

Algebra & Number Theory

Volume 4

2010

No. 1



mathematical sciences publishers

Algebra & Number Theory

www.jant.org

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

| | | | |
|----------------------|---|-----------------------|--|
| Georgia Benkart | University of Wisconsin, Madison, USA | Susan Montgomery | University of Southern California, USA |
| Dave Benson | University of Aberdeen, Scotland | Shigefumi Mori | RIMS, Kyoto University, Japan |
| Richard E. Borcherds | University of California, Berkeley, USA | Andrei Okounkov | Princeton University, USA |
| John H. Coates | University of Cambridge, UK | Raman Parimala | Emory University, USA |
| J-L. Colliot-Thélène | CNRS, Université Paris-Sud, France | Victor Reiner | University of Minnesota, USA |
| Brian D. Conrad | University of Michigan, USA | Karl Rubin | University of California, Irvine, USA |
| Hélène Esnault | Universität Duisburg-Essen, Germany | Peter Sarnak | Princeton University, USA |
| Hubert Flenner | Ruhr-Universität, Germany | Michael Singer | North Carolina State University, USA |
| Edward Frenkel | University of California, Berkeley, USA | Ronald Solomon | Ohio State University, USA |
| Andrew Granville | Université de Montréal, Canada | Vasudevan Srinivas | Tata Inst. of Fund. Research, India |
| Joseph Gubeladze | San Francisco State University, USA | J. Toby Stafford | University of Michigan, USA |
| Ehud Hrushovski | Hebrew University, Israel | Bernd Sturmfels | University of California, Berkeley, USA |
| Craig Huneke | University of Kansas, USA | Richard Taylor | Harvard University, USA |
| Mikhail Kapranov | Yale University, USA | Ravi Vakil | Stanford University, USA |
| Yujiro Kawamata | University of Tokyo, Japan | Michel van den Bergh | Hasselt University, Belgium |
| János Kollár | Princeton University, USA | Marie-France Vignéras | Université Paris VII, France |
| Hendrik W. Lenstra | Universiteit Leiden, The Netherlands | Kei-Ichi Watanabe | Nihon University, Japan |
| Yuri Manin | Northwestern University, USA | Andrei Zelevinsky | Northeastern University, USA |
| Barry Mazur | Harvard University, USA | Efim Zelmanov | University of California, San Diego, USA |

PRODUCTION

ant@mathscipub.org

Paulo Ney de Souza, Production Manager

Silvio Levy, Senior Production Editor


See inside back cover or www.jant.org for submission instructions.

Regular subscription rate for 2010: \$200.00 a year (\$140.00 electronic only).

Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory, ISSN 1937-0652, at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

PUBLISHED BY

 **mathematical sciences publishers**
<http://www.mathscipub.org>

A NON-PROFIT CORPORATION

Typeset in L^AT_EX

Copyright ©2010 by Mathematical Sciences Publishers

Density of rational points on diagonal quartic surfaces

Adam Logan, David McKinnon and Ronald van Luijk

Let a, b, c, d be nonzero rational numbers whose product is a square, and let V be the diagonal quartic surface in \mathbb{P}^3 defined by $ax^4 + by^4 + cz^4 + dw^4 = 0$. We prove that if V contains a rational point that does not lie on any of the 48 lines on V or on any of the coordinate planes, then the set of rational points on V is dense in both the Zariski topology and the real analytic topology.

1. Introduction

This paper is about the arithmetic of diagonal quartic surfaces, which are the surfaces $V_{a,b,c,d} \subset \mathbb{P}^3$ defined by the equation $ax^4 + by^4 + cz^4 + dw^4 = 0$ for nonzero $a, b, c, d \in \mathbb{Q}$. We will prove the following theorem.

Theorem 1.1. *Let $a, b, c, d \in \mathbb{Q}^*$ be nonzero rational numbers with $abcd$ square. Let $P = (x_0 : y_0 : z_0 : w_0)$ be a rational point on $V_{a,b,c,d}$, and suppose that $x_0 y_0 z_0 w_0 \neq 0$ and that P does not lie on any of the 48 lines of the surface. Then the set of rational points of the surface is dense in both the Zariski and the real analytic topology.*

We will also prove a generalization to arbitrary number fields of a weaker version of [Theorem 1.1](#). An easy consequence of [Theorem 1.1](#) is the following.

Theorem 1.2. *Let $a, b, c, d \in \mathbb{Q}^*$ be nonzero rational numbers with $abcd$ square and $a + b + c + d = 0$. Assume that no two of a, b, c, d sum to 0. Then the set of rational points of the surface $V_{a,b,c,d}$ is dense in both the Zariski and the real analytic topology.*

The surfaces $V_{a,b,c,d}$ are smooth quartic surfaces, which means that they are K3 surfaces. One of the most important open problems in the arithmetic of K3 surfaces is to determine whether there is a K3 surface over a number field on which the set of rational points is neither empty nor Zariski dense. [Theorem 1.1](#) shows that a diagonal quartic surface over \mathbb{Q} for which the product of the coefficients is a square does not have this property, unless all its rational points lie on the union of its 48

MSC2000: primary 11D25; secondary 14J28, 14G05.

Keywords: rational points, K3 surfaces, elliptic surfaces, quartic surfaces.

lines and the coordinate planes. However, no such diagonal surface is known and the authors believe that the condition in [Theorem 1.1](#) that P not lie on one of the 48 lines or on one of the coordinate planes may not be necessary.

Noam Elkies [[1988](#)] proved that the set of \mathbb{Q} -rational points on $V_{1,1,1,-1}$ is dense in both the Zariski topology and the real analytic topology. Martin Bright [[2006](#)] has exhibited a Brauer–Manin obstruction to the existence of rational points on many examples. Sir Peter Swinnerton-Dyer in his paper [[2000](#)] assumes like us that $abcd$ is a square. He uses one of the two elliptic fibrations that exist in this case to show that under certain specific conditions on the coefficients, $V_{a,b,c,d}$ does not satisfy the Hasse principle, while under some other hypotheses, including Schinzel’s hypothesis and the assumption that Tate–Shafarevich groups of elliptic curves are finite, the Hasse principle is satisfied. In particular, assuming these two big conjectures, it follows immediately from his work that if $abcd$ is a square but not a fourth power and no product of two coefficients or their negatives is a square and there is no Brauer–Manin obstruction to the Hasse principle, then the set of rational points is Zariski dense; the last hypothesis is obviously satisfied when $V_{a,b,c,d}(\mathbb{Q})$ is nonempty. By [Theorem 1.1](#) the fact that the set $V_{a,b,c,d}(\mathbb{Q})$ is nonempty indeed implies that it is Zariski dense, independent from Schinzel’s hypothesis and the assumption that Tate–Shafarevich groups of elliptic curves are finite, provided that we assume instead the existence of a rational point that does not lie on any of the 48 lines or any of the coordinate planes.

Jean-Louis Colliot-Thélène, Alexei Skorobogatov, and Swinnerton-Dyer also used Schinzel’s hypothesis and finiteness of Tate–Shafarevich groups to show in [[Colliot-Thélène et al. 1998](#)] that over arbitrary number fields, on semistable elliptic fibrations satisfying certain technical conditions, the Brauer–Manin obstruction coming from the vertical Brauer group is the only obstruction to the Hasse principle; and that if such a fibration contains a rational point, its set of rational points is Zariski dense. Olivier Wittenberg [[2007](#)] generalized their theory to the extent that Swinnerton-Dyer’s aforementioned result over the rational numbers becomes a special case of this more general setting, thus extending the result to arbitrary number fields.

Colliot-Thélène pointed out the method of Richmond [[1944](#)] to the authors, which takes a rational point P on $V = V_{a,b,c,d}$ to construct two new points over $\mathbb{Q}(\sqrt{abcd})$. Each of these two points is the unique last point of intersection between V and one of the two tangent lines to the singular node in the intersection between V and the tangent plane to V at P . In this paper we reinterpret this construction to study the arithmetic of the surface V .

In the next section, we exhibit two endomorphisms e_1 and e_2 of $V_{a,b,c,d}$ such that $e_1(P)$ and $e_2(P)$ are the two points given by Richmond’s construction. The diagonal surfaces have two elliptic fibrations and each fibration is fixed by one

of the two endomorphisms. Thus, if e_i is one of the endomorphisms and P is a rational point on the surface, we will consider the fibre C_i of the fibration fixed by the endomorphism e_i that passes through P . This is a curve, so we can study the divisor $(e_i(P)) - (P)$ on it. Subject to the hypotheses, we will see that it is almost never a torsion divisor, and hence that fibres with rational points tend to have positive rank.

Our results are very much in the spirit of the potential density results from [Bogomolov and Tschinkel 1999; 2000; Harris and Tschinkel 2000]. These papers describe a variety of techniques for proving density and potential density of rational points on a variety of surfaces, including in particular the diagonal quartic surfaces we consider in this paper. Our results improve on these only in that we strengthen the conclusion of the potential density results to actual density, and that we weaken the hypotheses on the density results to demanding only a single rational point satisfying a weak genericity condition. For an excellent overview of techniques used to prove density and potential density of rational points on algebraic varieties, please see Brendan Hassett's survey [2003].

2. The elliptic fibrations and endomorphisms

Definition 2.1. For $a, b, c, d \in \mathbb{Q}^*$ we let $V_{a,b,c,d}$ be the surface in \mathbb{P}^3 given by $ax^4 + by^4 + cz^4 + dw^4 = 0$. Set $V_0 = V_{1,1,1,1}$ and $V'_0 = V_{1,1,-1,-1}$. Let $\tau: \mathbb{P}^3 \rightarrow \mathbb{P}^3$ be the map that squares all four coordinates. Set $Q_{a,b,c,d} = \tau(V_{a,b,c,d})$.

Suppose $a, b, c, d \in \mathbb{Q}^*$ with $abcd \in (\mathbb{Q}^*)^2$ and write V and Q for $V_{a,b,c,d}$ and $Q_{a,b,c,d}$ respectively. Suppose that V has a rational point. Then Q , which is a nonsingular quadric surface defined by $ax^2 + by^2 + cz^2 + dw^2 = 0$, also contains a rational point. Since $abcd$ is a square, the two rulings on Q are defined over \mathbb{Q} ; see [Bruin 2008, Lemma 2.5].

Definition 2.2. Fix a rational point R on Q , and decompose the intersection of Q with the tangent plane to Q at R into two lines l_1, l_2 . Let $\pi_1, \pi_2: Q \rightarrow \mathbb{P}^1$ be two rulings on Q such that l_i is a fibre of π_i . For $i = 1, 2$, set $f_i = \pi_i \circ \tau: V \rightarrow \mathbb{P}^1$.

Our description of the two rulings shows that they can be defined over \mathbb{Q} . However, the two rulings do not depend on R in the following sense. Let R' be another rational point on Q . Then by the same construction we obtain two rulings, which we can number $\pi'_1, \pi'_2: Q \rightarrow \mathbb{P}^1$, such that for each i the maps π_i and π'_i coincide up to a linear automorphism of \mathbb{P}^1 .

Any two linear forms defining l_i define a map to \mathbb{P}^1 equal to π_j up to a linear transformation of \mathbb{P}^1 , with $i \neq j$. Using additional lines in the same family, we can obtain alternative equations for the rulings and remove the base locus. The f_i are elliptic fibrations on V , also well-defined up to an automorphism of \mathbb{P}^1 .

Definition 2.3. Fix fourth roots of a, b, c, d . Let $\iota_{a,b,c,d}$ be the $\overline{\mathbb{Q}}$ -isomorphism $V_{a,b,c,d} \rightarrow V_0$ defined by $(\sqrt[4]{ax} : \sqrt[4]{by} : \sqrt[4]{cz} : \sqrt[4]{dw})$. Fix fourth roots of 1 and -1 , and let $\iota'_{a,b,c,d}$ be the $\overline{\mathbb{Q}}$ -isomorphism $V_{a,b,c,d} \rightarrow V'_0$ defined by $\iota_{1,1,-1,-1}^{-1} \circ \iota_{a,b,c,d}$.

Note that the fibrations f_i of $V = V_{a,b,c,d}$ were constructed geometrically. Therefore, the fibrations of $V_{a,b,c,d}$ coincide with those of $V_{1,1,1,1}$ up to composition with $\iota_{a,b,c,d}$ and a linear automorphism of \mathbb{P}^1 .

When we study the geometric properties of diagonal quartics, it suffices to consider V_0 or V'_0 . It is only when we consider the arithmetic properties that we need to allow the coefficients to vary. While some formulas are more symmetrical on V_0 , some things are defined over \mathbb{Q} for V'_0 that are not for V_0 . For example, the two elliptic fibrations on V'_0 are defined by $(x^2 - z^2 : y^2 - w^2)$ and $(x^2 - w^2 : y^2 - z^2)$, whereas on V_0 they can only be described over \mathbb{Q} as maps to a curve isomorphic to the conic $x^2 + y^2 + z^2 = 0$. To give a fibration of V_0 over \mathbb{P}^1 requires changing base to a field over which this conic has a point.

Definition 2.4. Let μ denote the group of automorphisms of \mathbb{P}^3 that multiply each coordinate by a fourth root of unity, and let S_4 act on the coordinates of \mathbb{P}^3 . We will regard μ as inducing a subgroup of $\text{Aut } V$. Any permutation $\pi \in S_4$ induces an isomorphism from $V_{a,b,c,d}$ to $V_{a',b',c',d'}$, where (a', b', c', d') is the appropriate permutation of (a, b, c, d) .

Definition 2.5. Let G be the semidirect product $\mu \rtimes S_4$, with the obvious action of S_4 on μ . We will view G as a subgroup of $\text{Aut } V_0$, and through conjugation with $\iota_{a,b,c,d}$ also as a subgroup of $\text{Aut } V_{a,b,c,d}$.

Note that when G is viewed as acting on V_0 , the elements of S_4 correspond to \mathbb{Q} -automorphisms of V_0 ; this is not the case when G is considered as acting on a general $V_{a,b,c,d}$.

The surface V contains exactly 48 lines, on which G acts transitively. On V'_0 one of these lines is given by $x = z$ and $y = w$. (For facts regarding the set of lines on $V_{a,b,c,d}$, see for example [Pjateckiĭ-Šapiro and Šafarevič 1971].)

Definition 2.6. Let G_0 denote the index-2 subgroup of G that fixes the fibrations f_i (up to an automorphism of \mathbb{P}^1).

The group G_0 partitions the 48 lines into two orbits Λ_i of size 24 (with $i = 1, 2$), where Λ_i consists of the irreducible components of the 6 singular fibres of f_i , each being of type I_4 [Swinnerton-Dyer 2000, page 517]. The singular points of the fibres are exactly the 24 points with two coordinates zero, and each of these points is singular on its fibre in both fibrations.

Definition 2.7. Let Ω denote the set of these 24 points, and let U be the complement of Ω in V .

We will see that the “tangents” to the node at P that we described in the introduction can be characterized in a different manner as well, namely as the tangents to the fibres of the f_i through P . We first show that these tangents do not interfere too much with the singular fibres.

Lemma 2.8. *Fix a point $P \in U(\overline{\mathbb{Q}})$, and i, j such that $\{i, j\} = \{1, 2\}$. For $k = 1, 2$, let C_k be the fibre of f_k through P , and let M be the tangent line to C_j at P . Then M is not contained in C_i .*

Proof. Since this statement is completely geometric, we assume $V = V'_0$ without loss of generality. Note that M is well-defined because C_j is smooth at P . Suppose M is contained in C_i . Then M is one of the 48 lines. After acting on V by an appropriate element of G , the line M is given by $x = z$ and $y = w$, so there are $s, t \in \overline{\mathbb{Q}}$ such that $P = (s : t : s : t)$. Since M is contained in the fibre above $(0 : 1)$ of the fibration that sends $(x : y : z : w)$ to $(x^2 - z^2 : w^2 + y^2)$, the curve C_j is a fibre of the other fibration, so f_j can be given by $(x^2 + z^2 : w^2 + y^2)$, or equivalently $(w^2 - y^2 : x^2 - z^2)$. Since $f_j(P) = (s^2 : t^2)$, we conclude that C_j is given by $s^2(w^2 + y^2) = t^2(x^2 + z^2)$ and $t^2(w^2 - y^2) = s^2(x^2 - z^2)$. The tangent line to C_j at P is therefore also given by $s^2t(w + y) = t^2s(x + z)$ and $t^3(w - y) = s^3(x - z)$. Simple linear algebra shows that this does not contain M unless $st = 0$. This contradicts the assumption that $P \in U$, which shows that M is not contained in C_i . \square

The following proposition is fundamental to our work and shows how the case of diagonal V is special.

Proposition 2.9. *Fix a point $P \in U(\overline{\mathbb{Q}})$ and set $R = \tau(P)$. Let T_R denote the tangent space to Q at R , and set $A = \tau^{-1}(T_R)$. Fix $i \in \{1, 2\}$, and let C_i be the fibre of f_i through P . Let M denote the tangent line to C_i at P . Then M is contained in A . Furthermore, let T_P denote the tangent plane to V at P . If C_i is irreducible, then the intersection multiplicities $(M \cdot (T_P \cap V))_P$ and $(T_P \cdot C_i)_P$ are at least 3.*

Proof. Note that $C_i = \tau^{-1}(L_i)$, where L_1 and L_2 are the lines in $T_R \cap Q$, so we have $C_1 \cup C_2 = \tau^{-1}(T_R \cap Q) = \tau^{-1}(T_R) \cap \tau^{-1}(Q) = A \cap V$. By the assumption $P \in U$, the curve C_i is smooth at P , so M is well-defined. Without loss of generality, we assume that P is contained in the affine part $w = 1$, given by $P = (x_0, y_0, z_0)$. Since the statement of [Proposition 2.9](#) is completely geometric, we may assume that Q is given by $x^2 + y^2 + z^2 + 1 = 0$, so that V is given by $q_V = 0$ with $q_V = x^4 + y^4 + z^4 + 1$, and A by $q_A = 0$ with $q_A = x_0^2 x^2 + y_0^2 y^2 + z_0^2 z^2 + 1$. Note that at most one of the coefficients of the equation defining A is 0, so A is irreducible and smooth at P . The common tangent space T_P to V and A at P is given by $l = 0$, where

$$l = x_0^3(x - x_0) + y_0^3(y - y_0) + z_0^3(z - z_0) = x_0^3x + y_0^3y + z_0^3z + 1.$$

It turns out that since Q is diagonal, the surfaces A and V are more similar locally at P than is implied by the fact that they share a tangent space. Let $\mathbb{O}_{\mathbb{P}^3, P}$ and \mathfrak{m} be the local ring of P in \mathbb{P}^3 and its maximal ideal. Set $g = x_0^2(x - x_0)^2 + y_0^2(y - y_0)^2 + z_0^2(z - z_0)^2 \in \mathfrak{m}^2$. Then the quadratic approximations of q_A and q_V are $q_A \equiv 2l + g \pmod{\mathfrak{m}^3}$ and $q_V \equiv 4l + 6g \pmod{\mathfrak{m}^3}$. (Note that in fact $q_A = 2l + g$ as well.) Let $q_1, q_2 \in k[x, y, z]$ be quadrics such that C_i is given on A by $q_i = 0$. From $C_1 \cup C_2 = V \cap A$ we conclude that $q_V \equiv cq_1q_2 \pmod{q_A}$ for some nonzero constant c . Replacing q_1 by cq_1 , we find that there exists a quadric $r \in k[x, y, z]$ such that $q_V = q_1q_2 + q_Ar$. From $q_i \in \mathfrak{m}$ we find $4l \equiv q_V \equiv q_Ar \equiv 2lr \pmod{\mathfrak{m}^2}$, and since $2l \neq 0$ in $\mathfrak{m}/\mathfrak{m}^2$, this implies that $r \equiv 2 \pmod{\mathfrak{m}}$.

Let $\mathbb{O}_{M, P}$ and \mathfrak{n} denote the local ring of P on M and its maximal ideal, and let the reduction map $\mathbb{O}_{\mathbb{P}^3, P} \rightarrow \mathbb{O}_{M, P}$ be given by $s \mapsto \bar{s}$. Since M is contained in T_P , we have $\bar{l} = 0$. Since C_i is tangent to M , we have $\bar{q}_i \in \mathfrak{n}^2$, so $\bar{q}_1\bar{q}_2 \in \mathfrak{n}^3$. Note that this also holds when M is a component of C_i , because then we have $\bar{q}_i = 0$. Therefore, we find $6\bar{g} \equiv \bar{q}_V \equiv \bar{r}\bar{q}_A \equiv 2\bar{g} \pmod{\mathfrak{n}^3}$, and so $\bar{g} \in \mathfrak{n}^3$. This implies $\bar{q}_A = \bar{g} \in \mathfrak{n}^3$. If M were not contained in A , then this would imply that A intersects M at P with multiplicity at least 3, which is impossible because A is quadratic and M is linear. We conclude that M is indeed contained in A .

Now assume that C_i is irreducible. Then by [Lemma 2.8](#), the line M is not contained in $C_1 \cup C_2 = A \cap V$, so $M \not\subset V$. This implies that the first intersection is between curves that have no common components. Because C_i is the intersection of two quadrics, it is not contained in a hyperplane. The same holds for the second intersection.

The first intersection takes place in T_P and the multiplicity equals the valuation of \bar{q}_V in $\mathbb{O}_{M, P}$. From the congruence $\bar{q}_V \equiv 6\bar{g} \pmod{\mathfrak{n}^3}$ we conclude that $\bar{q}_V \in \mathfrak{n}^3$, so the multiplicity is at least 3. Let $\mathbb{O}_{C, P}$ and \mathfrak{p} denote the local ring of P on C_i and its maximal ideal, and let the reduction map $\mathbb{O}_{\mathbb{P}^3, P} \rightarrow \mathbb{O}_{C, P}$ be given by $s \mapsto \tilde{s}$. Since \tilde{q}_V vanishes on C_i , we have $4\tilde{l} + 6\tilde{g} \equiv 0 \pmod{\mathfrak{p}^3}$. Because \tilde{q}_A vanishes on C_i , we also have $2\tilde{l} + \tilde{g} = 0$. Together this implies $l \in \mathfrak{p}^3$. As l defines T_P , this implies that T_P intersects C_i at P with multiplicity at least 3. \square

Definition 2.10. For the rest of this section, fix a point $P \in U(\overline{\mathbb{Q}})$ and i, j such that $\{i, j\} = \{1, 2\}$. For $k = 1, 2$, let C_k be the fibre of f_k through P and M_k the tangent line to C_k at P .

Corollary 2.11. *The line M_j intersects C_i in a scheme of dimension 0 and degree 2 that contains the reduced point P . (The intersection may be a nonreduced scheme supported at P .)*

Proof. Let T_R and $A = \tau^{-1}(T_R)$ be as in [Proposition 2.9](#). Recall that $C_i = \tau^{-1}(L)$ for some line L in T_R , so C_i is defined in A by a single quadric. The line M_j is contained in A by [Proposition 2.9](#), but not in C_i by [Lemma 2.8](#), so the dimension

of the intersection is indeed 0. First suppose A is nonsingular. Then M_j is a line in one of the rulings on A . The curve C_i on A is of type $(2, 2)$, so it intersects M_j twice, counted with multiplicity. The claim follows immediately. Now assume that A is singular. Without loss of generality we assume $V = V_0$. Suppose $P = (x_0 : y_0 : z_0 : w_0)$, so that A is given by $x_0^2x^2 + y_0^2y^2 + z_0^2z^2 + w_0^2w^2 = 0$. The facts that A is singular and that $P \in U$ imply that exactly one of the coordinates of P is zero. We deduce that A is the cone over a smooth conic, and that P is not contained in any of the lines on V , as their equations imply that if one coordinate is zero, then so is another. Therefore C_i is smooth, so, as C_i is defined in A by a single equation, it does not contain the vertex S of A . This means we can naively apply the usual intersection theory to study the intersections of C_i with other curves. The line M_j is a line on A through the vertex S and intersects any hyperplane section that does not go through S once. Since C_i is a quadratic hypersurface section, we find $M_j \cdot C_i = 2$. Again, the claim follows. \square

Definition 2.12. Following [Corollary 2.11](#), we define morphisms $e_i, e_j : U \rightarrow V$. The morphism e_i sends any point R to the unique second intersection point between the fibre of f_i through R and the tangent at R to the fibre of f_j through R . The morphism e_j is defined by interchanging the roles of i and j .

By definition, e_i and e_j respect the fibrations f_i and f_j respectively.

Corollary 2.13. *Let T_P denote the tangent plane to V at P , and set $D = T_P \cap V$. If C_j is irreducible, then the line M_j intersects D in the divisor $3(P) + (e_i(P))$ of D . If C_i is irreducible, then T_P intersects C_i also in $3(P) + (e_i(P))$, but as a divisor on C_i .*

Proof. Let A be as in [Proposition 2.9](#). Then we have $M_j \subset A$ and $A \cap V = C_i \cup C_j$. If C_j is irreducible, then M_j is not contained in C_j , and by [Lemma 2.8](#) also not in C_i , so $M_j \not\subset V$, and $M_j \cap D$ is 0-dimensional. If C_i is irreducible, then it is not contained in T_P , so $T_P \cap C_i$ is 0-dimensional. Both intersections have degree 4 by Bézout's Theorem, applied in T_P and \mathbb{P}^3 respectively. By [Proposition 2.9](#) the intersection at P has multiplicity at least 3, so it suffices to show that $e_i(P)$ is contained in both intersections. This follows from $e_i(P) \in C_i \subset V$ and $e_i(P) \in M_j \subset T_P$. \square

Remark 2.14. Since the M_k intersect D at P with multiplicity at least 3, they are exactly the ‘‘tangent’’ lines to the node on D at P that we discussed in the introduction. By [Corollary 2.13](#) this means that the $e_i(P)$ are the two points obtained from P as described there.

Remark 2.15. Let H be a hyperplane section of the generic fibre $\mathcal{V}_i/\overline{\mathbb{Q}}(t)$ in \mathbb{P}^3 of f_i . By [Corollary 2.13](#), if we identify \mathcal{V}_i with $\text{Pic}^1(\mathcal{V}_i)$, then e_i is given by sending R to $H - 3R$ for any point R on \mathcal{V}_i .

Although a computer is useful, even by hand it is not impossible to check that, on an open subset, e_1 and e_2 are given by sending $(x_0 : y_0 : z_0 : w_0)$ to $(x_1 : y_1 : z_1 : w_1)$ with

$$\begin{aligned} x_1 &= x_0((3bcy_0^4z_0^4 + adx_0^4w_0^4)(ax_0^4 + dw_0^4) + 4Nx_0^2y_0^2z_0^2w_0^2(by_0^4 - cz_0^4)), \\ y_1 &= y_0((3acx_0^4z_0^4 + bdy_0^4w_0^4)(by_0^4 + dw_0^4) + 4Nx_0^2y_0^2z_0^2w_0^2(cz_0^4 - ax_0^4)), \\ z_1 &= z_0((3abx_0^4y_0^4 + cdz_0^4w_0^4)(cz_0^4 + dw_0^4) + 4Nx_0^2y_0^2z_0^2w_0^2(ax_0^4 - by_0^4)), \\ w_1 &= w_0(cdz_0^4w_0^4(cz_0^4 + dw_0^4) - abx_0^4y_0^4(9cz_0^4 + dw_0^4)), \end{aligned} \quad (1)$$

where N is one of the two square roots of $abcd$.

Definition 2.16. For each coordinate v of \mathbb{P}^3 , let $\sigma_v \in \mu$ denote the automorphism of \mathbb{P}^3 that negates the v -coordinate. For a pair of coordinates u, v , let $\sigma_{uv} = \sigma_u\sigma_v$.

Proposition 2.17. *The automorphisms σ_u commute with the maps e_i on V and with all the maps $\iota_{a,b,c,d}$.*

Proof. For the e_i , this follows immediately from the equations in (1). For the $\iota_{a,b,c,d}$ it is obvious. \square

Proposition 2.18. *Assume P is contained in a line that is an irreducible component of C_i . Then there are two different coordinates u, v of \mathbb{P}^3 such that $e_j(P) = \sigma_{uv}(P)$, while P and $e_i(P)$ lie on nonintersecting components of C_i and $e_i(P) \notin \Omega$. In particular, $e_i(P)$ lies on a line.*

Proof. By Proposition 2.17 we may assume $V = V_0'$. Let L be the line in C_i that contains P . Note that the group G acts by conjugation on the set of the three automorphisms of the form σ_{uv} with $u \neq v$. The group G also acts by conjugation on the pair of fibrations and acts accordingly on the set of the two sets Λ_i of lines. It follows that after acting with an appropriate element of G , we may assume that L is given by $x = z$ and $y = w$, so there are $s, t \in \overline{\mathbb{Q}}$ such that $P = (s : t : s : t)$. From $P \notin \Omega$ we get $st \neq 0$. Then f_i can be given by $(x : y : z : w) \mapsto (x^2 - z^2 : w^2 + y^2)$, while f_j can be given by $(x : y : z : w) \mapsto (x^2 + z^2 : w^2 + y^2)$. As e_i respects f_i , it is easy to check which equations in (1) give e_i . It turns out that e_i is given by (1) with $N = 1$, while e_j is given by $N = -1$. Substituting in (1), we find $e_j(P) = (-s : t : -s : t) = \sigma_{xz}(P)$ and $e_i(P) = (t^3 : -s^3 : -t^3 : s^3)$. It is clear that $e_i(P)$ is not contained in Ω and lies on the component of C_i given by $x + z = y + w = 0$, which is a line and does not intersect L . \square

Proposition 2.19. *Let $\pi \in S_4$ be an automorphism of V_0 in \mathbb{P}^3 given by permutation of the coordinates, and let S_4 act on $V = V_{a,b,c,d}$ by conjugating the action on V_0 with $\iota_{a,b,c,d}$. Then $\pi e_i = e_k \pi$, where $k = i$ if the permutation underlying π is even and $k = j$ if it is odd.*

Proof. The statement is purely geometric, so we may assume $V = V_0$. Note that π switches the rulings on the quadric given by $x^2 + y^2 + z^2 + w^2 = 0$ if and only if π is odd, and it permutes the two elliptic fibrations on V accordingly. The statement therefore follows from [Corollary 2.11](#). \square

We can rephrase [Proposition 2.19](#) by stating that inside the group $G = \mu \rtimes S_4$ we have $G_0 \cap S_4 = A_4$. We see that if we conjugate the equations for e_i in [\(1\)](#) by an element in A_4 , then we obtain a new set of equations for e_i . In particular this will be true for the subgroup $V_4 \subset A_4$ of products of disjoint cycles. If instead we conjugate the equations for e_i by an odd element of S_4 , we get a new set of equations for e_j .

Proposition 2.20. *The map e_i extends to an endomorphism of U . The sets of equations obtained by conjugating those in [\(1\)](#) with elements of V_4 are sufficient to define e_i on all of U .*

Proof. The set of all points R where none of these 4 sets of equations defines a regular map is determined on V by the vanishing of all 16 polynomials in the sets. One checks by computer that this set is supported on Ω . Now suppose that for some R we have $e_i(R) \in \Omega$, and let C_i be the fibre of f_i through R . Then $e_i(R)$ also lies on C_i , so C_i is a singular fibre, and [Proposition 2.18](#) contradicts $e_i(R) \in \Omega$. We conclude that $e_i(U) \subset U$. \square

Remark 2.21. In fact the e_i do not extend to any of the points in Ω . One way to prove this is to show that, for each point $R \in \Omega$ and each i , there are two lines that meet at R whose images under the e_i are disjoint. This reflects the fact that K3 surfaces do not have endomorphisms of degree greater than 1.

Proposition 2.22. *The following are equivalent: (a) $e_1(P) = P$, (b) $e_2(P) = P$, (c) exactly one of the coordinates of P is 0.*

Proof. Without loss of generality we suppose $V = V_0$. Let A be as in [Proposition 2.9](#) and assume $P = (x_0 : y_0 : z_0 : w_0)$. Then A is given by $x_0^2 x^2 + y_0^2 y^2 + z_0^2 z^2 + w_0^2 w^2 = 0$. Suppose (c) holds. Then A is the cone over a nonsingular conic, and from $M_1, M_2 \subset A$ we conclude that $M_1 = M_2$ is the unique line on A through P and the vertex of A . This implies that the M_i are both tangent to both the C_i , so the second intersection point in $M_1 \cap C_2$ and $M_2 \cap C_1$ is again P , proving (a) and (b). Alternatively, we can verify the statement by direct calculation: we may assume $x_0 = 0$ by [Proposition 2.19](#). Substituting into [\(1\)](#) and using $-y_0^4 = z_0^4 + w_0^4$, we simplify $e_i(P)$ to $(0 : -y_0^5 z_0^4 w_0^4 : -y_0^4 z_0^5 w_0^4 : -y_0^4 z_0^4 w_0^5) = (0 : y_0 : z_0 : w_0)$. Conversely, fix $k \in \{1, 2\}$ and assume $e_k(P) = P$. If C_k were singular, then P and $e_k(P)$ would lie on nonintersecting components of C_k by [Proposition 2.18](#), so we conclude that C_k is nonsingular. By [Corollary 2.13](#) the divisor $4(P) = 3(P) + (e_k(P))$ on C_k is linearly equivalent to a hyperplane section H . Since

multiplication by 4 on the Jacobian of C_k has degree 16, there are exactly 16 points S on C_k for which $4S$ is linearly equivalent to H . By the implication (c) \Rightarrow (a) & (b), we can already account for all 16 of these points, namely the intersection points of the coordinate planes with C_k , as each of the 4 planes intersects C_k in 4 different points. This shows that P is one of these points, which proves (c). \square

Proposition 2.23. *Suppose that C_i is irreducible. Then the divisor $(e_i^2(P)) - (P)$ on C_i is linearly equivalent to $-2(e_i(P)) + 2(P)$.*

Proof. Let H denote the hyperplane class on C_i . By [Corollary 2.13](#) we have $3(S) + (e_i(S)) \sim H$ for any point S on C_i . Applying this to $S = P$ and $S = e_i(P)$, we obtain $3(P) + (e_i(P)) \sim 3(e_i(P)) + (e_i^2(P))$, from which the statement follows. \square

Remark 2.24. [Proposition 2.23](#) tells us that if we give C_i the structure of an elliptic curve with origin P , then we have $e_i^2(P) = -2e_i(P)$, and by induction we obtain $e_i^n(P) = a_n e_i(P)$ with $a_1 = 1$ and $a_{n+1} = -3a_n + 1$.

Corollary 2.25. *Assume that C_i is irreducible. Then the divisor $(e_i(P)) - (P)$ has order dividing 3 if and only if $e_i^2(P) = e_i(P)$.*

Proof. By [Proposition 2.23](#), the order divides 3 if and only if $e_i^2(P)$ is linearly equivalent to $e_i(P)$. This is equivalent to $e_i^2(P) = e_i(P)$, because two different points cannot be linearly equivalent on a curve of positive genus. \square

Our goal is to prove that the class of the divisor $(e_i(P)) - (P)$ on C_i is often of infinite order in the Jacobian of C_i . It turns out that this class is 2 times the class of a divisor that has a simple description.

Proposition 2.26. *Assume that C_i is nonsingular. Then the divisors $(e_i(P)) - (P)$ and $2(\sigma_u P) - 2(P)$ on C_i are linearly equivalent, where u is any of the coordinates on \mathbb{P}^3 .*

Proof. As this statement is purely geometric, we may assume $V = V'_0$. By [Proposition 2.19](#), we may assume that f_i is given by $(x : y : z : w) \mapsto (x^2 - z^2 : y^2 - w^2)$, and since A_4 acts transitively on the coordinates, also that $u = y$. Write $P = (x_0 : y_0 : z_0 : w_0)$. Adding $4(P)$ to both sides and using [Corollary 2.13](#) to identify $(e_i(P)) + 3(P)$ with the hyperplane class on C_i , we see that it is enough to find a hyperplane whose intersection with C_i is $2(P) + 2(\sigma_y(P))$. A straightforward calculation shows that the plane $(s^2 + t^2)(w_0x - x_0w) - (s^2 - t^2)(w_0z - z_0w)$ has this property, where $(s : t) = (x_0^2 - z_0^2 : y_0^2 - w_0^2)$ is the image of P under f_i . \square

Proposition 2.27. *Assume C_i to be irreducible. Then for any two coordinates u, v of \mathbb{P}^3 , the divisor $2(\sigma_{uv}(P)) - 2(P)$ on C_i is principal.*

Proof. Twice applying [Proposition 2.26](#) to $\sigma_u(P)$, once with the coordinate u and once with v , we see that the divisors $2(\sigma_{uv}(P)) - 2(\sigma_u(P))$ and $2(P) - 2(\sigma_u(P))$ are linearly equivalent. The result follows immediately. \square

Proposition 2.28. *Let $P = (x_0 : y_0 : z_0 : w_0)$ and $V = V'_0$. Let C_1 be the fibre through P of the fibration given by $(x : y : z : w) \mapsto (x^2 + z^2 : y^2 + w^2)$, and let C_2 be the other fibre. For $k = 1, 2$, we let E_k be the elliptic curve C_k with P as origin, provided that C_k is nonsingular. Let i denote a fixed square root of -1 . If C_1 is nonsingular, then the rational points of exact order 4 on E_1 are the $(\pm z_0 : \pm w_0 : \pm x_0 : \pm y_0)$ with three $+$ signs and one $-$ sign; the other points of exact order 4 are given by*

$$\begin{aligned} (w_0 : \pm i z_0 : \pm i y_0 : x_0), & \quad (-w_0 : \mp i z_0 : \pm i y_0 : x_0), \\ (y_0 : \pm i x_0 : \pm i w_0 : -z_0), & \quad (y_0 : \pm i x_0 : \mp i w_0 : z_0). \end{aligned}$$

If C_2 is nonsingular, then on E_2 , the $(\pm w_0, \pm z_0, \pm y_0, \pm x_0)$ with three $+$ signs and one $-$ sign are all the rational points of exact order 4; the others are given by

$$\begin{aligned} (\pm i z_0 : w_0 : \pm i x_0 : y_0), & \quad (\pm i z_0 : -w_0 : \mp i x_0 : y_0), \\ (\mp i y_0 : x_0 : \pm i w_0 : z_0), & \quad (\pm i y_0 : -x_0 : \pm i w_0 : z_0). \end{aligned}$$

In particular, for each $k \in \{1, 2\}$ there is a set S_k of 12 automorphisms of V'_0 defined over $\mathbb{Q}(i)$ such that, for R in an open subset of V'_0 , the class of the divisor $(e_k(R)) - (R)$ on the fibre of f_k through R is of exact order 4 if and only if $e_k(R) = \alpha(R)$ for some $\alpha \in S_k$.

