference between ordinary and supersingular elliptic curves. Second, we show that $\mathbb{Z} \subset R$ is an integral extension, and that $\mathrm{Spec}(R)$ contains infinitely many irreducible components, such that R is nonnoetherian. Third, we describe the subring $R_\infty \subset R$ generated by the irreducible unipotent sheaves of prime power rank explicitly. Its spectrum is an inverse limit of copies of $\mathrm{Spec}(\mathbb{Z})$, which are glued together at the points corresponding to the prime p with respect to successively higher and higher infinitesimal identifications. The rings R_∞ admits a dense embedding into the ring or Witt vectors $W(\mathbb{Z})$. The localization $R_\infty \otimes \mathbb{Q}$ is the 0-dimensional ring of almost constant sequences in $(a_0, a_1, \ldots)$ of rational numbers, and its spectrum is the Alexandroff compactification of a countable discrete space.

The paper is organized as follows: Section 1 contains basic facts on the Krull–Schmidt Theorem and Fourier–Mukai transforms. In Section 2, we introduce the convolution ring R attached to formal groups, and relate them to tensor products of unipotent sheaves and the modular representation ring of the group of p-adic integers. The basic properties of the multiplication table are gathered in Section 3. I have included proofs in order to make the paper self-contained, although the results are probably not new. In Section 4 we show that $\mathbb{Z} \subset R$ is an integral ring extension. The core of the paper is contained in Section 5: Here we apply a variant of Lucas' Theorem on congruences of binomial coefficients to study the subring $R_\infty \subset R$ generated by elements with p-power rank and give a detailed description of its spectrum. In Section 6 we interpret these results in terms of Stone spaces, that is, compact totally discrete spaces.

Acknowledgement. I wish to thank Tobias Barthel, James Borger, Adrian Langer and the referee for inspiring comments.

1. Krull–Schmidt and Fourier–Mukai

We start by recalling elementary facts about the Krull–Schmidt Theorem. Let $\mathcal{C}$ be an abelian category. An object V is called *indecomposable* if $V \neq 0$, and in every decomposition $V = V_1 \oplus V_2$ we have either $V_1 = 0$ or $V_2 = 0$. If every object admits a decomposition $V = V_1 \oplus \ldots \oplus V_n$ into indecomposable objects and this decomposition is unique up to isomorphism and ordering of the summands, one says that the *Krull–Schmidt Theorem holds* for the category $\mathcal{C}$.

According to Atiyah's result [1], this is the case if each Hom set is endowed with the structure of a finite-dimensional k-vector space so that the composition maps are bilinear. A prominent example is the category of coherent sheaves with proper support on a scheme or algebraic stack of finite type over k, or on a complex analytic space.

For lack of better notation, we define the K-group $K(\mathcal{C})$ as the free abelian group generated by the isomorphism classes $[V]$ of objects in $\mathcal{C}$, modulo the relations $[V] = [V'] + [V'']$ coming from direct sum decompositions $V \simeq V' \oplus V''$. Note that we use only relations coming from split short exact sequences, rather than arbitrary short exact sequences. If the Krull–Schmidt Theorem holds, then $K(\mathcal{C})$ is the free abelian group generated by the isomorphism classes of indecomposable objects. Often the category $\mathcal{C}$ is endowed with tensor products, which induce a ring structure on the abelian group $K(\mathcal{C})$. Given two indecomposable objects V', V'', it is often a challenging problem to decompose $V' \otimes V''$ into indecomposable objects.

Let us now turn to abelian varieties. Fix a ground field k of characteristic $p \geq 0$, let A be an abelian variety, and consider the abelian category $\mathrm{Coh}(A)$ of coherent sheaves on A. Inside, we have the subcategory $\mathrm{Coh}_0(A)$ of all coherent sheaves supported by the origin $0 \in A$, and the subcategory $\mathrm{Coh}_u(A)$ of all unipotent sheaves. Here a coherent sheaf $\mathcal{F}$ is called *unipotent* if there is a filtration $0 = \mathcal{F}_0 \subset \mathcal{F}_1 \subset \ldots \subset \mathcal{F}_n = \mathcal{F}$ with subquotients $\mathcal{F}_i/\mathcal{F}_{i-1} \simeq \mathcal{O}_A$. Note that unipotent sheaves are locally free, and that tensor products of unipotent sheaves are unipotent.

A surprising result of Mukai tells us that there is a canonical equivalence of abelian categories $\mathrm{Coh}_0(A) \simeq \mathrm{Coh}_u(\hat{A})$, where $\hat{A} = \mathrm{Pic}^0_A$ is the dual abelian variety. Here it is most elegant to work with the triangulated category $D^b_{\mathrm{coh}}(A)$ of bounded complexes of coherent sheaves on A. Let $\mathcal{P}$ be the Poincaré bundle on $A \times \hat{A}$. The *Fourier–Mukai transform* is defined as

$$\Phi_{\mathcal{P}} : D^b_{\mathrm{coh}}(A) \longrightarrow D^b_{\mathrm{coh}}(\hat{A}), \quad \mathcal{F}^\bullet \longmapsto R\,\mathrm{pr}_{2*}(\mathcal{P} \otimes \mathrm{pr}_1^*(\mathcal{F}^\bullet)),$$

where pr_i denote the projections from $A \times \hat{A}$. According to Mukai's fundamental result ([16], Theorem 2.2), this functor is an equivalence of triangulated categories. Up to shift by $g = \dim(A)$, it induces an equivalence of abelian categories

$$\mathrm{Coh}_u(A) \longrightarrow \mathrm{Coh}_0(\hat{A}), \quad \mathcal{F} \longmapsto \Phi_{\mathcal{P}}(\mathcal{F})[g] = R^g\,\mathrm{pr}_{2*}(\mathcal{P} \otimes \mathrm{pr}_1^*(\mathcal{F})),$$

as discussed in loc. cit. Example 2.9. Note that Mukai observed this equivalence already in [15], Theorem 4.12. Moreover, he showed that the tensor product corresponds under the Fourier–Mukai transform to the convolution product, which we shall discuss in the next section. For a comprehensive account of Fourier–Mukai transforms, we refer to Huybrechts' monograph [11].

The upshot is that to understand the decomposition of tensor products of unipotent sheaves into irreducible ones, it suffices to understand the corresponding decomposition of convolution products for sheaves supported by the origin. The latter is "merely" linear algebra, and in some aspects a much simpler task.