Proof. One proof consists of finding a Weierstrass form for C_i , finding all 4-torsion points, and then pulling them back to our model. Instead, we show directly that for each S among the given points, the double $2S$ is one of the 2-torsion points $\sigma_{uv}(P)$ given in [Proposition 2.27](#). Take for instance the point $S = (z_0 : w_0 : x_0 : -y_0)$ on E_1 . The tangent plane to V at S is given by $l = 0$ with $l = z_0^3 x + w_0^3 y - x_0^3 z + y_0^3 w$. By [Corollary 2.13](#) this plane intersects C_1 with multiplicity 3 at S and multiplicity 1 at $e_1(S)$. One checks, for instance using [\(1\)](#), that the plane given by $m = 0$ with $m = z_0 w_0 (w_0 x - z_0 y) - x_0 y_0 (y_0 z + x_0 w)$ contains S and $e_1(S)$. It follows that the function $g = m/l$ on C_1 is regular everywhere, except perhaps for a double pole at S . Since C_1 is not contained in a plane, the function g is not constant. As C_1 has positive genus, the function g has more poles than just one simple pole, so g has exactly a double pole at S . Set $\lambda = g(P)$, then one easily checks that $g - \lambda$ also vanishes at $\sigma_{xz}(P)$, so we have $(g - \lambda) = P + \sigma_{xz}(P) - 2S$, which shows that on E_1 we have $2S = \sigma_{xz}(P)$, so by [Proposition 2.27](#), the point S has order exactly 4. The other points can be handled similarly. \square

The simplicity of the formulas in [Proposition 2.28](#) reflects the well-known fact that the Mordell–Weil groups of the Jacobians of these fibrations over $\mathbb{Q}(i)(t)$

are both isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$; see [Pjateckiĭ–Šapiro and Šafarevič 1971, paragraph 8].

Proposition 2.29. *Assume that P is defined over \mathbb{Q} and that all its coordinates are nonzero. If $(e_i(P)) - (P)$ is a torsion divisor class on C_i , its order is at most 4.*

Proof. Since the coordinates of P are all nonzero, the 2-torsion subgroup of the Mordell–Weil group of the Jacobian of C_i over \mathbb{Q} has order 4 by Proposition 2.27. By Mazur’s theorem [1977], the torsion subgroup of C_i is therefore $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2k\mathbb{Z}$ where $k \leq 4$. Accordingly, if $(e_i(P)) - (P)$ is torsion, then, since it is a multiple of 2 by Proposition 2.26, its order is at most 4. \square

Of course the order of $(e_i(P)) - (P)$ is 1 if and only if $e_i(P) = P$; that is, by Proposition 2.22, if and only if one of the coordinates of P is 0. In this case, P is fixed by both endomorphisms e_k , and the construction of this paper does not allow us to exhibit infinitely many rational points on V .

Proposition 2.30. *Assume that C_i is nonsingular. Then the exact order of the divisor $(e_i(P)) - (P)$ is 2 if and only if P lies on a line.*

Proof. Suppose that P lies on a line L . Then none of its coordinates is 0, as the intersection of any line with any coordinate plane is contained in Ω . By Proposition 2.22 this implies $e_i(P) \neq P$, so $e_i(P)$ and P are not linearly equivalent, as no two different points are linearly equivalent to each other on a curve of positive genus. The line L is a component of C_j with $j \neq i$, so by Proposition 2.18 we have $e_i(P) = \sigma_{uv}(P)$ for some coordinates u, v of \mathbb{P}^3 . By Proposition 2.27 we find immediately that $(e_i(P)) - (P)$ has order 2, thus proving one implication.

Note that each L of the 24 lines in the fibres of f_j intersect C_i in two points by Corollary 2.11, which are different by Lemma 2.8. This already gives 48 points S on C_i with $2(e_i(S)) \sim 2(S)$. By Proposition 2.22, the 16 intersection points of C_i with the coordinate planes also satisfy $2(e_i(S)) \sim 2(S)$, so that is 64 points total. Note that $3(S) + e_i(S)$ is linearly equivalent to a hyperplane section H on C_i for every point S on C_i by Corollary 2.13, so we have $2(e_i(S)) \sim 2(S)$ if and only if $8(S)$ is linearly equivalent to $2H$. Since multiplication by 8 on the Jacobian of C_i has degree 64, there are no points S with $8(S) \sim 2H$ other than the ones already described. This proves the converse. \square

3. Proof of the main theorem

Definition 3.1. Let k be a positive integer and $i \in \{1, 2\}$. Define T_{ki} to be the closure of the locus of points P on V for which C_i , the fibre of f_i through P , is nonsingular and where $(e_i(P)) - (P)$ is a divisor of exact order k on C_i .

In these terms, Proposition 2.22 states that $T_{11} = T_{12}$ is the intersection of V with the union of the coordinate planes. Likewise, in Proposition 2.30 we showed

that $T_{21} \cup T_{22}$ is contained in the union of the lines on V . Therefore, if a point P satisfies the hypotheses of our main theorem ([Theorem 1.1](#), repeated below as [Theorem 3.4](#)), it does not lie in T_{ki} for any $k, i \in \{1, 2\}$.

By [Corollary 2.25](#), we have that T_{3i} is the closure of $e_i^{-1}(T_{1i}) \setminus T_{1i}$. Now, T_{1i} consists of the intersections of the coordinate planes with V . Calling these X_1, X_2, X_3, X_4 , a straightforward computer calculation shows that $e_i^{-1}(X_j) = X_j \cup Y_{ij}$, where the Y_{ij} are geometrically irreducible. In other words, each T_{3i} is the union of four irreducible components. Also, as in [Proposition 2.28](#), the exact order of $e_i(P) - P$ is 4 if and only if $e_i(P) = \alpha(P)$, where α ranges over a certain set of 12 automorphisms. So T_{4i} is the union of 12 such curves, which are in fact geometrically irreducible.

Theorem 3.2. *The set T_{3i} is the union of geometrically irreducible curves of geometric genus 41, while T_{4i} is the union of geometrically irreducible curves of geometric genus 13.*

Proof. From the above, we can compute the T_{3i} and T_{4i} explicitly using any computer algebra package. Without loss of generality we assume that $V = V'_0$, given by $x^4 + y^4 = z^4 + w^4$, and that the fibration f_i is given by $(x : y : z : w) \mapsto (x^2 - z^2 : y^2 + w^2)$, so that in terms of [Proposition 2.28](#) we have $i = 2$. Then e_i is given by (1) with $N = 1$.

We first consider T_{4i} . Consider the automorphism $\alpha : V \rightarrow V$ given by $(x : y : z : w) \mapsto (-w : z : y : x)$, so that α is one of the 12 automorphisms of [Proposition 2.28](#) for which for any point $P \in U$ with $e_i(P) = \alpha(P)$, the divisor $(e_i(P)) - (P)$ has exact order 4 on the fiber of f_i through P . It is easily computed that the locus of such points is an irreducible curve D whose union with the skew quadrilateral $Q \subset V$ given by $w^2 + x^2 = y^2 - z^2 = 0$ is the degree-4 hypersurface section given by $yz(y^2 - z^2) = xw(x^2 + w^2)$. Note that a skew quadrilateral of lines has self-intersection 0 and intersects a hyperplane section with multiplicity 4. We deduce that the self-intersection D^2 equals 32, so that by the adjunction formula the arithmetic genus of D equals $\frac{1}{2}(D^2 + 2) = 17$. One also checks that D has four ordinary double points, namely at the singular points of Q . It follows that D has geometric genus $17 - 4 = 13$. The other components can be dealt with similarly, or by symmetry under the action of the group G_0 of [Definition 2.6](#).

For T_{3i} we consider the locus of points P for which $e_i(P)$ is contained in the coordinate plane $x = 0$. One checks that this locus is the union of this coordinate plane itself and an irreducible curve E whose union with the two disjoint skew quadrilaterals given by $x^2 - iy^2 = z^2 + iw^2 = 0$ and $x^2 + iy^2 = z^2 - iw^2 = 0$ is the degree-8 hypersurface section given by $x^2y^2(z^4 - w^4) = w^2z^2(x^4 + 3y^4)$. We deduce that the self-intersection E^2 equals 128, so that by the adjunction formula the arithmetic genus of E equals $\frac{1}{2}(E^2 + 2) = 65$. One also checks that E has an

ordinary double point at each of the 24 points of Ω of [Definition 2.7](#). It follows that E has geometric genus $65 - 24 = 41$. For the remaining coordinates we get three more isomorphic curves. \square

Proposition 3.3. *The intersection $(T_{31} \cup T_{41}) \cap (T_{32} \cup T_{42})$ does not contain any rational points outside the coordinate planes and the 48 lines on V .*

Proof. Suppose P is a rational point in the given intersection that is not on any of the coordinate planes, and set $Q = \iota_{a,b,c,d}(P) \in V_0$. Then the ratios of the fourth powers of the coordinates of Q are rational. By computer calculation, we will see that up to the action of G , there is only one such point on V_0 with this property. Working on V_0 , we intersect every component of T_{31} and T_{41} with every component of T_{32} and T_{42} , and remove extraneous points with one of the coordinates 0 or that lie on a line. Then we resolve these schemes into primary components over \mathbb{Q} . Since all of the intersections have dimension 0, we may use Magma to find all the $\overline{\mathbb{Q}}$ -points on these components. The only points for which the fourth powers of the coordinates have rational ratios are in the orbit under G (acting on V_0) of $(\eta : 1 : 1 : 1)$ with $\eta^4 = -3$, so Q is one of these points, defined over $\mathbb{Q}(i, \eta)$, where i denotes a square root of -1 , and P is its inverse image under $\iota_{a,b,c,d}$. Let $\alpha, \beta, \gamma, \delta$ be the fourth roots of a, b, c, d respectively that determine $\iota_{a,b,c,d}$, viewed as elements of a field $K = \mathbb{Q}(i, \alpha, \beta, \gamma, \delta, \eta)$. Fix an extension v_3 of the 3-adic valuation of \mathbb{Q} to K . Note that η is a uniformizer for v_3 ; we normalize so that $v_3(\eta) = 1$. Given a K -point $R = (r_0 : r_1 : r_2 : r_3)$ of V , let $v(R) = \sum_{i=0}^3 v_3(r_i)$ viewed as an element of $\mathbb{Z}/4\mathbb{Z}$. It is clear that $v(R)$ is well-defined, G -invariant, and 0 if R is defined over \mathbb{Q} . However, $v(P) = v_3(\eta/(\alpha\beta\gamma\delta))$, and from the fact that $abcd$ is a square it follows that $v_3(\alpha\beta\gamma\delta)$ is even. This is a contradiction, because $v_3(\eta) = 1$ and $v(P) = 0$. We conclude that such a P does not exist. \square

We are now ready to prove the main theorem, repeated here.

Theorem 3.4. *Let $a, b, c, d \in \mathbb{Q}^*$ be nonzero rational numbers with $abcd$ square. Let $P = (x_0 : y_0 : z_0 : w_0)$ be a rational point on $V_{a,b,c,d}$, and suppose that $x_0 y_0 z_0 w_0 \neq 0$ and that P does not lie on any of the 48 lines of the surface. Then the set of rational points of the surface is dense in both the Zariski and the real analytic topology.*

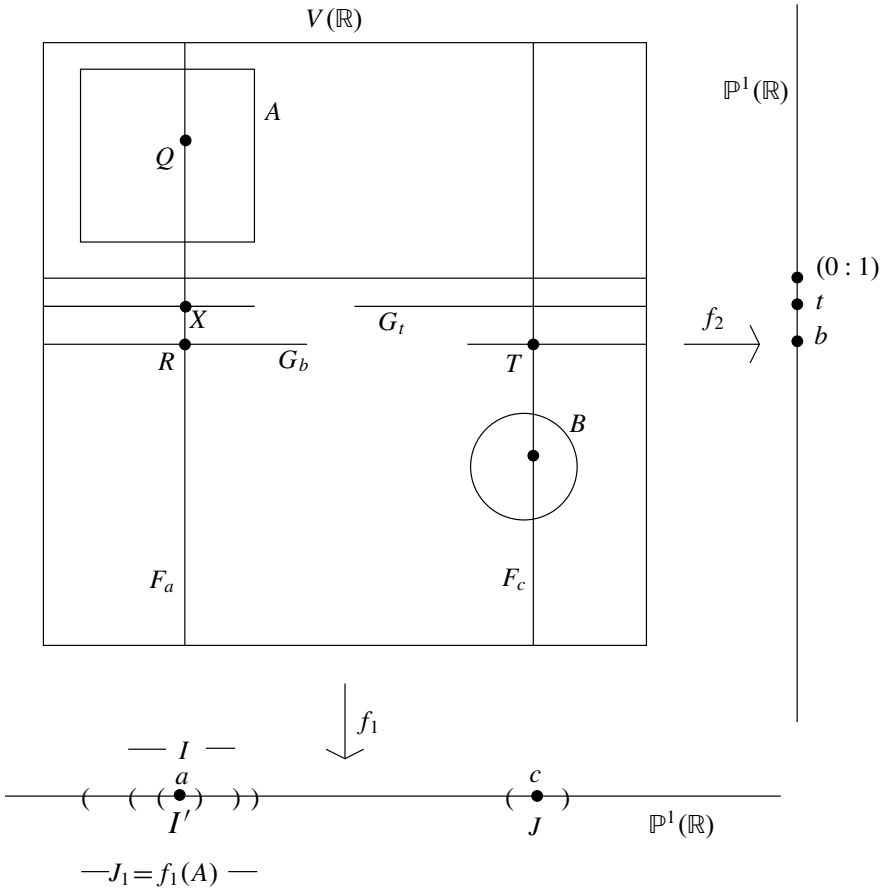
Proof. For $i = 1, 2$, let C_i denote the fibre of f_i through P , endowed with the structure of an elliptic curve with P as the origin. By assumption, $e_i(P)$ does not have order 1 or 2 on either C_i . That being so, [Proposition 3.3](#) assures us that for some i the order of $e_i(P)$ is infinite. Say (without loss of generality) that this i is 1. Then the subgroup S of $C_1(\mathbb{R})$ generated by $e_1(P)$ and the 2-torsion points is infinite and, in fact, dense in the real analytic topology. For each point Q in S , consider the divisor class $(e_2(Q)) - (Q)$ on the fibre of f_2 passing through Q . Its

order is 1 or 2 finitely often, by Propositions 2.22 and 2.30; by Theorem 3.2 it is 3 or 4 finitely often, because C_1 does not have genus 41 or 13 and so cannot be one of the curves on which the order of $(e_2(R)) - (R)$ is 3 or 4 for all R . In other words, there are only finitely many points Q in S for which the fibre of f_2 through Q contains only finitely many rational points. If $R \in S$ is not one of these finitely many points, then similarly the set of rational points on the fibre of f_2 through R is infinite and dense in the real analytic topology. Of course C_1 meets any fibre of f_2 in only finitely many points, so there are infinitely many distinct fibres of f_2 with infinitely many rational points. Zariski density follows.

Now we treat the real analytic topology. If a, b, c, d were all of the same sign, then $V = V_{a,b,c,d}$ would not have any real points, so we conclude that not all of them have the same sign. Since $abcd$ is a nonzero square, it is positive, so two of a, b, c, d are positive and two are negative. Without loss of generality, we assume that $a, d > 0$ and $b, c < 0$, and we choose real $\alpha, \beta, \gamma, \delta$ such that $\alpha^4 = a, \beta^4 = -b, \gamma^4 = -c$, and $\delta^4 = d$. Then over \mathbb{R} , one of the elliptic fibrations, say f_1 , is given by $(x : y : z : w) \mapsto (\alpha^2 x^2 - \beta^2 y^2 : \gamma^2 z^2 - \delta^2 w^2) = (\gamma^2 z^2 + \delta^2 w^2 : \alpha^2 x^2 + \beta^2 y^2)$, up to a linear automorphism of \mathbb{P}^1 . The fibration f_2 can be given by $(x : y : z : w) \mapsto (\alpha^2 x^2 - \beta^2 y^2 : \gamma^2 z^2 + \delta^2 w^2) = (\gamma^2 z^2 - \delta^2 w^2 : \alpha^2 x^2 + \beta^2 y^2)$. Let L be the line defined by $ax = \beta y$ and $\gamma z = \delta w$. Then L is contained in the fibre of f_2 above $(0 : 1)$ and it is easy to check that $L(\mathbb{R})$ maps surjectively to $f_1(V(\mathbb{R})) \subset \mathbb{P}^1(\mathbb{R})$.

We now show that there exists a nonempty open subset A of $V(\mathbb{R})$ in which the subset of rational points is dense. The locus of points on V where f_1 and f_2 do not give local parameters is of codimension 1. Since the set of rational points is Zariski dense, we can choose a rational point Q not on a line or a coordinate plane such that f_1 and f_2 give local parameters at Q . We choose Q such that the set of rational points on the fibre F of f_1 through Q is dense in $F(\mathbb{R})$ as well. Let $A \subset V(\mathbb{R})$ be an open neighbourhood of Q and $J_1, J_2 \subset \mathbb{P}^1(\mathbb{R})$ connected open subsets such that the map $f = (f_1, f_2) : A \rightarrow J_1 \times J_2$ is a homeomorphism. It suffices to show that $f(A \cap V(\mathbb{Q}))$ is dense in $J_1 \times J_2$. Set $s_i = f_i(Q)$, so that $f(Q) = (s_1, s_2)$. Choose $(r_1, r_2) \in J_1 \times J_2$. Since the rational points on F are dense in $F(\mathbb{R})$, following the proof of the density of rational points in the Zariski topology, we can choose a rational $t_2 \in J_2$, arbitrarily close to r_2 , such that $(s_1, t_2) = f(R)$ for some $R \in F(\mathbb{Q})$ for which the rational points in the fibre G of f_2 through R are dense. Therefore, there is a t_1 , arbitrarily close to r_1 , such that $(t_1, t_2) = f(T)$ for some $T \in G(\mathbb{Q})$. Since (t_1, t_2) can be chosen arbitrarily close to (r_1, r_2) , it follows that $V(\mathbb{Q}) \cap A$ is dense in A . The following diagram depicts the remainder of the argument.

Let $I \subset \mathbb{P}^1(\mathbb{R})$ be a nonempty connected open subset contained in $f_1(A) = J_1$. Suppose B is a nonempty open subset of $V(\mathbb{R})$ and let $J \subset \mathbb{P}^1(\mathbb{R})$ be a connected open subset contained in $f_1(B)$. Since $f_1(L) = f_1(f_2^{-1}((0 : 1)))$ contains I and J , for $t \in \mathbb{P}^1(\mathbb{R})$ close enough to $(0 : 1)$ the set $f_1(f_2^{-1}(t))$ intersects both I and J



nontrivially. Choose such a t close to $(0 : 1)$, let G_t denote the fibre $f_2^{-1}(t)$, and choose a nonempty connected open subset $I' \subset \mathbb{P}^1(\mathbb{R})$ contained in $I \cap f_1(G_t(\mathbb{R}))$. Since $V(\mathbb{Q}) \cap A$ is dense in A , we may choose $Q \in V(\mathbb{Q}) \cap A$ such that $a = f_1(Q)$ is contained in I' and the set of rational points on the fibre $F_a = f_1^{-1}(a)$ is dense in $F_a(\mathbb{R})$; moreover, such that the set S of those rational points R on F_a for which the set of rational points on the fibre of f_2 through R is dense, is itself dense in $F_a(\mathbb{R})$. Since $a \in I'$ is contained in $f_1(G_t(\mathbb{R}))$, there is an $X \in G_t(\mathbb{R})$ with $f_1(X) = a$, so we can find $R \in S \subset F_a(\mathbb{Q})$ such that R is arbitrarily close to X and thus $b = f_2(R)$ is arbitrarily close to t . Since $f_1(G_t(\mathbb{R}))$ intersects J nontrivially, we may choose R so close to X that also $f_1(G_b(\mathbb{R}))$ intersects J nontrivially, with $G_b = f_2^{-1}(b)$. Since the set of rational points on G_b is dense in $G_b(\mathbb{R})$, we can find a point $T \in G_b(\mathbb{Q})$ such that $c = f_1(T)$ is contained in J ; moreover, we can pick T so that the set of rational points on the fibre $F_c = f_1^{-1}(c)$ is dense in $F_c(\mathbb{R})$. Since $F_c(\mathbb{R})$ intersects B nontrivially and $F_c(\mathbb{Q})$ is dense in $F_c(\mathbb{R})$, we conclude

that B contains at least one rational point. Thus, any nonempty open subset of $V(\mathbb{R})$ contains at least one rational point, and we conclude that $V(\mathbb{Q})$ is dense in $V(\mathbb{R})$. \square

Remark 3.5. One might wonder about the possibility of proving that the rational points are dense in the p -adic topology as well as the real one. Sadly, the techniques of this paper are insufficient to prove this. To see this, note that our techniques start from a given rational point, and then move along fibres of the two fibrations to enter any given open set. In the p -adic topology, this is known to be impossible. For instance, there is an example of Swinnerton-Dyer, which is easy to verify, in which he shows that for the surface $x^4 + y^4 = 9z^4 + w^4$, every 3-adic point satisfies either $3|x/y$ or $3|y/x$, and all smooth fibres of each fibration contain only one of the two kinds of points.

It might be possible to prove something weaker using these techniques. For example, it might be possible to prove that there is some nonempty p -adic open set U on which the rational points are dense. We have not attempted to do this.

The second theorem from the introduction, also repeated here, follows almost immediately.

Theorem 3.6. *Let $a, b, c, d \in \mathbb{Q}^*$ be nonzero rational numbers with $abcd$ square and $a + b + c + d = 0$. Assume that no two of a, b, c, d sum to 0. Then the set of rational points of the surface $V_{a,b,c,d}$ is dense in both the Zariski and the real analytic topology.*

Proof. The surface $V_{a,b,c,d}$ contains the point $P = (1 : 1 : 1 : 1)$, which does not lie on a coordinate plane. Each of the 48 lines on V is contained in one of the sets $ax^4 + by^4 = 0$, $ax^4 + cz^4 = 0$, or $ax^4 + dw^4 = 0$. Since no two of a, b, c, d sum to zero, the point P does not lie on any of the lines. By [Theorem 1.1](#), the set of rational points of the surface is dense in both the Zariski and the real analytic topology. \square

Remark 3.7. [Theorem 1.2](#) is included to give a large family of surfaces for which we can prove unconditionally that the set of rational points is dense. Each surface $V = V_{a,b,c,d}$ with $a + b + c + d = 0$ contains the point $P = (1 : 1 : 1 : 1)$ and if $N^2 = abcd$, then V also contains the less trivial point $Q = (x : y : z : w)$ with

$$\begin{aligned} x &= (3bc + ad)(a + d) + 4N(b - c), \\ y &= (3ac + bd)(b + d) + 4N(c - a), \\ z &= (3ab + cd)(c + d) + 4N(a - b), \\ w &= -d(ab + ac + bc) - 9abc, \end{aligned} \tag{2}$$

which equals $e_i(P)$ for some $i \in \{1, 2\}$ by [\(1\)](#). [Theorem 1.2](#) appears weaker than [Theorem 1.1](#) because of the condition $a + b + c + d = 0$, but in fact [Theorem 1.1](#)

follows directly from [Theorem 1.2](#). Indeed, given a point $P' = (x_0 : y_0 : z_0 : w_0)$ on $V' = V_{a',b',c',d'}$, the map $(x : y : z : w) \mapsto (x_0^{-1}x : y_0^{-1}y : z_0^{-1}z : w_0^{-1}w)$ sends P' to $P = (1 : 1 : 1 : 1)$ and induces an isomorphism $\tau_{P'}$ from V' to $V = V_{a,b,c,d}$ with $a = a'x_0^4$, $b = b'y_0^4$, $c = c'z_0^4$, and $d = d'w_0^4$, satisfying $a + b + c + d = 0$. The point P' lies on a line in V' if and only if P lies on a line in V , which is the case if and only if two of a, b, c, d sum to 0. In a conversation, Andrew Granville reduced [\(1\)](#) to the equations in [\(2\)](#) and noted that the endomorphism e_i on V' can be recovered from these simpler formulas, as we have $e_i(P') = \tau_{P'}^{-1}(Q)$.

Remark 3.8. Without reference to the real analytic topology, [Theorem 1.1](#) and its proof also apply to rational function fields over \mathbb{Q} . Take, for instance, the function field $K = \mathbb{Q}(a, b, c)$, set $d = -a - b - c$, and define $L = K[x]/(x^2 - abcd)$. Then, as in [Theorem 1.2](#), we find that $V_{a,b,c,d}(L)$ is Zariski dense in $V_{a,b,c,d}$.

4. General number fields

[Theorem 1.1](#) does not generalize immediately to number fields, as Mazur's theorem does not either. Samir Siksek pointed out to us that one can prove the following statement for general number fields. Note that [Definition 2.3](#) applies to any number field.

Theorem 4.1. *There exists a Zariski open subset $U \subset V_{1,1,1,1}$, such that for each number field K there exists an integer n , such that for all $a, b, c, d \in K^*$ with $abcd \in K^{*2}$, if $\iota_{a,b,c,d}^{-1}(U) \subset V = V_{a,b,c,d}$ contains more than n points over K , then the set of K -rational points on V is Zariski dense.*

Proof. For each $P \in V$, let $o_i(P) \in \{1, 2, 3, \dots\} \cup \{\infty\}$ denote the order of $e_i(P)$ on the fibre of f_i through P with P as origin. We refer to $o_i(P)$ as the order of $e_i(P)$.

Recall that for any positive integer N , the curve $X_1(N)$ parametrizes pairs (E, P) , where E is an elliptic curve and P is a point of order N . The genus of $X_1(N)$ is at least 2 for $N = 13$ and $N \geq 16$ (see [[Ogg 1971](#), p. 109]). For the remaining N , that is, $N \in I := \{1, \dots, 12, 14, 15\}$, and $i \in \{1, 2\}$, let $T_{i,N}$ be the closure of the locus of all points P on $V_{1,1,1,1}$ such that $o_i(P) = N$. Let $U \subset V_{1,1,1,1}$ be the complement of the $T_{i,N}$, so that for all $P \in U$ we have $o_i(P) \notin I$.

Suppose K is a number field. By Merel's Theorem [[1996](#), Corollaire], there is an integer B , depending in fact only on the degree of K , such that any K -rational point of finite order on an elliptic curve over K has order at most B . Set

$$s = \sum_{\substack{N \leq B \\ N \notin I}} \#X_1(N)(K).$$

Note that s is well defined because for each N in the sum, the genus of $X_1(N)$ is at least 2, so $\#X_1(N)(K)$ is finite by Faltings' Theorem [1983]. We conclude that up to isomorphism over the algebraic closure of K , there are at most s elliptic curves over K containing a point of finite order $N \notin I$.

Take $a, b, c, d \in K^*$ with $abcd \in K^{*2}$, and let f_1, f_2 be the elliptic fibrations of $V = V_{a,b,c,d}$ over K as before. It is easy to check that the degree of the maps $j_i: \mathbb{P}^1 \rightarrow \mathbb{P}^1$ that send $t \in \mathbb{P}^1$ to the j -invariant of the fibre $f_i^{-1}(t)$ equals 24. Therefore there are at most $24s$ fibres of f_i , defined over K , of which the Jacobian contains a point over K of finite order $N \notin I$. Let $R = \sum_{k=1}^B k^2$, and take $n = 24sR$ and assume $U_{a,b,c,d} = \iota_{a,b,c,d}^{-1}(U)$ contains more than n points over K . Suppose that no fibre of f_1 contains more than R points of $U_{a,b,c,d}(K)$. Then there would at least be one point $P \in U_{a,b,c,d}(K)$ on a fibre of f_1 , say C , such that all K -rational torsion points on the Jacobian of C have order in I . From $P \in U_{a,b,c,d}$ we derive $o_i(P) \notin I$, so $e_i(P)$ has infinite order and C has infinitely many rational points. We conclude that there is a fibre of f_1 , say C_1 , with more than R points of $U_{a,b,c,d}(K)$. By Merel's Theorem, at least one of these points has infinite order, so that there are infinitely many K -rational points on C_1 .

As C_1 intersects $U_{a,b,c,d}$ nontrivially, infinitely many of these rational points Q lie in $U_{a,b,c,d}$, thus satisfying $o_2(Q) \notin I$. Since at most n points Q on V have finite order $o_2(Q) \notin I$ on the fiber of f_2 through Q , we get $o_2(Q) = \infty$ for infinitely many rational Q on C_1 . It follows that infinitely many fibres of f_2 contain infinitely many rational points, so the set of rational points is Zariski dense. \square

Acknowledgements

We thank Jean-Louis Colliot-Thélène, Samir Siksek, Andrew Granville, and Igor Dolgachev for useful discussions.

References

- [Bogomolov and Tschinkel 1999] F. Bogomolov and Y. Tschinkel, "On the density of rational points on elliptic fibrations", *Journ. Reine und Angew. Math.* **511** (1999), 87–93. MR 2000e:14025 Zbl 0916.14008
- [Bogomolov and Tschinkel 2000] F. Bogomolov and Y. Tschinkel, "Density of rational points on elliptic $K3$ surfaces", *Asian J. Math.* **4:2** (2000), 351–368. MR 2002b:14025 Zbl 0983.14008
- [Bright 2006] M. Bright, "Brauer groups of diagonal quartic surfaces", *J. Symbolic Comput.* **41:5** (2006), 544–558. MR 2007h:14022 Zbl 1129.14038
- [Bruin 2008] N. Bruin, "The arithmetic of Prym varieties in genus 3", *Compos. Math.* **144:2** (2008), 317–338. MR 2009f:11074 Zbl 1166.11022
- [Colliot-Thélène et al. 1998] J.-L. Colliot-Thélène, A. N. Skorobogatov, and P. Swinnerton-Dyer, "Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points", *Invent. Math.* **134:3** (1998), 579–650. MR 99k:11095 Zbl 0924.14011

- [Elkies 1988] N. Elkies, “On $A^4 + B^4 + C^4 = D^4$ ”, *Math. Comp.* **51**:184 (1988), 825–835. [MR 89h:11012](#) [Zbl 0698.10010](#)
- [Faltings 1983] G. Faltings, “Endlichkeitssätze für abelsche Varietäten über Zahlkörpern”, *Invent. Math.* **73**:3 (1983), 349–366. [MR 85g:11026a](#) [Zbl 0588.14026](#)
- [Harris and Tschinkel 2000] J. Harris and Y. Tschinkel, “Rational points on quartics”, *Duke Math J.* **104**:3 (2000), 477–500. [MR 2002h:14033](#) [Zbl 0982.14013](#)
- [Hassett 2003] B. Hassett, “Potential density of rational points on algebraic varieties”, pp. 223–282 in *Higher dimensional varieties and rational points* (Budapest, 2001), Bolyai Soc. Math. Stud. **12**, Springer, Berlin, 2003. [MR 2004j:14021](#) [Zbl 1092.14029](#)
- [Mazur 1977] B. Mazur, “Modular curves and the Eisenstein ideal”, *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186. [MR 80c:14015](#) [Zbl 0394.14008](#)
- [Merel 1996] L. Merel, “Bornes pour la torsion des courbes elliptiques sur les corps de nombres”, *Invent. Math.* **124**:1-3 (1996), 437–449. [MR 96i:11057](#) [Zbl 0936.11037](#)
- [Ogg 1971] A. P. Ogg, “Rational points of finite order on elliptic curves”, *Invent. Math.* **12** (1971), 105–111. [MR 45 #178](#) [Zbl 0216.05602](#)
- [Pjateckiĭ-Šapiro and Šafarevič 1971] I. I. Pjateckiĭ-Šapiro and I. R. Šafarevič, “Torelli’s theorem for algebraic surfaces of type K3”, *Izv. Akad. Nauk SSSR Ser. Mat.* **35** (1971), 530–572. In Russian. [MR 44 #1666](#)
- [Richmond 1944] H. W. Richmond, “On the Diophantine equation $F \equiv ax^4 + by^4 + cz^4 + dw^4 = 0$, the product $abcd$ being a square number”, *J. London Math. Soc.* **19** (1944), 193–194. [MR 7,244c](#) [Zbl 0060.09306](#)
- [Swinerton-Dyer 2000] H. P. F. Swinerton-Dyer, “Arithmetic of diagonal quartic surfaces, II”, *Proc. London Math. Soc.* (3) **80**:3 (2000), 513–544. [MR 2001d:11069](#) [Zbl 1066.11029](#)
- [Wittenberg 2007] O. Wittenberg, *Intersections de deux quadriques et pinceaux de courbes de genre 1/Intersections of two quadrics and pencils of curves of genus 1*, Lecture Notes in Mathematics **1901**, Springer, Berlin, 2007. [MR 2008b:14029](#) [Zbl 1122.14001](#)

Communicated by Jean-Louis Colliot-Thélène

Received 2008-12-27

Revised 2009-07-29

Accepted 2009-11-09

adam.m.logan@gmail.com

Centre de recherches mathématiques, Université de Montréal,
Case postale 6128, Succursale Centre-ville,
Montréal, QC H3C 3J7, Canada

dmckinno@math.uwaterloo.ca

Pure Mathematics Department, University of Waterloo,
Waterloo, ON N2L 3G1, Canada

rvl@math.leidenuniv.nl

Universiteit Leiden, Mathematisch Instituut, Postbus 9512,
2300 RA Leiden, Netherlands
<http://www.math.leidenuniv.nl/~rvl>

An Euler–Poincaré bound for equicharacteristic étale sheaves

Carl A. Miller

The Grothendieck–Ogg–Shafarevich formula expresses the Euler characteristic of an étale sheaf on a characteristic- p curve in terms of local data. The purpose of this paper is to prove an equicharacteristic version of this formula (a bound, rather than an equality). This follows work of R. Pink.

The basis for the proof of this result is the characteristic- p Riemann–Hilbert correspondence, which is a functorial relationship between two different types of sheaves on a characteristic- p scheme. In the paper we prove a one-dimensional version of this correspondence, considering both local and global settings.

1. Introduction

Let k be an algebraically closed field of characteristic $p > 0$. Let Y be a smooth projective k -curve, and let N be a constructible étale sheaf of \mathbb{F}_p -vector spaces on Y . We are concerned with computing the sizes of cohomology groups of the pair (Y, N) .

The following theorem (the Grothendieck–Ogg–Shafarevich formula) provides a starting point. For any étale \mathbb{F}_ℓ -sheaf M on Y , where ℓ denotes a prime different from p , let $\chi(Y, M)$ denote the Euler characteristic of M . (That is, $\chi(Y, M) = \sum_{i=0}^2 (-1)^i \dim_{\mathbb{F}_\ell} H^i(Y, M)$.)

Theorem 1.0.1. *Let ℓ be a prime which is not equal to p . Let G be a constructible \mathbb{F}_ℓ -sheaf on Y such that:*

- (1) G is locally constant on some open subcurve $Y' \subseteq Y$, and
- (2) $G_y = \{0\}$ for all points $y \in Y \setminus Y'$.

Then,

$$\chi(Y, G) = (2 - 2g)m - \sum_{y \in Y \setminus Y'} (m + \text{Sw}_y(G)), \quad (1.0.2)$$

MSC2000: primary 14F20; secondary 13A35, 14F30.

Keywords: characteristic- p curves, Grothendieck–Ogg–Shafarevich formula, étale sheaves, Riemann–Hilbert correspondence, Frobenius endomorphism, minimal roots.

The author was supported by NSF grant DMS-0502170 during the publication of this paper.

where g denotes the genus of Y and $m = \text{rank } G$.

In Equation (1.0.2), $\text{Sw}_y(G)$ denotes a local invariant called the ‘‘Swan conductor.’’ (See [Raynaud 1995] for a discussion of this formula.)

It is desirable to have a similar formula for the Euler characteristic of an \mathbb{F}_p -sheaf on Y . Unfortunately the equicharacteristic case presents some difficulties. It is possible to construct two \mathbb{F}_p -sheaves N_1 and N_2 on the same curve Y , both sharing the same rank and the same local data but possessing different Euler characteristics. (See Example 3.2.9.)

So an exact analogue of Theorem 1.0.1 is not possible. The purpose of this paper is to prove a *lower bound* for $\chi(Y, N)$ which matches the form of (1.0.2). This builds on previous work of R. Pink [2000].

The proof of the lower bound is based on the relationship between equicharacteristic étale sheaves and coherent \mathbb{O}_Y -modules. We will explain briefly the central ideas in the proof and then state the main result.

Let \mathcal{M} be a coherent \mathbb{O}_Y -module which has a Frobenius-linear endomorphism $\phi: \mathcal{M} \rightarrow \mathcal{M}$. Then the subsheaf $\mathcal{M}^\phi \subseteq \mathcal{M}$ is a constructible \mathbb{F}_p -étale sheaf on Y . There is an exact sequence

$$0 \longrightarrow \mathcal{M}^\phi \longrightarrow \mathcal{M} \xrightarrow{1-\phi} \mathcal{M} \longrightarrow 0. \quad (1.0.3)$$

This exact sequence determines a long exact sequence of cohomology groups. The long exact sequence can be used to prove

$$\chi(Y, \mathcal{M}^\phi) \geq \chi(Y, \mathcal{M}). \quad (1.0.4)$$

This allows us to use results from coherent cohomology to study the Euler characteristic $\chi(Y, \mathcal{M}^\phi)$. (This is an idea that is used in [Pink 2000].)

So, a general lower bound on $\chi(Y, N)$ is possible if there exists a canonical way to construct an exact sequence in the form of (1.0.3) for N . This paper offers such a canonical construction. The construction is based on the characteristic- p ‘‘Riemann–Hilbert’’ correspondence of M. Emerton and M. Kisin [2004].

Let

$$\mathcal{N} = \mathcal{H}om_{\mathbb{F}_p} (N, \mathbb{O}_Y). \quad (1.0.5)$$

This sheaf is a quasicoherent \mathbb{O}_Y -module. Also, the p th-power map on \mathbb{O}_Y induces a Frobenius-linear endomorphism $\mathcal{N} \rightarrow \mathcal{N}$. In the notation of [Emerton and Kisin 2004], \mathcal{N} is a left $\mathbb{O}_{F,Y}$ -module. The sheaf N can be recovered (except for sections with punctual support) from the sheaf \mathcal{N} . (See Theorem 2.3.11 in this paper.)

The sheaf \mathcal{N} possesses special submodules which are called *roots*. A root of \mathcal{N} is a coherent \mathbb{O}_Y -submodule $\mathcal{N}' \subseteq \mathcal{N}$ which satisfies some special properties (see Definition 2.1.3). The concept of a root is due to G. Lyubeznik [1997]. The special

properties of a root imply in particular the existence of an exact sequence

$$0 \longrightarrow N \longrightarrow (\mathcal{N}')^\vee \longrightarrow (\mathcal{N}')^\vee \longrightarrow 0, \quad (1.0.6)$$

where $(\mathcal{N}')^\vee$ denotes the coherent sheaf dual of \mathcal{N}' . Thus the Euler characteristic of N is related to the Euler characteristics of the roots of \mathcal{N} . In this paper we show that the sheaf \mathcal{N} possesses a canonical minimal root, \mathcal{N}_0 , and that the Euler characteristic of \mathcal{N}_0 can be computed from local information about the sheaf N .¹ Inequality (1.0.4) thus gives a lower bound on $\chi(Y, N)$. The following theorem is the result:

Theorem 1.0.7. *Let N be a constructible \mathbb{F}_p -étale sheaf on Y whose sections all have open support. Then*

$$\chi(Y, N) \geq (1 - g)(\text{rank } N) - \sum_{y \in Y} \mathfrak{C}(N_{(y)}). \quad (1.0.8)$$

(See Corollary 3.1.18.) In (1.0.8), the expression $\mathfrak{C}(N_{(y)})$ denotes a local invariant which is called the *minimal root index* of N at y .

In this paper we present a proof of the above theorem using the characteristic- p Riemann–Hilbert correspondence (a functorial relationship between $\mathbb{O}_{F,Y}$ -modules and \mathbb{F}_p -étale sheaves). This correspondence is developed in full generality in [Emerton and Kisin 2004]. Since we prefer to avoid the language of derived categories, we will not make direct use of the results from that paper. Instead we prove a miniature version of the correspondence which applies to curves. Our version includes both a local and global version of the Riemann–Hilbert correspondence, as well as functors relating the two. (See Theorems 2.3.11, 2.3.16, and 4.3.1.)

The body of the paper is divided into three sections. Section 2 develops basic theory for the study of $\mathbb{O}_{F,X}$ -modules and gives the statement of the characteristic- p Riemann–Hilbert correspondence. Section 3 proves the main result and offers some examples. It is shown in Section 3.3 that the main result is compatible with the previous results of Pink [2000]. Finally, Section 4 gives the full proof of the Riemann–Hilbert correspondence in dimension one.

1.1. Notation and conventions. Throughout this paper, let p denote a prime and let r denote a positive integer. Let k be an algebraically closed field of characteristic p . Let \mathbb{F}_{p^r} denote a finite field of p^r elements. Fix an embedding $\mathbb{F}_{p^r} \hookrightarrow k$.

All sheaves are assumed to be sheaves on an étale site. Thus, if X is a k -scheme, then \mathbb{O}_X denotes the étale structure sheaf of X . If x is a k -point of X , then $\mathbb{O}_{X,x}$ denotes the étale stalk of \mathbb{O}_X at x .

¹We note that the existence of canonical minimal roots was recently proved, independently, in a much broader context. See [Blickle 2008].

If X is a k -scheme, x is a closed point of X , and Q is an étale sheaf on X , then $Q_{(x)}$ denotes the pullback of Q via the morphism

$$\mathrm{Spec} \mathbb{O}_{X,x} \rightarrow X. \quad (1.1.1)$$

If X is a k -scheme and \mathcal{R} is a sheaf of rings on X , then $\mathbf{Mod}(X, \mathcal{R})$ denotes the category of sheaves of left \mathcal{R} -modules on X .

If S is a k -algebra, let $F_S: S \rightarrow S$ denote the Frobenius map. If X is a k -scheme, let $F_X: X \rightarrow X$ denote the Frobenius endomorphism.

All schemes are assumed to be Noetherian and separated.

2. Unit $\mathbb{O}_{F^r, X}$ -modules

This section covers some preliminaries. The central objects of concern are quasi-coherent sheaves that have Frobenius-linear endomorphisms. Following [Emerton and Kisin 2004], we consider these sheaves as modules over a particular sheaf of noncommutative rings (namely, $\mathbb{O}_{F^r, X}$).

2.1. Definitions. Let S be a k -algebra. Then $S[F^r]$ denotes the twisted polynomial algebra over S determined by the r th Frobenius endomorphism $F_S^r: S \rightarrow S$. Elements of $S[F^r]$ are thus finite sums of the form

$$\sum_{i \geq 0} s_i F^{ri}, \quad (2.1.1)$$

with $s_i \in S$, and multiplication is expressed by the rule $F^r s = s^{p^r} F^r$.

Likewise, let Z denote a k -scheme. Then $\mathbb{O}_{F^r, Z}$ denotes the sheaf of twisted polynomial rings determined by the r th Frobenius endomorphism of \mathbb{O}_Z . If $U \subseteq Z$ is any open subset, then $\mathbb{O}_{F^r, Z}(U) \cong \mathbb{O}_Z(U)[F^r]$.

A left $\mathbb{O}_{F^r, Z}$ -module is simply an \mathbb{O}_Z -module \mathcal{N} equipped with an endomorphism $\phi: \mathcal{N} \rightarrow \mathcal{N}$ satisfying the condition

$$\phi(fn) = f^{p^r} \phi(n) \quad \text{for any } U \subseteq Z, f \in \mathbb{O}_Z(U), n \in \mathcal{N}(U). \quad (2.1.2)$$

(The map ϕ is determined by the left-action of F^r .) This condition can be compactly expressed by saying that ϕ induces an \mathbb{O}_Z -linear morphism $F_Z^{r*} \mathcal{N} \rightarrow \mathcal{N}$.

Now we introduce some terminology from [Emerton and Kisin 2004]. If \mathcal{N} is a left $\mathbb{O}_{F^r, Z}$ -module, we call the morphism $F_Z^{r*} \mathcal{N} \rightarrow \mathcal{N}$ the *structural morphism* of \mathcal{N} . A *unit $\mathbb{O}_{F^r, Z}$ -module* is a left $\mathbb{O}_{F^r, Z}$ -module whose \mathbb{O}_Z -module structure is quasi-coherent and whose structural morphism is an isomorphism. A unit $\mathbb{O}_{F^r, Z}$ -module is a *locally finitely-generated unit (lfgu) $\mathbb{O}_{F^r, Z}$ -module* if, additionally, it is finitely-generated as a left $\mathbb{O}_{F^r, Z}$ -module on any affine open subset of Z .

Let $\mathbf{Mod}^u(Z, \mathbb{O}_{F^r, Z})$ and $\mathbf{Mod}^{lfgu}(Z, \mathbb{O}_{F^r, Z})$ denote, respectively, the full subcategories of $\mathbf{Mod}(Z, \mathbb{O}_{F^r, Z})$ consisting of the unit and lfgu $\mathbb{O}_{F^r, Z}$ -modules.

An lfgu $\mathbb{C}_{F^r, Z}$ -module is not necessarily coherent, but it must have a coherent \mathbb{C}_Z -submodule which generates it under the action of F^r . The following definition identifies a special class of coherent generators for an lfgu $\mathbb{C}_{F^r, Z}$ -module. The definition is due to Lyubeznik.

Definition 2.1.3. *Let Z be a k -scheme, and let \mathcal{N} be a unit $\mathbb{C}_{F^r, Z}$ -module. An \mathbb{C}_Z -submodule $\mathcal{N}' \subseteq \mathcal{N}$ is a root if*

- (1) *the \mathbb{C}_Z -module \mathcal{N}' is coherent,*
- (2) *the \mathbb{C}_Z -submodule of \mathcal{N} generated by $F^r(\mathcal{N}')$ contains \mathcal{N}' , and*
- (3) *as a left $\mathbb{C}_{F^r, Z}$ -module, \mathcal{N} is generated by \mathcal{N}' .*

Proposition 2.1.4. *Let W be a smooth irreducible k -scheme, and let \mathcal{P} be an lfgu $\mathbb{C}_{F^r, Z}$ -module. Then \mathcal{P} has a root.*

Proof. See [Emerton and Kisin 2004, Theorem 6.1.3]. □

Suppose that W and \mathcal{P} are as in the above proposition. Then the existence of a root for \mathcal{P} allows us to express \mathcal{P} as a union of coherent subsheaves. Let \mathcal{P}_0 be a root for \mathcal{P} , and let \mathcal{P}_i denote the \mathbb{C}_Z -submodule of \mathcal{P} generated by $F^{ri}(\mathcal{P}_0)$. The root properties imply that the subsheaves \mathcal{P}_i form an ascending sequence

$$\mathcal{P}_0 \subseteq \mathcal{P}_1 \subseteq \mathcal{P}_2 \subseteq \cdots \quad (2.1.5)$$

and $\bigcup \mathcal{P}_i = \mathcal{P}$.

Also, since we have assumed that W is *smooth*, some stronger statements can be made. The flatness of the Frobenius morphisms $F_W^{ri} : W \rightarrow W$ implies that there are injections $F_W^{ri*}\mathcal{P}_0 \rightarrow F_W^{ri*}\mathcal{P}$. Restricting the structural isomorphisms $F_W^{ri*}\mathcal{P} \rightarrow \mathcal{P}$ via these injections yields isomorphisms $F_W^{ri*}\mathcal{P}_0 \rightarrow \mathcal{P}_i$. These isomorphisms imply that all terms in the sequence (2.1.5) have the same generic rank. In particular, since \mathcal{P}_0 and \mathcal{P}_1 have the same generic rank, they concur on some dense open subset $U \subseteq W$. The filtration (2.1.5) therefore collapses:

$$\mathcal{P}_{0|U} = \mathcal{P}_{1|U} = \mathcal{P}_{2|U} = \cdots \quad (2.1.6)$$

We have proved the following useful proposition.

Proposition 2.1.7. *Let W be a smooth irreducible k -scheme, and let \mathcal{P} be an lfgu $\mathbb{C}_{F^r, W}$ -module. There must exist a dense open subset $U \subseteq W$ on which \mathcal{P} is coherent.*

The same reasoning applied to one-point schemes also proves the following:

Proposition 2.1.8. *Let L be a field of characteristic p , and let V be a finitely-generated unit $L[F^r]$ -module. Then V is finite-dimensional over L .*

2.2. The minimal root. We will focus now on one-dimensional schemes. Let Y denote a smooth projective k -curve.

Proposition 2.2.1. *Let \mathcal{N} be an lfgu $\mathbb{O}_{Fr,Y}$ -module. Let \mathcal{N}_0 be a root for \mathcal{N} which has minimal degree (as a coherent sheaf). Then \mathcal{N}_0 is contained in every other root of \mathcal{N} .*

Proof. Suppose that \mathcal{N}'_0 is another root for \mathcal{N} . Let $\mathcal{N}''_0 = \mathcal{N}'_0 \cap \mathcal{N}_0$. I claim that \mathcal{N}''_0 is also a root for \mathcal{N} . This can be seen as follows: let $\{\mathcal{N}_i\}_{i=0}^\infty$, $\{\mathcal{N}'_i\}_{i=0}^\infty$, and $\{\mathcal{N}''_i\}_{i=0}^\infty$ denote the induced filtrations for \mathcal{N} (described in Section 2.1). For any i , the module \mathcal{N}''_i is the image under the isomorphism

$$F_Y^{ri*}\mathcal{N} \rightarrow \mathcal{N} \quad (2.2.2)$$

of $F_Y^{ri*}(\mathcal{N}_0 \cap \mathcal{N}'_0)$. By the flatness of the Frobenius morphism,

$$F_Y^{ri*}(\mathcal{N}_0 \cap \mathcal{N}'_0) = (F_Y^{ri*}\mathcal{N}_0) \cap (F_Y^{ri*}\mathcal{N}'_0). \quad (2.2.3)$$

This equality implies that $\mathcal{N}''_i = \mathcal{N}_i \cap \mathcal{N}'_i$. The root properties for \mathcal{N}''_0 follow immediately from this fact. Therefore \mathcal{N}''_0 is indeed a root. Since \mathcal{N}''_0 is contained in \mathcal{N}_0 and its degree cannot be any smaller than that of \mathcal{N}_0 , we must have $\mathcal{N}_0 = \mathcal{N}''_0$. This proves the proposition. \square

We will refer to the root of minimal degree simply as the “minimal root” of the lfgu $\mathbb{O}_{Fr,Y}$ -module. The minimal root also has a local description, which we now construct. Note that for any unit $\mathbb{O}_{Fr,Y}$ -module \mathcal{N} , the stalk \mathcal{N}_y at any closed point y is a unit $\mathbb{O}_{Y,y}[F^r]$ -module. If \mathcal{N}_0 is a root of \mathcal{N} , then $(\mathcal{N}_0)_y$ is a root of \mathcal{N}_y . We define an invariant for these local roots.

Definition 2.2.4. *Let (A, \mathfrak{m}) be a Henselian DVR of characteristic p with $A/\mathfrak{m} \cong k$. Let Q be a finitely-generated unit $A[F^r]$ -module, and let $Q_0 \subseteq Q$ be a root for Q . Let $Q_1 \subseteq Q$ denote the A -submodule generated by $F^r(Q_0)$. Then the F^r -index of Q_0 is*

$$\frac{\dim_k Q_1/Q_0}{p^r - 1}. \quad (2.2.5)$$

Proposition 2.2.6. *Let (A, \mathfrak{m}) be a Henselian DVR of characteristic p with $A/\mathfrak{m} \cong k$. Let Q be a finitely-generated unit $A[F^r]$ -module. Then Q has a unique minimal root which is contained in every other root.*

Proof. This is a special case of [Blickle 2004, Theorem 2.10]. Alternatively, one can use Definition 2.2.4. Let $Q_0 \subseteq Q$ be the root with the smallest F^r -index. Then Q_0 must be contained in every other root by an argument similar to the proof of Proposition 2.2.1. \square

Definition 2.2.7. Let A and Q be defined as in [Definition 2.2.4](#). Then the minimal root index of Q (denoted $\mathfrak{C}(Q)$) is the F^r -index of the unique minimal root of Q .

We note the following basic proposition. The proof is elementary and is left to the reader.

Proposition 2.2.8. Let (A, \mathfrak{m}) be a Henselian DVR with $A/\mathfrak{m} \cong k$, and let Q be a unit $A[F^r]$ -module which is finitely-generated over A . Then the only root of Q is Q itself. The minimal root index of Q is 0.

Using [Proposition 2.2.6](#), we can characterize global minimal roots by their stalks:

Proposition 2.2.9. Let \mathcal{N} be an lfgu $\mathbb{O}_{F^r, Y}$ -module, and let \mathcal{N}_0 be the minimal root for \mathcal{N} . Then for any closed point $y \in Y$, the stalk $(\mathcal{N}_0)_y$ is the unique minimal root of \mathcal{N}_y .

Proof. This follows easily using [Proposition 2.1.7](#). Let $V \subseteq Y$ be a nonempty open subcurve on which \mathcal{N} is coherent. Then a coherent subsheaf $\mathcal{N}'_0 \subseteq \mathcal{N}$ is a root if and only if both of the following properties hold:

- (1) $(\mathcal{N}'_0)|_V = \mathcal{N}|_V$, and
- (2) $(\mathcal{N}'_0)_y$ is a root of \mathcal{N}_y for every $y \in Y \setminus V$.

The minimal root \mathcal{N}_0 is simply the root which has a minimal stalk at every point of $Y \setminus V$. \square

The compatibility of local and global minimal roots implies an important numerical relationship. Let \mathcal{N} be an lfgu $\mathbb{O}_{F^r, Y}$ -module and $\mathcal{N}_0 \subseteq \mathcal{N}$ be its minimal root. Let $\mathcal{N}_1 \subseteq \mathcal{N}$ denote the \mathbb{O}_Y -submodule generated by $F^r(\mathcal{N}_0)$. Then $\mathcal{N}_0/\mathcal{N}_1$ is a skyscraper sheaf whose stalk-dimension at any point y is equal to $(p^r - 1)\mathfrak{C}(\mathcal{N}_y)$. Therefore

$$\deg \mathcal{N}_1 = \deg \mathcal{N}_0 + (p^r - 1) \sum_{y \in Y} \mathfrak{C}(\mathcal{N}_y). \quad (2.2.10)$$

On the other hand, the isomorphism $F_Y^{r*} \mathcal{N}_0 \cong \mathcal{N}_1$ implies

$$\deg \mathcal{N}_1 = p^r \cdot \deg \mathcal{N}_0. \quad (2.2.11)$$

Combining these two equalities yields

$$\deg \mathcal{N}_0 = \sum_{y \in Y} \mathfrak{C}(\mathcal{N}_y). \quad (2.2.12)$$

This formula will be important in [Section 3](#).

2.3. Unit $\mathbb{O}_{F,X}$ -modules and étale sheaves. We continue to let Y denote a smooth projective k -curve. Let \mathcal{N} be an lfgu $\mathbb{O}_{Fr,Y}$ -module. Then the sheaf

$$\mathcal{H}om_{\mathbb{O}_{Fr,Y}}(\mathcal{N}, \mathbb{O}_Y) \quad (2.3.1)$$

has the structure of an étale sheaf of \mathbb{F}_{p^r} -vector spaces on Y . Thus there is a functor

$$\mathcal{H}om_{\mathbb{O}_{Fr,Y}}(\cdot, \mathbb{O}_Y) : \mathbf{Mod}^{f.u.}(Y, \mathbb{O}_{Fr,Y}) \rightarrow \mathbf{Mod}(Y, \mathbb{F}_{p^r}). \quad (2.3.2)$$

This functor has an alternative expression in terms of roots. Let \mathcal{N}_0 be a root for \mathcal{N} . Let \mathcal{N}_0^\vee be the coherent sheaf dual for \mathcal{N}_0 . There is a natural left $\mathbb{O}_{Fr,Y}$ -module structure on the sheaf \mathcal{N}_0^\vee , which can be described as follows. Let $\mathcal{N}_0 \subseteq \mathcal{N}_1 \subseteq \mathcal{N}_2 \subseteq \dots \subseteq \mathcal{N}$ denote the filtration induced by \mathcal{N}_0 . For any homomorphism $\phi : \mathcal{N}_0 \rightarrow \mathbb{O}_Y$, let $F^r(\phi) \in \mathcal{N}_0^\vee$ be the composition

$$\begin{array}{ccc} \mathcal{N}_0 & \longrightarrow & \mathcal{N}_1 & & \mathbb{O}_Y \\ & & \downarrow \cong & & \uparrow \cong \\ & & F_Y^{r*} \mathcal{N}_0 & \xrightarrow{F_Y^{r*}(\phi)} & F_Y^{r*} \mathbb{O}_Y \end{array} \quad (2.3.3)$$

This assignment makes \mathcal{N}_0^\vee a coherent (not necessarily unit) left $\mathbb{O}_{Fr,Y}$ -module.

Consider the restriction map

$$\mathcal{H}om_{\mathbb{O}_{Fr,Y}}(\mathcal{N}, \mathbb{O}_Y) \rightarrow \mathcal{H}om_{\mathbb{O}_Y}(\mathcal{N}_0, \mathbb{O}_Y) (= \mathcal{N}_0^\vee). \quad (2.3.4)$$

Sections in the image of this map arise from Frobenius invariant morphisms from \mathcal{N} to \mathbb{O}_Y , and are therefore invariant under the action of F^r on \mathcal{N}_0^\vee . Thus restriction actually determines a map

$$\mathcal{H}om_{\mathbb{O}_{Fr,Y}}(\mathcal{N}, \mathbb{O}_Y) \rightarrow (\mathcal{N}_0^\vee)^{F^r}. \quad (2.3.5)$$

On the other hand, suppose that $\psi : \mathcal{N}_0 \rightarrow \mathbb{O}_Y$ is a homomorphism which is invariant under F^r . Then ψ determines a series of maps

$$\mathcal{N}_i \longrightarrow F_Y^{ri*} \mathcal{N}_0 \xrightarrow{F_Y^{ri*}(\psi)} \mathbb{O}_Y, \quad i = 0, 1, 2, \dots \quad (2.3.6)$$

which are all compatible. Taken together these determine a homomorphism $\mathcal{N} \rightarrow \mathbb{O}_Y$ which is $\mathbb{O}_{Fr,Y}$ -linear. This association is an inverse to (2.3.5), and thus we see that there is in fact an isomorphism,

$$\mathcal{H}om_{\mathbb{O}_{Fr,Y}}(\mathcal{N}, \mathbb{O}_Y) \cong (\mathcal{N}_0^\vee)^{F^r}. \quad (2.3.7)$$

So, the sheaf $\mathcal{H}om_{\mathbb{O}_{Fr,Y}}(\mathcal{N}, \mathbb{O}_Y)$ can be identified with a subsheaf of the coherent \mathbb{O}_X -module \mathcal{N}_0^\vee .

The relationship between étale sheaves of \mathbb{F}_{p^r} -vector spaces and lfgu $\mathbb{O}_{Fr, Y}$ -modules can be more fully understood with the addition of a second functor. Let N be a sheaf of \mathbb{F}_{p^r} -vector spaces on Y . Then the sheaf of \mathbb{O}_Y -modules

$$\mathcal{H}om_{\mathbb{F}_{p^r}}(N, \mathbb{O}_Y) \quad (2.3.8)$$

has a natural structure of a left $\mathbb{O}_{Fr, Y}$ -module given by the Frobenius endomorphism of \mathbb{O}_Y . Thus there is a functor

$$\mathcal{H}om_{\mathbb{F}_{p^r}}(\cdot, \mathbb{O}_Y) : \mathbf{Mod}(Y, \mathbb{F}_{p^r}) \rightarrow \mathbf{Mod}(Y, \mathbb{O}_{Fr, Y}). \quad (2.3.9)$$

If \mathcal{N} is the lfgu $\mathbb{O}_{Fr, Y}$ -module from above, then the sheaf

$$\mathcal{N}'' := \mathcal{H}om_{\mathbb{F}_{p^r}}(\mathcal{H}om_{\mathbb{O}_{Fr, Y}}(\mathcal{N}, \mathbb{O}_Y), \mathbb{O}_Y) \quad (2.3.10)$$

is a left $\mathbb{O}_{Fr, Y}$ -module. There is also a natural “double-dual” homomorphism $\mathcal{N} \rightarrow \mathcal{N}''$. The functors $\mathcal{H}om_{\mathbb{O}_{Fr, Y}}(\cdot, \mathbb{O}_Y)$ and $\mathcal{H}om_{\mathbb{F}_{p^r}}(\cdot, \mathbb{O}_Y)$ are the basis for the characteristic- p Riemann–Hilbert correspondence.

We quote here (for use in [Section 3](#)) three results which summarize the Riemann–Hilbert correspondence on a curve. The first two results are proved in [Section 4.2](#). The third result follows from the first via isomorphism [\(2.3.7\)](#).

The Riemann–Hilbert correspondence on Y is an equivalence between two categories: the category of torsion-free lfgu $\mathbb{O}_{Fr, Y}$ -modules, and the category of constructible \mathbb{F}_{p^r} -sheaves on Y in which all sections have open support.

Theorem 2.3.11. *Let \mathcal{N} be an lfgu $\mathbb{O}_{Fr, Y}$ -module which is torsion-free as an \mathbb{O}_Y -module. Then the sheaf*

$$\mathcal{H}om_{\mathbb{O}_{Fr, Y}}(\mathcal{N}, \mathbb{O}_Y) \quad (2.3.12)$$

is a constructible \mathbb{F}_{p^r} -sheaf in which all sections have open support. The double-dual homomorphism

$$\mathcal{N} \rightarrow \mathcal{H}om_{\mathbb{F}_{p^r}}(\mathcal{H}om_{\mathbb{O}_{Fr, Y}}(\mathcal{N}, \mathbb{O}_Y), \mathbb{O}_Y) \quad (2.3.13)$$

is an isomorphism.

Let N be a constructible \mathbb{F}_{p^r} -étale sheaf on Y in which all sections have open support. Then the sheaf

$$\mathcal{H}om_{\mathbb{F}_{p^r}}(N, \mathbb{O}_Y) \quad (2.3.14)$$

is an lfgu $\mathbb{O}_{Fr, Y}$ -module which has no \mathbb{O}_Y -torsion. The double-dual homomorphism

$$N \rightarrow \mathcal{H}om_{\mathbb{O}_{Fr, Y}}(\mathcal{H}om_{\mathbb{F}_{p^r}}(N, \mathbb{O}_Y), \mathbb{O}_Y) \quad (2.3.15)$$

is an isomorphism.

²[Theorem 2.3.11](#) is proved in [Section 4.5](#). [Theorem 2.3.16](#) is a combination of [Propositions 4.4.1](#) and [4.4.6](#).

Theorem 2.3.16. *Let \mathcal{N} be an lfgu $\mathbb{O}_{Fr, Y}$ -module. Let y be a closed point of Y . Then the natural homomorphism*

$$\mathcal{H}om_{\mathbb{O}_{Fr, Y}}(\mathcal{N}, \mathbb{O}_Y)_y \rightarrow \text{Hom}_{\mathbb{O}_{Y, y}[Fr]}(\mathcal{N}_y, \mathbb{O}_{Y, y}) \quad (2.3.17)$$

is an isomorphism.

Let N be a constructible \mathbb{F}_{p^r} -sheaf on Y . Then the natural homomorphism

$$\mathcal{H}om_{\mathbb{F}_{p^r}}(N, \mathbb{O}_Y)_y \rightarrow \text{Hom}_{\mathbb{F}_{p^r}}(N_{(y)}, \mathbb{O}_{\text{Spec } \mathbb{O}_{Y, y}}) \quad (2.3.18)$$

is an isomorphism.³

Proposition 2.3.19. *Let N be a constructible \mathbb{F}_{p^r} -sheaf on Y whose sections all have open support. Let*

$$\mathcal{N} = \mathcal{H}om_{\mathbb{F}_{p^r}}(N, \mathbb{O}_Y), \quad (2.3.20)$$

and let \mathcal{N}_0 be a root for \mathcal{N} . Then there is an isomorphism,

$$N \xrightarrow{\cong} (\mathcal{N}_0^\vee)^{Fr}. \quad (2.3.21)$$

3. The Euler characteristic of an étale \mathbb{F}_{p^r} -sheaf

Throughout this section, let Y denote a smooth projective k -curve.

If N is a constructible \mathbb{F}_{p^r} -sheaf on Y , let

$$\chi(Y, N) = \dim_{\mathbb{F}_{p^r}} H^0(Y, N) - \dim_{\mathbb{F}_{p^r}} H^1(Y, N). \quad (3.0.22)$$

This section establishes a lower bound on $\chi(Y, N)$ using the theory developed in [Section 2](#).

3.1. Main result. The following lemma provides the final preparation for the main theorem.

Lemma 3.1.1. *Let \mathcal{N}' be a left $\mathbb{O}_{Fr, Y}$ -module which is coherent and locally free as an \mathbb{O}_Y -module. Then the morphism*

$$(1 - Fr)(\cdot): \mathcal{N}' \rightarrow \mathcal{N}' \quad (3.1.2)$$

is surjective.

Proof. Let y be a closed point of Y . We will show that morphism (3.1.2) is surjective at y . Choose any étale neighborhood $U \rightarrow Y$ of y , and any section $n \in \mathcal{N}'(U)$. By replacing U with a subordinate neighborhood if necessary, we may assume that \mathcal{N}' is globally free on U . We may also assume that U is affine. Let $U = \text{Spec } S$.

³Here $N_{(y)}$ denotes the pullback of N via the natural morphism $\text{Spec } \mathbb{O}_{Y, y} \rightarrow Y$.

Let $\{e_1, \dots, e_\ell\}$ be a basis for the free S -module $\mathcal{N}'(U)$. Choose elements $\{s_{ij} \mid 1 \leq i \leq \ell, 1 \leq j \leq \ell\}$ such that

$$F^r(e_i) = \sum_j s_{ij} e_j. \quad (3.1.3)$$

Let $n = \sum_{k=1}^{\ell} a_k e_k$, with $a_k \in S$.

Let $V \rightarrow U$ be the morphism of affine schemes defined by the ring extension

$$S' := S[T_1, T_2, \dots, T_\ell] / \langle \{T_j - a_j - \sum_i T_i^{p^r} s_{ij}\}_{j=1}^{\ell} \rangle. \quad (3.1.4)$$

Note that this is an étale extension (since the module of relative differentials vanishes). The section

$$\sum_k T_k \otimes e_k \in \mathcal{N}'(V) \quad (3.1.5)$$

maps to $n|_V$ under (3.1.2) (as the reader may verify). Therefore $n|_V$ is contained in the image of (3.1.2). Since $V \rightarrow U$ is finite and therefore surjective, n itself is contained in the image of (3.1.2). This completes the proof. \square

Now we are ready to prove the main result. The basic method of our proof is borrowed from [Pink 2000].

Theorem 3.1.6. *Let \mathcal{N} be a constructible \mathbb{F}_{p^r} -étale sheaf on Y whose sections all have open support. Let*

$$\mathcal{N} = \mathcal{H}om_{\mathbb{F}_{p^r}}(\mathcal{N}, \mathcal{O}_Y). \quad (3.1.7)$$

Let g denote the genus Y , and let m denote the rank of \mathcal{N} . Then,

$$\chi(Y, \mathcal{N}) \geq (1 - g)m - \sum_{y \in Y} \mathfrak{C}(\mathcal{N}_y). \quad (3.1.8)$$

Proof. Let \mathcal{N}_0 be the minimal root of \mathcal{N} , and let \mathcal{N}_0^\vee denote its coherent dual. The sheaf \mathcal{N}_0^\vee has the structure of a left $\mathcal{O}_{Fr, Y}$ -module (as discussed in Section 2.3). By Proposition 2.3.19 and Lemma 3.1.1, this gives an exact sequence

$$0 \longrightarrow \mathcal{N} \longrightarrow \mathcal{N}_0^\vee \xrightarrow{1-F^r} \mathcal{N}_0^\vee \longrightarrow 0. \quad (3.1.9)$$

Therefore the cohomology groups of \mathcal{N} and \mathcal{N}_0^\vee are related by the long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(Y, \mathcal{N}) \longrightarrow H^0(Y, \mathcal{N}_0^\vee) \longrightarrow H^0(Y, \mathcal{N}_0^\vee) \longrightarrow \\ H^1(Y, \mathcal{N}) \longrightarrow H^1(Y, \mathcal{N}_0^\vee) \longrightarrow H^1(Y, \mathcal{N}_0^\vee) \longrightarrow 0. \end{aligned} \quad (3.1.10)$$

The finite-dimensional k -vector spaces $H^0(Y, \mathcal{N}_0^\vee)$ and $H^1(Y, \mathcal{N}_0^\vee)$ are left $k[F^r]$ -modules, the first one being unit. There exist left $k[F^r]$ -module isomorphisms

$$H^0(Y, \mathcal{N}_0^\vee) \cong k^{\oplus t_0}, \quad (3.1.11)$$

$$H^1(Y, \mathcal{N}_0^\vee) \cong k^{\oplus t_1} \oplus W, \quad (3.1.12)$$

where W is a left $k[F^r]$ -module with a nilpotent F^r -action. (See [Deligne and Katz 1973, Section 1] for a discussion of this type of decomposition.)

Based on these isomorphisms, we can see that the map

$$(1 - F^r)(\cdot) : H^0(Y, \mathcal{N}_0^\vee) \rightarrow H^0(Y, \mathcal{N}_0^\vee) \quad (3.1.13)$$

is surjective, and therefore (3.1.10) splits up into two short exact sequences:

$$0 \longrightarrow H^0(Y, N) \longrightarrow H^0(Y, \mathcal{N}_0^\vee) \xrightarrow{1-F^r} H^0(Y, \mathcal{N}_0^\vee) \longrightarrow 0, \quad (3.1.14)$$

$$0 \longrightarrow H^1(Y, N) \longrightarrow H^1(Y, \mathcal{N}_0^\vee) \xrightarrow{1-F^r} H^1(Y, \mathcal{N}_0^\vee) \longrightarrow 0.$$

We can see further that the \mathbb{F}_{p^r} -dimension of $H^0(Y, N)$ is the same as the k -dimension of $H^0(Y, \mathcal{N}_0^\vee)$, and the \mathbb{F}_{p^r} -dimension of $H^1(Y, N)$ is no greater than the k -dimension of $H^1(Y, \mathcal{N}_0^\vee)$. Thus we obtain the inequality

$$\chi(Y, N) \geq \chi(Y, \mathcal{N}_0^\vee), \quad (3.1.15)$$

where $\chi(Y, \mathcal{N}_0^\vee) = \dim_k H^0(Y, \mathcal{N}_0^\vee) - \dim_k H^1(Y, \mathcal{N}_0^\vee)$. Now Theorem 3.1.6 follows easily from the Riemann–Roch formula. By the discussion at the end of Section 2.2,

$$\deg \mathcal{N}_0 = \sum_{y \in Y} \mathfrak{C}(\mathcal{N}_y). \quad (3.1.16)$$

Therefore by the Riemann–Roch theorem,

$$\begin{aligned} \chi(Y, N) &\geq \chi(Y, \mathcal{N}_0^\vee) = (1 - g)m + \deg \mathcal{N}_0^\vee \\ &= (1 - g)m - \deg \mathcal{N}_0 = (1 - g)m - \sum_{y \in Y} \mathfrak{C}(\mathcal{N}_y). \quad \square \end{aligned}$$

An alternate (and perhaps more interesting) formulation of Theorem 3.1.6 is allowed if we extend some of our notation. If N is a constructible \mathbb{F}_{p^r} -sheaf on Y , and y is a closed point of Y , then let $\mathfrak{C}(N_{(y)})$ denote the minimal root index of the Riemann–Hilbert dual

$$\mathrm{Hom}_{\mathbb{F}_{p^r}}(N_{(y)}, \mathbb{C}_{\mathrm{Spec} \mathbb{C}_{Y,y}}). \quad (3.1.17)$$

By Theorem 2.3.16, this dual is isomorphic to \mathcal{N}_y . The following corollary follows immediately.

Corollary 3.1.18. *Let N be a constructible \mathbb{F}_{p^r} -étale sheaf on Y whose sections all have open support. Let g denote the genus of Y and m the rank of N . Then,*

$$\chi(Y, N) \geq (1 - g)m - \sum_{y \in Y} \mathfrak{C}(N_{(y)}). \quad (3.1.19)$$

3.2. Examples. We will illustrate [Theorem 3.1.6](#) and [Corollary 3.1.18](#) via two examples on the projective line.

We begin with a brief discussion in the local setting. As it turns out, the local terms from [Corollary 3.1.18](#) are easy to calculate explicitly in the case of rank-one sheaves. Let y be a closed point of Y . Let $A = \mathbb{O}_{Y,y}$, and let K be the fraction field of A . Let $t \in K$ be a local parameter. Let K'/K be a degree- $(p^r - 1)$ extension having an element t' which satisfies $(t')^{p^r - 1} = t$.

For each $i = 0, 1, 2, \dots, (p^r - 2)$, consider the \mathbb{F}_{p^r} -subsheaf of $\mathbb{O}_{\text{Spec } A}$ generated by the element $(t')^i \in K'$. Call this sheaf V_i . Each such sheaf is a rank-one \mathbb{F}_{p^r} -sheaf with no global sections. The sheaves $V_0, V_1, \dots, V_{p^r - 2}$ taken together express all of the isomorphism types of nontrivial rank-one \mathbb{F}_{p^r} -sheaves on $\text{Spec } A$.

Now consider the set of all \mathbb{F}_{p^r} -linear morphisms from V_i into $\mathbb{O}_{\text{Spec } A}$. One such morphism is simply the inclusion $f_i: V_i \hookrightarrow \mathbb{O}_{\text{Spec } A}$. The Riemann–Hilbert dual

$$\mathcal{V}_i = \text{Hom}_{\mathbb{F}_{p^r}}(V_i, \mathbb{O}_{\text{Spec } A}) \quad (3.2.1)$$

is a one-dimensional K -vector space generated by the morphism f_i . As the reader may verify, the left $A[F^r]$ -module structure of \mathcal{V}_i is given by

$$F^r(f_i) = t^i \cdot f_i. \quad (3.2.2)$$

Calculating the minimal root index for V_i is thus straightforward. The smallest A -module in \mathcal{V}_i which satisfies the root properties is the A -module generated by $t^{-1}f_i$. The F^r -index of this module is $1 - i/(p^r - 1)$. Therefore,

$$\mathfrak{C}(V_i) = 1 - \frac{i}{p^r - 1}. \quad (3.2.3)$$

In the examples that follow, we will use the following notation: if Z is a k -scheme, then $\underline{\mathbb{F}_{p^r}}_Z$ (or simply $\underline{\mathbb{F}_{p^r}}$) denotes the constant \mathbb{F}_{p^r} -sheaf on Z .

Example 3.2.4. Suppose that $p > 2$. Let \mathbb{P}^1 denote the projective line over k . Let $\alpha: \mathbb{P}^1 \rightarrow \mathbb{P}^1$ denote the double-cover of \mathbb{P}^1 which maps 0 to 0 , ∞ to ∞ , and is ramified at both of those points. Define

$$N = \alpha_*(\underline{\mathbb{F}_{p^r}}_{\mathbb{P}^1}). \quad (3.2.5)$$

The sheaf N is a rank-2 sheaf which is locally constant at every point except for 0 and ∞ . The stalk N_∞ decomposes as a direct sum

$$N_\infty \cong W \oplus W', \quad (3.2.6)$$

in which W is a trivial rank-one sheaf, and W' is isomorphic to the sheaf $V_{(p^r-1)/2}$ from the classification above. Therefore,

$$\mathfrak{C}(N_\infty) = \mathfrak{C}(W) + \mathfrak{C}(W') = \frac{1}{2}. \quad (3.2.7)$$

A similar calculation shows that $\mathfrak{C}(N_0) = \frac{1}{2}$.

In this case, [Corollary 3.1.18](#) asserts:

$$\chi(Y, N) \geq (1-0) \cdot 2 - \sum_{y \in Y} \mathfrak{C}(N_{(y)}) = 2 - (\frac{1}{2} \cdot 2) = 1. \quad (3.2.8)$$

On the other hand, the Euler characteristic of N can be calculated directly. The dimensions of the cohomology groups of $N = \alpha_* \underline{\mathbb{F}}_{p^r}$ are the same as those of $\underline{\mathbb{F}}_{p^r}$ (this can be seen from a Leray–Serre spectral sequence). Therefore $\chi(\mathbb{P}^1, N) = \chi(\mathbb{P}^1, \underline{\mathbb{F}}_{p^r}) = 1$. So the formula from [Corollary 3.1.18](#) actually computes $\chi(\mathbb{P}^1, N)$ exactly.

Example 3.2.9. Now suppose $p > 5$. Let E be an elliptic curve, and let $\beta: E \rightarrow \mathbb{P}^1$ be a degree-2 morphism which has 4 ramified points, each of ramification index 2. Label the ramified points as $q_1, q_2, q_3, q_4 \in \mathbb{P}^1$.

Let $N = \beta_*(\underline{\mathbb{F}}_{p^r})$. Then N is locally constant on $\mathbb{P}^1 \setminus \{q_1, q_2, q_3, q_4\}$, and by a calculation similar to the one in [Example 3.2.4](#),

$$\mathfrak{C}(N_{q_i}) = \frac{1}{2} \quad \text{for } i = 1, 2, 3, 4. \quad (3.2.10)$$

So [Theorem 3.1.6](#) asserts

$$\chi(\mathbb{P}^1, N) \geq (1-0) \cdot 2 - \sum_{i=1}^4 \mathfrak{C}(N_{q_i}) = 0. \quad (3.2.11)$$

In actuality, $\chi(\mathbb{P}^1, N)$ is equal to $\chi(E, \underline{\mathbb{F}}_{p^r})$. This quantity can be equal to 0 or 1, depending on whether on E is a supersingular elliptic curve.

So, [Corollary 3.1.18](#) yields an equality if and only if E is an ordinary elliptic curve.

3.3. The minimal root index of a tame sheaf. The discussion at the beginning of the previous subsection will lead us to a more general calculation of the minimal root index. Again, let y be a closed point of the curve Y , let $A = \mathbb{O}_{Y,y}$, and let K be the fraction field of A . Let t be a local parameter in A .

We need the following proposition and corollary.

Proposition 3.3.1. *Let a and b be positive integers. Let Q be a finitely-generated unit $A[F^a]$ -module. Then the minimal root index of Q when considered as a unit $A[F^{ab}]$ -module is the same as the minimal root index of Q when considered as a unit $A[F^a]$ -module.*

Proof. Let $Q_0 \subseteq ({}_{A[F^{ab}]}Q)$ be the minimal root for Q considered as an $A[F^{ab}]$ -module. For any $i \geq 0$, let $Q_{i/b}$ be the submodule of Q generated by $F^{ai}(Q_0)$. The module $Q_{1/b}$ is also a root for ${}_{A[F^{ab}]}Q$. (This is clear via the isomorphism $F^{a*}Q \rightarrow Q$.) Since both Q_0 and $Q_{1/t}$ are roots for ${}_{A[F^{ab}]}Q$, the intersection $Q_0 \cap Q_{1/b}$ is a root for ${}_{A[F^{ab}]}Q$ (by similar reasoning to that in the proof of [Proposition 2.2.1](#)). Since Q_0 is the minimal root for ${}_{A[F^{ab}]}Q$, it follows that $Q_0 \cap Q_{1/b} = Q_0$. Therefore $Q_0 \subseteq Q_{1/b}$, which means that Q_0 is a root not only for ${}_{A[F^{ab}]}Q$ but for Q itself.