Remark 1.1. As Adrian Langer pointed out to me, there is a more general approach to describe unipotent sheaves via the Tannakian formalism, which works over arbitrary proper schemes X with $k = H^0(X, \mathcal{O}_X)$. As Nori observed in [17], Chapter IV, Section 1, the unipotent sheaves $\mathcal{F}$ comprise a Tannaka category $\mathcal{U}(X)$, and the choice of a rational point $x_0 \in X$ defines a fiber functor to the category of finite-dimensional k-vector spaces. In turn, the automorphism algebra of the fiber functor, which receives from the tensor product in the Tannaka category the structure of a Hopf algebra, defines an inverse system of finite group schemes G_α, an the Tannaka category $\mathcal{U}(X)$ becomes isomorphic to the Tannaka category of representations of the inverse system G_α on finite-dimensional k-vector spaces.

Remark 1.2. Burban and Kreussler showed that an equivalence between the category of unipotent bundles and the category of torsion sheaves supported by the origin also holds for nodal Weierstraß cubics (see [5], Theorem 2.21). It seems possible to extend the setting of the present paper into this direction.

2. Formal groups and convolution rings

Fix a ground field k of characteristic $p \geq 0$, and let $\mathfrak{X} = \operatorname{Spf}(k[[t]])$ be the formal affine line. Consider the category $\operatorname{Coh}_0(\mathfrak{X})$ of all coherent $\mathcal{O}_{\mathfrak{X}}$-modules $\mathcal{F}$ supported by the origin $0 \in \mathfrak{X}$. Then $V = \Gamma(\mathfrak{X}, \mathcal{F})$ is a finite dimensional vector space endowed with a nilpotent endomorphism $\varphi : V \to V$ induced by the action of the indeterminate $t \in k[[t]]$. In fact, the functor

$$\mathcal{F} \longmapsto (V, \varphi)$$

is an equivalence between $\operatorname{Coh}_0(\mathfrak{X})$ and the category of finite-dimensional vector spaces endowed with a nilpotent endomorphism. Using the Jordan normal form, we conclude that each indecomposable object is isomorphic to precisely one $\mathcal{F}_n$, $n \geq 1$. This $\mathcal{F}_n$ corresponds to the n-dimensional vector space $V = k[[t]]/(t^n)$ with the shift operator $\varphi(t^i) = t^{i+1}$, or equivalently to the standard vector space $V = k^n$ with Jordan matrix

$$J_n = \begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix} \in \operatorname{Mat}(n, k).$$

Let $f_n = [\mathcal{F}_n]$ be its isomorphism class, such that $K(\operatorname{Coh}_0(\mathfrak{X}))$ is the free abelian group generated by the f_n, $n \geq 1$. How to decompose a given $\mathcal{F} \in \operatorname{Coh}_0(\mathfrak{X})$? It turns out that the Hilbert function

$$l_{\mathcal{F}}(i) = \dim H^0(\mathfrak{X}, \mathcal{F}/\mathfrak{m}^i\mathcal{F}), \quad \mathfrak{m} = tk[[t]]$$

does the job:

Lemma 2.1. *Write $[\mathcal{F}] = \sum \lambda_i f_i$. Then we have $\lambda_i = 2l_{\mathcal{F}}(i) - l_{\mathcal{F}}(i+1) - l_{\mathcal{F}}(i-1)$.*

Proof. By additivity, it suffices to treat the case $\mathcal{F} = \mathcal{F}_n$. Set $l(i) = l_{\mathcal{F}_n}(i)$. We compute

$$l(i) = \dim k[[t]]/(t^n, t^i) = \begin{cases} i & \text{if } i \leq n; \\ n & \text{else.} \end{cases}$$

Whence the first discrete derivative $l'(i) = l(i+1) - l(i)$ takes values

$$l'(i) = \begin{cases} 1 & \text{if } i \leq n-1; \\ 0 & \text{else.} \end{cases}$$

In turn, the second discrete derivative $l''(i) = l(i+2) - 2l(i+1) + l(i)$ is zero, except for $l''(n-1) = -1$. The assertion follows. □

Now choose a *formal group law* $F(x,y) \in k[[x,y]]$, and regard $\mathfrak{X}$ as a *formal group.* Let $\mu : \mathfrak{X} \times \mathfrak{X} \to \mathfrak{X}$ be the resulting multiplication morphism, which is given by $k[[t]] \to k[[x,y]]$, $t \mapsto F$, and consider the *convolution product*

$$\mathcal{F} \star \mathcal{F}' = \mu_*(\mathcal{F} \otimes_k \mathcal{F}')$$

for objects $\mathcal{F} \in \mathrm{Coh}_0(\mathfrak{X})$. In terms of vector spaces with nilpotent endomorphisms, the convolution product is given by $V \otimes V'$, with the induced nilpotent endomorphism $F(\varphi \otimes \mathrm{id}_{V'}, \mathrm{id}_V \otimes \varphi')$, which by abuse of notation we simply denote by $F(\varphi, \varphi')$. It is easy to see that the convolution product endows the free abelian group $K(\mathrm{Coh}_0(\mathfrak{X}))$ with a ring structure.

Recall that by Lazard's results [12], the isomorphism classes of 1-dimensional formal groups over algebraically closed ground fields of characteristic $p > 0$ correspond to a single numerical invariant, the *height* $h \in \{\infty, 1, 2, \ldots\}$. The formal additive group $\hat{\mathbb{G}}_a$, say with $F(x,y) = x + y$, has height $h = \infty$, whereas the formal multiplicative group $\hat{\mathbb{G}}_m$, say with $F(x,y) = x + y + xy$, has height $h = 1$. All other cases cannot be expressed in terms of polynomials, and to my knowledge there is no *explicit* formula known for the formal group laws with $1 < h < \infty$. Somewhat surprising, the formal group law plays almost no role for the multiplication table in our ring $K(\mathrm{Coh}_0(\mathfrak{X}))$:

Proposition 2.2. *The multiplicative structure of the ring* $K(\mathrm{Coh}_0(\mathfrak{X}))$ *depends only on the characteristic* $p \geq 0$ *of our ground field* k.

Proof. Set $\mathcal{F} = \mathcal{F}_m \star \mathcal{F}_n$. In light of Lemma 2.1, it suffices to check that the Hilbert function $l_{\mathcal{F}}(i) = \dim k[[x,y]]/(x^m, y^n, F^i)$ depends only on $p \geq 0$ rather then of F. By definition, a formal group law $F(x,y)$ satisfies $F(x,0) = x$ and $F(0,y) = y$, whence is of the form $F(x,y) = x + y + xyv = ux + y$ for some $u, v \in k[[x,y]]$ with u invertible. Setting $x' = ux$, we have

$$k[[x,y]]/(x^m, y^n, F^i) = k[[x',y]]/(x'^m, y^n, (x'+y)^i).$$

The latter is clearly independent of the formal group law F, and in fact gives the Hilbert function with respect to the formal additive group $\hat{\mathbb{G}}_a$. Note that the dependence on the characteristic $p \geq 0$ enters via the binomial expansion of $(x'+y)^i$ over k, as we shall see in the next section. □

We call the ring $R = K(\mathrm{Coh}_0(\mathfrak{X}))$ the *convolution ring* in characteristic $p \geq 0$. Note that the underlying abelian group is free, with basis f_i, $i \geq 1$, and that the multiplication table $f_m f_n = \sum \lambda_i f_i$ depends only on the characteristic $p \geq 0$. The unit element is $f_1 = 1$. For some formulas, it is convenient to define $f_0 = 0$. Clearly, the ring does not change under base field extensions $k \subset k'$. The convolution ring is essentially the ring of unipotent locally free sheaves on elliptic curves with respect to tensor products:

Proposition 2.3. *The ring* $K(\mathrm{Coh}_u(E))$ *of unipotent locally free sheaves on an elliptic curve* E *in characteristic* $p \geq 0$ *is isomorphic to the convolution ring* R *in characteristic* p.

Proof. Let $\mathfrak{X}$ be the formal group attached to the elliptic curve $\hat{E} = E$. Clearly, we have $\mathrm{Coh}_0(\mathfrak{X}) = \mathrm{Coh}_0(\hat{E})$. According to [15], Theorem 4.12, the Fourier–Mukai transform

$$\mathrm{Coh}_u(E) \longrightarrow \mathrm{Coh}_0(\hat{E}), \quad \mathcal{F} \longmapsto \Phi_{\mathcal{P}}(\mathcal{F})[g] = R^g \operatorname{pr}_{2*}(\mathcal{P} \otimes \operatorname{pr}_1^*(\mathcal{F}))$$

is an equivalence of categories, and transforms tensor products into convolution products. The assertion follows. □

In particular, it plays no role whether the elliptic curve E is ordinary or supersingular. This property, however, seems to enter if one considers the action of Frobenius.

The multiplicities in $f_m f_n = \sum \lambda_i f_i$ are related to a difficult problem in linear algebra:

Proposition 2.4. *The multiplicities λ_i are the number of Jordan blocks J_i in the Jordan normal form of the endomorphism $J_m \otimes \mathrm{id} + \mathrm{id} \otimes J_n$ of $k^m \otimes k^n$.*

Proof. We may choose the additive formal group law $F(x, y) = x + y$, and the assertion follows from the definition of convolution products. □

This problem was studied in characteristic zero, for example, by Roth [22] and Trampus [24]; for more recent developments in positive characteristics, see McFall [14] and Norman [18].

There is also an interesting connection to representation theory: Let $p > 0$, and consider the additive profinite group $G = \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^m\mathbb{Z}$ of p-adic integers. Let $\mathcal{R}$ be the category of continuous representations of G on finite-dimensional $\mathbb{F}_p$-vector spaces. Such a representation $G \to \mathrm{GL}(n, \mathbb{F}_p)$ factors over a finite quotient $\mathbb{Z}/p^m\mathbb{Z}$, and the image of the generator $1 \in \mathbb{Z}/p^m\mathbb{Z}$ is a matrix $A \in \mathrm{GL}(n, \mathbb{F}_p)$ whose minimal polynomial divides $T^{p^m} - 1 = (T-1)^{p^m}$. Whence the matrix $A - E_n$ is nilpotent, where $E_n \in \mathrm{Mat}(n, \mathbb{F}_p)$ denotes the unit matrix. The upshot is that $K(\mathcal{R})$ is the free abelian group generated by classes f_i', $i \geq 1$ corresponding to the unipotent Jordan matrices $J_i + E_i$. In turn, we obtain a bijection of abelian groups

$$R \longrightarrow K(\mathcal{R}), \quad f_i \longmapsto f_i'.$$

The tensor product endows $K(\mathcal{R})$ with a ring structure; we call it the *ring of continuous modular representations.*

Proposition 2.5. *The preceding bijection respects multiplication, and yields an identification of the convolution ring R in characteristic p with the ring $K(\mathcal{R})$.*

Proof. Here we use the multiplicative formal group law $F(x, y) = x + y + xy = (x+1)(y+1) - 1$, together with the fact that tensor products of unipotent matrices are unipotent. Clearly, the number of unipotent Jordan blocks $J_i + E_i$ in the Jordan normal form of the unipotent endomorphism $(J_m + E_m) \otimes (J_n + E_n)$ is the same as the number of nilpotent Jordan blocks J_i in the corresponding nilpotent endomorphism $F(J_m, J_n) = (J_m + E_m) \otimes (J_n + E_n) - E_{mn}$. □

This ring of continuous modular representations was studied, for example, by Srinivasan [23], Green [8], and Ralley [21].

3. The multiplication table

We keep the notation from the preceding section, and start to investigate the multiplication table of the convolution ring R in characteristic $p \geq 0$, whose underlying abelian group is defined in terms of the formal affine line $\mathfrak{X} = \mathrm{Spf}(k[[t]])$. Its multiplication is defined with the help of a formal group law $F(x, y)$, but depends only on the characteristic $p \geq 0$. We therefore assume from now on that the formal group law is simply $F(x, y) = x + y$.

Recall that R is the free abelian group on the generators f_n, $n \geq 1$. These classes are given by the coherent sheaves $\mathcal{F}_n$, which in turn correspond to the vector spaces $k[[t]]/(t^n)$ endowed with the shift operator, or equivalently the vector space k^n endowed with the Jordan matrix J_n. We start with two obvious facts:

Proposition 3.1. *Let $m, n \geq 0$ be integers, and write $f_m f_n = \sum \lambda_i f_i$. Then $\sum i\lambda_i = mn$*

Proof. Set $V = k[[t]]/(t^m)$ and $V' = k[[t]]/(t^n)$. Clearly $\sum i\lambda_i$ must be the dimension of $V \otimes V'$, which indeed is mn. □

Proposition 3.2. *Let $0 \leq m \leq n$ be integers, and write $f_m f_n = \sum \lambda_i f_i$. Then we have $\sum \lambda_i = m$.*

Proof. The integer $\sum \lambda_i$ is the number of Jordan blocks in the Jordan normal form of $F(J_m, J_n)$. Equivalently, it is the dimension of $\mathcal{F}/t\mathcal{F}$, where $\mathcal{F} = \mathcal{F}_m \star \mathcal{F}_n$. The latter equals the dimension of

$$k[[x, y]]/(x^m, y^n, F) = k[[x, y]]/(x^m, y^n, x + y)$$

which clearly equals m. □

The next observation permits us to translate certain problems from linear algebra into commutative algebra:

Proposition 3.3. *Let $m, n \geq 1$ be integers, and write $f_m f_n = \sum \lambda_i f_i$. Then the largest integer $r \geq 1$ with $\lambda_r \neq 0$ coincides with the smallest integer $s \geq 1$ with the property $(x + y)^s \equiv 0$ modulo (x^m, y^n).*

Proof. The largest integer $r \geq 1$ with $\lambda_r \neq 0$ is nothing but the size of the largest Jordan block in the Jordan normal form of the nilpotent endomorphism $F(J_m, J_n)$ of $k^m \otimes k^n$. In turn, this is the smallest integer $s \geq 1$ with $F(J_m, J_n)^s = 0$. The linear map $k[[x, y]]/(x^m, y^n) \to \mathrm{End}(k^m \otimes k^n)$ given by $x \mapsto J_m \otimes \mathrm{id}$ and $y \mapsto \mathrm{id} \otimes J_m$ is injective, which can be seen by identifying the vector space $k^m \otimes k^n$ with the k-algebra $k[[x, y]]/(x^m, y^n)$. Consequently, our $s \geq 1$ is also the smallest integer with $F(x, y)^s \in (x^m, y^n)$. □

With this at hand we deduce several useful facts:

Proposition 3.4. *Let $m, n \geq 0$ be integers, and write $f_m f_n = \sum \lambda_i f_i$. Then $\lambda_i = 0$ for all $i \geq m + n$.*

Proof. By the Binomial Theorem, $F(x, y)^{m+n-1} = (x + y)^{m+n-1}$ is contained in the ideal (x^m, y^n), and the assertion follows from Lemma 3.3. □

Proposition 3.5. *We have*

$$f_2 f_n = \begin{cases} f_{n-1} + f_{n+1} & \textit{if } p \textit{ does not divide } n; \\ 2f_n & \textit{else,} \end{cases}$$

for all $n \geq 1$.

Proof. The case $n = 1$ is trivial, so assume $n \geq 2$. According to Proposition 3.2 and 3.4, we have $f_2 f_n = f_i + f_j$ for some $i \leq j \leq n+1$, which furthermore satisfies $i + j = 2n$ by Proposition 3.1. The only solutions are $i = j = n$ and $i = n-1$, $j = n+1$. Clearly $(x+y)^n \equiv \binom{n}{1} xy^{n-1}$ modulo (x^2, y^n), and therefore $(x+y)^n \equiv 0$ if and only if p divides n. Now the assertion follows from Lemma 3.3. □

Corollary 3.6. *The ring R is integral if and only if $p = 0$. In this case, the homomorphism of rings $\mathbb{Z}[X] \to R$ defined by $X \mapsto f_2$ is bijective.*

Proof. If $p \neq 0$, then $(f_2 - 2f_1)f_p = 0$, whence the ring R is not integral. Now suppose $p = 0$. Using the relation $f_2 f_n = f_{n-1} + f_{n+1}$, we inductively infer that $f_2^n = f_{n+1} + \sum_{i \leq n} \lambda_i f_i$ for some coefficients λ_i. Consider the standard $\mathbb{Z}$-bases $t^j \in \mathbb{Z}[X]$ and $f_{j+1} \in R$, $j \geq 0$. With respect to these bases, the matrix of $\mathbb{Z}[X] \to R$, viewed as a homomorphism of free $\mathbb{Z}$-modules, is an upper triangular matrix all whose diagonal entries are 1, whence is invertible. □

Corollary 3.7. *Let $1 \leq m \leq n$ be integers. If $p = 0$ or $p > m + n - 2$, then*

$$f_m f_n = \sum_{i=0}^{m-1} f_{m+n-1-2i}.$$

Proof. By induction on $m \geq 1$. The case $m = 1$ is trivial. Now suppose $m \geq 2$, such that $f_m = f_2 f_{m-1} - f_{m-2}$ by Proposition 3.5. We have inductively

$$\begin{aligned} f_m f_n &= f_2 f_{m-1} f_n - f_{m-2} f_n \\ &= f_2 \sum_{i=0}^{m-2} f_{m+n-2-2i} - \sum_{i=0}^{m-3} f_{m+n-3-2i} \\ &= \sum_{i=0}^{m-2} (f_{m+n-3-2i} + f_{m+n-1-2i}) - \sum_{i=0}^{m-3} f_{m+n-3-2i} \\ &= f_{n-m+1} + \sum_{i=0}^{m-2} f_{m+n-1-2i}, \end{aligned}$$

as desired. □

The following observation will be crucial in the next section:

Proposition 3.8. *Let $m, n \geq 0$, and write $f_m f_n = \sum \lambda_i f_i$. Let $r \geq 0$ be an integer so that p divides $\binom{m+n-2-a}{m-1-b}$ for all $0 \leq b \leq a \leq m+n-2-r$. Then $\lambda_i = 0$ for all integers $i > r$.*

Proof. We have

$$(x+y)^r \equiv \sum \binom{r}{j} x^j y^{r-j} \quad \text{modulo } (x^m, y^n),$$

where the sum runs over all integers j subject to the conditions

$$0 \leq j \leq r, \quad j \leq m-1, \quad r - j \leq n-1. \tag{1}$$

Setting $r = m + n - 2 - a$ and $j = m - 1 - b$, we observe that the conditions in (1) ensures that $0 \leq b \leq a \leq m + n - 2 - r$. Whence $(x+y)^r \equiv 0$ modulo (x^m, y^n). Now Lemma 3.3 implies that $\lambda_{r+1} = \lambda_{r+2} = \ldots = 0$. □

4. Convolution rings as integral extensions

From now on, we assume that the characteristic is $p > 0$. The ring extension $\mathbb{Z} \subset R$ is obviously faithfully flat, since R is a nonzero free $\mathbb{Z}$-module. In this section we shall see that the ring extension is also integral, in other words, each element from R is a root of a monic polynomial with integer coefficients. This hinges on the following observation:

Lemma 4.1. *Let $q = p^\nu$ and $m, n \leq q$. Then $f_m f_n = \sum \lambda_i f_i$ with $\lambda_i = 0$ for $i > q$.*

Proof. In light of Proposition 3.3, it suffices to check $(x+y)^q \equiv 0$ modulo (x^m, y^n). But this is obvious because $(x+y)^q = x^q + y^q$. □

This directly leads to:

Theorem 4.2. *The ring extension $\mathbb{Z} \subset R$ is integral. In particular, we have $\dim(R) = 1$.*

Proof. Given a prime power $q = p^\nu$, the subgroup $R' \subset R$ generated by the $f_1, f_2, \ldots, f_q$ is a subring, according to Lemma 4.1. This subring is obviously a finite $\mathbb{Z}$-algebra. The upshot is that R is a union of subrings that are finite $\mathbb{Z}$-algebras. Consequently R is an integral $\mathbb{Z}$-algebra. The statement about the dimension follows from [4], Chapter VIII, §2, No. 3, Theorem 1. □

5. Application of Lucas' Theorem

We now shall study products $f_m f_n$ in the convolution ring R where the indices m, n are p-powers. Our results hinge on the classical Theorem of Lucas on congruences for binomial coefficients ([13], Section 21). Let $a, b \geq 0$ be integers, and $a = \sum a_i p^i$ and $b = \sum b_i p^i$ be their p-adic expansion, with digits $0 \leq a_i, b_i < p$. Then Lucas Theorem asserts

$$\binom{a}{b} \equiv \prod_i \binom{a_i}{b_i} \mod p.$$

For our purposes, the following variant is useful: Fix a prime power $q = p^i$, and now consider the q-adic expansion $a = \sum a_i q^i$ and $b = \sum b_i q^i$, with digits $0 \leq a_i, b_i < q$.

Lemma 5.1. *With the preceding notation, we also have $\binom{a}{b} \equiv \prod_i \binom{a_i}{b_i}$ modulo p.*

Proof. This can be seen as in the prove of Lucas' Theorem given by Fine [7]. We reproduce the argument for the sake of the reader: Fix $a = \sum a_i q^i$. Inside the polynomial ring $\mathbb{F}_p[T]$, we have

$$(1+T)^a = \prod_{i \geq 0} (1 + T^{q^i})^{a_i} = \prod_{i \geq 0} \sum_{c \geq 0} \binom{a_i}{c} T^{cq^i} = \sum_{c_0, c_1, \ldots \geq 0} \prod_{i \geq 0} \binom{a_i}{c_i} T^{c_i q^i}.$$

In the latter sum, a summand vanishes if $c_i \geq a_i$ for one index $i \geq 0$, an in particular if $c_i \geq p$ for one $i \geq 0$. Discarding these trivial summands and using the uniqueness of q-adic expansions with digits $0 \leq b_i < q$ for the numbers $b = \sum b_i q^i$, the above expression equals $\sum_{b \geq 0} \prod_{i \geq 0} \binom{a_i}{b_i} T^b$. The result follows by comparing with the binomial expansion of $(1+T)^a$. □

The following congruence property of successive binomial coefficients will be crucial for us:

Lemma 5.2. *Let $q = p^\nu$ and $0 \leq m \leq q$ be integers. Then $\binom{m+q-2-a}{q-1-b} \equiv 0$ modulo p for all integers $0 \leq b \leq a \leq m-2$.*

Proof. Clearly, the first digit of the q-adic expansions of $m+q-2-a$ and $q-1-b$ are $m-2-a$ and $q-1-b$, respectively. The assumptions yield the inequality $m-2-a < q-1-b$, which ensures $\binom{m-2-a}{q-1-b} = 0$. The statement now follows from Lemma 5.1. □

Proposition 5.3. *Let $q = p^\nu$ and $0 \leq m \leq q$ be integers. Then $f_m f_q = m f_q$.*

Proof. Write $f_m f_q = \sum \lambda_i f_i$. In light of Lemma 5.2, we may apply Proposition 3.8 with $n = r = q$ and deduce that $\lambda_i = 0$ for $i > q$. Whence we have the inequality $i\lambda_i \leq q\lambda_i$ for all i. We also know $\sum \lambda_i = m$ and $\sum i\lambda_i = mq$. Whence

$$mq = \sum i\lambda_i \leq \sum q\lambda_i = qm.$$

It follows that all our inequalities $i\lambda_i \leq q\lambda_i$ are actually equalities. The latter implies $\lambda_1 = \ldots = \lambda_{q-1} = 0$, and finally $\lambda_q = m$. □

These relations have rather strange consequences. Consider the subset

$$S = \left\{ p^j f_{p^i} \mid i, j \geq 0 \right\} \subset R.$$

This is a multiplicative subset by Proposition 5.3, and p becomes invertible in the localization $S^{-1}R$. We thus have a canonical map $\mathbb{Z}[p^{-1}] \to S^{-1}R$.

Proposition 5.4. *The canonical map $\mathbb{Z}[p^{-1}] \to S^{-1}R$ is bijective.*

Proof. To check that the map is surjective, it suffices to verify that $f_m/1 \in S^{-1}R$ is in its image. Choose some $q = p^\nu$ with $m \leq q$. Then $f_m f_q = m f_q$, whence $f_m/1 = m/1$ lies in the image. The map is also injective: Suppose $m/p^\nu \in \mathbb{Z}[p^{-1}]$ maps to zero. Then $mp^j f_{p^i} = 0$ for some $i, j \geq 0$, whence $m = 0$. □

Given an integers $\nu \geq 0$, we now consider the subgroup $R_\nu \subset R$ generated by the $f_1, f_p, \ldots, f_{p^\nu} \in R$. According to Proposition 5.3, this is a subring, whence a finite flat $\mathbb{Z}$-algebra of rank $\nu + 1$.

Proposition 5.5. *The ring R_ν is reduced.*

Proof. Let $x = \sum_{i \geq j} \mu_i f_{p^i}$ be a nonzero element, say with $\mu_j \neq 0$. We compute $x^2 = \mu_j^2 p^j f_{p^j} + \sum_{i > j} \mu'_i f_{p^i}$ for certain integers μ'_i. It follows that $x^2 \neq 0$, and this implies that R_ν is reduced. □

We now seek to understand the geometry of the map $\operatorname{Spec}(R_\nu) \to \operatorname{Spec}(\mathbb{Z})$. To this end, we first turn our attention to the fiber ring $R_\nu \otimes \mathbb{F}_p$.