The above reasoning shows that the minimal root for ${}_{A[F^{ab}]}Q$ contains the minimal root for Q . But the reverse inclusion is obvious. So we see that Q_0 is the minimal root for both ${}_{A[F^{ab}]}Q$ and Q . Thus,

$$\begin{aligned} \mathfrak{c}({}_{A[F^{ab}]}Q) &= \frac{\dim_k(Q_1/Q_0)}{p^{ab} - 1} = \frac{\sum_{i=0}^{b-1} \dim_k(Q_{(i+1)/b}/Q_{i/t})}{p^{ab} - 1} \\ &= \frac{\sum_{i=0}^{b-1} (p^{ai}) \dim_k(Q_{1/b}/Q_0)}{p^{ab} - 1} = \frac{\dim_k(Q_{1/b}/Q_0)}{p^a - 1} = \mathfrak{c}(Q). \quad \square \end{aligned}$$

Corollary 3.3.2. *Let W be a constructible \mathbb{F}_{p^a} -sheaf on $\text{Spec } A$ whose sections all have open support. Then the minimal root index of the $\mathbb{F}_{p^{ab}}$ -sheaf*

$$\mathbb{F}_{p^{ab}} \otimes_{\mathbb{F}_{p^a}} W \tag{3.3.3}$$

is the same as the minimal root index of W .

Proof. Let ${}^{\circ}W$ be the Riemann–Hilbert dual of W . Then the Riemann–Hilbert dual of $\mathbb{F}_{p^{ab}} \otimes W$ is ${}_{A[F^{ab}]}{}^{\circ}W$. \square

Now, let K^{tame}/K denote the direct limit of all tame extensions of K (that is, extensions of order coprime to p). A sheaf on $\text{Spec } A$ will be called a tame sheaf if its monodromy representation factors through $\text{Gal}(K^{\text{tame}}/K)$.

Every finite quotient of $\text{Gal}(K^{\text{tame}}/K)$ is an abelian group of order coprime to p . Therefore, any finite-image representation of $\text{Gal}(K^{\text{tame}}/K)$ over an algebraically closed field of characteristic p decomposes into one-dimensional representations. This fact has a natural consequence for sheaves on $\text{Spec } A$: if W is a tame constructible \mathbb{F}_{p^r} -sheaf on $\text{Spec } A$ whose sections all have open support, then there exists a field extension $\mathbb{F}_{p^{rb}}/\mathbb{F}_{p^r}$ such that the sheaf $\mathbb{F}_{p^{rb}} \otimes W$ decomposes into a direct sum of rank-one $\mathbb{F}_{p^{rb}}$ -sheaves.

Let V be an $\mathbb{F}_{p^{rb}}$ -sheaf of rank one on $\text{Spec } A$ which has no global sections. Then (as discussed in [Section 3.2](#)), there is a natural way to associate V with a

subsheaf of $\mathbb{O}_{\text{Spec } A}$. The sheaf V is isomorphic to the $\mathbb{F}_{p^{rb}}$ -subsheaf of $\mathbb{O}_{\text{Spec } A}$ generated by some element $s \in K^{\text{tame}}$ which satisfies $s^c = t^d$ for some integers c and d with $0 \leq d < c$, $p \nmid c$.

Let λ_V denote the quantity $\frac{d}{c}$. Then the minimal root index of V is

$$\mathfrak{C}(V) = 1 - \lambda_V. \quad (3.3.4)$$

The following proposition follows immediately.

Proposition 3.3.5. *Let W be a constructible tame \mathbb{F}_{p^r} -sheaf on $\text{Spec } A$ which has no global sections. Let $\mathbb{F}_{p^{rb}}/\mathbb{F}_{p^r}$ be a field extension such that $\mathbb{F}_{p^{rb}} \otimes W$ can be decomposed into a direct sum of rank-one sheaves. Then*

$$\mathfrak{C}(W) = \sum_V (1 - \lambda_V), \quad (3.3.6)$$

where the sum is taken over all summands in the decomposition of $\mathbb{F}_{p^{rb}} \otimes W$. \square

We note in passing that [Proposition 3.3.5](#) makes the minimal root index compatible with the local terms used in [[Pink 2000](#)]. Specifically: if N is a constructible \mathbb{F}_{p^r} -sheaf on Y such that $N_y = \{0\}$ and $N_{(y)}$ is tame, the rational invariant $\text{LT}_Y^{\mathbb{F}_{p^r}} N$ [[Pink 2000](#), Definition 5.3] is exactly equal to the minimal root index of $N_{(y)}$.

4. The Riemann–Hilbert correspondence on a curve

The purpose of this section is to prove the characteristic- p Riemann–Hilbert correspondence in dimension one. Our approach is to build the proof in stages, beginning in the local setting and then proceeding to the global.

Throughout this section, let Y denote a smooth irreducible projective k -curve.

4.1. The Riemann–Hilbert correspondence over a field. Suppose that L_0 is a separably closed field of characteristic p . Let P_0 be a finitely-generated unit $L_0[F']$ -module. Then P_0 must have an L_0 -basis which is invariant under the action of F' . This basis determines an $L_0[F']$ -module isomorphism $P_0 \cong (L_0)^{\oplus d}$ for some $d \geq 0$ [[Deligne and Katz 1973](#), Proposition 1.1].

More generally, if L is any field of characteristic p , and P is a finitely-generated unit $L[F']$ -module, then there exists a finite separable extension L'/L such that $L' \otimes_L P$ is a trivial $L'[F']$ -module.

The following proposition about sheaves on $\text{Spec } L$ follows easily.

Proposition 4.1.1. *Let L be a field of characteristic p , and let $T = \text{Spec } L$. Then for any lfgu $\mathbb{O}_{F^r, T}$ -module \mathcal{V} , the double-dual morphism*

$$\mathcal{V} \rightarrow \mathcal{H}om_{\mathbb{F}_{p^r}}(\mathcal{H}om_{\mathbb{O}_{F^r, T}}(\mathcal{V}, \mathbb{O}_T), \mathbb{O}_T) \quad (4.1.2)$$

is an isomorphism. For any constructible \mathbb{F}_{p^r} -sheaf V on T , the double-dual morphism

$$V \rightarrow \mathcal{H}om_{\mathbb{O}_{F^r, T}}(\mathcal{H}om_{\mathbb{F}_{p^r}}(V, \mathbb{O}_T), \mathbb{O}_T) \quad (4.1.3)$$

is an isomorphism. \square

4.2. The local structure of an $\mathbb{O}_{F^r, Y}$ -module on a curve. Let A be a Henselization of the local ring $k[t]_{(t)}$. Let K denote the fraction field of A . Note that for any closed point $y \in Y$, the local ring $\mathbb{O}_{Y, y}$ is isomorphic to A . Therefore, we are interested in the structure of unit $A[F^r]$ -modules.

We will refer to a unit $A[F^r]$ -module as *torsion-free* if it has no A -torsion. Suppose that Q is a torsion-free finitely-generated unit $A[F^r]$ -module. Then let

$$Q^{\text{vec}} = \bigcap_{i=0}^{\infty} t^i Q. \quad (4.2.1)$$

The module Q^{vec} is the largest K -vector space contained in Q . This definition can be easily generalized to modules over any DVR. The reader may check the following elementary assertions:

- (1) The module Q^{vec} is a finitely-generated unit $K[F^r]$ -module.
- (2) The quotient Q/Q^{vec} is a finitely-generated unit $A[F^r]$ -module.
- (3) For any finite integral extension of rings $A \hookrightarrow A'$,

$$(A' \otimes_A Q)^{\text{vec}} = A' \otimes_A Q^{\text{vec}}. \quad (4.2.2)$$

There is an exact sequence

$$0 \rightarrow Q^{\text{vec}} \rightarrow Q \rightarrow Q/Q^{\text{vec}} \rightarrow 0 \quad (4.2.3)$$

for any torsion-free finitely-generated unit $A[F^r]$ -module Q . In this subsection we are going to show that the quotient Q/Q^{vec} always has a trivial structure.

We begin with an algebraic lemma.

Lemma 4.2.4. *Let Q be a unit $A[F^r]$ -module which is a free A -module of finite rank. Then, any F^r -invariant element of Q/tQ can be uniquely lifted to an F^r -invariant element of Q .*

Proof. The lemma may be formulated in terms of commutative algebra. Let $\{q_1, \dots, q_n\}$ be any A -module basis for Q . Since Q is a unit $A[F^r]$ -module, the set $\{F^r(q_1), \dots, F^r(q_n)\}$ is another basis, and there exists an invertible A -matrix (c_{ij}) such that

$$q_i = \sum_{j=1}^n c_{ij} F^r(q_j). \quad (4.2.5)$$

An element

$$\sum_{k=1}^n a_k q_k \in Q, \quad (a_k \in A) \quad (4.2.6)$$

is F^r -invariant if and only if

$$\sum_{k=1}^n a_k^{p^r} F^r(q_k) = \sum_{k=1}^n a_k q_k = \sum_{k=1}^n a_k \sum_{j=1}^n c_{kj} F^r(q_j), \quad (4.2.7)$$

or equivalently,

$$a_k^{p^r} = \sum_{\ell=1}^n a_\ell c_{\ell k} \quad (4.2.8)$$

for each $k = 1, 2, \dots, n$. Let

$$R = A[X_1, \dots, X_n] / \left(\left\{ X_k^{p^r} - \sum_{\ell=1}^n X_\ell c_{\ell k} \right\}_{k=1}^n \right). \quad (4.2.9)$$

Then F^r -invariant elements of Q may be specified by A -homomorphisms from R into A , while F^r -invariant elements of Q/tQ may be specified by A -homomorphisms from R into k . The claim made in the lemma, then, is equivalent to the assertion that every element of $\text{Hom}_A(R, k)$ can be lifted to an element of $\text{Hom}_A(R, A)$.

This assertion becomes evident once we understand the structure of R . The extension $A \rightarrow R$ is finite, flat, and unramified (as the reader may check), and therefore étale. Since A is a Henselian local ring, R is simply a finite direct sum of copies of A . \square

Proposition 4.2.10. *Let Q be a unit $A[F^r]$ -module which is a free A -module of finite rank. Then there exists an $A[F^r]$ -module isomorphism $Q \cong A^{\oplus d}$ for some d .*

Proof. Choose an F^r -invariant k -basis for Q/tQ . There is a unique F^r -invariant lifting of this set to Q by [Lemma 4.2.4](#). By Nakayama's lemma, this lifting is an A -module basis, and so it determines the desired isomorphism. \square

Proposition 4.2.11. *Suppose that Q is a torsion-free unit $A[F^r]$ -module for which there exists a $K[F^r]$ -module isomorphism,*

$$K \otimes_A Q \cong K^{\oplus d} \quad (4.2.12)$$

(with $d \geq 1$). Then there exists an $A[F^r]$ -module isomorphism

$$Q \cong K^{\oplus d'} \oplus A^{\oplus (d-d')} \quad (4.2.13)$$

for some d' with $0 \leq d' \leq d$.

Proof. Let $Q' \subseteq K^{\oplus d}$ be the image of Q under the injection $Q \rightarrow K \otimes_A Q \rightarrow K^{\oplus d}$. I claim first that $Q' \supseteq (A^{\oplus d})$. Suppose that this were not so. Then, the module

$$S := (A^{\oplus d}) / (Q' \cap A^{\oplus d}) \quad (4.2.14)$$

is a nontrivial unit $A[F^r]$ -module. This module is a torsion A -module, and therefore has finite dimension over k . But then the structural isomorphism

$$F_A^{r*} S \rightarrow S \quad (4.2.15)$$

implies that $(p^r) \dim_k S = \dim_k S$, which is impossible. Therefore Q' contains $(A^{\oplus d})$.

Now consider the intersection of Q' with the subset

$$t^{-1}(k^{\oplus d}) = \{(t^{-1}c_1, \dots, t^{-1}c_d) \mid c_i \in k\} \subseteq K^{\oplus d}. \quad (4.2.16)$$

The intersection $Q' \cap t^{-1}(k^{\oplus d})$ has a Frobenius-linear endomorphism given by

$$Q' \cap t^{-1}(k^{\oplus d}) \xrightarrow{F^r(\cdot)} Q' \cap t^{-p^r}(k^{\oplus d}) \xrightarrow{(\cdot)^{(t^{p^r-1})}} Q' \cap t^{-1}(k^{\oplus d}). \quad (4.2.17)$$

We can find a k -basis $\{\lambda_1, \lambda_2, \dots, \lambda_{d'}\}$ for $Q' \cap t^{-1}(k^{\oplus d})$ consisting of elements which are fixed by this endomorphism. The elements in this basis can be written as

$$\lambda_i = t^{-1}e_i, \quad (4.2.18)$$

where $e_i \in (\mathbb{F}_{p^r})^{\oplus d} \subset K^{\oplus d}$.

Note that since $t^{-1}e_i \in Q'$, the $A[F^r]$ -module structure of Q' implies that $t^{-M}e_i \in Q'$ for any $M > 0$. Now enlarge the set $\{e_1, \dots, e_{d'}\}$ to a d -element set $\{e_1, \dots, e_d\}$ which is a basis for $(\mathbb{F}_{p^r})^{\oplus d}$. The basis $\{e_1, \dots, e_d\}$ determines a map

$$K^{\oplus d'} \oplus A^{\oplus(d-d')} \rightarrow Q', \quad (4.2.19)$$

which is easily seen to be an isomorphism. This completes the proof. \square

Proposition 4.2.20. *Let Q be a torsion-free finitely-generated unit $A[F^r]$ -module such that $Q^{\text{vec}} = \{0\}$. Then there exists an $A[F^r]$ -module isomorphism $Q \cong A^{\oplus d}$ for some $d \geq 0$.*

Proof. The module $K \otimes_A Q$ is a finitely-generated unit $K[F^r]$ -module. Choose a finite separable extension K'/K which trivializes Q . Let $A' \subseteq K'$ be the integral closure of A in K' . Let $Q' = A' \otimes_A Q$.

The module Q' is a torsion-free unit $A'[F^r]$ -module such that $Q' \otimes_{A'} K'$ is isomorphic to $(K')^{\oplus d}$ for some d . Note that A' , like A , is a Henselian local ring,

and in fact there exists an isomorphism between the pair (A', K') and (A, K) . Via this isomorphism, we can apply [Proposition 4.2.11](#) to find an isomorphism

$$Q' \cong K'^{\oplus d'} \oplus A'^{\oplus(d-d')}. \quad (4.2.21)$$

Now since $Q'^{\text{vec}} = \{0\}$, clearly we must have $d' = 0$. Thus $Q' \cong A'^{\oplus d}$.

The inclusion $Q \hookrightarrow Q'$ makes Q isomorphic to a submodule of a finitely-generated A -module. Therefore Q is itself a finitely-generated A -module. The desired result now follows from [Proposition 4.2.10](#). \square

Proposition 4.2.22. *Let Q be a torsion-free finitely-generated unit $A[F^r]$ -module. Then Q/Q^{vec} is isomorphic to $A^{\oplus d}$ for some $d \geq 0$.*

Proof. Immediate from [Proposition 4.2.20](#). \square

4.3. The local Riemann–Hilbert correspondence. We now prove the Riemann–Hilbert correspondence over the local rings $\mathbb{O}_{Y,y}$.

Theorem 4.3.1. *Let y be a closed point of Y , and let $Z = \text{Spec } \mathbb{O}_{Y,y}$. Let \mathcal{V} be an lfgu $\mathbb{O}_{F^r,Z}$ -module which is torsion-free (as an \mathbb{O}_Z -module). Then the sheaf*

$$\mathcal{H}om_{\mathbb{O}_{F^r,Z}}(\mathcal{V}, \mathbb{O}_Z) \quad (4.3.2)$$

is a constructible \mathbb{F}_{p^r} -sheaf whose sections all have open support. The double-dual morphism

$$\mathcal{V} \rightarrow \mathcal{H}om_{\mathbb{F}_{p^r}}(\mathcal{H}om_{\mathbb{O}_{F^r,Z}}(\mathcal{V}, \mathbb{O}_Z), \mathbb{O}_Z) \quad (4.3.3)$$

is an isomorphism.

Let V be a constructible \mathbb{F}_{p^r} -sheaf on Z whose sections all have open support. Then

$$\mathcal{H}om_{\mathbb{F}_{p^r}}(V, \mathbb{O}_Z) \quad (4.3.4)$$

is a torsion-free lfgu $\mathbb{O}_{F^r,Z}$ -module. The double-dual morphism

$$V \rightarrow \mathcal{H}om_{\mathbb{O}_{F^r,Z}}(\mathcal{H}om_{\mathbb{F}_{p^r}}(V, \mathbb{O}_Z), \mathbb{O}_Z) \quad (4.3.5)$$

is an isomorphism.

Proof. It is helpful at this point to assign labels to the functors in the Riemann–Hilbert correspondence. Let

$$\mathbf{S}_Z(\cdot) = \mathcal{H}om_{\mathbb{O}_{F^r,Z}}(\cdot, \mathbb{O}_Z) \quad (4.3.6)$$

and

$$\mathbf{M}_Z(\cdot) = \mathcal{H}om_{\mathbb{F}_{p^r}}(\cdot, \mathbb{O}_Z). \quad (4.3.7)$$

For any \mathbb{F}_{p^r} -sheaf M on Z , let $M^{\text{con}} \subseteq M$ denote the subsheaf which is generated by the global sections of M . For any torsion-free unit $\mathbb{O}_{Fr, Z}$ -module \mathcal{M} , let $\mathcal{M}^{\text{vec}} \subseteq \mathcal{M}$ denote the subsheaf generated by $\Gamma(Z, \mathcal{M})^{\text{vec}} \subseteq \Gamma(Z, \mathcal{M})$ (using notation from the previous subsection).

These two constructions satisfy a duality property under the Riemann–Hilbert correspondence. Suppose that ϕ is a global section of $\mathbf{M}_Z(M)$ (that is, an \mathbb{F}_{p^r} -linear morphism from M into \mathbb{O}_Z). If ϕ is contained in $\mathbf{M}_Z(M)^{\text{vec}}$, then it is easy to see that the morphism of global sections,

$$\Gamma(Z, M) \xrightarrow{\phi} \Gamma(Z, \mathbb{O}_Z)(= \mathbb{O}_{Y, y}), \quad (4.3.8)$$

must be trivial. The converse is also true. The set of morphisms ϕ for which (4.3.8) is trivial form a K -vector space (isomorphic to $\text{Hom}_{\mathbb{F}_{p^r}}(M|_{\text{Spec } K}, \mathbb{O}_{\text{Spec } K})$) which is contained in $\mathbf{M}_Z(M)^{\text{vec}}$.

Thus, $\mathbf{M}_Z(M)^{\text{vec}}$ is equal to the sheaf of morphisms $M \rightarrow \mathbb{O}_Z$ that kill M^{con} .

Now suppose that \mathcal{M} is a torsion-free finitely-generated unit $\mathbb{O}_{Fr, Z}$ -module. It is clear that any \mathbb{O}_Z -morphism $\mathcal{M} \rightarrow \mathbb{O}_Z$ must kill \mathcal{M}^{vec} . And, since $\mathcal{M}/\mathcal{M}^{\text{vec}} \cong \mathbb{O}_Z^{\oplus d}$ for some d , it is easily seen that any section of $\mathcal{H}om_{\mathbb{O}_{Fr, Z}}(\mathcal{M}, \mathbb{O}_Z)$ which kills \mathcal{M}^{vec} can be extended to a global section. Therefore $\mathbf{S}_Z(\mathcal{M})^{\text{con}}$ is the subsheaf of $\mathbf{S}_Z(\mathcal{M})$ consisting of morphisms which kill \mathcal{M}^{vec} .

We can now prove the local Riemann–Hilbert correspondence by building on [Proposition 4.1.1](#) and [Proposition 4.2.22](#). The duality discussed above implies that the sequence

$$0 \rightarrow \mathbf{S}_Z(\mathcal{V}/\mathcal{V}^{\text{vec}}) \rightarrow \mathbf{S}_Z(\mathcal{V}) \rightarrow \mathbf{S}_Z(\mathcal{V}^{\text{vec}}) \rightarrow 0 \quad (4.3.9)$$

is exact. The sheaf $\mathbf{S}_Z(\mathcal{V}/\mathcal{V}^{\text{vec}})$ is constructible (in fact, constant), and the sheaf $\mathbf{S}_Z(\mathcal{V}^{\text{vec}})$ is constructible; therefore $\mathbf{S}_Z(\mathcal{V})$ is constructible. There is a diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{V}^{\text{vec}} & \longrightarrow & \mathcal{V} & \longrightarrow & \mathcal{V}/\mathcal{V}^{\text{vec}} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathbf{M}_Z(\mathbf{S}_Z(\mathcal{V}^{\text{vec}})) & \longrightarrow & \mathbf{M}_Z(\mathbf{S}_Z(\mathcal{V})) & \longrightarrow & \mathbf{M}_Z(\mathbf{S}_Z(\mathcal{V}/\mathcal{V}^{\text{vec}})) \longrightarrow 0 \end{array}$$

in which the vertical arrows are double-dual morphisms. The outer vertical arrows are isomorphisms by [Proposition 4.1.1](#) and [Proposition 4.2.22](#), and so the inner arrow is an isomorphism by the 5-lemma.

The second part of [Theorem 4.3.1](#) follows similarly. \square

4.4. Local-to-global compatibility. The next two propositions show that the functors in the Riemann–Hilbert correspondence are compatible with localization.

Proposition 4.4.1. *Let X be a smooth k -curve, and let x be a closed point of X . Let M be a constructible \mathbb{F}_{p^r} -sheaf on X . Then the natural homomorphism*

$$\mathcal{H}om_{\mathbb{F}_{p^r}}(M, \mathbb{O}_X)_x \rightarrow \mathrm{Hom}_{\mathbb{F}_{p^r}}(M_{(x)}, \mathbb{O}_{\mathrm{Spec} \mathbb{O}_{X,x}}) \quad (4.4.2)$$

is an isomorphism.

Proof. By replacing X with an appropriate étale neighborhood of x , we may make the following assumptions:

- (1) X is affine.
- (2) There is a finite Galois morphism of curves

$$\begin{aligned} Z &\rightarrow X \\ z &\mapsto x, \end{aligned}$$

that is totally ramified at x and étale elsewhere, and such that $M_{|Z \setminus \{z\}}$ is constant.

Let R be the coordinate ring of the curve X , and let S be the coordinate ring of the (affine) curve $Z \setminus \{z\}$. The automorphism group $G := \mathrm{Aut}(Z/X)$ acts on S . Morphisms from the sheaf M to the sheaf \mathbb{O}_X can be expressed as commutative diagrams

$$\begin{array}{ccc} \Gamma(M, Z \setminus \{z\}) & \longrightarrow & S \\ \uparrow & & \uparrow \\ \Gamma(M, X) & \longrightarrow & R \end{array} \quad (4.4.3)$$

in which the top map is G -equivariant. Likewise morphisms from the sheaf $M_{(x)}$ to the sheaf $\mathbb{O}_{\mathrm{Spec} \mathbb{O}_{X,x}}$ can be expressed as commutative diagrams

$$\begin{array}{ccc} \Gamma(M, Z \setminus \{z\}) & \longrightarrow & S \otimes_R \mathbb{O}_{X,x} \\ \uparrow & & \uparrow \\ \Gamma(M, X) & \longrightarrow & \mathbb{O}_{X,x} \end{array} \quad (4.4.4)$$

in which the top map is G -equivariant.

Suppose that we are given a diagram in the form of (4.4.4) above. Then since $\Gamma(M, Z \setminus \{z\})$ and $\Gamma(M, X)$ are both finite, there exists an étale subextension $B \subseteq \mathbb{O}_{X,x}$ of R such that the images of the top and bottom maps are contained in $S \otimes_R B$ and B , respectively. Thus we obtain a diagram

$$\begin{array}{ccc} \Gamma(M, Z \setminus \{z\}) & \longrightarrow & S \otimes_R B \\ \uparrow & & \uparrow \\ \Gamma(M, X) & \longrightarrow & B \end{array} \quad (4.4.5)$$

This argument shows that any morphism from $M_{(x)}$ to $\mathbb{C}_{\mathrm{Spec} \mathbb{C}_{X,x}}$ can be extended to an affine étale neighborhood of x . This proves the proposition. \square

Proposition 4.4.6. *Let X be a smooth k -curve, and let x be a closed point of X . Let \mathcal{M} be an lfgu $\mathbb{C}_{Fr,X}$ -module. Then the natural homomorphism*

$$\mathcal{H}om_{\mathbb{C}_{Fr,X}}(\mathcal{M}, \mathbb{C}_X)_x \rightarrow \mathrm{Hom}_{\mathbb{C}_{X,x}[Fr]}(\mathcal{M}_x, \mathbb{C}_{X,x}) \quad (4.4.7)$$

is an isomorphism.

Proof. Replacing X with an open subcurve if necessary, we may assume that X is affine. Let $X = \mathrm{Spec} R$.

It suffices to show that any $\mathbb{C}_{X,x}[Fr]$ -module homomorphism $\mathcal{M}_x \rightarrow \mathbb{C}_{X,x}$ can be extended to an étale neighborhood of x . Let $\phi: \mathcal{M}_x \rightarrow \mathbb{C}_{X,x}$ be such a homomorphism. Let

$$\{m_1, \dots, m_\ell\} \subseteq \Gamma(\mathcal{M}, X) \quad (4.4.8)$$

be a finite subset which generates \mathcal{M} as an $\mathbb{C}_{Fr,X}$ -module. Find an étale subextension $R \hookrightarrow R'$ of $R \hookrightarrow \mathbb{C}_{X,x}$ which is large enough that R' contains the set

$$\{\phi((m_1)_x), \phi((m_2)_x), \dots, \phi((m_\ell)_x)\} \subseteq \mathbb{C}_{X,x}. \quad (4.4.9)$$

Then the homomorphism ϕ can be extended to a homomorphism from $\mathcal{M}_{|\mathrm{Spec} R'}$ to $\mathbb{C}_{\mathrm{Spec} R'}$. \square

4.5. The proof of the global Riemann–Hilbert correspondence. We will now complete the proof of the Riemann–Hilbert correspondence on Y (Theorem 2.3.11).

Proposition 4.5.1. *Let N be a constructible \mathbb{F}_{p^r} -sheaf on Y . Then the sheaf*

$$\mathcal{H}om_{\mathbb{F}_{p^r}}(N, \mathbb{C}_Y) \quad (4.5.2)$$

is an lfgu $\mathbb{C}_{Fr,Y}$ -module.

Proof. Let \mathcal{N}' denote the sheaf (4.5.2) above. Since N is constructible, there exists an open subcurve $V \subseteq Y$ on which N is locally constant of finite rank. The restriction $\mathcal{N}'|_V$ is a coherent \mathbb{C}_V -module.

We can prove the desired properties of \mathcal{N}' from the analogous properties of its stalks. Note that Theorem 4.3.1 and Proposition 4.4.1 imply that each stalk \mathcal{N}'_y , $y \in Y$, is a finitely-generated unit $\mathbb{C}_{Y,y}[Fr]$ -module. Since the structural morphism $F_Y^r * \mathcal{N}' \rightarrow \mathcal{N}'$ is an isomorphism at each closed point $y \in Y$, it is globally an isomorphism. Moreover, since $\mathcal{N}'|_V$ is a locally finitely-generated $\mathbb{C}_{Fr,V}$ -module, and each stalk \mathcal{N}'_y at points y outside of V is a finitely-generated $\mathbb{C}_{Y,y}[Fr]$ -module, the sheaf \mathcal{N}' is a locally finitely-generated $\mathbb{C}_{Fr,Y}$ -module.

It remains only to show that \mathcal{N}' is quasicohherent. Let $j: V \rightarrow Y$ denote the inclusion map. Consider the homomorphism

$$\mathcal{N}' \hookrightarrow j_*(\mathcal{N}'|_V). \quad (4.5.3)$$

The sheaf $j_*(\mathcal{N}'_{|V})$ is quasicoherent. The cokernel of (4.5.3) is easily seen to be a quasicoherent skyscraper sheaf. Therefore \mathcal{N}' is quasicoherent. This completes the proof. \square

Proposition 4.5.4. *Let \mathcal{N} be an lfgu $\mathbb{O}_{Fr, Y}$ -module. Then the \mathbb{F}_{p^r} -sheaf*

$$\mathcal{H}om_{\mathbb{O}_{Fr, Y}}(\mathcal{N}, \mathbb{O}_Y) \quad (4.5.5)$$

is constructible.

Proof. Let N' denote sheaf (4.5.5) above. Theorem 4.3.1 and Proposition 4.4.6 imply that the stalks of N' are finite. To prove that N' is constructible, it suffices to show that there exists a nontrivial étale morphism $Z \rightarrow Y$ such that $N'_{|Z}$ is constant.

Let η be the generic point of Y . Let L denote a separable closure of the residue field of η , and let

$$\bar{\eta}: \text{Spec } L \rightarrow Y \quad (4.5.6)$$

denote the corresponding geometric generic point. The stalk $\mathcal{N}_{\bar{\eta}}$ is a finitely-generated unit $L[F^r]$ -module, which must be trivial.

Consider the finite subset

$$(\mathcal{N}_{\bar{\eta}})^{F^r} \subseteq \mathcal{N}_{\bar{\eta}}.$$

There exists an étale open $U \rightarrow Y$ such that all elements of this subset can be realized as sections of \mathcal{N} on U . Let $\mathcal{P} \subseteq \mathcal{N}_{|U}$ be the subsheaf generated by the F^r -invariant sections of $\Gamma(U, \mathcal{N})$. This subsheaf is a trivial $\mathbb{O}_{Fr, U}$ -module.

The generic rank of \mathcal{P} is the same as that of $\mathcal{N}_{|U}$. Since $\mathcal{N}_{|U}$ is coherent on a dense open subset of U (by Proposition 2.1.7), it is easily seen that the sheaves $\mathcal{N}_{|U}$ and \mathcal{P} agree on some nonempty open subset $U' \subseteq U$.

Then, since $\mathcal{N}_{|U'}$ is a trivial $\mathbb{O}_{Fr, U'}$ -module, the dual sheaf $\mathcal{N}'_{|U'}$ is constant. This completes the proof. \square

Proof of Theorem 2.3.11. Propositions 4.5.1 and 4.5.4 assert that (2.3.12) is a constructible \mathbb{F}_{p^r} -sheaf and that (2.3.14) is an lfgu $\mathbb{O}_{Fr, Y}$ -module. The rest of the assertions in the theorem follow from Theorem 4.3.1 via Propositions 4.4.1 and 4.4.6. \square

Acknowledgements

This paper is the published version of my thesis from UC Berkeley. I gratefully acknowledge the help of my mentors, who have had extensive influence on the shape of the material here: Arthur Ogus (my thesis advisor), Martin Olsson, and Brian Conrad. I also thank Manuel Blickle, Igor Dolgachev, Kiran Kedlaya, Genady Lyubeznik, Mark Kisin, Jacob Lurie, Brian Osserman, Richard Pink, Bjorn Poonen, Karen Smith, and Nicolas Stalder for helpful discussions.

References

- [Blickle 2004] M. Blickle, “The intersection homology D -module in finite characteristic”, *Math. Ann.* **328**:3 (2004), 425–450. [MR 2005a:14005](#) [Zbl 1065.14006](#)
- [Blickle 2008] M. Blickle, “Minimal γ -sheaves”, *Algebra Number Theory* **2**:3 (2008), 347–368. [MR 2407119](#) [Zbl 05529329](#)
- [Deligne and Katz 1973] P. Deligne and N. Katz (editors), *Groupes de monodromie en géométrie algébrique, II: Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II)*, Lecture Notes in Math. **340**, Springer, Berlin, 1973. [MR 50 #7135](#) [Zbl 0275.14015](#)
- [Emerton and Kisin 2004] M. Emerton and M. Kisin, *The Riemann–Hilbert correspondence for unit F -crystals*, *Astérisque* **293**, Soc. Math. France, Paris, 2004. [MR 2005e:14027](#) [Zbl 1056.14025](#)
- [Lyubeznik 1997] G. Lyubeznik, “ F -modules: applications to local cohomology and D -modules in characteristic $p > 0$ ”, *J. Reine Angew. Math.* **491** (1997), 65–130. [MR 99c:13005](#) [Zbl 0904.13003](#)
- [Pink 2000] R. Pink, “Euler–Poincaré formula in equal characteristic under ordinarity assumptions”, *Manuscripta Math.* **102**:1 (2000), 1–24. [MR 2001j:11048](#) [Zbl 1010.11034](#)
- [Raynaud 1995] M. Raynaud, “Caractéristique d’Euler–Poincaré d’un faisceau et cohomologie des variétés abéliennes”, pp. 129–147, Exp. No. 286 in *Séminaire Bourbaki*, Vol. 9, Soc. Math. France, Paris, 1995. [MR 1608794](#)

Communicated by Hélène Esnault

Received 2009-03-21

Revised 2009-10-21

Accepted 2009-11-23

carlmi@umich.edu

*Department of Mathematics, 530 Church Street,
University of Michigan, Ann Arbor, MI 48109, United States*
<http://www.umich.edu/~carlmi/>

Reflexivity and rigidity for complexes, I

Commutative rings

Luchezar L. Avramov, Srikanth B. Iyengar and Joseph Lipman

To our friend and colleague, Hans-Bjørn Foxby.

A notion of rigidity with respect to an arbitrary semidualizing complex C over a commutative noetherian ring R is introduced and studied. One of the main results characterizes C -rigid complexes. Specialized to the case when C is the relative dualizing complex of a homomorphism of rings of finite Gorenstein dimension, it leads to broad generalizations of theorems of Yekutieli and Zhang concerning rigid dualizing complexes, in the sense of Van den Bergh. Along the way, new results about derived reflexivity with respect to C are established. Noteworthy is the statement that derived C -reflexivity is a local property; it implies that a finite R -module M has finite G -dimension over R if $M_{\mathfrak{m}}$ has finite G -dimension over $R_{\mathfrak{m}}$ for each maximal ideal \mathfrak{m} of R .

| | |
|----------------------------------|----|
| Introduction | 48 |
| 1. Depth | 50 |
| 2. Derived reflexivity | 53 |
| 3. Semidualizing complexes | 55 |
| 4. Perfect complexes | 57 |
| 5. Invertible complexes | 62 |
| 6. Duality | 67 |
| 7. Rigidity | 70 |
| 8. Relative dualizing complexes | 73 |
| Appendix: Homological invariants | 80 |
| Acknowledgments | 84 |
| References | 84 |

MSC2000: primary 13D05, 13D25; secondary 13C15, 13D03.

Keywords: semidualizing complexes, perfect complexes, invertible complexes, rigid complexes, relative dualizing complexes, derived reflexivity, finite Gorenstein dimension.

Our research was partly supported by NSF grant DMS 0803082 (Avramov), NSF grant DMS 0602498 (Iyengar), and NSA grant H98230-06-1-0010 (Lipman).

Introduction

Rigidification means, roughly, endowing a type of object with extra structure so as to eliminate nonidentity automorphisms. For example, a rigidification for dualizing sheaves on varieties over perfect fields plays an important role in [Lipman 1984]. We will be concerned with rigidifying complexes arising from Grothendieck duality theory, both in commutative algebra and in algebraic geometry. This paper is devoted to the algebraic situation; the geometric counterpart is treated in [Avramov et al. 2010b].

Let R be a noetherian ring and $D(R)$ its derived category. We write $D_b^f(R)$ for the full subcategory of *homologically finite complexes*, that is to say, complexes M for which the R -module $H(M)$ is finitely generated. Given complexes M and C in $D_b^f(R)$ one says that M is *derived C -reflexive* if the canonical map

$$\delta_M^C : M \longrightarrow \mathrm{RHom}_R(\mathrm{RHom}_R(M, C), C)$$

is an isomorphism and $\mathrm{RHom}_R(M, C)$ is homologically finite. When the ring R has finite Krull dimension, the complex C is said to be *dualizing for R* if δ_M^C is an isomorphism for *all* homologically finite complexes M . In [Hartshorne 1966, p. 258, 2.1] it is proved that when C is isomorphic to some bounded complex of injective modules, C is dualizing if and only if it is *semidualizing*, meaning that the canonical map

$$\chi^C : R \longrightarrow \mathrm{RHom}_R(C, C)$$

is an isomorphism.

Even when $\mathrm{Spec} R$ is connected, dualizing complexes for R differ by shifts and the action of the Picard group of the ring [Hartshorne 1966, p. 266, 3.1]. Such a lack of uniqueness has been a source of difficulties. Building on work of Van den Bergh [1997] and extensively using differential graded algebras, Yekutieli and Zhang [2008; 2009] have developed for algebras of finite type over a regular ring K of finite Krull dimension a theory of *rigid relative to K* dualizing complexes. The additional structure that they carry makes them unique up to unique rigid isomorphism.

Our approach to rigidity applies to any noetherian ring R and takes place entirely within its derived category: We say that M is *C -rigid* if there is an isomorphism

$$\mu : M \xrightarrow{\cong} \mathrm{RHom}_R(\mathrm{RHom}_R(M, C), M),$$

called a *C -rigidifying isomorphism* for M . In the context described in the previous paragraph we prove, using the main result of [Avramov et al. 2010a], that rigidity in the sense of Van den Bergh, Yekutieli, and Zhang coincides with *C -rigidity* for a specific complex C .

The precise significance of C -rigidity is explained by the following result. It is abstracted from [Theorem 7.3](#), which requires no connectedness hypothesis.

Theorem 1. *If C is a semidualizing complex, then $\mathrm{RHom}_R(\chi^C, C)^{-1}$ is a C -rigidifying isomorphism.*

When $\mathrm{Spec} R$ is connected and M is nonzero and C -rigid, with C -rigidifying isomorphism μ , there exists a unique isomorphism $\alpha: C \xrightarrow{\sim} M$ making the following diagram commute:

$$\begin{array}{ccc}
 C & \xrightarrow{\mathrm{RHom}_R(\chi^C, C)^{-1}} & \mathrm{RHom}_R(\mathrm{RHom}_R(C, C), C) \\
 \alpha \downarrow & & \downarrow \mathrm{RHom}_R(\mathrm{RHom}_R(\alpha, C), \alpha) \\
 M & \xrightarrow{\mu} & \mathrm{RHom}_R(\mathrm{RHom}_R(M, C), M)
 \end{array}$$

Semidualizing complexes, identified by Foxby [1972] and Golod [1984] in the case of modules, have received considerable attention in [Avramov and Foxby 1997] and in the work of Christensen, Frankild, Sather-Wagstaff, and Taylor [Christensen 2001; Frankild and Sather-Wagstaff 2007; Frankild et al. 2009]. However, to achieve our goals we need to go further back and rethink basic propositions concerning derived reflexivity. This is the content of Sections 1 through 6, from which we highlight some results.

Theorem 2. *When C is semidualizing, M is derived C -reflexive if (and only if) there exists some isomorphism $M \simeq \mathrm{RHom}_R(\mathrm{RHom}_R(M, C), C)$ in $\mathrm{D}(R)$, if (and only if) $M_{\mathfrak{m}}$ is derived $C_{\mathfrak{m}}$ -reflexive for each maximal ideal \mathfrak{m} of R .*

This is part of [Theorem 3.3](#). One reason for its significance is that it delivers derived C -reflexivity bypassing a delicate step, the verification that $\mathrm{RHom}_R(M, C)$ is homologically finite. Another is that it establishes that derived C -reflexivity is a local property. This implies, in particular, that a finite R -module M has finite G-dimension (Gorenstein dimension) in the sense of Auslander and Bridger [1969] if it has that property at each maximal ideal of R ; see [Corollary 6.3.4](#).