Proposition 5.6. *The $\mathbb{F}_p$-algebra $R_\nu \otimes \mathbb{F}_p$ is isomorphic to the local Artin ring $\mathbb{F}_p[x_1, \ldots, x_\nu]/(x_1, \ldots, x_\nu)^2$.*

Proof. Proposition 5.3 implies that $(f_{p^i} \otimes 1)(f_{p^j} \otimes 1) = 0$ for $1 \leq i, j \leq \nu$. Whence we obtain a homomorphism

$$\mathbb{F}_p[x_1, \ldots, x_\nu]/(x_1, \ldots, x_\nu)^2 \longrightarrow R_\nu \otimes \mathbb{F}_p, \quad x_i \longmapsto f_{p^i} \otimes 1,$$

which is obviously surjective. This map is bijective, because both algebras have the same dimension as vector spaces over $\mathbb{F}_p$. □

Next we look at the rings $R_\nu[1/p] = R_\nu \otimes \mathbb{Z}[1/p]$ obtained by inverting p, which we view as an algebra over $\mathbb{Z}[1/p]$. The elements

$$e_i = f_{p^i} \otimes 1/p^i \in R_\nu[p^{-1}], \qquad 0 \leq i \leq \nu$$

form a $\mathbb{Z}[1/p]$-basis and satisfy the relations $e_ie_j = e_j$ for $0 \leq i \leq j \leq \nu$. These relations imply that the linear maps

$$\varphi_j : R_\nu[1/p] \longrightarrow \mathbb{Z}[1/p], \quad e_i \longmapsto \begin{cases} 1 & \text{if } i \leq j, \\ 0 & \text{else} \end{cases}$$

are homomorphisms of algebras. In turn, we obtain a homomorphism of algebras

$$\Phi_\nu : R_\nu[1/p] \longrightarrow \prod_{i=0}^{\nu} \mathbb{Z}[1/p], \quad x \longmapsto (\varphi_0(x), \varphi_1(x), \ldots, \varphi_\nu(x)).$$

Proposition 5.7. *The homomorphism $\Phi_\nu : R_\nu[1/p] \to \prod_{i=0}^{\nu} \mathbb{Z}[1/p]$ is bijective.*

Proof. Both $\mathbb{Z}[1/p]$-modules in question are free of rank $\nu + 1$, whence it suffices to check that Φ_ν is surjective. Clearly, the images

$$\Phi_\nu(e_i) = (\underbrace{0, \ldots, 0}_{i \text{ entries}}, 1, \ldots, 1) \in \prod_{i=0}^{\nu} \mathbb{Z}[1/p], \quad 0 \leq i \leq \nu \tag{2}$$

are module generators, whence the result. $\square$

Remark 5.8. As James Borger pointed out to me, the rings R_ν are related to the *ring of Witt vectors* $W(\mathbb{Z})$. For a general exposition of Witt vectors, we refer to [4], Chapter 9, §1. Recall that the Witt vector $(1, 0, 0, \ldots) \in W(\mathbb{Z})$ is the identity element, and that the Verschiebung

$$V : W(\mathbb{Z}) \to W(\mathbb{Z}), \quad (a_0, a_1, \ldots) \longmapsto (0, a_0, a_1, \ldots)$$

is an endomorphism of the underlying additive group. Consider the additive map

$$R_\nu \longrightarrow W(\mathbb{Z}), \quad f_{p^i} \longmapsto V^i(1).$$

This map is a homomorphism of rings, because we have $V^i(1) \times V^j(1) = p^i V^j(1)$ for $i \leq j$. The latter follows with induction on $i \geq 0$ from loc. cit., No. 5, Proposition 3. Using the commutative diagram

$$\begin{array}{ccc} W_\nu(\mathbb{Z}) & \longrightarrow & \prod_{i=0}^{\nu} \mathbb{Z} \\ \downarrow & & \downarrow \\ W_\nu(\mathbb{Q}) & \xrightarrow[\simeq]{} & \prod_{i=0}^{\nu} \mathbb{Q}, \end{array}$$

where the vertical maps are the canonical inclusions and the horizontal maps are given by the ghost components, we infer that $W_\nu(\mathbb{Z})$ is a finite flat $\mathbb{Z}$-algebra of rank $\nu+1$. It is generated by the images of the $V^i(1)$, which follows with induction on $\nu \geq 0$ from loc. cit., No. 6, Lemma 4. The upshot is that the composite maps $R_\nu \to W_\nu(\mathbb{Z})$ are surjective, whence bijective. Using that that canonical map $W(\mathbb{Z}) \to \varprojlim W_n(\mathbb{Z})$ is bijective, we conclude that the union $\bigcup_\nu R_\nu$ might be regarded as a dense subring of $W(\mathbb{Z})$.

We now come to the second main result of this paper:

Theorem 5.9. *The affine scheme* $\operatorname{Spec}(R)$ *contains infinitely many irreducible components. In particular, the ring* R *is not noetherian.*

Proof. Seeking a contradiction, we assume that the spectrum of R has only finitely many irreducible components. Then the spectrum X of the localization $R\otimes\mathbb{Q}$ also has only finitely many irreducible components, say $X = X_1\cup\ldots\cup X_\nu$. Now consider the subalgebra $R_\nu\otimes\mathbb{Q}\subset R\otimes\mathbb{Q}$, and let $f : X\to Y_\nu$ be the induced morphism of affine scheme. The space $Y_\nu = \operatorname{Spec}(R_\nu\otimes\mathbb{Q})$ is discrete and contains $\nu+1$ points $y_0, y_1, \ldots, y_\nu\in Y_\nu$. Without loss of generality we may assume that $f(X_i)\neq y_0$ for all i, that is, $y_0\notin f(X)$. On the other hand, the map $f : X\to Y_\nu$ is dominant, because $R_\nu\to R$ is injective, contradiction. □

We now may use Proposition 5.7 to determine the normalization of the reduced ring R_ν. Consider the induced map $R_\nu\hookrightarrow R_\nu[p^{-1}]\to\prod_{i=0}^{\nu}\mathbb{Z}[1/p]$. According to Formula (2), we have

$$\Phi_\nu(f_{p^i}) = (\underbrace{0,\ldots,0}_{i\text{ entries}}, p^i,\ldots,p^i), \tag{3}$$

whence there is a factorization $\Phi_\nu : R_\nu\to\prod_{i=0}^{\nu}\mathbb{Z}$.

Proposition 5.10. *The inclusion* $R_\nu\subset\prod_{i=0}^{\nu}\mathbb{Z}$ *is the normalization of the reduced ring* R_ν *in its total fraction ring.*

Proof. The map in question becomes bijective after inverting p, and the ring $\prod_{i=0}^{\nu}\mathbb{Z}$ is normal. We infer that the normalization is of the form $\prod_{i=0}^{\nu}R_i\subset\prod_{i=0}^{\nu}\mathbb{Z}$ for some subrings $R_i\subset\mathbb{Z}$. Since the ring $\mathbb{Z}$ contains only one subring, namely itself, the inclusion in question must be the normalization of R_ν. □

Proposition 5.11. *The image of the inclusion map* $\Phi_\nu : R_\nu\to\prod_{i=0}^{\nu}\mathbb{Z}$ *is the subring consisting of elements of the form* $(b_0,\ldots,b_\nu)$ *with* $b_j\equiv b_{j-1}$ *modulo* p^j *for* $1\leq j\leq\nu$.

Proof. Clearly, the entries $b_0=\ldots=b_{i-1}=0$ and $b_i=\ldots=b_\nu=p^i$ of $\Phi_\nu(f_{p^i})$ satisfy the conditions. By additivity, these conditions hold for all images. Conversely, suppose we have entries with $b_j\equiv b_{j-1}$ modulo p^j for $1\leq j\leq\nu$. By induction on ν, we have $\Phi_{\nu-1}(x) = (b_0,\ldots,b_{\nu-1})$ for some $x=\sum_{i=0}^{\nu-1}\lambda_i f_{p^i}$. Then $\Phi_\nu(x) = (b_0,\ldots,b_{\nu-1},b_{\nu-1})$ and $\Phi_\nu(x+\lambda_\nu f_{p^\nu}) = (b_0,\ldots,b_{\nu-1},b_{\nu-1}+\lambda_\nu p^\nu)$. Since $b_\nu\equiv b_{\nu-1}$ modulo p^ν, some λ_ν solves the equation $b_\nu = b_{\nu-1}+\lambda_\nu p^\nu$. Whence $(b_0,\ldots,b_\nu)$ lies in the image. □

Now recall that the *conductor ideal* $\mathfrak{c}\subset R_\nu$ for the birational inclusion $R_\nu\subset\prod_{i=0}^{\nu}\mathbb{Z}$ is defined as the annihilator ideal of $\operatorname{coker}(\Phi_\nu) = (\prod_{i=0}^{\nu}\mathbb{Z})/R_\nu$. This is the largest ideal in R_ν that is at the same time an ideal in the overring $\prod_{i=0}^{\nu}\mathbb{Z}$.

Proposition 5.12. *The conductor ideal* $\mathfrak{c}\subset\prod_{i=0}^{\nu}\mathbb{Z}$ *is the principal ideal generated by* $(p,p^2,\ldots,p^\nu,p^\nu)$.

Proof. Let $(b_0,\ldots,b_n)\in\mathfrak{c}$. Then we have $b_ia_i\equiv b_{i-1}a_{i-1}$ modulo p^i, for all $a_i\in\mathbb{Z}$, $1\leq i\leq\nu$. Setting $a_i=0$ and $a_{i-1}=1$ we deduce $b_{i-1}\in p^i\mathbb{Z}$. Moreover, $a_\nu=1$ and $a_{\nu-1}=0$ yields $b_\nu\in p^\nu\mathbb{Z}$. Whence the conductor algebra is contained in the principal ideal defined by $(p,p^2,\ldots,p^\nu,p^\nu)$. Conversely, it is easy to check that the latter element lies in the conductor ideal. □

We thus have an identification of residue rings

$$(\prod_{i=0}^{\nu} \mathbb{Z})/\mathfrak{c} = (\prod_{i=0}^{\nu-1} \mathbb{Z}/p^{i+1}\mathbb{Z}) \times \mathbb{Z}/p^{\nu}\mathbb{Z},$$

and $\Phi_\nu(f_{p^i}) \in \prod_{i=0}^{\nu} \mathbb{Z}$, $1 \leq i \leq \nu$ vanishes modulo $\mathfrak{c}$. In turn, we obtain a commutative diagram

$$\begin{array}{ccc} \prod_{i=0}^{\nu} \mathbb{Z} & \longrightarrow & (\prod_{i=0}^{\nu} \mathbb{Z})/\mathfrak{c} \\ \uparrow & & \uparrow \\ R_\nu & \longrightarrow & \mathbb{Z}/p^\nu\mathbb{Z} \end{array}$$

where the map on the right is the diagonal map, and the lower map is given by sending f_{p^i}, $1 \leq i \leq \nu$ to zero. According to general properties of conductor ideals, this diagram is cartesian, and the induced commutative diagram of affine schemes

$$\begin{array}{ccc} \bigcup_{i=0}^{\nu} \operatorname{Spec}(\mathbb{Z}) & \longleftarrow & \operatorname{Spec}((\prod_{i=0}^{\nu} \mathbb{Z})/\mathfrak{c}) \\ \downarrow & & \downarrow \\ \operatorname{Spec}(R_\nu) & \longleftarrow & \operatorname{Spec}(\mathbb{Z}/p^\nu\mathbb{Z}) \end{array}$$

is cartesian and cocartesian [6]. Roughly speaking, the scheme $\operatorname{Spec}(R_\nu)$ is obtained from $\nu + 1$ disjoint copies of $\operatorname{Spec}(\mathbb{Z})$ by gluing the copies along the points of characteristic p together, with higher and higher infinitesimal identification along successive copies.

6. Stone spaces

Keeping the notation from the previous section, we now consider the subring

$$R_\infty = \bigcup_{\nu \geq 0} R_\nu \subset R,$$

which is a free $\mathbb{Z}$-module generated by all the $f_{p^i} \in R$ with $i \geq 0$. We seek to understand its spectrum. To achieve this, we merely have to analyze the canonical inclusion $R_\nu \subset R_{\nu+1}$. To simplify things, we shall tensor with $\mathbb{Q}$. Consider the diagram

$$\begin{array}{ccc} R_\nu & \longrightarrow & R_{\nu+1} \\ {\scriptstyle\Phi_\nu}\downarrow & & \downarrow{\scriptstyle\Phi_{\nu+1}} \\ \prod_{i=0}^{\nu} \mathbb{Q} & \longrightarrow & \prod_{i=0}^{\nu+1} \mathbb{Q} \end{array} \tag{4}$$

where the lower map is given by $(a_0, \ldots, a_\nu) \mapsto (a_0, \ldots, a_\nu, a_\nu)$, that is, by duplicating the last entry. It follows from Formula (3) that this diagram is commutative. Set $Y_\nu = \operatorname{Spec}(\prod_{i=0}^{\nu+1} \mathbb{Q})$. The induced map $Y_{\nu+1} \to Y_\nu$ is easy to understand: If $y_i^\nu \in Y_\nu$ denotes the point corresponding to the i-th projection $\prod_{i=0}^{\nu} \mathbb{Q} \to \mathbb{Q}$, then we have

$$y_i^{\nu+1} \longmapsto \begin{cases} y_i^\nu & \text{if } i \leq \nu \\ y_\nu^\nu & \text{if } i = \nu + 1. \end{cases}$$