In [Theorem 5.6](#) we characterize pairs of mutually reflexive complexes:

Theorem 3. *The complexes C and M are semidualizing and satisfy $C \simeq L \otimes_R M$ for some invertible graded R -module L if and only if M is derived C -reflexive, C is derived M -reflexive, and $\mathrm{H}(M)_{\mathfrak{p}} \neq 0$ holds for every $\mathfrak{p} \in \mathrm{Spec} R$.*

In the last section we apply our results to the *relative dualizing complex* D^σ attached to an algebra $\sigma: K \rightarrow S$ essentially of finite type over a noetherian ring K ; see [Avramov et al. 2010a, 1.1 and 6.2]. We show that D^σ is semidualizing if and only if σ has finite G-dimension in the sense of [Avramov and Foxby 1997]. One case when the G-dimension of σ is finite is if S has finite flat dimension as a

K -module. In this context, it follows from a result of [Avramov et al. 2010a] that D^σ -rigidity is equivalent to rigidity relative to K , in the sense of [Yekutieli and Zhang 2009]. We prove:

Theorem 4. *If K is Gorenstein, the flat dimension of the K -module S is finite, and $\dim S$ is finite, then D^σ is dualizing for S and is rigid relative to K .*

When moreover $\text{Spec } S$ is connected, D^σ is the unique, up to unique rigid isomorphism, nonzero complex in $D_b^f(S)$ that is rigid relative to K .

This result, which is contained in Theorem 8.5.6, applies in particular when K is regular, and is a broad generalization of one of the main results in [Yekutieli and Zhang 2009].

Our terminology and notation are mostly in line with literature in commutative algebra. In particular, we put “homological” gradings on complexes, so at first sight some formulas may look unfamiliar to experts used to cohomological conventions. More details may be found in the Appendix, where we also prove results on Poincaré series and Bass series of complexes invoked repeatedly in the body of the text.

Several objects studied in this paper were introduced by Hans-Bjørn Foxby, and various techniques used below were initially developed by him. We have learned a lot about the subject from his articles, his lectures, and through collaborations with him. This work is dedicated to him in appreciation and friendship.

1. Depth

Throughout the paper R denotes a *commutative noetherian ring*. An R -module is said to be “finite” if it can be generated, as an R -module, by finitely many elements.

The *depth* of a complex M over a local ring R with residue field k is the number

$$\text{depth}_R M = \inf\{n \in \mathbb{Z} \mid \text{Ext}_R^n(k, M) \neq 0\}.$$

We focus on a global invariant that appears in work of Chouinard and Foxby:

$$\text{Rfd}_R M = \sup\{\text{depth } R_{\mathfrak{p}} - \text{depth}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} \mid \mathfrak{p} \in \text{Spec } R\}. \quad (1.0.1)$$

See 1.6 for a different description of this number. Our goal is to prove:

Theorem 1.1. *Every complex M in $D_b^f(R)$ satisfies $\text{Rfd}_R M < \infty$.*

The desired inequality is obvious for rings of finite Krull dimension. To handle the general case, we adapt the proof of a result of Gabber; see Proposition 1.5.

A couple of simple facts are needed to keep the argument going:

1.2. If $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$ is an exact sequence of complexes then one has

$$\text{Rfd}_R M \leq \max\{\text{Rfd}_R L, \text{Rfd}_R N\}.$$

Indeed, for every $\mathfrak{p} \in \text{Spec } R$ and each $n \in \mathbb{Z}$ one has an induced exact sequence

$$\text{Ext}_{R_{\mathfrak{p}}}^n(R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}, L_{\mathfrak{p}}) \rightarrow \text{Ext}_{R_{\mathfrak{p}}}^n(R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}, M_{\mathfrak{p}}) \rightarrow \text{Ext}_{R_{\mathfrak{p}}}^n(R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}, N_{\mathfrak{p}})$$

that yields $\text{depth}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} \geq \min\{\text{depth}_{R_{\mathfrak{p}}} L_{\mathfrak{p}}, \text{depth}_{R_{\mathfrak{p}}} N_{\mathfrak{p}}\}$.

The statement below is an Auslander–Buchsbaum equality for complexes:

1.3. Each bounded complex F of finite free modules over a local ring R has

$$\text{depth}_R F = \text{depth } R - \sup H(k \otimes_R F);$$

see [Foxby 1979, 3.13]. This formula is an immediate consequence of the isomorphisms

$$\text{RHom}_R(k, F) \simeq \text{RHom}_R(k, R) \otimes_R^{\mathbb{L}} F \simeq \text{RHom}_R(k, R) \otimes_k^{\mathbb{L}} (k \otimes_R F)$$

in $D(R)$, where the first one holds because F is finite free.

Proof of Theorem 1.1. It's enough to prove that $\text{Rfd}_R M < \infty$ holds for cyclic modules. Indeed, replacing M with a quasiisomorphic complex we may assume $\text{amp } M = \text{amp } H(M)$. If one has $\text{amp } M = 0$, then M is a shift of a finite R -module, so an induction on the number of its generators, using 1.2, shows that $\text{Rfd}_R M$ is finite. Assume the statement holds for all complexes of a given amplitude. Since $L = \Sigma^i M_i$ with $i = \inf M$ is a subcomplex of M , and one has $\text{amp}(M/L) < \text{amp } M$, using 1.2 and induction we obtain $\text{Rfd}_R M \leq \max\{\text{Rfd}_R L, \text{Rfd}_R (M/L)\} < \infty$.

By way of contradiction, assume $\text{Rfd}_R (R/J) = \infty$ holds for some ideal J of R . Since R is noetherian, we may choose J so that $\text{Rfd}_R (R/I)$ is finite for each ideal I with $I \supsetneq J$. The ideal J is prime: otherwise one would have an exact sequence

$$0 \rightarrow R/J' \rightarrow R/J \rightarrow R/I \rightarrow 0,$$

where J' is a prime ideal associated to R/J with $J' \supsetneq J$; this implies $I \supsetneq J$, so in view of 1.2 the exact sequence yields $\text{Rfd}_R (R/J) < \infty$, which is absurd.

Set $S = R/J$, fix a finite generating set of J , let g denote its cardinality, and E be the Koszul complex on it. As S is a domain and $\bigoplus_i H_i(E)$ is a finite S -module, we may choose $f \in R \setminus J$ so that each S_f -module $H_i(E)_f$ is free. Now $(J, f) \supsetneq J$ implies that $j = \text{Rfd}_R (R/(J, f))$ is finite. To get the desired contradiction we prove

$$\text{depth } R_{\mathfrak{p}} - \text{depth}_{R_{\mathfrak{p}}} S_{\mathfrak{p}} \leq \max\{j - 1, g\} \quad \text{for each } \mathfrak{p} \in \text{Spec } R.$$

In the case $\mathfrak{p} \not\supseteq J$ one has $\text{depth}_{R_{\mathfrak{p}}} S_{\mathfrak{p}} = \infty$, so the inequality obviously holds.

When $\mathfrak{p} \supseteq (J, f)$ the exact sequence

$$0 \rightarrow S \xrightarrow{f} S \rightarrow R/(J, f) \rightarrow 0$$

yields $\text{depth}_{R_{\mathfrak{p}}} S_{\mathfrak{p}} = \text{depth}_{R_{\mathfrak{p}}}(R/(J, f))_{\mathfrak{p}} + 1$, and hence one has

$$\text{depth } R_{\mathfrak{p}} - \text{depth}_{R_{\mathfrak{p}}} S_{\mathfrak{p}} \leq j - 1.$$

It remains to treat the case $f \notin \mathfrak{p} \supseteq J$. Set $k = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$, $d = \text{depth}_{R_{\mathfrak{p}}} S_{\mathfrak{p}}$, and $s = \sup H(E_{\mathfrak{p}})$. In the second quadrant spectral sequence

$$\begin{aligned} {}^2E_{p,q} = \text{Ext}_{R_{\mathfrak{p}}}^{-p}(k, H_q(E_{\mathfrak{p}})) &\implies \text{Ext}_{R_{\mathfrak{p}}}^{-p-q}(k, E_{\mathfrak{p}}), \\ {}^r d^{p,q} : {}^r E_{p,q} &\longrightarrow {}^r E_{p-r, q+r-1}, \end{aligned}$$

one has ${}^2E_{p,q} = 0$ for $q > s$, and also for $p > -d$ because each $H_q(E_{\mathfrak{p}})$ is a finite direct sum of copies of $S_{\mathfrak{p}}$. Therefore, the sequence converges strongly and yields

$$\text{Ext}_{R_{\mathfrak{p}}}^i(k, E_{\mathfrak{p}}) \cong \begin{cases} 0 & \text{for } i < d - s, \\ \text{Ext}_{R_{\mathfrak{p}}}^d(k, H_s(E_{\mathfrak{p}})) \neq 0 & \text{for } i = d - s. \end{cases}$$

The formula above implies $\text{depth}_{R_{\mathfrak{p}}} E_{\mathfrak{p}} = d - s$. This gives the first equality below, with the second equality coming from 1.3.

$$\begin{aligned} \text{depth } R_{\mathfrak{p}} - \text{depth}_{R_{\mathfrak{p}}} S_{\mathfrak{p}} &= \text{depth } R_{\mathfrak{p}} - \text{depth}_{R_{\mathfrak{p}}} E_{\mathfrak{p}} - s \\ &= \sup H(k \otimes_{R_{\mathfrak{p}}} E_{\mathfrak{p}}) - s \\ &\leq g - s \leq g. \end{aligned} \quad \square$$

A complex in $D_-(R)$ is said to have *finite injective dimension* if it is isomorphic in $D(R)$ to a bounded complex of injective R -modules. The next result, due to Ischebeck [1969, 2.6] when M and N are modules, can be deduced from [Christensen et al. 2002, 4.13].

Lemma 1.4. *Let R be a local ring and N in $D_b^f(R)$ a complex of finite injective dimension. For each M in $D_b^f(R)$ there is an equality*

$$\sup\{n \in \mathbb{Z} \mid \text{Ext}_R^n(M, N) \neq 0\} = \text{depth } R - \text{depth } M - \inf H(N).$$

Proof. Let k be the residue field k of R . The first isomorphism below holds because N has finite injective dimension and M is in $D_b^f(R)$ (see [Avramov and Foxby 1991, 4.4.I]):

$$\begin{aligned} H(k \otimes_R^{\mathbb{L}} \text{RHom}_R(M, N)) &\cong H(\text{RHom}_R(\text{RHom}_R(k, M), N)) \\ &\cong H(\text{RHom}_k(\text{RHom}_R(k, M), \text{RHom}_R(k, N))) \\ &\cong \text{Hom}_k(H(\text{RHom}_R(k, M)), H(\text{RHom}_R(k, N))). \end{aligned}$$

The other isomorphisms are standard. One deduces the second equality below:

$$\begin{aligned} \inf H(\text{RHom}_R(M, N)) &= \inf H(k \otimes_R^{\mathbb{L}} \text{RHom}_R(M, N)) \\ &= \inf H(\text{RHom}_R(k, N)) + \text{depth}_R M. \end{aligned}$$

The first one comes from [Lemma A.4.3](#). In particular, for $M = R$ this yields

$$\inf H(\mathrm{RHom}_R(k, N)) = \inf H(N) - \mathrm{depth} R.$$

Combining the preceding equalities, one obtains the desired assertion. \square

The next result is due to Gabber [[Conrad 2000](#), 3.1.5]; Goto [[1982](#)] had proved it for $N = R$.

Proposition 1.5. *For each N in $D_b^f(R)$ the following conditions are equivalent.*

- (i) *For each $\mathfrak{p} \in \mathrm{Spec} R$ the complex $N_{\mathfrak{p}}$ has finite injective dimension over $R_{\mathfrak{p}}$.*
- (ii) *For each M in $D_b^f(R)$ one has $\mathrm{Ext}_R^n(M, N) = 0$ for $n \gg 0$.*
- (ii') *For each $\mathfrak{m} \in \mathrm{Max} R$ one has $\mathrm{Ext}_R^n(R/\mathfrak{m}, N) = 0$ for $n \gg 0$.*

Proof. (i) \implies (ii). For each prime \mathfrak{p} , [Lemma 1.4](#) yields the second equality below:

$$\begin{aligned} -\inf H(\mathrm{RHom}_R(M, N)_{\mathfrak{p}}) &= -\inf H(\mathrm{RHom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}})) \\ &= \mathrm{depth} R_{\mathfrak{p}} - \mathrm{depth}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} - \inf H(N_{\mathfrak{p}}) \\ &\leq \mathrm{Rfd}_R M - \inf H(N). \end{aligned}$$

[Theorem 1.1](#) thus implies the desired result.

(ii') \implies (i). Since N is in $D_b^f(R)$ for each integer n , one has an isomorphism

$$\mathrm{Ext}_{R_{\mathfrak{m}}}^n(R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}, N_{\mathfrak{m}}) \cong \mathrm{Ext}_R^n(R/\mathfrak{m}, N)_{\mathfrak{m}}.$$

Thus, the hypothesis and [A.5.1](#) imply $N_{\mathfrak{m}}$ has finite injective dimension over $R_{\mathfrak{m}}$. By localization, $N_{\mathfrak{p}}$ has finite injective dimension over $R_{\mathfrak{p}}$ for each prime $\mathfrak{p} \subseteq \mathfrak{m}$. \square

Notes 1.6. In [[Christensen et al. 2002](#), 2.1] the number $\mathrm{Rfd}_R M$ is defined by the formula

$$\mathrm{Rfd}_R M = \sup\{n \in \mathbb{Z} \mid \mathrm{Tor}_n^R(T, M) \neq 0\},$$

where T ranges over the R -modules of finite flat dimension, and is called the *large restricted flat dimension* of M (hence the notation). With this definition, formula [\(1.0.1\)](#) is due to Foxby (see [[Christensen 2000](#), Notes, p. 131]) and is proved in [[Christensen 2000](#), 5.3.6; [Christensen et al. 2002](#), 2.4(b)]. For M of finite flat dimension one has $\mathrm{Rfd}_M = \mathrm{fd}_R M$ [[Christensen 2000](#), 5.4.2(b); [Christensen et al. 2002](#), 2.5] and then [\(1.0.1\)](#) goes back to [[Chouinard 1976](#), 1.2].

2. Derived reflexivity

For every pair C, M in $D(R)$ there is a canonical *biduality morphism*

$$\delta_M^C: M \rightarrow \mathrm{RHom}_R(\mathrm{RHom}_R(M, C), C), \quad (2.0.1)$$

induced by the morphism of complexes $m \mapsto (\alpha \mapsto (-1)^{|m||\alpha|}\alpha(m))$. We say that M is *derived C -reflexive* if both M and $\mathrm{RHom}_R(M, C)$ are in $D_b^f(R)$, and δ_M^C is an isomorphism. Some authors write “ C -reflexive” instead of “derived C -reflexive”.

Recall that the *support* of a complex M in $D_b^f(R)$ is the set

$$\mathrm{Supp}_R M = \{\mathfrak{p} \in \mathrm{Spec} R \mid H(M)_{\mathfrak{p}} \neq 0\}.$$

Theorem 2.1. *Let R be a noetherian ring and C a complex in $D_b^f(R)$.*

For each complex M in $D_b^f(R)$, the following conditions are equivalent.

- (i) M is derived C -reflexive.
- (ii) $\mathrm{RHom}_R(M, C)$ is derived C -reflexive and $\mathrm{Supp}_R M \subseteq \mathrm{Supp}_R C$ holds.
- (iii) $\mathrm{RHom}_R(M, C)$ is in $D_+(R)$, and for every $\mathfrak{m} \in \mathrm{Max} R$ one has

$$M_{\mathfrak{m}} \simeq \mathrm{RHom}_{R_{\mathfrak{m}}}(\mathrm{RHom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, C_{\mathfrak{m}}), C_{\mathfrak{m}}) \quad \text{in } D(R_{\mathfrak{m}}).$$

- (iv) $U^{-1}M$ is derived $U^{-1}C$ -reflexive for each multiplicatively closed set $U \subseteq R$.

The proof is based on a useful criterion for derived C -reflexivity.

2.2. Let C and M be complexes of R -modules, and set $h = \mathrm{RHom}_R(-, C)$.

The composition $h(\delta_M^C) \circ \delta_{h(M)}^C$ is the identity map of $h(M)$, so the map

$$H(\delta_{h(M)}^C): H(h(M)) \rightarrow H(h^3(M))$$

is a split monomorphism. Thus, if $h(M)$ is in $D^f(R)$ and there exists some isomorphism $H(h(M)) \cong H(h^3(M))$, then $\delta_{h(M)}^C$ and $h(\delta_M^C)$ are isomorphisms in $D(R)$.

The following proposition is an unpublished result of Foxby.

Proposition 2.3. *If for C and M in $D_b^f(R)$ there exists an isomorphism*

$$\mu: M \simeq \mathrm{RHom}_R(\mathrm{RHom}_R(M, C), C) \quad \text{in } D(R),$$

then the biduality morphism δ_M^C is an isomorphism as well.

Proof. Set $h = \mathrm{RHom}_R(-, C)$. Note that $h(M)$ is in $D_b^f(R)$ because C and M are in $D_b^f(R)$. The morphism μ induces an isomorphism $H(h^3(M)) \cong H(h(M))$. Each R -module $H_n(h(M)) = \mathrm{Ext}_R^{-n}(M, C)$ is finite, so we conclude from 2.2 that $\delta_{h(M)}^C$ is an isomorphism in $D(R)$, and hence $\delta_{h^2(M)}^C$ is one as well. The square

$$\begin{array}{ccc} M & \xrightarrow[\simeq]{\mu} & h^2(M) \\ \delta_M^C \downarrow & & \simeq \downarrow \delta_{h^2(M)}^C \\ h^2(M) & \xrightarrow[\simeq]{h^2(\mu)} & h^4(M) \end{array}$$

in $D(R)$ commutes and implies that δ_M^C is an isomorphism, as desired. \square

Proof of Theorem 2.1. (i) \implies (ii). This follows from 2.2 and A.6.

(ii) \implies (i). Set $h = \mathrm{RHom}_R(-, C)$ and form the exact triangle in $D(R)$:

$$M \xrightarrow{\delta_M^C} h^2(M) \longrightarrow N \longrightarrow$$

As $h(M)$ is C -reflexive, one has $h^2(M) \in D_b^f(R)$, so the exact triangle above implies that N is in $D_b^f(R)$. Since $\mathrm{Supp}_R M \subseteq \mathrm{Supp}_R C$ holds, using A.6 one obtains

$$\begin{aligned} \mathrm{Supp}_R N &\subseteq \mathrm{Supp}_R M \cup \mathrm{Supp}_R h^2(M) \\ &= \mathrm{Supp}_R M \cup (\mathrm{Supp}_R M \cap \mathrm{Supp}_R C) \subseteq \mathrm{Supp}_R C. \end{aligned}$$

On the other hand, the exact triangle above induces an exact triangle

$$h(N) \longrightarrow h^3(M) \xrightarrow{h(\delta_M^C)} h(M) \longrightarrow$$

Since $h(M)$ is C -reflexive $\delta_{h(M)}^C$ is an isomorphism, so 2.2 shows that $h(\delta_M^C)$ is an isomorphism as well. The second exact triangle now gives $H(h(N)) = 0$. The already established inclusion $\mathrm{Supp}_R N \subseteq \mathrm{Supp}_R C$ and A.6 yield

$$\mathrm{Supp}_R N = \mathrm{Supp}_R N \cap \mathrm{Supp}_R C = \mathrm{Supp}_R \mathrm{RHom}_R(N, C) = \emptyset.$$

This implies $N = 0$ in $D(R)$, and hence δ_M^C is an isomorphism.

(i) \implies (iv). This is a consequence of the hypothesis $\mathrm{RHom}_R(M, C) \in D_+^f(R)$.

(iv) \implies (iii). With $U = \{1\}$ the hypotheses in (iv) implies $\mathrm{RHom}_R(M, C)$ is in $D_+^f(R)$, while the isomorphism in (iii) is the special case $U = R \setminus \mathfrak{m}$.

(iii) \implies (i). For each $\mathfrak{m} \in \mathrm{Max} R$, Proposition 2.3 yields that $\delta_{M_{\mathfrak{m}}}^{C_{\mathfrak{m}}}$ is an isomorphism, in $D(R_{\mathfrak{m}})$. One has a canonical isomorphism

$$\lambda_{\mathfrak{m}}: \mathrm{RHom}_R(\mathrm{RHom}_R(M, C), C)_{\mathfrak{m}} \xrightarrow{\cong} \mathrm{RHom}_{R_{\mathfrak{m}}}(\mathrm{RHom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, C_{\mathfrak{m}}), C_{\mathfrak{m}}),$$

because $\mathrm{RHom}_R(M, C)$ is in $D_+^f(R)$ and M is in $D_b^f(R)$. Now using the equality $\delta_{M_{\mathfrak{m}}}^{C_{\mathfrak{m}}} = \lambda_{\mathfrak{m}}(\delta_M^C)_{\mathfrak{m}}$ one sees that $(\delta_M^C)_{\mathfrak{m}}$ is an isomorphism, and hence so is δ_M^C . \square

3. Semidualizing complexes

For each complex C there is a canonical *homothety morphism*

$$\chi^C: R \rightarrow \mathrm{RHom}_R(C, C) \quad \text{in } D(R) \quad (3.0.1)$$

induced by $r \mapsto (c \mapsto rc)$. As in [Christensen 2001, 2.1], we say that C is *semidualizing* if it is in $D_b^f(R)$ and χ^C an isomorphism. We bundle convenient recognition criteria in:

Proposition 3.1. *For a complex C in $D_b^f(R)$ the following are equivalent:*

(i) C is semidualizing.

- (i') R is derived C -reflexive.
(ii) C is derived C -reflexive and $\text{Supp}_R C = \text{Spec } R$.
(iii) For each $\mathfrak{m} \in \text{Max } R$ there is an isomorphism

$$R_{\mathfrak{m}} \simeq \text{RHom}_{R_{\mathfrak{m}}}(C_{\mathfrak{m}}, C_{\mathfrak{m}}) \quad \text{in } D(R_{\mathfrak{m}}).$$

- (iv) $U^{-1}C$ is semidualizing for $U^{-1}R$ for each multiplicatively closed set $U \subseteq R$.

Proof. To see that (i) and (i') are equivalent, decompose χ^C as

$$R \xrightarrow{\delta_R^C} \text{RHom}_R(\text{RHom}_R(R, C), C) \xrightarrow{\cong} \text{RHom}_R(C, C),$$

with isomorphism induced by the canonical isomorphism $C \xrightarrow{\cong} \text{RHom}_R(R, C)$. Conditions (i') through (iv) are equivalent by [Theorem 2.1](#) applied with $M = R$. \square

Next we establish a remarkable property of semidualizing complexes. It uses the invariant $\text{Rfd}_R(-)$ discussed in [Section 1](#).

Theorem 3.2. *If C is a semidualizing complex for R and L is a complex in $D_-^f(R)$ with $\text{RHom}_R(L, C) \in D_b^f(R)$, then L is in $D_b^f(R)$; more precisely, one has*

$$\inf H(L) \geq \inf H(C) - \text{Rfd}_R \text{RHom}_R(L, C) > -\infty.$$

Proof. For each $\mathfrak{m} \in \text{Max } R \cap \text{Supp}_R L$ one has a chain of relations

$$\begin{aligned} \inf H(L_{\mathfrak{m}}) &= -\text{depth}_{R_{\mathfrak{m}}} C_{\mathfrak{m}} + \text{depth}_{R_{\mathfrak{m}}} \text{RHom}_R(L, C)_{\mathfrak{m}} \\ &= \inf H(C_{\mathfrak{m}}) - \text{depth } R_{\mathfrak{m}} + \text{depth}_{R_{\mathfrak{m}}} \text{RHom}_R(L, C)_{\mathfrak{m}} \\ &\geq \inf H(C) - \text{Rfd}_R \text{RHom}_R(L, C) \\ &> -\infty \end{aligned}$$

with equalities given by [Lemma A.5.3](#), applied first with $M = L$ and $N = C$, then with $M = C = N$; the first inequality is clear, and the second one holds by [Theorem 1.1](#). Now use the equality $\inf H(L) = \inf_{\mathfrak{m} \in \text{Max } R} \{\inf H(L_{\mathfrak{m}})\}$. \square

The next theorem parallels [Theorem 2.1](#). The impact of the hypothesis that C is semidualizing can be seen by comparing condition (iii) in these results: one need not assume $\text{RHom}_R(M, C)$ is bounded. In particular, reflexivity with respect to a semidualizing complex can now be *defined* by means of property (i') alone. Antecedents of the theorem are discussed in [3.4](#).

Theorem 3.3. *Let C be a semidualizing complex for R .*

For a complex M in $D_b^f(R)$ the following conditions are equivalent:

- (i) M is derived C -reflexive.
(i') There exists an isomorphism $M \simeq \text{RHom}_R(\text{RHom}_R(M, C), C)$.

- (ii) $\mathrm{RHom}_R(M, C)$ is derived C -reflexive.
 (iii) For each $\mathfrak{m} \in \mathrm{Max} R$ there is an isomorphism

$$M_{\mathfrak{m}} \simeq \mathrm{RHom}_{R_{\mathfrak{m}}}(\mathrm{RHom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, C_{\mathfrak{m}}), C_{\mathfrak{m}}) \quad \text{in } \mathrm{D}(R_{\mathfrak{m}}).$$

Furthermore, these conditions imply the following inequalities

$$\mathrm{amp} \mathrm{H}(\mathrm{RHom}_R(M, C)) \leq \mathrm{amp} \mathrm{H}(C) - \inf \mathrm{H}(M) + \mathrm{Rfd}_R M < \infty.$$

Proof. (i) \iff (ii). Apply [Theorem 2.1](#), noting that $\mathrm{Supp}_R C = \mathrm{Spec} R$, by [A.6](#).

(i) \implies (i'). This implication is a tautology.

(i') \implies (iii). This holds because [Theorem 3.2](#), applied with $L = \mathrm{RHom}_R(M, C)$, shows that $\mathrm{RHom}_R(M, C)$ is bounded, and so the given isomorphism localizes.

(iii) \implies (i). For each $\mathfrak{m} \in \mathrm{Max} R$ the complex $C_{\mathfrak{m}}$ is semidualizing for $R_{\mathfrak{m}}$ by [Proposition 3.1](#). One then has a chain of (in)equalities

$$\begin{aligned} \inf \mathrm{H}(\mathrm{RHom}_R(M, C)) &= \inf_{\mathfrak{m} \in \mathrm{Max} R} \{\inf \mathrm{H}(\mathrm{RHom}_R(M, C)_{\mathfrak{m}})\} \\ &= \inf_{\mathfrak{m} \in \mathrm{Max} R} \{\inf \mathrm{H}(\mathrm{RHom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, C_{\mathfrak{m}}))\} \\ &\geq \inf_{\mathfrak{m} \in \mathrm{Max} R} \{\inf \mathrm{H}(C_{\mathfrak{m}}) - \mathrm{Rfd}_{R_{\mathfrak{m}}} M_{\mathfrak{m}}\} \\ &\geq \inf \mathrm{H}(C) - \sup_{\mathfrak{m} \in \mathrm{Max} R} \{\mathrm{Rfd}_{R_{\mathfrak{m}}} M_{\mathfrak{m}}\} \\ &= \inf \mathrm{H}(C) - \mathrm{Rfd}_R M \\ &> -\infty, \end{aligned}$$

where the first inequality comes from [Theorem 3.2](#) applied over $R_{\mathfrak{m}}$ to the complex $L = \mathrm{RHom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, C_{\mathfrak{m}})$, while the last inequality is given by [Theorem 1.1](#). It now follows from [Theorem 2.1](#) that M is derived C -reflexive.

The relations above and [A.1](#) yield the desired bounds on amplitude. \square

Notes 3.4. The equivalence (i) \iff (ii) in [Theorem 3.3](#) follows from [[Christensen 2000](#), 2.1.10; [2001](#), 2.11]; see [[Frankild et al. 2009](#), 3.3]. When $\dim R$ is finite, a weaker form of (iii) \implies (i) is proved in [[Frankild and Sather-Wagstaff 2007](#), 2.8]: $\delta_{M_{\mathfrak{m}}}^{C_{\mathfrak{m}}}$ an isomorphism for all $\mathfrak{m} \in \mathrm{Max} R$ implies that δ_M^C is one.

When R is Cohen–Macaulay and local each semidualizing complex C satisfies $\mathrm{amp} \mathrm{H}(C) = 0$, so it is isomorphic to a shift of a finite module; see [[Christensen 2001](#), 3.4].

4. Perfect complexes

Recall that a complex of R -modules is said to be *perfect* if it is isomorphic in $\mathrm{D}(R)$ to a bounded complex of finite projective modules. For ease of reference we collect, with complete proofs, some useful tests for perfection; the equivalence of

(i) and (ii) is contained in [Christensen 2000, 2.1.10], while the argument that (i) are (iii) are equivalent is modelled on a proof when M is a module, due to Bass and Murthy [Bass and Murthy 1967, 4.5].

Theorem 4.1. *For a complex M in $D_b^f(R)$ the following conditions are equivalent.*

- (i) M is perfect.
- (ii) $\mathrm{RHom}_R(M, R)$ is perfect.
- (iii) $M_{\mathfrak{m}}$ is perfect in $D(R_{\mathfrak{m}})$ for each $\mathfrak{m} \in \mathrm{Max} R$.
- (iii') $P_{M_{\mathfrak{m}}}^{R_{\mathfrak{m}}}(t)$ is a Laurent polynomial for each $\mathfrak{m} \in \mathrm{Max} R$.
- (iv) $U^{-1}M$ is perfect in $D(U^{-1}R)$ for each multiplicatively closed set $U \subseteq R$.

Proof. (iv) \implies (iii). This implication is a tautology.

(iii) \implies (i). Choose a resolution $F \xrightarrow{\sim} M$ with each F^i finite free and zero for $i \ll 0$. Set $s = \sup H(F) + 1$ and $H = \mathrm{Im}(\partial_s^F)$, and note that the complex $\Sigma^{-s}F_{\geq s}$ is a free resolution of H . Since each R -module $\mathrm{Im}(\partial_n^F)$ is finite, the subset of primes $\mathfrak{p} \in \mathrm{Spec} R$ with $\mathrm{Im}(\partial_n^F)_{\mathfrak{p}}$ projective over $R_{\mathfrak{p}}$ is open. It follows that the set

$$D_n = \{\mathfrak{p} \in \mathrm{Spec} R \mid \mathrm{pd}_{R_{\mathfrak{p}}} H_{\mathfrak{p}} \leq n\}$$

is open in $\mathrm{Spec} R$ for every $n \geq 0$. One has $D_n \subseteq D_{n+1}$ for $n \geq 0$, and the hypothesis means $\bigcup_{n \geq 0} D_n = \mathrm{Spec} R$. As $\mathrm{Spec} R$ is noetherian, it follows that $D_p = \mathrm{Spec} R$ holds for some $p \geq 0$, so that $\mathrm{Im}(\partial_{s+p}^F)$ is projective. Taking $E_n = 0$ for $n > s + p$, $E_{s+p} = \mathrm{Im}(\partial_{s+p}^F)$, and $E_n = F_n$ for $n < s + p$ one gets a perfect subcomplex E of F . The inclusion $E \rightarrow F$ is a quasiisomorphism, so F is perfect.

(i) \implies (iv) and (i) \implies (ii). In $D(R)$ one has $M \simeq F$ with F a bounded complex of finite projective R -modules. This implies isomorphisms $U^{-1}M \simeq U^{-1}F$ in $D(U^{-1}R)$ and $\mathrm{RHom}_R(M, R) \simeq \mathrm{RHom}_R(F, R)$ in $D(R)$, with bounded complexes of finite projective modules on their right hand sides.

(ii) \implies (i). The perfect complex $N = \mathrm{RHom}_R(M, R)$ is evidently derived R -reflexive, so the implication (ii) \implies (i) in Theorem 2.1 applied with $C = R$ gives $M \simeq \mathrm{RHom}_R(N, R)$; as we have just seen, $\mathrm{RHom}_R(N, R)$ is perfect along with N .

(iii) \iff (iii'). We may assume that R is local with maximal ideal \mathfrak{m} . By A.4.1, there is an isomorphism $F \simeq M$ in $D(R)$, with each F_n finite free, $\partial(F) \subseteq \mathfrak{m}F$, and $P_M^R(t) = \sum_{n \in \mathbb{Z}} \mathrm{rank}_R F_n t^n$. Thus, M is perfect if and only if $F_n = 0$ holds for all $n \gg 0$; that is, if and only if $P_M^R(t)$ is a Laurent polynomial. \square

The following elementary property of perfect complexes is well known:

4.2. If M and N are perfect complexes, then so are $M \otimes_R^{\mathbb{L}} N$ and $\mathrm{RHom}_R(M, N)$.

To prove a converse we use a version of a result from [Foxby and Iyengar 2003], which incorporates a deep result in commutative algebra, the New Intersection Theorem.

Theorem 4.3. *When M is a perfect complex of R -modules and N a complex in $D^f(R)$ satisfying $\text{Supp}_R N \subseteq \text{Supp}_R M$, the following inequalities hold:*

$$\begin{aligned} \sup H(N) &\leq \sup H(M \otimes_R^L N) - \inf H(M), \\ \inf H(N) &\geq \inf H(M \otimes_R^L N) - \sup H(M), \\ \text{amp } H(N) &\leq \text{amp } H(M \otimes_R^L N) + \text{amp } H(M). \end{aligned}$$

If $M \otimes_R^L N$ or $\text{RHom}_R(M, N)$ is in $D_b(R)$, then N is in $D_b^f(R)$.

Proof. For each \mathfrak{p} in $\text{Supp}_R N$ the complex $M_{\mathfrak{p}}$ is perfect and nonzero in $D(R_{\mathfrak{p}})$.

The second link in the following chain comes from [Foxby and Iyengar 2003, 3.1], and the rest are standard:

$$\begin{aligned} \sup H(N)_{\mathfrak{p}} &= \sup H(N_{\mathfrak{p}}) \\ &\leq \sup H(M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}}^L N_{\mathfrak{p}}) - \inf H(M_{\mathfrak{p}}) \\ &= \sup H(M \otimes_R^L N)_{\mathfrak{p}} - \inf H(M)_{\mathfrak{p}} \\ &\leq \sup H(M \otimes_R^L N) - \inf H(M). \end{aligned}$$

The first inequality follows, as one has $\sup H(N) = \sup_{\mathfrak{p} \in \text{Supp } N} \{\sup H(N)_{\mathfrak{p}}\}$.

Lemma A.4.3 gives the second link in the next chain, and the rest are standard:

$$\begin{aligned} \inf H(N)_{\mathfrak{p}} &= \inf H(N_{\mathfrak{p}}) \\ &= \inf H(M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}}^L N_{\mathfrak{p}}) - \inf H(M)_{\mathfrak{p}} \\ &= \inf H(M \otimes_R^L N)_{\mathfrak{p}} - \inf H(M)_{\mathfrak{p}} \\ &\geq \inf H(M \otimes_R^L N) - \sup H(M). \end{aligned}$$

The second inequality follows, as one has $\inf H(N) = \inf_{\mathfrak{p} \in \text{Supp } N} \{\inf H(N)_{\mathfrak{p}}\}$.

The first two inequalities imply the third one, which contains the assertion concerning $M \otimes_R^L N$. In turn, it implies the assertion concerning $\text{RHom}_R(M, N)$, because the complex $\text{RHom}_R(M, R)$ is perfect along with M , one has

$$\text{Supp}_R N \subseteq \text{Supp}_R M = \text{Supp}_R \text{RHom}_R(M, R)$$

due to A.6, and there is a canonical isomorphism

$$\text{RHom}_R(M, R) \otimes_R^L N \simeq \text{RHom}_R(M, N). \quad \square$$

Corollary 4.4. *Let M be a perfect complex and N a complex in $D^f(R)$ satisfying $\text{Supp}_R N \subseteq \text{Supp}_R M$. If $M \otimes_R^L N$ or $\text{RHom}_R(M, N)$ is perfect, then so is N .*

Proof. Suppose $M \otimes_R^L N$ is perfect; then $N \in D_b^f(R)$ holds, by Theorem 4.3. For each $\mathfrak{m} \in \text{Max } R$, Theorem 4.1 and Lemma A.4.3 imply that $P_{M_{\mathfrak{m}}}^{R_{\mathfrak{m}}}(t)P_{N_{\mathfrak{m}}}^{R_{\mathfrak{m}}}(t)$ is a

Laurent polynomial, and hence so is $P_{N_m}^R(t)$. Another application of [Theorem 4.1](#) now shows that N is perfect.

The statement about $\mathrm{RHom}_R(M, N)$ follows from the one concerning derived tensor products, by using the argument for the last assertion of the theorem. \square

Next we establish a stability property of derived reflexivity. The forward implication is well known; see, for instance, [[Christensen 2001](#), 3.17].

Theorem 4.5. *Let M be a perfect complex and C a complex in $D_-^f(R)$.*

If N in $D(R)$ is derived C -reflexive, then so is $M \otimes_R^L N$.

Conversely, for N in $D^f(R)$ satisfying $\mathrm{Supp}_R N \subseteq \mathrm{Supp}_R M$, if $M \otimes_R^L N$ is derived C -reflexive, then so is N .

Proof. We may assume that M is a bounded complex of finite projective R -modules.

Note that derived C -reflexivity is preserved by translation, direct sums, and direct summands, and that if two of the complexes in some exact triangle are derived C -reflexive, then so is the third. A standard induction on the number of nonzero components of M shows that when N is derived C -reflexive, so is $M \otimes_R N$.

Assume that $M \otimes_R^L N$ is derived C -reflexive and $\mathrm{Supp}_R N \subseteq \mathrm{Supp}_R M$ holds. [Theorem 4.3](#) gives $N \in D_b^f(R)$. For the complex $M^* = \mathrm{RHom}_R(M, R)$ and the functor $h(-) = \mathrm{RHom}_R(-, C)$, in $D(R)$ there is a natural isomorphism

$$M^* \otimes_R^L h(N) \simeq h(M \otimes_R^L N).$$

Now $h(N)$ is in $D^f(R)$ because N is in $D_b^f(R)$ and C is in $D_-^f(R)$, by [[Hartshorne 1966](#), p. 92, 3.3]. Since M is perfect, one has that

$$\mathrm{Supp}_R h(N) \subseteq \mathrm{Supp}_R N \subseteq \mathrm{Supp}_R M = \mathrm{Supp}_R M^*,$$

so [Theorem 4.3](#) gives $h(N) \in D_b^f(R)$. Thus, $h^2(N)$ is in $D^f(R)$, so the isomorphism

$$M \otimes_R^L h^2(N) \simeq h^2(M \otimes_R^L N) \tag{4.5.1}$$

and [Theorem 4.3](#) yield $h^2(N) \in D_b^f(R)$. Forming an exact triangle

$$N \xrightarrow{\delta_N^C} h^2(N) \longrightarrow W \longrightarrow$$

one then gets $W \in D_b^f(R)$ and $\mathrm{Supp}_R W \subseteq \mathrm{Supp}_R N$.