We now consider the inverse limit $Y = \varprojlim Y_\nu \subset \prod Y_\nu$. Being an inverse limit of finite discrete spaces, it is a *Stone space*, that is, a compact and totally disconnected space. In our case it consists of the points

$$y_i = (y_0^0, y_1^1, \ldots, y_i^i, y_i^{i+1}, y_i^{i+2} \ldots) \in Y, \quad i \geq 0,$$

whose entries become eventually constant in the lower index, together with the distinguished point

$$y_\infty = (y_0^0, y_1^1, y_2^2, \ldots) \in Y,$$

whose entries always change in the lower index. We now come back to our ring R_∞:

Theorem 6.1. *The ring $R_\infty \otimes \mathbb{Q}$ is 0-dimensional. Its spectrum is homeomorphic, as a topological space, to Y, and this is the Alexandroff compactification of the discrete space $\{y_0, y_1, \ldots\}$ obtained by putting the point y_∞ at "infinity".*

Proof. Let $\mathrm{pr}_\nu : Y \to Y_\nu$ be the canonical projection onto the ν-th factor. The subspace $\{y_0, y_1, \ldots\} = Y \smallsetminus \{y_\infty\}$ is discrete, because $\mathrm{pr}_\nu^{-1}(y_i^\nu) = \{y_i\}$ whenever $i < \nu$. Since Y is compact, it must be the Alexandroff compactification of the discrete subspace $Y \smallsetminus \{y_\infty\}$, by the uniqueness of the latter ([3], §9, No. 8, Theorem 4).

We clearly have $R_\infty = \varinjlim_\nu R_\nu$, whence there is a canonical continuous map $\mathrm{Spec}(R_\infty) \to \varprojlim_\nu \mathrm{Spec}(R_\nu)$, and the latter is a homeomorphism by [9], Corollary 8.2.10. In particular, $R_\infty \otimes \mathbb{Q}$ has Krull dimension zero. □

Reduced 0-dimensional rings are also called *absolutely flat*, or *von Neumann regular*. It is easy to give an explicit description of $R_\infty \otimes \mathbb{Q}$. Let us call a sequence of rational numbers $(a_0, a_1, \ldots)$ *almost constant* if $a_i = a_{i+1} = \ldots$ for some index $i \geq 0$. The description of R_∞ given by (4) immediately gives:

Proposition 6.2. *The ring $R_\infty \otimes \mathbb{Q}$ is isomorphic to the subring of $\prod_{i=0}^\infty \mathbb{Q}$ whose elements are the almost constant sequences $(a_0, a_1, \ldots)$.*

Having understood the ring R_∞, one next should analyze the ring extension $R_\infty \subset R$. Let us mention the following:

Proposition 6.3. *The fiber of the morphism* $\mathrm{Spec}(R) \to \mathrm{Spec}(R_\infty)$ *over the point y_∞ consist of only one point.*

Proof. For each $f_{p^i} \in R_\infty$, the open subset $D(f_{p^i}) \subset \mathrm{Spec}(R_\infty)$ contains y_∞ by (3), and we also have $y_\infty \in D(p)$. The assertion now follows from Proposition 5.4. □

References

[1] M. Atiyah: On the Krull–Schmidt theorem with application to sheaves. Bull. Soc. Math. France 84 (1956), 307–317.

[2] M. Atiyah: Vector bundles over an elliptic curve. Proc. London Math. Soc. 7 (1957) 414–452.

[3] N. Bourbaki: Topologie générale. Chapitres 1–4. Hermann, Paris, 1971.

[4] N. Bourbaki: Algèbre commutative. Chapitre 8–9. Masson, Paris, 1983.

[5] I. Burban, B. Kreussler: Derived categories of irreducible projective curves of arithmetic genus one. Compos. Math. 142 (2006), 1231–1262.

[6] D. Ferrand: Conducteur, descente et pincement. Bull. Soc. Math. France 131 (2003), 553–585.

[7] N. Fine: Binomial coefficients modulo a prime. Amer. Math. Monthly 54, (1947). 589–592.

[8] J. Green: The modular representation algebra of a finite group. Illinois J. Math. 6 (1962) 607–619.

[9] A. Grothendieck: Éléments de géométrie algébrique IV: Étude locale des schémas et des morphismes de schémas. Publ. Math., Inst. Hautes Étud. Sci. 28 (1966).
[10] G. Hein, D. Ploog: Fourier–Mukai transforms and stable bundles on elliptic curves. Beiträge Algebra Geom. 46 (2005), 423–434.
[11] D. Huybrechts: Fourier–Mukai transforms in algebraic geometry. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, Oxford, 2006.
[12] M. Lazard: Sur les groupes de Lie formels à un paramètre. Bull. Soc. Math. France 83 (1955), 251–274.
[13] E. Lucas: Théorie des Fonctions Numériques Simplement Périodiques. Amer. J. Math. 1 (1878), 197–240.
[14] J. McFall: How to compute the elementary divisors of the tensor product of two matrices. Linear and Multilinear Algebra 7 (1979), 193–201.
[15] S. Mukai: Semi-homogeneous vector bundles on an abelian variety. J. Math. Kyoto Univ. 18 (1978), 239–272.
[16] S. Mukai: Duality between $D(X)$ and $D(\hat{X})$ with its application to Picard sheaves. Nagoya Math. J. 81 (1981), 153-175.
[17] M. Nori: The fundamental group-scheme. Proc. Indian Acad. Sci. Math. Sci. 91 (1982), 73–122.
[18] C. Norman: On Jordan bases for the tensor product and Kronecker sum and their elementary divisors over fields of prime characteristic. Linear Multilinear Algebra 56 (2008), 415–451.
[19] T. Oda: Vector bundles on an elliptic curve. Nagoya Math. J. 43 (1971), 41–72.
[20] A. Polishchuk: Abelian varieties, theta functions and the Fourier transform. Cambridge Tracts in Mathematics 153. Cambridge University Press, Cambridge, 2003.
[21] T. Ralley: Decomposition of products of modular representations. J. London Math. Soc. 44 (1969), 480–484.
[22] W. Roth: On direct product matrices. Bull. Amer. Math. Soc. 40 (1934), 461–468.
[23] B. Srinivasan: The modular representation ring of a cyclic p-group. Proc. London Math. Soc. 14 (1964), 677–688.
[24] A. Trampus: A canonical basis for the matrix transformation $X \to AX + XB$. J. Math. Anal. Appl. 14 (1966), 242–252.

Mathematisches Institut, Heinrich-Heine-Universität, 40225 Düsseldorf, Germany
E-mail address: schroeer@math.uni-duesseldorf.de