In the induced exact triangle

$$M \otimes_R^L N \xrightarrow{M \otimes_R^L \delta_N^C} M \otimes_R^L h^2(N) \longrightarrow M \otimes_R^L W \longrightarrow$$

the morphism $M \otimes_R^L \delta_N^C$ is an isomorphism, as its composition with the isomorphism in (4.5.1) is equal to $\delta_{M \otimes_R^L N}^C$, which is an isomorphism by hypothesis. Thus, we

obtain

$$M \otimes_R^L W = 0 \quad \text{in } D(R),$$

hence $W = 0$ by [A.6](#), so δ_N^C is an isomorphism. \square

Sometimes, the perfection of a complex can be deduced from its homology.

Let H be a graded R -module. We say that H is (finite) graded projective if it is bounded and for each $i \in \mathbb{Z}$ the R -module H_i is (finite) projective.

4.6. If M is a complex of R -modules such that $H(M)$ is projective, then $M \simeq H(M)$ in $D(R)$, by [[Avramov et al. 2010a](#), 1.6]. Thus when $H(M)$ is in addition finite, M is perfect.

We recall some facts about projectivity and idempotents; see also [[Avramov and Iyengar 2008](#), 2.5].

4.7. Let H be a finite graded projective R -module.

The $R_{\mathfrak{p}}$ -module $(H_i)_{\mathfrak{p}}$ then is finite free for every $\mathfrak{p} \in \text{Spec } R$ and every $i \in \mathbb{Z}$, and one has $(H_i)_{\mathfrak{p}} = 0$ for almost all i , so H defines a function

$$r_H: \text{Spec } R \rightarrow \mathbb{N} \quad \text{given by } r_H(\mathfrak{p}) = \sum_{i \in \mathbb{Z}} \text{rank}_{R_{\mathfrak{p}}}(H_i)_{\mathfrak{p}}.$$

One has $r_H(\mathfrak{p}) = \text{rank}_{R_{\mathfrak{p}}}\left(\bigoplus_{i \in \mathbb{Z}} H_i\right)_{\mathfrak{p}}$; since the R -module $\bigoplus_{i \in \mathbb{Z}} H_i$ is finite projective, r_H is constant on each connected component of $\text{Spec } R$.

We say that H has rank d , and write $\text{rank}_R H = d$, if $r_H(\mathfrak{p}) = d$ holds for every $\mathfrak{p} \in \text{Spec } R$. We say that H is invertible if it is graded projective of rank 1.

4.8. Let $\{a_1, \dots, a_s\}$ be the (unique) complete set of orthogonal primitive idempotents of R . The open subsets $D_{a_i} = \{\mathfrak{p} \in \text{Spec } R \mid \mathfrak{p} \not\ni a_i\}$ for $i = 1, \dots, s$ are then the distinct connected components of $\text{Spec } R$.

An element a of R is idempotent if and only if $a = a_{i_1} + \dots + a_{i_r}$ with indices $1 \leq i_1 < \dots < i_r \leq s$; this sequence of indices is uniquely determined.

Let a be an idempotent and $-_a$ denote localization at the multiplicatively closed set $\{1, a\}$ of R . For all M and N in $D(R)$ there are canonical isomorphisms

$$M \simeq M_a \oplus M_{1-a} \quad \text{and} \\ \text{RHom}_R(M_a, N) \simeq \text{RHom}_R(M_a, N_a) \simeq \text{RHom}_R(M, N_a).$$

In particular, when M is in $D_b^f(R)$ so is M_a , and there is an isomorphism $M \simeq M_a$ in $D(R)$ if and only if one has $\text{Supp}_R M = D_a$.

Every graded R -module L has a canonical decomposition $L = \bigoplus_{i=1}^s L_{a_i}$.

The next result sounds — for the first time in this paper — the theme of rigidity.

Theorem 4.9. *Let L be a complex in $D_-^f(R)$.*

If M in $D_b^f(R)$ satisfies $\text{Supp}_R M \supseteq \text{Supp}_R L$ and there is an isomorphism

$$M \simeq \text{RHom}_R(L, M) \quad \text{or} \quad M \simeq L \otimes_R^L M,$$

then for some idempotent a in R the R_a -module $H_0(L)_a$ is invertible and one has

$$L \simeq H_0(L) \simeq H_0(L)_a \simeq L_a \quad \text{in } D(R).$$

The element a is determined by either one of the following equalities:

$$\text{Supp}_R M = \{\mathfrak{p} \in \text{Spec } R \mid \mathfrak{p} \not\supseteq a\} = \text{Supp}_R L.$$

Proof. If $H(M) = 0$, then the hypotheses imply $\text{Supp}_R L = \emptyset$, so $a = 0$ is the desired idempotent. For the rest of the proof we assume $H(M) \neq 0$.

If $M \simeq \text{RHom}_R(L, M)$ holds and \mathfrak{m} is in $\text{Max } R \cap \text{Supp}_R M$, then [Lemma A.5.3](#) shows that $L_{\mathfrak{m}}$ is in $D_+^f(R_{\mathfrak{m}})$ and gives the second equality below:

$$I_{R_{\mathfrak{m}}}^{M_{\mathfrak{m}}}(t) = I_{R_{\mathfrak{m}}}^{\text{RHom}_R(L, M)_{\mathfrak{m}}}(t) = P_{L_{\mathfrak{m}}}^{R_{\mathfrak{m}}}(t) \cdot I_{R_{\mathfrak{m}}}^{M_{\mathfrak{m}}}(t).$$

As $I_{R_{\mathfrak{m}}}^{M_{\mathfrak{m}}}(t) \neq 0$ by [A.5.2](#), this gives $P_{L_{\mathfrak{m}}}^{R_{\mathfrak{m}}}(t) = 1$, and hence $L_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ by [A.4.1](#). Thus, for every $\mathfrak{p} \in \text{Supp}_R M$ one has $L_{\mathfrak{p}} \simeq R_{\mathfrak{p}}$, which yields

$$\text{Supp}_R M = \text{Supp}_R L = \text{Supp}_R H_0(L)$$

and shows the R -module $H_0(L)$ is projective with $\text{rank}_{R_{\mathfrak{p}}} H_0(L)_{\mathfrak{p}} = 1$ for each $\mathfrak{p} \in \text{Supp}_R H_0(L)$. The rank of a projective module is constant on connected components of $\text{Spec } R$, and therefore $\text{Supp}_R H_0(L)$ is a union of such components, whence, by [4.8](#), there is a unique idempotent $a \in R$, such that

$$\text{Supp}_R H_0(L) = \{\mathfrak{p} \in \text{Spec } R \mid \mathfrak{p} \not\supseteq a\},$$

and the graded R_a -module $H(L)_a$ is invertible. The preceding discussion, [4.8](#), and [4.6](#) give isomorphisms $L \simeq H_0(L) \simeq H_0(L)_a \simeq L_a$ in $D(R)$.

A similar argument, using [Lemma A.4.3](#) and [A.4.2](#), applies if $M \simeq L \otimes_R^L M$. \square

5. Invertible complexes

We say that a complex in $D(R)$ is *invertible* if it is semidualizing and perfect.

The following canonical morphisms, defined for all L, M , and N in $D(R)$, play a role in characterizing invertible complexes and in using them: *Evaluation*

$$\text{RHom}_R(L, N) \otimes_R^L L \longrightarrow N \tag{5.0.1}$$

is induced by the chain map $\lambda \otimes l \mapsto \lambda(l)$. *Tensor-evaluation* is the composition

$$\begin{aligned} \mathrm{RHom}_R(M \otimes_R^L L, N) \otimes_R^L L &\xrightarrow{\simeq} \mathrm{RHom}_R(L \otimes_R^L M, N) \otimes_R^L L \\ &\xrightarrow{\simeq} \mathrm{RHom}_R(L, \mathrm{RHom}_R(M, N)) \otimes_R^L L \quad (5.0.2) \\ &\longrightarrow \mathrm{RHom}_R(M, N), \end{aligned}$$

where the isomorphisms are canonical and the last arrow is given by evaluation.

The equivalence of conditions (i) and (i') in the result below shows that for complexes with zero differential, invertibility agrees with the notion in 4.7. Invertible complexes coincide with the *tilting complexes* of Frankild, Sather-Wagstaff, and Taylor, see [Frankild et al. 2009, 4.7], where some of the following equivalences are proved.

Proposition 5.1. *For $L \in D_b^f(R)$ the following conditions are equivalent.*

- (i) L is invertible in $D(R)$.
- (i') $H(L)$ is an invertible graded R -module.
- (ii) $\mathrm{RHom}_R(L, R)$ is invertible in $D(R)$.
- (ii') $\mathrm{Ext}_R(L, R)$ is an invertible graded R -module.
- (iii) For each $\mathfrak{p} \in \mathrm{Spec} R$ one has $L_{\mathfrak{p}} \simeq \Sigma^{r(\mathfrak{p})} R_{\mathfrak{p}}$ in $D(R_{\mathfrak{p}})$ for some $r(\mathfrak{p}) \in \mathbb{Z}$.
- (iii') For each $\mathfrak{m} \in \mathrm{Max} R$ one has $P_{L_{\mathfrak{m}}}^{R_{\mathfrak{m}}}(t) = t^{r(\mathfrak{m})}$ for some $r(\mathfrak{m}) \in \mathbb{Z}$.
- (iv) $U^{-1}L$ is invertible in $D(U^{-1}R)$ for each multiplicatively closed set $U \subseteq R$.
- (v) For some N in $D^f(R)$ there is an isomorphism $N \otimes_R^L L \simeq R$.
- (vi) For each N in $D(R)$ the evaluation map (5.0.1) is an isomorphism.
- (vi') For all M, N in $D(R)$ the tensor-evaluation map (5.0.2) is an isomorphism.

Proof. (i) \iff (iv). This follows from Proposition 3.1 and Theorem 4.1.

(i) \implies (vi). The first two isomorphisms below hold because L is perfect:

$$\mathrm{RHom}_R(L, N) \otimes_R^L L \simeq \mathrm{RHom}_R(L, L \otimes_R^L N) \simeq \mathrm{RHom}_R(L, L) \otimes_R^L N \simeq N.$$

The third one holds because L is semidualizing.

(vi) \implies (vi'). In (5.0.2), use (5.0.1) with $\mathrm{RHom}_R(M, N)$ in place of N .

(vi') \implies (vi). Set $M = R$ in (5.0.2).

(vi) \implies (v). Setting $N = R$ one gets an isomorphism $\mathrm{RHom}_R(L, R) \otimes_R^L L \simeq R$.

Note that $\mathrm{RHom}_R(L, R)$ is in $D_b^f(R)$, since L is in $D_b^f(R)$.

Condition (v) localizes, and the already-proved equivalence of (i) and (iv) shows that conditions (i) and (ii) can be checked locally. Clearly, the same holds true for conditions (i'), (ii'), (iii'), and (iii). Thus, in order to finish the proof it suffices to show that when R is a local ring there exists a string of implications linking (v) to (i) and passing through the remaining conditions.

(v) \implies (iii'). [Lemma A.4.3](#) gives $P_N^R(t) \cdot P_L^R(t) = 1$. Such an equality of formal Laurent series implies $P_L^R(t) = t^r$ and $P_N^R(t) = t^{-r}$ for some integer r .

(iii') \implies (iii). This follows from [A.4.1](#).

(iii) \implies (i'). This implication is evident.

(i') \implies (ii'). As $H(L)$ is projective one has $L \simeq H(L)$ in $D(R)$ (see [4.6](#)), hence

$$\mathrm{Ext}_R(L, R) \cong \mathrm{Ext}_R(H(L), R) \cong \mathrm{Hom}_R(H(L), R).$$

Now note that the graded module $\mathrm{Hom}_R(H(L), R)$ is invertible because $H(L)$ is.

(ii') \implies (ii). Because $H(\mathrm{RHom}_R(L, R))$ is projective, [4.6](#) gives the first isomorphism below; the second one holds (for some $r \in \mathbb{Z}$) because R is local:

$$\mathrm{RHom}_R(L, R) \simeq H(\mathrm{RHom}_R(L, R)) = \mathrm{Ext}_R(L, R) \simeq \Sigma^r R.$$

(ii) \implies (i). The invertible complex $L' = \mathrm{RHom}_R(L, R)$ is evidently derived R -reflexive, so the implication (ii) \implies (i) in [Theorem 2.1](#) applies with $C = R$. It gives $L \simeq \mathrm{RHom}_R(L', R)$; now note that $\mathrm{RHom}_R(L', R)$ is invertible along with L . \square

Recall that $\mathrm{Pic}(R)$ denotes the *Picard group* of R , such that its elements are isomorphism classes of invertible R -modules, multiplication is induced by tensor product over R , and the class of $\mathrm{Hom}_R(L, R)$ is the inverse of that of L . A derived version of this construction is given in [[Frankild et al. 2009](#), 4.1] and is recalled below; it coincides with the derived Picard group of R relative to itself, in the sense of Yekutieli [[1999](#), 3.1].

5.2. When L is an invertible complex, we set

$$L^{-1} = \mathrm{RHom}_R(L, R).$$

Condition (vi) of [Proposition 5.1](#) gives for each $N \in D(R)$ an isomorphism

$$\mathrm{RHom}_R(L, N) \simeq L^{-1} \otimes_R^L N.$$

In view of [4.6](#), condition (i') of [Proposition 5.1](#) implies that the isomorphism classes $[L]$ of invertible complexes L in $D(R)$ form a set, which we call $\mathrm{DPic}(R)$. As derived tensor products are associative and commutative, $\mathrm{DPic}(R)$ carries the natural structure of an abelian group, with unit element $[R]$, and $[L]^{-1} = [L^{-1}]$. Following [[Frankild et al. 2009](#), 4.3.1], we refer to it as the *derived Picard group* of R .

We say that complexes M and N are *derived Picard equivalent* if there is an isomorphism $N \simeq L \otimes_R^L M$ for some invertible complex L .

Clearly, if N and N' are complexes in $D(R)$ which satisfy $L \otimes_R^L N \simeq L \otimes_R^L N'$ or $\mathrm{RHom}_R(L, N) \simeq \mathrm{RHom}_R(L, N')$, then $N \simeq N'$.

The derived Picard group of a local ring R is the free abelian group with generator $[\Sigma R]$; see [Frankild et al. 2009, 4.3.4]. In general, one has the following description, which is a special case of [Yekutieli 1999, 3.5]. We include a proof, for the sake of completeness.

Proposition 5.3. *There exists a canonical isomorphism of abelian groups*

$$\mathrm{DPic}(R) \xrightarrow{\cong} \prod_{i=1}^s (\mathrm{Pic}(R_{a_i}) \times \mathbb{Z}),$$

where $\{a_1, \dots, a_s\}$ is the complete set of primitive orthogonal idempotents; see 4.8.

Proof. By Proposition 5.1, every element of $\mathrm{DPic}(R)$ is equal to $[L]$ for some graded invertible R -module L . In the canonical decomposition from 4.8 each R_{a_i} -module L_{a_i} is graded invertible. It is indecomposable because $\mathrm{Spec}(R_{a_i})$ is connected, hence $L_{a_i} \cong \Sigma^{n_i} L_i$ with uniquely determined invertible R_{a_i} -module L_i and $n_i \in \mathbb{Z}$. The map $[L] \mapsto (([L_1], n_1), \dots, ([L_s], n_s))$ gives the desired isomorphism. \square

Other useful properties of derived Picard group actions are collected in the next two results, which overlap with [Frankild et al. 2009, 4.8]; we include proofs for completeness.

Lemma 5.4. *For L invertible, and C and M in $D_b^f(R)$, the following are equivalent.*

- (i) M is derived C -reflexive.
- (ii) M is derived $L \otimes_R^L C$ -reflexive.
- (iii) $L \otimes_R^L M$ is derived C -reflexive.

Proof. (i) \implies (ii). Since L is invertible, the morphism

$$\vartheta : L \otimes_R^L \mathrm{RHom}_R(M, C) \rightarrow \mathrm{RHom}_R(M, L \otimes_R^L C)$$

represented by $l \otimes \alpha \mapsto (m \mapsto l \otimes \alpha(m))$, is an isomorphism: It suffices to check the assertion after localizing at each $\mathfrak{p} \in \mathrm{Spec} R$, where it follows from $L_{\mathfrak{p}} \cong R_{\mathfrak{p}}$. In particular, since $\mathrm{RHom}_R(M, C)$ is in $D_b^f(R)$, so is $\mathrm{RHom}_R(M, L \otimes_R^L C)$. Furthermore, in $D(R)$ there is a commutative diagram of canonical morphisms

$$\begin{array}{ccc} M & \xrightarrow{\delta_M^{L \otimes_R^L C}} & \mathrm{RHom}_R(\mathrm{RHom}_R(M, L \otimes_R^L C), L \otimes_R^L C) \\ \delta_M^C \downarrow \cong & & \cong \downarrow \mathrm{RHom}_R(\vartheta, L \otimes_R^L C) \\ \mathrm{RHom}_R(\mathrm{RHom}_R(M, C), C) & \xrightarrow[\cong]{\lambda} & \mathrm{RHom}_R(L \otimes_R^L \mathrm{RHom}_R(M, C), L \otimes_R^L C) \end{array}$$

with $\lambda(\alpha) = L \otimes_R^L \alpha$, which is an isomorphism, as is readily verified by localization. Thus, M is derived $L \otimes_R^L C$ -reflexive.

(ii) \implies (i). The already established implication (i) \implies (ii) shows that M is reflexive with respect to $L^{-1} \otimes_R^L (L \otimes_R^L C)$, which is isomorphic to C .

(i) \iff (iii) This follows from [Theorem 4.5](#). \square

From [Proposition 3.1](#) and [Lemma 5.4](#), we obtain:

Lemma 5.5. *For L invertible and C in $D_b^f(R)$ the following are equivalent.*

(i) C is semidualizing.

(ii) $L \otimes_R^L C$ is semidualizing.

(iii) L is derived C -reflexive. \square

Invertible complexes are used in [[Frankild et al. 2009](#), 5.1] to characterize mutual reflexivity of a pair of semidualizing complexes. The next theorem is fundamentally different, in that the semidualizing property is part of its conclusions, not of its hypotheses.

Theorem 5.6. *For B and C in $D_b^f(R)$ the following conditions are equivalent.*

(i) B is derived C -reflexive, C is derived B -reflexive, and $\text{Supp}_R B = \text{Spec } R$.

(ii) B is semidualizing, $\text{RHom}_R(B, C)$ is invertible, and the evaluation map

$$\text{RHom}_R(B, C) \otimes_R^L B \rightarrow C$$

is an isomorphism in $D(R)$.

(iii) B and C are semidualizing and derived Picard equivalent.

Proof. (i) \implies (ii). The hypotheses pass to localizations and, by [Propositions 3.1](#) and [5.1](#), the conclusions can be tested locally. We may thus assume R is local.

Set $F = \text{RHom}_R(B, C)$ and $G = \text{RHom}_R(C, B)$. In view of [Lemma A.5.3](#), the isomorphisms $B \simeq \text{RHom}_R(F, C)$ and $C \simeq \text{RHom}_R(G, B)$ yield

$$I_R^B(t) = P_F^R(t) \cdot I_R^C(t) \quad \text{and} \quad I_R^C(t) = P_G^R(t) \cdot I_R^B(t).$$

As $I_R^B(t) \neq 0$ holds (see [A.5.2](#)) these equalities imply $P_F^R(t) \cdot P_G^R(t) = 1$, hence $P_F^R(t) = t^r$ holds for some r . [Proposition 5.1](#) now gives $F \simeq \Sigma^r R$, so one gets

$$B \simeq \text{RHom}_R(F, C) \simeq \text{RHom}_R(\Sigma^r R, C) \simeq \Sigma^{-r} C.$$

Thus, B is derived B -reflexive, hence semidualizing by [Proposition 3.1](#). A direct verification shows that the following evaluation map is an isomorphism:

$$\text{RHom}_R(\Sigma^{-r} C, C) \otimes_R^L \Sigma^{-r} C \rightarrow C.$$

(ii) \implies (iii) [Lemma 5.5](#) shows that C is semidualizing; the rest is clear.

(iii) \implies (i). [Proposition 3.1](#) shows that B satisfies $\text{Supp}_R B = \text{Spec } R$ and is derived B -reflexive. From [Lemma 5.4](#) we then see that B is derived C -reflexive. A second loop, this time starting from C , shows that C is derived B -reflexive. \square

Taking $B = R$ one recovers a result contained in [[Christensen 2001](#), 8.3].

Corollary 5.7. *A complex in $D(R)$ is invertible if and only if it is semidualizing and derived R -reflexive.* \square

6. Duality

We say that a contravariant R -linear exact functor $d: D(R) \rightarrow D(R)$ is a *duality* on a subcategory A of $D(R)$ if it satisfies $d(A) \subseteq A$ and $d^2|_A$ is isomorphic to id^A .

In this section we link dualities on subcategories of $D_b^f(R)$ to semidualizing complexes. In the ‘extremal’ cases, when the subcategory equals $D_b^f(R)$ itself or when the semidualizing complex is the module R , we recover a number of known results and answer some open questions.

6.1. Reflexive subcategories. For each complex C in $D(R)$, set

$$h_C = \text{RHom}_R(-, C): D(R) \longrightarrow D(R).$$

The *reflexive subcategory* of C is the full subcategory of $D(R)$ defined by

$$R_C = \{M \in D_b^f(R) \mid M \simeq h_C^2(M)\}.$$

By [Proposition 2.3](#), the functor h_C is a duality on R_C provided $h_C(R_C) \subseteq R_C$ holds. We note that, under an additional condition, such a C has to be semidualizing.

Proposition 6.1.1. *Let d be a duality on a subcategory A of $D_b^f(R)$.*

If A contains R , then the complex $C = d(R)$ is semidualizing and A is contained in R_C ; furthermore, for each R -module M in A there is an isomorphism

$$M \simeq \text{RHom}_R(d(M), C).$$

Proof. Let M be an R -module. For each $n \in \mathbb{Z}$ one then has isomorphisms

$$\begin{aligned} \text{Ext}_R^n(d(M), C) &\cong \text{Hom}_{D(R)}(d(M), \Sigma^n C) \\ &\cong \text{Hom}_{D(R)}(R, \Sigma^n d^2(M)) \\ &\cong \text{Hom}_{D(R)}(R, \Sigma^n M) \\ &\cong \text{Ext}_R^n(R, M) \\ &\cong \begin{cases} M & \text{for } n = 0; \\ 0 & \text{for } n \neq 0. \end{cases} \end{aligned}$$

It follows that $\text{RHom}_R(d(M), C)$ is isomorphic to M in $D(R)$. For $M = R$ this yields $\text{RHom}_R(C, C) \simeq R$, so C is semidualizing by [Proposition 3.1](#). \square

Next we show that semidualizing complexes do give rise to dualities and that, furthermore, they are determined by their reflexive subcategories.

Theorem 6.1.2. *Let C be a semidualizing complex for R .*

The functor h_C is a duality on R_C , the natural transformation $\delta^C: \text{id} \rightarrow h_C^2$ restricts to an isomorphism of functors on R_C , and R is in R_C .

A complex B in $D_b^f(R)$ satisfies $R_B = R_C$ if and only if B is derived Picard equivalent to C (in which case B is semidualizing).

Proof. [Theorem 3.3](#) implies that h_C takes values in R_C and that δ^C restricts to an isomorphism on R_C , while [Proposition 3.1](#) shows that R and C are in R_C .

The last assertion results from [Theorem 5.6](#). □

The preceding results raise the question of whether every duality functor on a subcategory of $D_b^f(R)$ is representable on its reflexive subcategory.

6.2. Dualizing complexes. Let D be a complex in $D(R)$.

Recall that D is said to be *dualizing* for R if it is semidualizing and of finite injective dimension. If D is dualizing, then $R_D = D_b^f(R)$; see [[Hartshorne 1966](#), p. 258, 2.1].

In the language of Hartshorne [[1966](#), p. 286], the complex D is *pointwise dualizing* for R if it is in $D_b^-(R)$ and the complex D_p is dualizing for R_p for each $p \in \text{Spec } R$. When in addition D is in $D_b^f(R)$, we say that it is *strongly pointwise dualizing*; this terminology is due to Gabber; see [[Conrad 2000](#), p. 120], also for discussion on why the latter concept is the more appropriate one.

For a different treatment of dualizing complexes, see Neeman [[2008](#)].

The next result is classical; see [[Hartshorne 1966](#), p. 283, 7.2; p. 286, Remark 1; p. 288, 8.2].

6.2.1. Let D be a complex in $D_b^f(R)$. The complex D is dualizing if and only if it is pointwise dualizing and $\dim R$ is finite.

The equivalence of conditions (i) and (ii) in the next result is due to Gabber; see [[Conrad 2000](#), 3.1.5]. Traces of his argument can be found in our proof, as it refers to [Theorem 3.3](#), and thus depends on [Theorem 1.1](#).

Theorem 6.2.2. *For D in $D(R)$ the following conditions are equivalent.*

- (i) D is strongly pointwise dualizing for R .
- (ii) h_D is a duality on $D_b^f(R)$.
- (iii) D is in $D_b^f(R)$, and for each $\mathfrak{m} \in \text{Max } R$ and finite R -module M , one has

$$M_{\mathfrak{m}} \simeq \text{RHom}_{R_{\mathfrak{m}}}(\text{RHom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, D_{\mathfrak{m}}), D_{\mathfrak{m}}) \quad \text{in } D(R_{\mathfrak{m}}).$$

Proof. (i) \implies (iii). By definition, $D \in D_b^f(R)$ and D_m is dualizing for R_m . Moreover, it is clear that $M_m \in D_b^f(R_m) = R_{D_m}$.

(iii) \implies (i). Let \mathfrak{m} be a maximal ideal of R . For $M_m = R_m$ the hypothesis implies that D_m is semidualizing; see [Proposition 3.1](#). For $M = R/\mathfrak{m}$ it implies, by the first part of [Lemma A.5.3](#), that $\mathrm{RHom}_{R_m}(R_m/\mathfrak{m}R_m, D_m) \in D_b^f(R_m)$; this means that D_m has finite injective dimension over R_m ; see [A.5.1](#). Localization shows that D_p has the corresponding properties for every prime ideal \mathfrak{p} of R , contained in \mathfrak{m} .

(iii) \iff (ii). The complex D is semidualizing — by [Proposition 3.1](#) if (iii) holds, by [Proposition 6.1.1](#) if (ii) holds; so the equivalence results from [Theorem 3.3](#). \square

Corollary 6.2.3. *The ring R is Gorenstein if and only if the complex R is strongly pointwise dualizing, if and only if each complex in $D_b^f(R)$ is derived R -reflexive.*

Proof. For arbitrary R and $\mathfrak{p} \in \mathrm{Spec} R$, the complex R_p is semidualizing for R_p . Thus, the first two conditions are equivalent because — by definition — the ring R is Gorenstein if and only if R_p has a finite injective resolution as a module over itself for each \mathfrak{p} . The second and third conditions are equivalent by [Theorem 6.2.2](#). \square

Given a homomorphism $R \rightarrow S$ of rings, recall that $\mathrm{RHom}_R(S, -)$ is a functor from $D(R)$ to $D(S)$. The next result is classical; see [[Hartshorne 1966](#), p. 260, 2.4].

Corollary 6.2.4. *If $R \rightarrow S$ is a finite homomorphism of rings and $D \in D_b^f(R)$ is pointwise dualizing for R , then $\mathrm{RHom}_R(S, D)$ is pointwise dualizing for S .*

Proof. Set $D' = \mathrm{RHom}_R(S, D)$. For each M in $D_b^f(S)$ one has

$$\mathrm{RHom}_R(M, D) \simeq \mathrm{RHom}_S(M, D') \quad \text{in } D(S).$$

It shows that $\mathrm{RHom}_S(M, D')$ is in $D_b^f(S)$, and that the restriction of h_D to $D_b^f(S)$ is equivalent to $h_{D'}$. [Theorem 6.2.2](#) then shows that D' is pointwise dualizing. \square

It follows from [Corollaries 6.2.3](#) and [6.2.4](#) that if S is a homomorphic image of a Gorenstein ring, then it admits a strongly pointwise dualizing complex. Kawasaki [[2002](#), 1.4] proved that if S has a *dualizing complex*, then S is a homomorphic image of some Gorenstein ring of finite Krull dimension, so we ask:

Question 6.2.5. Does the existence of a strongly pointwise dualizing complex for S imply that S is a homomorphic image of some Gorenstein ring?

6.3. Finite G -dimension. The category R_R of derived R -reflexive complexes contains all perfect complexes, but may be larger. To describe it we use a notion from module theory: An R -module G is *totally reflexive* when it is finite,

$$\begin{aligned} \mathrm{Hom}_R(\mathrm{Hom}_R(G, R), R) &\cong G && \text{and} \\ \mathrm{Ext}_R^n(\mathrm{Hom}_R(G, R), R) &= 0 = \mathrm{Ext}_R^n(G, R) && \text{for all } n \geq 1. \end{aligned}$$

A complex of R -modules is said to have *finite G -dimension* (for *Gorenstein dimension*) if it is quasi-isomorphic to a bounded complex of totally reflexive modules. The study of modules of finite G -dimension was initiated by Auslander and Bridger [1969]. The next result, taken from [Christensen 2000, 2.3.8], is due to Foxby.

6.3.1. A complex in $D(R)$ is in R_R if and only if it has finite G -dimension.

Theorems 2.1 and 3.3 specialize to:

Theorem 6.3.2. For a complex $M \in D_b^f(R)$ the following are equivalent.

- (i) M is derived R -reflexive.
- (ii) $\mathrm{RHom}_R(M, R)$ is derived R -reflexive.
- (iii) For each $\mathfrak{m} \in \mathrm{Max} R$ there is an isomorphism

$$M_{\mathfrak{m}} \simeq \mathrm{RHom}_{R_{\mathfrak{m}}}(\mathrm{RHom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, R_{\mathfrak{m}}), R_{\mathfrak{m}}) \quad \text{in } D(R_{\mathfrak{m}}).$$

- (iv) $U^{-1}M$ is derived $U^{-1}R$ -reflexive for each multiplicatively closed set U . \square

Combining 6.3.1 and Corollary 6.2.3, we obtain a new proof of a result due to Auslander and Bridger [1969, 4.20] (when $\dim R$ is finite) and to Goto [1982] (in general).

Corollary 6.3.3. The ring R is Gorenstein if and only if every finite R -module has finite G -dimension. \square

It is easy to check that if a complex M has finite G -dimension over R , then so does the complex of $R_{\mathfrak{p}}$ -modules $M_{\mathfrak{p}}$, for any prime ideal \mathfrak{p} . Whether the converse holds had been an open question, which we settle as a corollary of 6.3.1 and Theorem 6.3.2:

Corollary 6.3.4. A homologically finite complex M has finite G -dimension if (and only if) the complex $M_{\mathfrak{m}}$ has finite G -dimension over $R_{\mathfrak{m}}$ for every $\mathfrak{m} \in \mathrm{Max} R$. \square

7. Rigidity

Over an arbitrary commutative ring, we introduce a concept of rigidity of one complex relative to another, and establish the properties responsible for the name. In Section 8.5 we show how to recover the notion of rigidity for complexes over commutative algebras, defined by Van den Bergh, Yekutieli and Zhang.

Let C be a complex in $D(R)$. We say that a complex M in $D(R)$ is C -rigid if there exists an isomorphism

$$\mu: M \xrightarrow{\simeq} \mathrm{RHom}_R(\mathrm{RHom}_R(M, C), M) \quad \text{in } D(R). \quad (7.0.1)$$

In such a case, we call μ a C -rigidifying isomorphism and (M, μ) a C -rigid pair.

Example 7.1. Let C be a semidualizing complex. For each idempotent element $a \in R$, using (3.0.1) and 4.8 one obtains a canonical composite isomorphism

$$\begin{aligned} \gamma_a: C_a &\xrightarrow{\cong} \mathrm{RHom}_R(R, C_a) \\ &\xrightarrow{\mathrm{RHom}_R(\chi^C, C_a)^{-1}} \mathrm{RHom}_R(\mathrm{RHom}_R(C, C), C_a) \\ &\xrightarrow{\cong} \mathrm{RHom}_R(\mathrm{RHom}_R(C_a \oplus C_{1-a}, C), C_a) \\ &\xrightarrow{\cong} \mathrm{RHom}_R(\mathrm{RHom}_R(C_a, C), C_a). \end{aligned}$$

Thus, for each idempotent a there exists a *canonical C -rigid pair* (C_a, γ_a) .

Theorem 7.2. *Let C be a semidualizing complex.*

A complex $M \in \mathbf{D}_b^f(R)$ is C -rigid if and only if it satisfies

$$M \simeq C_a \quad \text{in } \mathbf{D}(R) \tag{7.2.1}$$

for some idempotent a in R ; such an idempotent is determined by the condition

$$\mathrm{Supp}_R M = \{\mathfrak{p} \in \mathrm{Spec} R \mid \mathfrak{p} \not\ni a\}. \tag{7.2.2}$$

Proof. The “if” part comes from Example 7.1, so assume that M is C -rigid.

Set $L = \mathrm{RHom}_R(M, C)$ and let $M \simeq \mathrm{RHom}_R(L, M)$ be a rigidifying isomorphism. Theorem 4.9 produces a unique idempotent a in R satisfying (7.2.2), and such that the complex L_a is invertible in $\mathbf{D}(R_a)$. Hence, L_a is derived C_a -reflexive in $\mathbf{D}(R_a)$ by Lemma 5.4. Thus, $\mathrm{RHom}_{R_a}(M_a, C_a)$ is derived C_a -reflexive, and hence so is M_a , by Theorem 3.3. This explains the second isomorphism below:

$$\mathrm{RHom}_{R_a}(L_a, C_a) \simeq \mathrm{RHom}_{R_a}(\mathrm{RHom}_{R_a}(M_a, C_a), C_a) \simeq M_a \simeq \mathrm{RHom}_{R_a}(L_a, M_a).$$

The third one is a localization of the rigidifying isomorphism. Hence $M_a \simeq C_a$ in $\mathbf{D}(R_a)$; see 5.2. It remains to note that one has $M \simeq M_a$ in $\mathbf{D}(R)$; see 4.8. \square

A *morphism of C -rigid pairs* is a commutative diagram

$$(\alpha) = \begin{array}{ccc} M & \xrightarrow{\mu} & \mathrm{RHom}_R(\mathrm{RHom}_R(M, C), M) \\ \downarrow \alpha & & \downarrow \mathrm{RHom}_R(\mathrm{RHom}_R(\alpha, C), \alpha) \\ N & \xrightarrow{\nu} & \mathrm{RHom}_R(\mathrm{RHom}_R(N, C), N) \end{array}$$

in $\mathbf{D}(R)$. The C -rigid pairs and their morphisms form a category, where composition is given by $(\beta)(\alpha) = (\beta\alpha)$ and $\mathrm{id}^{(M, \mu)} = (\mathrm{id}^M)$.

The next result explains the name ‘rigid complex’. The result is deduced from Theorem 7.2 by transposing a beautiful observation of Yekutieli and Zhang [2008, proof of 4.4]: A morphism of rigid pairs is a natural isomorphism from a functor in M that is linear to one that is quadratic, so it must be given by an idempotent.

Theorem 7.3. *If C is a semidualizing complex and (M, μ) and (N, ν) are C -rigid pairs in $D_b^f(R)$, then the following conditions are equivalent.*

- (i) *There is an equality $\text{Supp}_R N = \text{Supp}_R M$.*
- (ii) *There is an isomorphism $M \simeq N$ in $D(R)$.*
- (iii) *There is a unique isomorphism of C -rigid pairs $(M, \mu) \simeq (N, \nu)$.*

Proof. (i) \implies (iii). Let $\alpha: C_a \xrightarrow{\sim} M$ be an isomorphism in $D(R)$ given by (7.2.1), with a the idempotent defined by formula (7.2.2). It suffices to prove that (M, μ) is uniquely isomorphic to the C -rigid pair (C_a, γ_a) from Example 7.1. Since it is equivalent to prove the same in $D(R_a)$, we may replace R by R_a and drop all references to localization at $\{1, a\}$.

Set $\tilde{\alpha} = \text{RHom}_R(\text{RHom}_R(\alpha, C), \alpha)$: this is an isomorphism, and hence so is $\alpha^{-1} \circ \mu^{-1} \circ \tilde{\alpha} \circ \gamma: C \rightarrow C$. As C is semidualizing, there is an isomorphism

$$H_0(\chi^C): R \xrightarrow{\cong} H_0(\text{RHom}_R(C, C)) = \text{Hom}_{D(R)}(C, C),$$

of rings, so $\alpha^{-1} \circ \mu^{-1} \circ \tilde{\alpha} \circ \gamma = H_0(\chi^C)(u)$ for some unit u in R . The next computation shows that $(u^{-1}\alpha): (C, \gamma) \rightarrow (M, \mu)$ is an isomorphism of C -rigid pairs:

$$\begin{aligned} \text{RHom}_R(\text{RHom}_R(u^{-1}\alpha, C), u^{-1}\alpha) \circ \gamma &= u^{-2}(\tilde{\alpha} \circ \gamma) \\ &= u^{-2} \cdot u(\mu \circ \alpha) \\ &= \mu \circ (u^{-1}\alpha). \end{aligned}$$

Let $(\beta): (C, \gamma) \rightarrow (M, \mu)$ also be such an isomorphism. The isomorphism $H_0(\chi^C)$ implies that in $D(R)$ one has $\beta^{-1} \circ u^{-1}\alpha = v \text{id}^C$ for some unit $v \in R$, whence $v \text{id}^C$ is a rigid endomorphism of the rigid pair (C, γ) . Thus

$$\begin{aligned} v\gamma &= \gamma \circ (v \text{id}^C) \\ &= \text{RHom}_R(\text{RHom}_R(v \text{id}^C, C), v \text{id}^C) \circ \gamma \\ &= v^2 \text{RHom}_R(\text{RHom}_R(\text{id}^C, C), \text{id}^C) \circ \gamma \\ &= v^2\gamma. \end{aligned}$$

As v and γ are invertible one gets $(v-1)\text{id}^C = 0$, hence $v-1 \in \text{Ann}_R C = 0$. This gives $v = 1$, from where one obtains $\beta^{-1} \circ u^{-1}\alpha = \text{id}^C$, and finally $(\beta) = (u^{-1}\alpha)$.

(iii) \implies (ii) \implies (i). These implications are evident. \square

An alternative formulation of the preceding result is sometimes useful.

Remark 7.4. Let (M, μ) be a C -rigid pair in $D_b^f(R)$, and N a complex in $D_b^f(R)$.

For each isomorphism $\alpha: N \xrightarrow{\cong} M$ in $D(R)$, set

$$\rho(\alpha) = (\mathrm{RHom}_R(\mathrm{RHom}_R(\alpha, C), \alpha))^{-1} \circ \mu \circ \alpha;$$

this is a morphism from N to $\mathrm{RHom}_R(\mathrm{RHom}_R(N, C), N)$.

Theorem 7.3 shows that the assignment $\alpha \mapsto (N, \rho(\alpha))$ yields a bijection

$$\{\text{isomorphisms from } N \text{ to } M\} \leftrightarrow \{\text{rigid pairs } (N, \nu) \text{ isomorphic to } (M, \mu)\}$$

We finish with a converse, of sorts, to [Example 7.1](#).

Proposition 7.5. *If C in $D_b^f(R)$ is C -rigid, then there exist an idempotent a in R , a semidualizing complex B for R_a , and an isomorphism $C \simeq B$ in $D(R)$.*

Proof. By hypothesis, $C \simeq \mathrm{RHom}_R(\mathrm{RHom}_R(C, C), C)$. [Theorem 4.9](#) and [4.8](#) provide an idempotent $a \in R$ such that the R_a -module $H_0(\mathrm{RHom}_R(C, C)_a)$ is invertible and in $D(R)$ there are natural isomorphisms $C \simeq C_a$ and

$$H_0(\mathrm{RHom}_R(C, C)_a) \simeq \mathrm{RHom}_R(C, C)_a \simeq \mathrm{RHom}_{R_a}(C_a, C_a).$$

It follows that the homothety map

$$\chi: R_a \rightarrow \mathrm{Hom}_{D(R_a)}(C_a, C_a) \cong H_0(\mathrm{RHom}_{R_a}(C_a, C_a))$$

turns $\mathrm{Hom}_{D(R_a)}(C_a, C_a)$ into *both* an invertible R_a -module *and* an R_a -algebra. Localizing at prime ideals of R_a , one sees that such a χ must be an isomorphism; so the proposition holds with $B = C_a$. \square

8. Relative dualizing complexes

In this section K denotes a commutative noetherian ring, S a commutative ring, and $\sigma: K \rightarrow S$ a homomorphism of rings that is assumed to be *essentially of finite type*: This means that σ can be factored as a composition

$$K \hookrightarrow K[x_1, \dots, x_e] \rightarrow W^{-1}K[x_1, \dots, x_e] = Q \twoheadrightarrow S \quad (8.0.1)$$

of homomorphisms of rings, where x_1, \dots, x_e are indeterminates, W is a multiplicatively closed set, the first two maps are canonical, the equality defines Q , and the last arrow is surjective; the map σ is *of finite type* if one can choose $W = \{1\}$.

As usual, $\Omega_{Q|K}$ stands for the Q -module of Kähler differentials; for each $n \in \mathbb{Z}$ we set $\Omega_{Q|K}^n = \bigwedge^n \Omega_{Q|K}$. Fixing the factorization [\(8.0.1\)](#), we define a *relative dualizing complex* for σ by means of the following equality:

$$D^\sigma = \Sigma^e \mathrm{RHom}_Q(S, \Omega_{Q|K}^e). \quad (8.0.2)$$

Our goal here is to determine when D^σ is semidualizing, invertible, or dualizing. It turns out that each one of these properties is equivalent to some property of the

homomorphism σ , which has been studied earlier in a different context. We start by introducing notation and terminology that will be used throughout the section.

For every \mathfrak{q} in $\text{Spec } S$ we let $\mathfrak{q} \cap K$ denote the prime ideal $\sigma^{-1}(\mathfrak{q})$ of K , and write $\sigma_{\mathfrak{q}}: K_{\mathfrak{q} \cap K} \rightarrow S_{\mathfrak{q}}$ for the induced local homomorphism; it is essentially of finite type.

Recall that a ring homomorphism $\dot{\sigma}: K \rightarrow P$ is said to be (*essentially*) *smooth* if it is (essentially) of finite type, flat, and for each ring homomorphism $K \rightarrow k$, where k is a field, the ring $k \otimes_K P$ is regular; by [Grothendieck 1967, 17.5.1] this notion of smoothness is equivalent to the one defined in terms of lifting of homomorphisms. When $\dot{\sigma}$ is essentially smooth $\Omega_{P|K}$ is finite projective over P ; in case $\Omega_{P|K}$ has rank d (see 4.7) we say that $\dot{\sigma}$ has *relative dimension* d . The P -module $\Omega_{P|K}^d$ is then invertible.

An (*essential*) *smoothing* of σ (of relative dimension d) is a decomposition

$$K \xrightarrow{\dot{\sigma}} P \xrightarrow{\sigma'} S \quad (8.0.3)$$

of σ with $\dot{\sigma}$ (essentially) smooth of fixed relative dimension (equal to d) and σ' *finite*, meaning that S is a finite P -module via σ' ; an essential smoothing of σ always exists; see (8.0.1).

8.1. Basic properties. Fix an essential smoothing (8.0.3) of relative dimension d .

8.1.1. By [Avramov et al. 2010a, 1.1], there exists an isomorphism

$$D^\sigma \simeq \Sigma^d \text{RHom}_P(S, \Omega_{P|K}^d) \quad \text{in } D(S).$$

8.1.2. For each M in $D_b^f(S)$ there are isomorphisms

$$\begin{aligned} \text{RHom}_S(M, D^\sigma) &= \text{RHom}_S(M, \Sigma^d \text{RHom}_P(S, \Omega_{P|K}^d)) \\ &\simeq \Sigma^d \text{RHom}_P(M, \Omega_{P|K}^d) \\ &\simeq \text{RHom}_P(M, P) \otimes_P \Sigma^d \Omega_{P|K}^d \end{aligned}$$

in $D(S)$, because $\Omega_{P|K}^d$ is an invertible P -module.

Proposition 8.1.3. *If $U \subseteq K$ and $V \subseteq S$ are multiplicatively closed sets satisfying $\sigma(U) \subseteq V$, and $\tilde{\sigma}: U^{-1}K \rightarrow V^{-1}S$ is the induced map, then one has*

$$d^{\tilde{\sigma}} \simeq v^{-1}d^\sigma \quad \text{in } D(v^{-1}S).$$

Proof. set $v' = \sigma'^{-1}(v)$. in the induced factorization $u^{-1}k \rightarrow (v')^{-1}p \rightarrow v^{-1}s$ of $\tilde{\sigma}$, the first map is essentially smooth of relative dimension d and the second one is finite. the first and the last isomorphisms in the next chain hold by 8.1.1, the rest

because localization commutes with modules of differentials and exterior powers:

$$\begin{aligned}
 D^{\tilde{\sigma}} &\simeq \Sigma^d \operatorname{RHom}_{(V')^{-1}P}((V')^{-1}S, \Omega_{(V')^{-1}P|U^{-1}K}^d) \\
 &\simeq \Sigma^d \operatorname{RHom}_{(V')^{-1}P}((V')^{-1}S, (V')^{-1}\Omega_{P|K}^d) \\
 &\simeq (V')^{-1} \Sigma^d \operatorname{RHom}_P(S, \Omega_{P|K}^d) \\
 &\simeq V^{-1} D^{\sigma}. \quad \square
 \end{aligned}$$

Proposition 8.1.4. *If $\varphi : S \rightarrow T$ is a finite homomorphism of rings, then for the map $\tau = \varphi\sigma : K \rightarrow T$ there is an isomorphism*

$$D^{\tau} \simeq \operatorname{RHom}_S(T, D^{\sigma}) \quad \text{in } \mathbf{D}(T).$$

Proof. The result comes from the following chain of isomorphisms:

$$\begin{aligned}
 D^{\tau} &\simeq \Sigma^d \operatorname{RHom}_P(T, \Omega_{P|K}^d) \\
 &\simeq \operatorname{RHom}_S(T, \Sigma^d \operatorname{RHom}_P(S, \Omega_{P|K}^d)) \\
 &= \operatorname{RHom}_S(T, D^{\sigma}),
 \end{aligned}$$

where the first one is obtained from the factorization $K \xrightarrow{\kappa} P \xrightarrow{\varphi\sigma'} T$ of τ and the second one by adjunction. \square

8.2. Derived D^{σ} -reflexivity. A standard calculation shows that derived D^{σ} -reflexivity can be read off any essential smoothing (see (8.0.3)).

Proposition 8.2.1. *A complex M in $\mathbf{D}(S)$ is derived D^{σ} -reflexive if and only if M is derived P -reflexive when viewed as a complex in $\mathbf{D}(P)$.*

Proof. Evidently, M is in $\mathbf{D}_b^f(S)$ if and only if it is in $\mathbf{D}_b^f(P)$. From 8.1.2 one sees that $\operatorname{RHom}_S(M, D^{\sigma})$ is in $\mathbf{D}_b^f(S)$ if and only if $\operatorname{RHom}_P(M, P)$ is in $\mathbf{D}_b^f(P)$.

Set $\Omega = \Sigma^d \Omega_{P|K}^d$, where d is the relative dimension of $K \rightarrow P$, and let $\Omega \rightarrow I$ be a semiinjective resolution in $\mathbf{D}(P)$. Thus, D^{σ} is isomorphic to $\operatorname{Hom}_P(S, I)$ in $\mathbf{D}(S)$. The biduality morphism δ_M^{Ω} in $\mathbf{D}(P)$ is realized by a morphism

$$M \rightarrow \operatorname{Hom}_P(\operatorname{Hom}_P(M, I), I)$$

of complexes of S -modules; see (2.0.1). Its composition with the natural isomorphism of complexes of S -modules

$$\operatorname{Hom}_P(\operatorname{Hom}_P(M, I), I) \cong \operatorname{Hom}_S(\operatorname{Hom}_S(M, \operatorname{Hom}_P(S, I)), \operatorname{Hom}_P(S, I))$$

represents the morphism $\delta_M^{D^{\sigma}}$ in $\mathbf{D}(S)$. It follows that M is derived D^{σ} -reflexive if and only if it is derived Ω -reflexive. Since Ω is an invertible P -module, the last condition is equivalent — by Lemma 5.4 — to the derived P -reflexivity of M . \square

A complex M in $D_+(S)$ is said to have *finite flat dimension* over K if M is isomorphic in $D(K)$ to a bounded complex of flat K -modules; we then write $\text{fd}_K M < \infty$.

When $\text{fd}_K S$ is finite we say that σ is of *finite flat dimension* and write $\text{fd } \sigma < \infty$.

8.2.2. A complex M in $D_b^f(S)$ satisfies $\text{fd}_K M < \infty$ if and only if it is perfect in $D(P)$ for some (equivalently, any) factorization (8.0.3) of σ ; see [Avramov et al. 2010a, beginning of §6].

Corollary 8.2.3. *A complex M in $D_b^f(S)$ with $\text{fd}_K M < \infty$ is derived D^σ -reflexive.*

Proof. By 8.2.2 the complex M is perfect in $D(P)$. It is then obviously derived P -reflexive, and so is derived D^σ -reflexive by the previous proposition. \square

8.3. Gorenstein base rings. Relative dualizing complexes and their absolute counterparts (see 6.2) are compared in the next result, where the “if” part is classical.

Theorem 8.3.1. *The complex D^σ is strongly pointwise dualizing for S if and only if the ring $K_{\mathfrak{q} \cap K}$ is Gorenstein for every prime ideal \mathfrak{q} of S .*

Proof. Factor σ as in (8.0.1) and set $\mathfrak{p} = \mathfrak{q} \cap K$. The homomorphism $\sigma_{\mathfrak{q}}: K_{\mathfrak{p}} \rightarrow S_{\mathfrak{q}}$ satisfies $(D^\sigma)_{\mathfrak{q}} \cong D^{\sigma_{\mathfrak{q}}}$ by Proposition 8.1.3. Localizing, we may assume that σ is a local homomorphism $(K, \mathfrak{p}) \rightarrow (S, \mathfrak{q})$, and that the ring Q is local. As the ring $Q/\mathfrak{p}Q$ is regular, K is Gorenstein if and only if Q is too; see [Matsumura 1986, 23.4]. Thus, replacing Q with K we may further assume that σ is surjective.

If K is Gorenstein, then $D^\sigma = \text{RHom}_K(S, K)$ holds so it is dualizing for S by Corollaries 6.2.3 and 6.2.4.

When D^σ is dualizing for S , the residue field $k = S/\mathfrak{q}$ is derived D^σ -reflexive; see Theorem 6.2.2. By Proposition 8.2.1 it is also derived K -reflexive, which implies $\text{Ext}_K^n(k, K) = 0$ for $n \gg 0$. Thus, K is Gorenstein; see [Matsumura 1986, 18.1]. \square

8.4. Homomorphisms of finite G-dimension. When the P -module S has finite G-dimension (see 6.3) we say that σ has *finite G-dimension* and write $\text{G-dim } \sigma < \infty$. By the following result, this notion is independent of the choice of factorization.

Proposition 8.4.1. *The following conditions are equivalent.*

- (i) D^σ is semidualizing for S .
- (ii) σ has finite G-dimension.
- (iii) σ_n has finite G-dimension for each $n \in \text{Max } S$.

Proof. (i) \iff (ii). By Proposition 3.1, D^σ is semidualizing for S if and only if S is derived D^σ -reflexive. By Proposition 8.2.1 this is equivalent to S being derived P -reflexive in $D(P)$, and hence, by 6.3.1, to S having finite G-dimension over P .

(ii) \iff (iii). Proposition 8.1.3 yields an isomorphism $D^{\sigma_n} \simeq (D^\sigma)_n$ for each n . Given (i) \iff (ii), the desired equivalence follows from Proposition 3.1. \square

Combining the proposition with [Theorem 8.3.1](#) and [Corollary 8.2.3](#), one obtains:

Corollary 8.4.2. *Each condition below implies that σ has finite G-dimension:*

(i) *The ring $K_{n \cap K}$ is Gorenstein for every $n \in \text{Max } S$.*

(ii) *The homomorphism σ has finite flat dimension.* □

Notes 8.4.3. A notion of finite G-dimension that applies to arbitrary local homomorphisms is defined in [[Avramov and Foxby 1997](#)]. [Proposition 8.4.1](#) and [[Avramov and Foxby 1997](#), 4.3, 4.5] show that the definitions agree when both apply; thus, [Corollary 8.4.2](#) recovers [[Avramov and Foxby 1997](#), 4.4.1, 4.4.2].

8.5. Relative rigidity. [Proposition 8.4.1](#) and [Theorem 7.2](#) yield:

Theorem 8.5.1. *Assume that σ has finite G-dimension.*

A complex M in $D_b^f(S)$ is D^σ -rigid if and only if it is isomorphic to D_a^σ for some idempotent $a \in S$; such an idempotent is uniquely defined. □

This theorem greatly strengthens some results of [[Yekutieli and Zhang 2009](#)], where rigidity is defined using a derived version of Hochschild cohomology, due to Quillen: there is a functor

$$\text{RHom}_{S \otimes_K^L S}(S, - \otimes_K^L -): D(S) \times D(S) \rightarrow D(S)$$

(see [[Avramov et al. 2010a](#), §3] for details of the construction) which has the following properties:

8.5.2. Quillen's *derived Hochschild cohomology modules* (see [[Quillen 1970](#), §3]) are given by

$$\text{Ext}_{S \otimes_K^L S}^n(S, M \otimes_K^L N) = H_{-n}(\text{RHom}_{S \otimes_K^L S}(S, M \otimes_K^L N)).$$

8.5.3. When S is K -flat one can replace $S \otimes_K^L S$ with $S \otimes_K S$; see [[Avramov et al. 2010a](#), Remark 3.4].

8.5.4. When $\text{fd } \sigma$ is finite, for every complex M in $D_b^f(S)$ with $\text{fd}_K M < \infty$ and for every complex N in $D(S)$, by [[Avramov et al. 2010a](#), Theorem 4.1] there exists an isomorphism

$$\text{RHom}_{S \otimes_K^L S}(S, M \otimes_K^L N) \simeq \text{RHom}_S(\text{RHom}_S(M, D^\sigma), N) \quad \text{in } D(S).$$

Yekutieli and Zhang [[2008](#), 4.1] define M in $D(S)$ to be *rigid relative to K* if M is in $D_b^f(S)$, satisfies $\text{fd}_K M < \infty$, and admits a *rigidifying isomorphism*

$$\mu: M \xrightarrow{\cong} \text{RHom}_{S \otimes_K^L S}(S, M \otimes_K^L M) \quad \text{in } D(S).$$

By [8.5.3](#), when K is a field, this coincides with the notion introduced by Van den Bergh [[1997](#), 8.1]. On the other hand, ([7.0.1](#)) and [8.5.4](#), applied with $N = M$, give:

8.5.5. When $\text{fd } \sigma$ is finite, M in $D_b^f(S)$ is rigid relative to K if and only if $\text{fd}_K M$ is finite and M is D^σ -rigid.

From Theorems 8.5.1 and 8.3.1 we now obtain:

Theorem 8.5.6. *Assume that K is Gorenstein and $\text{fd } \sigma$ is finite.*

The complex D^σ then is pointwise dualizing for S and is rigid relative to K .

A complex M in $D_b^f(S)$ is rigid relative to K if and only if $D_a^\sigma \cong M$ holds for some idempotent a in S . More precisely, when δ and μ are rigidifying isomorphisms for D^σ and M , respectively, there exists a commutative diagram

$$\begin{array}{ccc}
 D_a^\sigma & \xrightarrow[\simeq]{\delta_a} & \text{RHom}_{S \otimes_K^L S}(S, D_a^\sigma \otimes_K^L D_a^\sigma) \\
 \alpha \downarrow \simeq & & \simeq \downarrow \text{RHom}_{S \otimes_K^L S}(S, \alpha \otimes_K^L \alpha) \\
 M & \xrightarrow[\mu]{\simeq} & \text{RHom}_{S \otimes_K^L S}(S, M \otimes_K^L M)
 \end{array}$$

where both the idempotent a and the isomorphism α are uniquely defined. \square

In [Yekutieli and Zhang 2009] the ring K is assumed regular of finite Krull dimension. This implies $\text{fd}_K M < \infty$ for all $M \in D_b^f(S)$, so $\text{fd } \sigma < \infty$ holds, and also that S is of finite Krull dimension, since it is essentially of finite type over K . Therefore [Yekutieli and Zhang 2009, 1.1(a), alias 3.6(a) and 1.2, alias 3.10] are special cases of Theorem 8.5.6.

There also is a converse, stemming from 6.2.1 and Theorem 8.3.1.

Finally, we address a series of comments made at the end of [Yekutieli and Zhang 2009, §3]; they are given in quotation marks, but notation and references are changed to match ours.

Notes 8.5.7. The paragraph preceding [Yekutieli and Zhang 2009, 3.10] reads: “Next comes a surprising result that basically says ‘all rigid complexes are dualizing’. The significance of this result is yet unknown.” It states: If K and S are regular, $\dim S$ is finite, and S has no idempotents other than 0 and 1, then a rigid complex is either zero or dualizing.

Theorem 7.2 provides an explanation of this phenomenon: Under these conditions S has finite global dimension, so every semidualizing complex is dualizing.

Notes 8.5.8. Concerning [Yekutieli and Zhang 2009, 3.14]: “The standing assumptions that the base ring K has finite global dimension seems superfluous.” See Theorem 8.5.6.

“However, it seems necessary for K to be Gorenstein—see [Yekutieli and Zhang 2009, Example 3.16].” Compare Theorems 8.5.1 and 8.5.6.

“A similar reservation applies to the assumption that S is regular in Theorem 3.10 (Note the mistake in [Yekutieli and Zhang 2008, Theorem 0.6]: there too S

has to be regular).” [Theorem 8.5.6](#) shows that the regularity hypothesis can be weakened significantly.

8.6. Quasi-Gorenstein homomorphisms. The map σ is said to be *quasi-Gorenstein* if in [\(8.0.1\)](#) for each $\mathfrak{n} \in \text{Max } S$ the $\mathcal{Q}_{\mathfrak{n} \cap \mathcal{Q}}$ -module $S_{\mathfrak{n}}$ has finite G -dimension and satisfies $\text{RHom}_{\mathcal{Q}_{\mathfrak{n} \cap \mathcal{Q}}}(S_{\mathfrak{n}}, \mathcal{Q}_{\mathfrak{n} \cap S}) \simeq \Sigma^{r(\mathfrak{n})} S_{\mathfrak{n}}$ for some $r(\mathfrak{n}) \in \mathbb{Z}$; see [[Avramov and Foxby 1997](#), 5.4, 6.7, 7.8, 8.4]; when this holds σ has finite G -dimension by [Corollary 6.3.4](#).

By part (i) of the next theorem, quasi-Gorensteinness is a property of σ , not of the factorization. The equivalence of (ii) and (iii) also follows from [[Avramov and Iyengar 2008](#), 2.2].

Theorem 8.6.1. *The following conditions are equivalent:*

- (i) D^σ is invertible in $\text{D}(S)$.
- (i') D^σ is derived S -reflexive in $\text{D}(S)$ and $G\text{-dim } \sigma < \infty$.
- (ii) σ is quasi-Gorenstein.
- (iii) $\text{Ext}_P(S, P)$ is an invertible graded S -module.

Proof. (i) \iff (i'). This results from [Proposition 8.4.1](#) and [Corollary 5.7](#).

(i) \iff (iii). By [8.1.2](#), one has $D^\sigma \simeq \Sigma^d \text{RHom}_P(S, P) \otimes_P^L \Omega_{P|K}^d$ in $\text{D}(S)$. It implies that D^σ is invertible in $\text{D}(S)$ if and only if $\text{RHom}_P(S, P)$ is. By [Proposition 5.1](#), the latter condition holds if and only if $\text{Ext}_P(S, P)$ is invertible.

(i') & (iii) \implies (ii). Indeed, for every $\mathfrak{n} \in \text{Spec } S$ the finiteness of $G\text{-dim } \sigma$ implies that of $G\text{-dim}_{P_{\mathfrak{n} \cap P}} S_{\mathfrak{n}}$, and the invertibility of $\text{Ext}_P(S, P)$ implies an isomorphism $\text{RHom}_{P_{\mathfrak{n} \cap P}}(S_{\mathfrak{n}}, P_{\mathfrak{n} \cap P}) \simeq \Sigma^{r(\mathfrak{n})} S_{\mathfrak{n}}$ for some $r(\mathfrak{n}) \in \mathbb{Z}$; see [Proposition 5.1](#).

(ii) \implies (iii). This follows from [Proposition 5.1](#). □

A quasi-Gorenstein homomorphism σ with $\text{fd}_K S < \infty$ is said to be *Gorenstein*; see [[Avramov and Foxby 1997](#), 8.1]. When σ is flat, it is Gorenstein if and only if for every $\mathfrak{q} \in \text{Spec } S$ and $\mathfrak{p} = \mathfrak{q} \cap K$ the ring $(K_{\mathfrak{p}}/\mathfrak{p}K_{\mathfrak{p}}) \otimes_K S$ is Gorenstein; see [[Avramov and Foxby 1997](#), 8.3]. The next result uses derived Hochschild cohomology; see [8.5.2](#). For flat σ it is proved in [[Avramov and Iyengar 2008](#), 2.4].

Theorem 8.6.2. *The map σ is Gorenstein if and only if $\text{fd } \sigma$ is finite and the graded S -module $\text{Ext}_{S \otimes_K^L S}(S, S \otimes_K^L S)$ is invertible. When σ is Gorenstein one has*

$$D^\sigma \simeq \text{Ext}_{S \otimes_K^L S}(S, S \otimes_K^L S)^{-1} \quad \text{in } \text{D}(S),$$

and one can replace $S \otimes_K^L S$ with $S \otimes_K S$ in case σ is flat.

Proof. We may assume that $\text{fd } \sigma$ is finite. One then gets an isomorphism

$$\text{RHom}_S(D^\sigma, S) \simeq \text{RHom}_{S \otimes_K^L S}(S, S \otimes_K^L S) \quad \text{in } \text{D}(S) \quad (8.0.4)$$

from 8.5.4 with $M = S = N$. The following equivalences then hold:

$$\begin{aligned} \sigma \text{ is Gorenstein} &\iff D^\sigma \text{ is invertible} && \text{[by Theorem 8.6.1]} \\ &\iff \text{RHom}_S(D^\sigma, S) \text{ is invertible} && \text{[by Proposition 5.1]} \\ &\iff \text{RHom}_{S \otimes_K^L S}(S, S \otimes_K^L S) \text{ is invertible} && \text{[by (8.0.4)]} \\ &\iff \text{Ext}_{S \otimes_K^L S}(S, S \otimes_K^L S) \text{ is invertible} && \text{[by Proposition 5.1]} \end{aligned}$$

When D^σ is invertible, (8.0.4) and 4.6 yield isomorphisms

$$(D^\sigma)^{-1} \simeq \text{RHom}_{S \otimes_K^L S}(S, S \otimes_K^L S) \simeq \text{Ext}_{S \otimes_K^L S}(S, S \otimes_K^L S) \quad \text{in } \text{D}(S),$$

whence the desired expression for D^σ . The last assertion comes from 8.5.3. \square

Combining Theorem 8.6.2, Proposition 8.1.4, and the isomorphism in 8.1.2, we see that D^σ can be computed from factorizations through arbitrary Gorenstein homomorphisms — not just through essentially smooth ones, as provided by 8.1.1.

Corollary 8.6.3. *If $K \xrightarrow{x} Q \xrightarrow{x'} S$ is a factorization of σ with x Gorenstein and x' finite, then there is an isomorphism*

$$D^\sigma \simeq \text{RHom}_Q(S, Q) \otimes_Q \text{Ext}_{Q \otimes_K^L Q}(Q, Q \otimes_K^L Q)^{-1} \quad \text{in } \text{D}(S). \quad \square$$

Appendix: Homological invariants

Let R be a commutative noetherian ring.

Complexes of R -modules have differentials of degree -1 . Modules are identified with complexes concentrated in degree zero. For every graded R -module H we set

$$\inf H = \inf\{n \in \mathbb{Z} \mid H_n \neq 0\} \quad \text{and} \quad \sup H = \sup\{n \in \mathbb{Z} \mid H_n \neq 0\}.$$

The *amplitude* of H is the number $\text{amp } H = \sup H - \inf H$. Thus $H = 0$ is equivalent to $\inf H = \infty$; to $\sup H = -\infty$; to $\text{amp } H = -\infty$, and also to $\text{amp } H < 0$.

We write $\text{D}(R)$ for the derived category of R -modules, and Σ for its translation functor. Various full subcategories of $\text{D}(R)$ are used in this text. Our notation for them is mostly standard: the objects of $\text{D}_+(R)$ are the complexes M with $\inf H(M) > -\infty$, those of $\text{D}_-(R)$ are the complexes M with $\sup H(M) < \infty$, and $\text{D}_b(R) = \text{D}_+(R) \cap \text{D}_-(R)$. Also, $\text{D}^f(R)$ is the category of complexes M with $H_n(M)$ finite for each $n \in \mathbb{Z}$, and we set $\text{D}_+^f(R) = \text{D}^f(R) \cap \text{D}_+(R)$, etc.

For complexes M and N in $D(R)$ we write $M \otimes_R^{\mathbb{L}} N$ for the derived tensor product, $\mathrm{RHom}_R(M, N)$ for the derived complex of homomorphisms, and set

$$\mathrm{Tor}_n^R(M, N) = H_n(M \otimes_R^{\mathbb{L}} N) \quad \text{and} \quad \mathrm{Ext}_R^n(M, N) = H_{-n}(\mathrm{RHom}_R(M, N)).$$

Standard spectral sequence arguments give the following well known assertions:

A.1. For all complexes M and N in $D(R)$ there are inequalities

$$\begin{aligned} \sup H(\mathrm{RHom}_R(M, N)) &\leq \sup H(N) - \inf H(M), \\ \inf H(M \otimes_R^{\mathbb{L}} N) &\geq \inf H(M) + \inf H(N). \end{aligned}$$

If M is in $D_+^f(R)$ and N is in $D_-^f(R)$, then $\mathrm{RHom}_R(M, N)$ is in $D_-^f(R)$.

If M and N are in $D_+^f(R)$, then so is $M \otimes_R^{\mathbb{L}} N$.

For ease of reference, we list some canonical isomorphisms:

A.2. Let \mathfrak{m} be a maximal ideal of R and set $k = R/\mathfrak{m}$. For all complexes M in $D(R)$ and N in $D_-^f(R)$ there are isomorphisms of graded k -vector spaces

$$\begin{aligned} k \otimes_R^{\mathbb{L}} M &\cong (k \otimes_R^{\mathbb{L}} M)_{\mathfrak{m}} \cong k \otimes_R^{\mathbb{L}} M_{\mathfrak{m}} \cong k \otimes_{R_{\mathfrak{m}}}^{\mathbb{L}} M_{\mathfrak{m}}; \\ \mathrm{RHom}_R(k, N) &\cong \mathrm{RHom}_R(k, N)_{\mathfrak{m}} \cong \mathrm{RHom}_R(k, N_{\mathfrak{m}}) \cong \mathrm{RHom}_{R_{\mathfrak{m}}}(k, N_{\mathfrak{m}}). \end{aligned}$$

We write that (R, \mathfrak{m}, k) is a *local ring* to indicate that R is a commutative noetherian ring with unique maximal ideal \mathfrak{m} and with residue field $k = R/\mathfrak{m}$.

The statements below may be viewed as partial converses to those in [A.1](#).

A.3. Let (R, \mathfrak{m}, k) be a local ring and M a complex in $D^f(R)$.

If $\mathrm{RHom}_R(k, M)$ is in $D_-(R)$, then M is in $D_-(R)$.

If $k \otimes_R^{\mathbb{L}} M$ is in $D_+(R)$, then M is in $D_+(R)$.

See [[Foxby and Iyengar 2003](#), 2.5, 4.5] for the original proofs. The proof of [[Avramov and Iyengar 2008](#), 1.5] gives a shorter, simpler, argument for the second assertion; it can be adapted to cover the first one.

Many arguments in this paper utilize invariants of local rings with values in the ring $\mathbb{Z}[[t]][[t^{-1}]]$ of formal Laurent series in t with integer coefficients. The *order* of such a series $F(t) = \sum_{n \in \mathbb{Z}} a_n t^n$ is the number

$$\mathrm{ord}(F(t)) = \inf\{n \in \mathbb{Z} \mid a_n \neq 0\}.$$

To obtain the expressions for Poincaré series and Bass series in Lemmas [A.4.3](#) and [A.5.3](#) below, we combine ideas from Foxby's proofs [[1977](#), 4.1, 4.2] with the results in [A.3](#); this allows us to relax some boundedness conditions in [[Foxby 1977](#)].

A.4 (Poincaré series). For a local ring (R, \mathfrak{m}, k) and for M in $D_+^f(R)$, in view of [A.1](#) the formula below defines a formal Laurent series, called the *Poincaré series* of M :

$$P_M^R(t) = \sum_{n \in \mathbb{Z}} \text{rank}_k \text{Tor}_n^R(k, M) t^n.$$

A.4.1. When (R, \mathfrak{m}, k) is a local ring, each complex $M \in D_+^f(R)$ admits a resolution $F \xrightarrow{\sim} M$ with $F \in D_+^f(R)$, such that $\partial(F) \subseteq \mathfrak{m}F$ holds and each F_n is free of finite rank; this forces $\inf F = \inf H(M)$. Since $k \otimes_R F$ is a complex of k -vector spaces with zero differential, there are isomorphisms

$$k \otimes_R^L M \simeq k \otimes_R F \simeq H(k \otimes_R F) \quad \text{in } D(R),$$

which imply equalities $\text{rank}_k \text{Tor}_n^R(k, M) = \text{rank}_R F_n$ for all $n \in \mathbb{Z}$.

In [A.4.2](#) and [Lemma A.4.3](#) below, the ring R is not assumed local.

A.4.2. For M in $D_+^f(R)$ and \mathfrak{p} in $\text{Spec } R$ the conditions $\mathfrak{p} \in \text{Supp } M$ and $P_{M_{\mathfrak{p}}}^{R_{\mathfrak{p}}}(t) \neq 0$ are equivalent; when they hold, one has $\text{ord}(P_{M_{\mathfrak{p}}}^{R_{\mathfrak{p}}}(t)) = \inf H(M_{\mathfrak{p}})$.

Indeed, both assertions are immediate consequences of [A.4.1](#).

Lemma A.4.3. *Let M and N be complexes in $D^f(R)$ and \mathfrak{p} be a prime ideal of R . If $(M \otimes_R^L N)_{\mathfrak{p}}$ is in $D_+(R_{\mathfrak{p}})$, then so are $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$, and there are equalities*

$$\begin{aligned} P_{(M \otimes_R^L N)_{\mathfrak{p}}}^{R_{\mathfrak{p}}}(t) &= P_{M_{\mathfrak{p}}}^{R_{\mathfrak{p}}}(t) \cdot P_{N_{\mathfrak{p}}}^{R_{\mathfrak{p}}}(t), \\ \inf H((M \otimes_R^L N)_{\mathfrak{p}}) &= \inf H(M_{\mathfrak{p}}) + \inf H(N_{\mathfrak{p}}). \end{aligned}$$

Proof. In $D(R_{\mathfrak{p}})$ one has $(M \otimes_R^L N)_{\mathfrak{p}} \simeq M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}}^L N_{\mathfrak{p}}$, so it suffices to treat the case when (R, \mathfrak{p}, k) is local. Note the following isomorphisms of graded vector spaces:

$$\begin{aligned} H(k \otimes_R^L (M \otimes_R^L N)) &\cong H((k \otimes_R^L M) \otimes_k^L (k \otimes_R^L N)) \\ &\cong H(k \otimes_R^L M) \otimes_k H(k \otimes_R^L N). \end{aligned}$$

The hypotheses and [A.1](#) yield $H_n(k \otimes_R^L (M \otimes_R^L N)) = 0$ for $n \ll 0$, so the isomorphism implies that $k \otimes_R^L M$ and $k \otimes_R^L N$ are in $D_+(R)$, and thus M and N are in $D_+^f(R)$ by [A.3](#). When they are, for each $n \in \mathbb{Z}$ one has an isomorphism of k -vector spaces

$$\begin{aligned} (H(k \otimes_R^L M) \otimes_k H(k \otimes_R^L N))_n &\cong \bigoplus_{i+j=n} H_i(k \otimes_R^L M) \otimes_k H_j(k \otimes_R^L N) \\ &\cong \bigoplus_{i+j=n} \text{Tor}_i^R(k, M) \otimes_k \text{Tor}_j^R(k, N). \end{aligned}$$

By equating the generating series for the ranks over k , we get the desired equality of Poincaré series; comparing orders and using [A.4.2](#) gives the second equality. \square

A.5 (Bass series). For a local ring (R, \mathfrak{m}, k) and for N in $D_-^f(R)$, in view of [A.1](#) the following formula defines a formal Laurent series, called the *Bass series* of N :

$$I_R^N(t) = \sum_{n \in \mathbb{Z}} \text{rank}_k \text{Ext}_R^n(k, N) t^n.$$

A.5.1. For a local ring R and N in $D_-^f(R)$ one has $\text{ord}(I_R^N(t)) = \text{depth}_R N$; this follows from the definition of depth (see [Section 1](#)). Furthermore, $I_R^N(t)$ is a Laurent polynomial if and only if N has finite injective dimension; see, for example, [[Avramov and Foxby 1991](#), 5.5].

In the remaining statements the ring R is not necessarily local.

A.5.2. For N in $D_-^f(R)$ and \mathfrak{p} in $\text{Spec } R$, the conditions $\mathfrak{p} \in \text{Supp } N$ and $I_{R_{\mathfrak{p}}}^{N_{\mathfrak{p}}}(t) \neq 0$ are equivalent; when they hold, one has $\text{ord}(I_{R_{\mathfrak{p}}}^{N_{\mathfrak{p}}}(t)) = \text{depth}_{R_{\mathfrak{p}}} N_{\mathfrak{p}}$.

Indeed, in view of [A.5.1](#), the assertions follow from the fact that $\text{depth}_{R_{\mathfrak{p}}} N_{\mathfrak{p}} < \infty$ is equivalent to $H(N_{\mathfrak{p}}) \neq 0$; see, for instance, [[Foxby and Iyengar 2003](#), 2.5].

Lemma A.5.3. *Let M and N be complexes in $D^f(R)$ and \mathfrak{p} a prime ideal of R .*

If $\text{RHom}_R(M, N)$ is in $D_-(R)$ then $M_{\mathfrak{p}}$ is in $D_+^f(R_{\mathfrak{p}})$.

If, in addition, \mathfrak{p} is the unique maximal ideal of R , or \mathfrak{p} is maximal and N is in $D_-^f(R)$, or M is in $D_+^f(R)$ and N is in $D_-^f(R)$, then there are equalities

$$\begin{aligned} I_{R_{\mathfrak{p}}}^{\text{RHom}_R(M, N)_{\mathfrak{p}}}(t) &= P_{M_{\mathfrak{p}}}^{R_{\mathfrak{p}}}(t) \cdot I_{R_{\mathfrak{p}}}^{N_{\mathfrak{p}}}(t), \\ \text{depth}_{R_{\mathfrak{p}}}(\text{RHom}_R(M, N)_{\mathfrak{p}}) &= \inf(H(M_{\mathfrak{p}})) + \text{depth}_{R_{\mathfrak{p}}}(N_{\mathfrak{p}}). \end{aligned}$$

Proof. Assume first that \mathfrak{p} is maximal and set $k = R/\mathfrak{p}$. One gets isomorphisms

$$\begin{aligned} H(\text{RHom}_R(k, \text{RHom}_R(M, N))) &\cong H(\text{RHom}_R(k \otimes_R^{\mathbb{L}} M, N)) \\ &\cong H(\text{RHom}_k(k \otimes_R^{\mathbb{L}} M, \text{RHom}_R(k, N))) \\ &\cong \text{Hom}_k(H(k \otimes_R^{\mathbb{L}} M), H(\text{RHom}_R(k, N))) \end{aligned}$$

of graded k -vector spaces by using standard maps. In view of [A.1](#), for $n \gg 0$ one has $H_n(\text{RHom}_R(k, \text{RHom}_R(M, N))) = 0$, so the isomorphisms yield $k \otimes_R^{\mathbb{L}} M \in D_+(R)$ and $\text{RHom}_R(k, N) \in D_-(R)$. When R is local, one gets $M \in D_+^f(R)$ and $N \in D_-^f(R)$ from [A.3](#). For general R , this implies $M_{\mathfrak{p}} \in D_+^f(R_{\mathfrak{p}})$ in view of the isomorphism $k \otimes_R^{\mathbb{L}} M \simeq k \otimes_{R_{\mathfrak{p}}}^{\mathbb{L}} M_{\mathfrak{p}}$ from [A.2](#). If N is in $D_-^f(R)$, then by referring once more to *loc. cit.* we can rewrite the isomorphisms above in each degree n in the form

$$\begin{aligned} \text{Ext}_{R_{\mathfrak{p}}}^n(k, \text{RHom}_R(M, N)_{\mathfrak{p}}) &\cong \text{Hom}_k(\text{Tor}^{R_{\mathfrak{p}}}(k, M_{\mathfrak{p}}), \text{Ext}_{R_{\mathfrak{p}}}(k, N_{\mathfrak{p}}))_{-n} \\ &\cong \bigoplus_{i-j=n} \text{Hom}_k(\text{Tor}_i^{R_{\mathfrak{p}}}(k, M_{\mathfrak{p}}), \text{Ext}_{R_{\mathfrak{p}}}^{-j}(k, N_{\mathfrak{p}})). \end{aligned}$$

For the generating series for the ranks over k these isomorphisms give

$$\begin{aligned} I_{R_p}^{\mathrm{RHom}_R(M,N)_p}(t) &= \left(\sum_{i \in \mathbb{Z}} \mathrm{rank}_k \mathrm{Tor}_i^{R_p}(k, M_p) t^i \right) \left(\sum_{j \in \mathbb{Z}} \mathrm{rank}_k \mathrm{Ext}_{R_p}^j(k, N_p) t^j \right) \\ &= P_{M_p}^{R_p}(t) \cdot I_{R_p}^{N_p}(t). \end{aligned}$$

Equating orders of formal Laurent and using [A.5.2](#) one gets the second equality.

Let now \mathfrak{p} be an arbitrary prime ideal and \mathfrak{m} a maximal ideal containing \mathfrak{p} . The preceding discussion shows that $M_{\mathfrak{m}}$ is in $D_+^f(R_{\mathfrak{m}})$, hence $M_{\mathfrak{p}}$ is in $D_+^f(R_{\mathfrak{p}})$. When M is in $D_+^f(R)$ and N is in $D_-^f(R)$ one has $\mathrm{RHom}_R(M, N)_{\mathfrak{p}} \cong \mathrm{RHom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}})$, so the desired equalities follow from those that have already been established. \square

A.6. The *support* of a complex M in $D_b^f(R)$ is the set

$$\mathrm{Supp}_R M = \{\mathfrak{p} \in \mathrm{Spec} R \mid H(M)_{\mathfrak{p}} \neq 0\}.$$

One has $\mathrm{Supp}_R M = \emptyset$ if and only if $H(M) = 0$, if and only if $M \simeq 0$ in $D(R)$.

For all complexes M, N in $D_b^f(R)$ there are equalities

$$\mathrm{Supp}_R(M \otimes_R^L N) = \mathrm{Supp}_R M \cap \mathrm{Supp}_R N = \mathrm{Supp}_R \mathrm{RHom}_R(M, N).$$

This follows directly from [A.4.2](#), [A.5.2](#), and Lemmas [A.4.3](#) and [A.5.3](#).

Acknowledgments

We are grateful to Lars Winther Christensen, Amnon Neeman, and Sean Sather-Wagstaff for their comments and suggestions on earlier versions of this article.

References

- [Auslander and Bridger 1969] M. Auslander and M. Bridger, *Stable module theory*, Memoirs of the American Mathematical Society **94**, American Mathematical Society, Providence, R.I., 1969. [MR 42 #4580](#) [Zbl 0204.36402](#)
- [Avramov and Foxby 1991] L. L. Avramov and H.-B. Foxby, “Homological dimensions of unbounded complexes”, *J. Pure Appl. Algebra* **71**:2-3 (1991), 129–155. [MR 93g:18017](#) [Zbl 0737.16002](#)
- [Avramov and Foxby 1997] L. L. Avramov and H.-B. Foxby, “Ring homomorphisms and finite Gorenstein dimension”, *Proc. London Math. Society* (3) **75**:2 (1997), 241–270. [MR 98d:13014](#) [Zbl 0901.13011](#)
- [Avramov and Iyengar 2008] L. L. Avramov and S. B. Iyengar, “Gorenstein algebras and Hochschild cohomology”, *Michigan Math. J.* **57** (2008), 17–35. [MR 2009k:13047](#) [Zbl 0560.4517](#)
- [Avramov et al. 2010a] L. L. Avramov, S. B. Iyengar, J. Lipman, and S. Nayak, “Reduction of derived Hochschild functors over commutative algebras and schemes”, *Adv. Math.* **30** (2010), 735–772. [arXiv 0904.4004](#)
- [Avramov et al. 2010b] L. L. Avramov, S. B. Iyengar, and J. Lipman, “Reflexivity and rigidity for complexes, II: Schemes”, preprint, 2010. [arXiv 1001.3450](#)

- [Bass and Murthy 1967] H. Bass and M. P. Murthy, “Grothendieck groups and Picard groups of abelian group rings”, *Ann. of Math. (2)* **86** (1967), 16–73. [MR 36 #2671](#) [Zbl 0157.08202](#)
- [van den Bergh 1997] M. van den Bergh, “Existence theorems for dualizing complexes over non-commutative graded and filtered rings”, *J. Algebra* **195**:2 (1997), 662–679. [MR 99b:16010](#) [Zbl 0894.16020](#)
- [Chouinard 1976] L. G. Chouinard, II, “On finite weak and injective dimension”, *Proc. Amer. Math. Soc.* **60** (1976), 57–60. [MR 54 #5217](#) [Zbl 0343.13005](#)
- [Christensen 2000] L. W. Christensen, *Gorenstein dimensions*, Lecture Notes in Mathematics **1747**, Springer, Berlin, 2000. [MR 2002e:13032](#) [Zbl 0965.13010](#)
- [Christensen 2001] L. W. Christensen, “Semi-dualizing complexes and their Auslander categories”, *Trans. Amer. Math. Soc.* **353**:5 (2001), 1839–1883. [MR 2002a:13017](#) [Zbl 0969.13006](#)
- [Christensen et al. 2002] L. W. Christensen, H.-B. Foxby, and A. Frankild, “Restricted homological dimensions and Cohen–Macaulayness”, *J. Algebra* **251**:1 (2002), 479–502. [MR 2003e:13022](#) [Zbl 1073.13501](#)
- [Conrad 2000] B. Conrad, *Grothendieck duality and base change*, Lecture Notes in Mathematics **1750**, Springer, Berlin, 2000. [MR 2002d:14025](#) [Zbl 0992.14001](#)
- [Foxby 1972] H.-B. Foxby, “Gorenstein modules and related modules”, *Math. Scand.* **31** (1972), 267–284. [MR 48 #6094](#) [Zbl 0272.13009](#)
- [Foxby 1977] H.-B. Foxby, “Isomorphisms between complexes with applications to the homological theory of modules”, *Math. Scand.* **40**:1 (1977), 5–19. [MR 56 #5584](#) [Zbl 0356.13004](#)
- [Foxby 1979] H.-B. Foxby, “Bounded complexes of flat modules”, *J. Pure Appl. Algebra* **15**:2 (1979), 149–172. [MR 83c:13008](#) [Zbl 0411.13006](#)
- [Foxby and Iyengar 2003] H.-B. Foxby and S. Iyengar, “Depth and amplitude for unbounded complexes”, pp. 119–137 in *Commutative algebra* (Grenoble/Lyon, 2001), edited by L. L. Avramov et al., Contemp. Math. **331**, Amer. Math. Soc., Providence, RI, 2003. [MR 2004k:13028](#) [Zbl 1096.13516](#)
- [Frankild and Sather-Wagstaff 2007] A. Frankild and S. Sather-Wagstaff, “Reflexivity and ring homomorphisms of finite flat dimension”, *Comm. Algebra* **35**:2 (2007), 461–500. [MR 2007m:13022](#) [Zbl 1118.13015](#)
- [Frankild et al. 2009] A. J. Frankild, S. Sather-Wagstaff, and A. Taylor, “Relations between semi-dualizing complexes”, *J. Commut. Algebra* **1**:3 (2009), 393–436. [MR 2524860](#)
- [Golod 1984] E. S. Golod, “ G -dimension and generalized perfect ideals”, pp. 62–66 in *Algebraic geometry and its applications*, Trudy Mat. Inst. Steklov. **165**, 1984. In Russian; translated in *Proc. Steklov Inst. Math.* **165** (1985), 62–66. [MR 85m:13011](#) [Zbl 0577.13008](#)
- [Goto 1982] S. Goto, “Vanishing of $\text{Ext}_A^i(M, A)$ ”, *J. Math. Kyoto Univ.* **22**:3 (1982), 481–484. [MR 84c:13019](#) [Zbl 0527.13012](#)
- [Grothendieck 1967] A. Grothendieck, “Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas IV”, *Inst. Hautes Études Sci. Publ. Math.* **32** (1967), 361. [MR 39 #220](#) [Zbl 0153.22301](#)
- [Hartshorne 1966] R. Hartshorne, *Residues and duality*, Lecture notes of a seminar on the work of A. Grothendieck, given at Harvard 1963/64. With an appendix by P. Deligne. Lecture Notes in Mathematics, No. 20, Springer, Berlin, 1966. [MR 36 #5145](#) [Zbl 0212.26101](#)
- [Ischebeck 1969] F. Ischebeck, “Eine Dualität zwischen den Funktoren Ext und Tor ”, *J. Algebra* **11** (1969), 510–531. [MR 38 #5894](#)

- [Kawasaki 2002] T. Kawasaki, “On arithmetic Macaulayfication of Noetherian rings”, *Trans. Amer. Math. Soc.* **354**:1 (2002), 123–149. MR 2002i:13001 Zbl 1087.13502
- [Lipman 1984] J. Lipman, *Dualizing sheaves, differentials and residues on algebraic varieties*, Astérisque **117**, 1984. MR 86g:14008 Zbl 0562.14003
- [Matsumura 1986] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Math. **8**, Cambridge University Press, Cambridge, 1986. MR 88h:13001 Zbl 0603.13001
- [Neeman 2008] A. Neeman, “Derived categories and Grothendieck duality”, 2008, Available at www.crm.es/Publications/08/Pr791.pdf. To appear in *Triangulated categories* (Leeds, 2006), London Math. Soc. Lecture Note Ser. Cambridge University Press.
- [Quillen 1970] D. Quillen, “On the (co-) homology of commutative rings”, pp. 65–87 in *Applications of categorical algebra* (New York, 1968), edited by A. Heller, Proc. Sympos. Pure Math. **17**, Amer. Math. Soc., Providence, R.I., 1970. MR 41 #1722 Zbl 0234.18010
- [Yekutieli 1999] A. Yekutieli, “Dualizing complexes, Morita equivalence and the derived Picard group of a ring”, *J. London Math. Soc.* (2) **60**:3 (1999), 723–746. MR 2001i:16008 Zbl 0954.16006
- [Yekutieli and Zhang 2008] A. Yekutieli and J. J. Zhang, “Rigid complexes via DG algebras”, *Trans. Amer. Math. Soc.* **360**:6 (2008), 3211–3248. MR 2008m:16016 Zbl 1165.18009
- [Yekutieli and Zhang 2009] A. Yekutieli and J. J. Zhang, “Rigid dualizing complexes over commutative rings”, *Algebr. Represent. Theory* **12**:1 (2009), 19–52. MR 2471449 Zbl 05619084

Communicated by Craig Huneke

Received 2009-04-15

Revised 2009-07-15

Accepted 2009-08-18

avramov@math.unl.edu

*Department of Mathematics, University of Nebraska,
Lincoln, NE 68588, United States*

iyengar@math.unl.edu

*Department of Mathematics, University of Nebraska,
Lincoln, NE 68588, United States*
www.math.unl.edu/~siyengar2

jlipman@purdue.edu

*Department of Mathematics, Purdue University,
W. Lafayette, IN 47907, United States*

The Picard group of $\mathcal{M}_{1,1}$

William Fulton and Martin Olsson

We compute the Picard group of the moduli stack of elliptic curves and its canonical compactification over general base schemes.

1. Introduction

Let $\mathcal{M}_{1,1}$ denote the moduli stack (over \mathbb{Z}) classifying elliptic curves, and for a scheme S let $\mathcal{M}_{1,1,S}$ denote the fiber product $S \times_{\text{Spec}(\mathbb{Z})} \mathcal{M}_{1,1}$. Mumford [1965] computed the Picard group $\text{Pic}(\mathcal{M}_{1,1,S})$ when S is the spectrum of a field of characteristic not 2 or 3 and found it to be cyclic of order 12. Our aim in this paper is to compute the Picard group $\text{Pic}(\mathcal{M}_{1,1,S})$ for more general base schemes S , as well as to compute the Picard group $\text{Pic}(\overline{\mathcal{M}}_{1,1,S})$ for the standard compactification $\overline{\mathcal{M}}_{1,1}$ of $\mathcal{M}_{1,1}$.

Recall that on $\mathcal{M}_{1,1}$ there is the Hodge bundle λ . For any morphism $t : T \rightarrow \mathcal{M}_{1,1}$ corresponding to an elliptic curve $f : E \rightarrow T$, the pullback $t^*\lambda$ is the line bundle $f_*\Omega_{E/T}^1$. Equivalently, if $f : \mathcal{E} \rightarrow \mathcal{M}_{1,1}$ denotes the universal elliptic curve, then $\lambda = f_*\Omega_{\mathcal{E}/\mathcal{M}_{1,1}}^1$. This bundle extends canonically to $\overline{\mathcal{M}}_{1,1}$. Namely, let $\tilde{f} : \tilde{\mathcal{E}} \rightarrow \overline{\mathcal{M}}_{1,1}$ denote the extension of \mathcal{E} provided by the Tate curve and let $\omega_{\tilde{\mathcal{E}}/\overline{\mathcal{M}}_{1,1}}$ denote the relative dualizing sheaf. Then the sheaf $\tilde{f}_*\omega_{\tilde{\mathcal{E}}/\overline{\mathcal{M}}_{1,1}}$ is a line bundle on $\overline{\mathcal{M}}_{1,1}$ extending λ . In what follows we will abuse notation and write also λ for this line bundle on $\overline{\mathcal{M}}_{1,1}$.

Recall the following basic facts and definitions about elliptic curves (see for example [Deligne 1975, §1]). If Λ is a ring and $t : \text{Spec}(\Lambda) \rightarrow \mathcal{M}_{1,1}$ is a morphism corresponding to an elliptic curve E/Λ , then after replacing Λ by an étale extension the family E can be described by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (1-1)$$

Define

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, & b_4 &= a_1a_3 + 2a_4, & b_6 &= a_3^2 + 4a_6, \\ b_8 &= -a_1a_3a_4 - a_4^2 + a_1^2a_6 + a_2a_3^2 + 4a_2a_6, \end{aligned} \quad (1-2)$$

MSC2000: primary 14D22; secondary 14D05.

Keywords: moduli spaces, stacks, Picard group.

Olsson was partially supported by NSF grant DMS-0555827 and an Alfred P. Sloan fellowship.

and the discriminant

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \in \Lambda^*. \quad (1-3)$$

With these chosen coordinates a basis for $t^* \lambda$ is given by the *invariant differential*

$$\pi = dx / (2y + a_1 x + a_3). \quad (1-4)$$

Any two choices of coordinates (1-1) differ by a transformation

$$x' = u^2 x + r, \quad y' = u^3 y + s u^2 x + t, \quad (1-5)$$

where $u \in \Lambda^*$ and $r, s, t \in \Lambda$. One can compute that the invariant differential π' obtained from the coordinates (x', y') is equal to $u^{-1} \pi$, and that the discriminant Δ' in the coordinates (x', y') is equal to $u^{12} \Delta$. In particular, the element $\Delta \pi^{\otimes 12} \in t^* \lambda^{\otimes 12}$ is independent of the choice of coordinates, and therefore defines a trivialization of $\lambda^{\otimes 12}$ over $\mathcal{M}_{1,1}$.

Let $p : \mathcal{M}_{1,1,S} \rightarrow \mathbb{A}_S^1$ be the map defined by the j -invariant

$$j = (b_2^2 - 24b_4)^3 / \Delta. \quad (1-6)$$

Theorem 1.1. *Let S be a scheme. Then the map*

$$\mathbb{Z}/(12) \times \text{Pic}(\mathbb{A}_S^1) \rightarrow \text{Pic}(\mathcal{M}_{1,1,S}), \quad (i, \mathcal{L}) \mapsto \lambda^{\otimes i} \otimes p^* \mathcal{L} \quad (1-7)$$

is an isomorphism if either of the following hold:

- (i) S is a $\mathbb{Z}[1/2]$ -scheme.
- (ii) S is reduced.

Remark 1.2. As we observe in [Remark 6.4](#) the theorem fails for nonreduced schemes in characteristic 2.

Theorem 1.3. *The map*

$$\mathbb{Z} \times \text{Pic}(S) \rightarrow \text{Pic}(\overline{\mathcal{M}}_{1,1,S}), \quad (n, M) \mapsto \lambda^n \otimes_{\mathcal{O}_S} M \quad (1-8)$$

is an isomorphism for any scheme S .

The paper is organized as follows. In [Section 2](#) we give a proof of [Theorem 1.1](#) in the case when 6 is invertible on the base. In this case the orders of the stabilizer groups of $\mathcal{M}_{1,1,S}$ are invertible on S (the stack $\mathcal{M}_{1,1,S}$ is *tame*), which makes it easy to relate the invertible sheaves on $\mathcal{M}_{1,1,S}$ and on its coarse moduli space (see [Lemma 2.3](#)). In [Section 3](#) we then give a separate argument proving [Theorem 1.1](#) which works when the base S is normal. Using this case of a normal base, we then prove [Theorem 1.1](#) when S is reduced in [Section 4](#). Once the case of reduced S is established, the general statement of [Theorem 1.1](#) reduces to studying the relationship between deformation theory of line bundles on $\mathcal{M}_{1,1,S}$ and its coarse

space. This essentially amounts to computing the coherent cohomology groups of $\mathcal{M}_{1,1,S}$, which occupies [Section 5](#). Finally in [Section 6](#) we use similar techniques to prove [Theorem 1.3](#).

Remark 1.4. By standard limit arguments it suffices to prove the above results in the case when S is of finite type over an excellent Dedekind ring. In what follows we will therefore restrict ourselves to such schemes unless otherwise stated.

2. When 6 is invertible on S

Though the case when 6 is invertible follows from the more technical work in subsequent sections, we include here a proof in the case of a $\mathbb{Z}[1/6]$ -scheme since it is much easier than the more general cases.

The following lemma is well-known (and does not require that 6 be invertible in S), but we include a proof for the convenience of the reader.

Lemma 2.1. *For any locally noetherian scheme S , the map $\bar{\pi} : \bar{\mathcal{M}}_{1,1,S} \rightarrow \mathbb{P}_S^1$ (resp. $\pi : \mathcal{M}_{1,1,S} \rightarrow \mathbb{A}_S^1$) given by the j -invariant identifies \mathbb{P}_S^1 (resp. \mathbb{A}_S^1) with the coarse moduli space of $\bar{\mathcal{M}}_{1,1,S}$ (resp. $\mathcal{M}_{1,1,S}$).*

Proof. Since the square

$$\begin{array}{ccc} \mathcal{M}_{1,1,S} & \hookrightarrow & \bar{\mathcal{M}}_{1,1,S} \\ \downarrow \pi & & \downarrow \bar{\pi} \\ \mathbb{A}_S^1 & \hookrightarrow & \mathbb{P}_S^1 \end{array}$$

is cartesian, it suffices to show that $\bar{\pi}$ identifies \mathbb{P}_S^1 with the coarse moduli space of $\bar{\mathcal{M}}_{1,1,S}$.

Let $\tilde{\pi} : \bar{\mathcal{M}}_{1,1,S} \rightarrow X$ be the coarse moduli space (which exists by [\[Keel and Mori 1997\]](#)). By the universal property of the coarse moduli space, there exists a unique morphism $f : X \rightarrow \mathbb{P}_j^1$ such that $f \circ \tilde{\pi} = \bar{\pi}$. Since $\bar{\pi}$ is proper and quasifinite, the morphism f is also proper and quasifinite and therefore f is finite. Furthermore, by [\[Abramovich and Vistoli 2002, 2.2.1\]](#) we have $\tilde{\pi}_* \mathcal{O}_{\bar{\mathcal{M}}_{1,1,S}} = \mathcal{O}_X$. It therefore suffices to show that the map $\mathcal{O}_{\mathbb{P}_j^1} \rightarrow \tilde{\pi}_* \mathcal{O}_{\bar{\mathcal{M}}_{1,1,S}}$ is an isomorphism. It suffices to verify this locally in the flat topology on S , so we may further assume that S is the spectrum of a complete noetherian local ring A . In addition, since the morphism $\bar{\pi}$ is proper, the theorem on formal functions for stacks [\[Olsson 2005, §3\]](#) implies that it suffices to show the result over $\text{Spec}(A/\mathfrak{m}_A^n)$ for all n . This reduces the proof to the case when S is the spectrum of an artinian local ring A . Let k be the residue field of A , and let $J \subset A$ be an ideal with J annihilated by the maximal ideal of A (so that J is a k -vector space). Set $A_0 := A/J$. Pushing forward the

exact sequence

$$0 \rightarrow J \otimes \mathbb{O}_{\overline{\mathcal{M}}_{1,1,k}} \rightarrow \mathbb{O}_{\overline{\mathcal{M}}_{1,1,A}} \rightarrow \mathbb{O}_{\overline{\mathcal{M}}_{1,1,A_0}} \rightarrow 0 \tag{2-1}$$

to \mathbb{P}_A^1 we obtain a commutative diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & (\bar{\pi}_* \mathbb{O}_{\overline{\mathcal{M}}_{1,1,k}}) \otimes J & \longrightarrow & \bar{\pi}_* \mathbb{O}_{\overline{\mathcal{M}}_{1,1,A}} & \longrightarrow & \bar{\pi}_* \mathbb{O}_{\overline{\mathcal{M}}_{1,1,A_0}} \\
 & & \uparrow a & & \uparrow b & & \uparrow c \\
 0 & \longrightarrow & (\mathbb{O}_{\mathbb{P}_k^1}) \otimes J & \longrightarrow & \mathbb{O}_{\mathbb{P}_A^1} & \longrightarrow & \mathbb{O}_{\mathbb{P}_{A_0}^1} \longrightarrow 0.
 \end{array} \tag{2-2}$$

By induction and the case when A is a field, we get that a and c are isomorphisms and therefore b is an isomorphism also. □

Assume for the rest of this section that S is a $\mathbb{Z}[1/6]$ -scheme.

Let $\tilde{s}_4 : S \rightarrow \mathcal{M}_{1,1,S}$ be the section corresponding to the elliptic curve with automorphism group μ_4 ($y^2 = x^3 + x$ with $\Delta = -64$, $j = 1728$) and $\tilde{s}_6 : S \rightarrow \mathcal{M}_{1,1,S}$ the section corresponding to the elliptic curve with automorphism group μ_6 ($y^2 + y = x^3$ with $\Delta = -27$, $j = 0$). These sections define closed immersions $s_4 : B\mu_{4,S} \hookrightarrow \mathcal{M}_{1,1,S}$ and $s_6 : B\mu_{6,S} \hookrightarrow \mathcal{M}_{1,1,S}$. For any line bundle \mathcal{L} on $\mathcal{M}_{1,1,S}$ the pullback $s_4^* \mathcal{L}$ (resp. $s_6^* \mathcal{L}$) corresponds to a line bundle M_4 (resp. M_6) on S with action of the group μ_4 (resp. μ_6). We thus get maps

$$\rho_4 : \mu_4 \rightarrow \underline{\text{Aut}}(M_4) \simeq \mathbb{G}_m, \quad \rho_6 : \mu_6 \rightarrow \underline{\text{Aut}}(M_6) \simeq \mathbb{G}_m$$

defining characters $\chi_4 \in \mathbb{Z}/(4)$ and $\chi_6 \in \mathbb{Z}/(6)$.

Lemma 2.2. *The pair (χ_4, χ_6) lies in $\mathbb{Z}/(12) \subset \mathbb{Z}/(4) \times \mathbb{Z}/(6)$.*

Proof. The construction of the pair (χ_4, χ_6) commutes with arbitrary base change on S , so it suffices to consider the case when S is the spectrum of an algebraically closed field, $S = \text{Spec}(k)$. We have to show that $\rho_4|_{\mu_2} = \rho_6|_{\mu_2}$. Write $k[[t]]$ for the completion of the local ring of \mathbb{A}_j^1 at $j = 1728$ and let $k[[z]]$ be the completion of the local ring of $\mathcal{M}_{1,1,S}$ at the point corresponding to the curve $y^2 = x^3 + x$. Then for suitable choices of the coordinates t and z the map $k[[t]] \rightarrow k[[z]]$ sends t to z^2 , and the action of μ_4 is given by $\zeta * z = \zeta^2 \cdot z$. Furthermore we can write $\mathcal{L}|_{k[[z]]} = k[[z]] \cdot e$ for some basis e , such that ρ_4 acts by $\zeta * e = \zeta^4 e$. From this we see that $\rho_4|_{\mu_2}$ is equal to the character defined by the action of μ_2 on the fiber of \mathcal{L} at the generic point of $\mathcal{M}_{1,1,S}$. Similarly, $\rho_6|_{\mu_2}$ is equal to the action on the generic fiber. □

We therefore obtain a map

$$\text{Pic}(\mathcal{M}_{1,1,S}) \rightarrow \mathbb{Z}/(12), \quad \mathcal{L} \mapsto (\chi_4, \chi_6), \tag{2-3}$$

and it follows from the construction that this map is a homomorphism. Let K denote the kernel.

Recall that a Deligne–Mumford stack \mathcal{X} is called *tame* if for every algebraically closed field Ω and point $\bar{x} : \text{Spec}(\Omega) \rightarrow \mathcal{X}$ the order of the automorphism group of \bar{x} is relatively prime to the characteristic of Ω .

Lemma 2.3. *Let \mathcal{X} be a tame Deligne–Mumford stack with coarse moduli space $\pi : \mathcal{X} \rightarrow X$. Let \mathcal{L} be an invertible sheaf on \mathcal{X} such that for every geometric point $\bar{x} \rightarrow \mathcal{X}$ the action of the stabilizer group $G_{\bar{x}}$ on $\mathcal{L}(\bar{x})$ is trivial. Then $\pi_*\mathcal{L}$ is an invertible sheaf on X and $\pi^*\pi_*\mathcal{L} \rightarrow \mathcal{L}$ is an isomorphism.*

Proof. It suffices to prove the lemma after passing to the strict henselization of X at a geometric point \bar{x} . Let $A = \mathbb{O}_{X, \bar{x}}$ and $B = \mathbb{O}_{\mathcal{X}, \bar{x}}$. Then, as explained in [Olsson 2006, 2.12], if Γ denotes the stabilizer group of \bar{x} then there is a natural action of Γ on B such that $\mathcal{X} = [\text{Spec}(B)/\Gamma]$. Let M be the free B -module with Γ -action of rank 1 defining \mathcal{L} . Since Γ has order invertible in $k(\bar{x})$ (since \mathcal{X} is tame), the representation category of Γ is semisimple. By our assumptions, the reduction $M \otimes k(\bar{x})$ is generated by an invariant element, and choosing a lifting to an invariant element of M we see that we can write $M = B \cdot e$ where Γ acts trivially on e . Then $\pi_*\mathcal{L}$ is just $A \cdot e$ and the lemma is immediate. \square

Corollary 2.4. *The homomorphism $\pi^* : \text{Pic}(\mathbb{A}_S^1) \rightarrow K$ is an isomorphism.*

Proof. We show that if \mathcal{L} is a line bundle with $(\chi_4, \chi_6) = (0, 0)$, then $\pi_*\mathcal{L}$ is an invertible sheaf on \mathbb{A}_S^1 and $\pi^*\pi_*\mathcal{L} \rightarrow \mathcal{L}$ is an isomorphism. By Lemma 2.3 it suffices to show that for any geometric point $\bar{x} \rightarrow \mathcal{M}_{1,1,S}$, the action of the stabilizer group of \bar{x} on $\mathcal{L}(\bar{x})$ is trivial. For this we may assume that S is the spectrum of an algebraically closed field. By our assumptions, the actions ρ_4 and ρ_6 are trivial. By the argument used in the proof of Lemma 2.2, this implies that the action of the generic stabilizer is also trivial. From this it follows that the action is trivial at every point since over $\mathbb{A}^1 - \{0, 1728\}$ the stack $\mathcal{M}_{1,1,S}$ is a μ_2 -gerbe. \square

Lemma 2.5. *The image of λ in $\mathbb{Z}/(12)$ is a generator. In particular (2-3) is surjective.*

Proof. It suffices to consider the case when S is the spectrum of a field, in which case the above shows that $\text{Pic}(\mathcal{M}_{1,1,S})$ injects into $\mathbb{Z}/(12)$. We can in fact compute directly the image of λ in $\mathbb{Z}/(4) \times \mathbb{Z}/(6)$. The image in $\mathbb{Z}/(4)$ corresponds to the representation of μ_4 given by the action on the invariant differential $dx/2y$ of the curve $y^2 = x^3 + x$. An element $\zeta \in \mu_4$ acts by $(x, y) \mapsto (\zeta^2 x, \zeta y)$, and therefore the action on $dx/2y$ is equal to multiplication by ζ . Therefore the image of λ in $\mathbb{Z}/(4)$ is equal to 1.

Similarly, the image of λ in $\mathbb{Z}/(6)$ corresponds to the character given by the invariant differential $dx/(2y+1)$ of the curve $y^2 + y = x^3$. Write $\mu_6 = \mu_2 \times \mu_3$. Then $(-1, 1)$ acts by $(x, y) \mapsto (x, -y-1)$ and $(1, \zeta)$ acts by $(x, y) \mapsto (\zeta x, y)$. Therefore $(-1, 1)$ acts on the invariant differential by multiplication by -1 and

$(1, \zeta)$ acts by multiplication by ζ . It follows that λ maps to 1 in $\mathbb{Z}/(6)$ which implies that λ is a generator in $\mathbb{Z}/(12)$. □

Corollary 2.6. *The map $\lambda \times \pi^* : (\mathbb{Z}/12) \times \text{Pic}(\mathbb{A}_S^1) \rightarrow \text{Pic}(\mathcal{M}_{1,1,S})$ is an isomorphism.*

3. The case of a normal affine scheme S

Write $S = \text{Spec}(\Lambda)$ with Λ a normal ring. Let U be the scheme

$$U := \text{Spec}(\Lambda[a_1, a_2, a_3, a_4, a_6][1/\Delta]), \tag{3-1}$$

where Δ is as in (1-3). Equation (1-1) defines a family of elliptic curves $E \rightarrow U$. Let G denote the group scheme with underlying scheme $\text{Spec}(\Lambda[u^\pm, r, s, t])$ with group law defined by

$$(u', r', s', t') \cdot (u, r, s, t) = (uu', u^2r' + r, us' + s, u^3t' + u^2r's + t). \tag{3-2}$$

The group G acts on E over the action on U via the formulas [Deligne 1975, 1.6], and $\mathcal{M}_{1,1,S}$ is isomorphic to the stack theoretic quotient $[U/G]$.

Proposition 3.1. *The pullback map*

$$\text{Pic}(S) \rightarrow \text{Pic}(U) \tag{3-3}$$

is an isomorphism.

Proof. The key point is the following result of Ischebeck [1979, §4].

Lemma 3.2. *Let $\Delta \in \mathbb{Z}[t_1, \dots, t_n]$ be a polynomial satisfying*

- (i) *The greatest common divisor of the coefficients of its nonconstant monomials is 1.*
- (ii) *For any field k the image of Δ in $k[t_1, \dots, t_n]$ is irreducible.*

Then for any noetherian normal ring Λ , the pullback homomorphism

$$\text{Pic}(\Lambda) \rightarrow \text{Pic}(\Lambda[t_1, \dots, t_n][1/\Delta]) \tag{3-4}$$

is an isomorphism.

Proof. The assumptions are used as follows:

- (1) Assumption (i) implies that the map $\text{Spec}(\mathbb{Z}[t_1, \dots, t_n][1/\Delta]) \rightarrow \text{Spec}(\mathbb{Z})$ is surjective and hence faithfully flat. It follows that the map

$$\text{Spec}(\Lambda[t_1, \dots, t_n][1/\Delta]) \rightarrow \text{Spec}(\Lambda) \tag{3-5}$$

is also faithfully flat.

(2) By the preceding observation, the divisor $V(\Delta) \subset \text{Spec}(\Lambda[t_1, \dots, t_n])$ does not contain any fibers, and by (ii) its generic fiber is nonempty and irreducible. From this it follows that $V(\Delta)$ is irreducible.

It follows that there is an exact sequence of Weil divisor class groups [Fulton 1998, 1.8]

$$\mathbb{Z}[V(\Delta)] \xrightarrow{0} \text{Cl}(\Lambda[t_1, \dots, t_n]) \rightarrow \text{Cl}(\Lambda[t_1, \dots, t_n][1/\Delta]) \longrightarrow 0. \quad (3-6)$$

We conclude that

$$\text{Cl}(\Lambda) \simeq \text{Cl}(\Lambda[t_1, \dots, t_n]) \simeq \text{Cl}(\Lambda[t_1, \dots, t_n][1/\Delta]). \quad (3-7)$$

The normality of Λ implies that the natural maps from the Picard groups to the Weil divisor class groups are injective. Therefore, it suffices to show that if $D \in \text{Cl}(\Lambda)$ is a Weil divisor whose image in $\text{Cl}(\Lambda[t_1, \dots, t_n][1/\Delta])$ is in the image of $\text{Pic}(\Lambda[t_1, \dots, t_n][1/\Delta])$, then D is obtained from a line bundle on $\text{Spec}(\Lambda)$. This follows from the observation that $\Lambda \rightarrow \Lambda[t_1, \dots, t_n][1/\Delta]$ is faithfully flat [Ischebeck 1979, §4, Satz 6]. \square

We apply the lemma to $\Delta \in \mathbb{Z}[a_1, \dots, a_6]$; (i) is immediate and (ii) follows from the calculations in [Deligne 1975, §3, §4] (Note that though these sections concern characteristics prime to 6, the same calculations give the irreducibility of Δ over arbitrary fields.) \square

The isomorphism $\mathcal{M}_{1,1,S} \simeq [U/G]$ defines a morphism $\sigma : \mathcal{M}_{1,1,S} \rightarrow BG$. For a character $\chi : G \rightarrow \mathbb{G}_m$ defining a line bundle on BG , let L_χ be the line bundle on $\mathcal{M}_{1,1,S}$ obtained by pullback along σ .

Lemma 3.3. *Let \mathcal{L} be a line bundle on $\mathcal{M}_{1,1,S}$ such that the pullback L of \mathcal{L} to U is trivial. Then $\mathcal{L} \simeq L_\chi$ for some character $\chi : G \rightarrow \mathbb{G}_m$.*

Proof. Fix a basis $e \in L$.

Let \mathcal{F} be the sheaf on the category of affine S -schemes (with the étale topology) which to any morphism of affine schemes $S' \rightarrow S$ associates $\Gamma(U_{S'}, \mathbb{O}_{U_{S'}}^*)$. There is an inclusion of sheaves $\mathbb{G}_m \subset \mathcal{F}$ given by the inclusions $\Gamma(S', \mathbb{O}_{S'}^*) \subset \Gamma(U_{S'}, \mathbb{O}_{U_{S'}}^*)$. For any $S' \rightarrow S$ and $g \in G(S')$, we get an element $u_g \in \mathcal{F}(S')$ defined by the condition that $g(e) = u_g \cdot e \in L$. This defines a map of sheaves (not necessarily a homomorphism)

$$f : G \rightarrow \mathcal{F}. \quad (3-8)$$

To prove the lemma it suffices to show that f has image contained in $\mathbb{G}_m \subset \mathcal{F}$ (note that it is clear that if this holds then the map $G \rightarrow \mathbb{G}_m$ is a homomorphism).

Since G is an affine scheme, the map f is determined by a section $u_0 \in \mathcal{F}(G)$. Since G is normal and connected, this section $u_0 \in \Gamma(U_G, \mathbb{O}_{U_G}^*)$ can be written uniquely as $\beta \Delta^m$, where $\beta \in \Gamma(G, \mathbb{O}_G^*)$ and $m \in \mathbb{Z}$. We need to show that $m = 0$.

For this, note that the image of u_0 under the map $\mathcal{F}(G) \rightarrow \mathcal{F}(S)$ defined by the identity section $e : S \rightarrow G$ is equal to 1. It follows that $e^*(\beta) \cdot \Delta^m$ is equal to 1 in $\Gamma(U, \mathcal{O}_U^*)$ which implies that $m = 0$. \square

Lemma 3.4. *Any homomorphism $G \rightarrow \mathbb{G}_m$ factors through the projection*

$$\chi_0 : G \rightarrow \mathbb{G}_m, \quad (u, r, s, t) \mapsto u. \tag{3-9}$$

Proof. There are three injective homomorphisms

$$j_r, j_s, j_t : \mathbb{G}_a \hookrightarrow G \tag{3-10}$$

sending $x \in \mathbb{G}_a$ to $(1, x, 0, 0)$, $(1, 0, x, 0)$, and $(1, 0, 0, x)$ respectively. The formula

$$(1, r, 0, 0)(1, 0, s, 0)(1, 0, 0, t - rs) = (1, r, s, t) \tag{3-11}$$

shows that the subgroup of G generated by the images of these three inclusions is equal to the kernel of χ_0 . Since any homomorphism $\mathbb{G}_a \rightarrow \mathbb{G}_m$ is trivial, it follows that any homomorphism $G \rightarrow \mathbb{G}_m$ has kernel containing $\text{Ker}(\chi_0)$. \square

Lemma 3.5. *Let $n, m \in \mathbb{Z}$ be integers. Then $L_{\chi_0^n} \simeq L_{\chi_0^m}$ if and only if $n \equiv m \pmod{12}$.*

Proof. Observe that

$$L_{\chi_0^n} \otimes L_{\chi_0^m}^{-1} \simeq L_{\chi_0^{n-m}},$$

so it suffices to show that $L_{\chi_0^n} \simeq \mathcal{O}_{\mathcal{M}_{1,1,S}}$ if and only if $12 \mid n$.

Choose a basis $e \in L_{\chi_0^n}(U)$ such that G acts on e through χ_0^n . Then an isomorphism $\mathcal{O}_{\mathcal{M}_{1,1,S}} \simeq L_{\chi_0^n}$ is given by a function $\epsilon \in \Gamma(U, \mathcal{O}_U^*)$ such that the action of G on $\epsilon^{-1} \cdot e$ is trivial. Equivalently we want a global section $\epsilon \in \Gamma(U, \mathcal{O}_U^*)$ such that G acts on ϵ through χ_0^n . Since

$$\Gamma(U, \mathcal{O}_U^*) \simeq \Lambda^* \cdot \Delta^{\mathbb{Z}},$$

and G acts on Δ through χ_0^{12} , such a unit ϵ exists if and only if $12 \mid n$. \square

Let $\iota : L_{\chi_0^{12}} \simeq \mathcal{O}_{\mathcal{M}_{1,1,S}}$ be the trivialization defined by Δ . This trivialization enables us to speak of $L_{\chi_0^n}$ for any class $n \in \mathbb{Z}/(12)$.

By [Proposition 3.1](#), if \mathcal{L} is a line bundle on $\mathcal{M}_{1,1,S}$, then the pullback of \mathcal{L} to U is isomorphic to the pullback of a line bundle M on S . Trivializing this line bundle M locally on S , we see that locally on S we have an isomorphism $\mathcal{L} \simeq L_{\chi_0^n}$, for a unique class $n \in \mathbb{Z}/(12)$. From the uniqueness it follows that to any connected S and line bundle \mathcal{L} on $\mathcal{M}_{1,1,S}$, there exists a unique class $n \in \mathbb{Z}/(12)$ and line bundle M on S such that

$$\mathcal{L} \simeq M \otimes L_{\chi_0^n}.$$

Moreover, such a line bundle \mathcal{L} is trivial if and only if M is trivial and n is the zero element of $\mathbb{Z}/(12)$.

The line bundle λ is trivialized over U by the invariant differential π defined in (1-4), and as mentioned in the introduction the action of $(u, r, s, t) \in G$ on π is through the character $G \rightarrow \mathbb{G}_m$ sending (u, r, s, t) to u^{-1} . Therefore

$$\lambda \simeq L_{\chi_0^{-1}}.$$

This completes the proof of [Theorem 1.1](#) in the case when S is affine and normal. \square

A very similar argument can be used to prove [Theorem 1.3](#) in the case when the base scheme S is affine and normal. Let $c_4 = b_2^2 - 24b_4$. Then one can show (see for example [[Silverman 2009](#), III.1.4]) that (1-1) is nodal precisely when $\Delta = 0$ and $c_4 \neq 0$. Let \tilde{U} denote

$$\text{Spec}(\Lambda[a_1, a_2, a_3, a_4, a_6]) - V(\Delta, c_4). \tag{3-12}$$

Again, the group scheme G acts on \tilde{U} and $\bar{\mathcal{M}}_{1,1,S} \simeq [\tilde{U}/G]$.

Lemma 3.6. (i) *The map*

$$\text{Pic}(\Lambda) \rightarrow \text{Pic}(\tilde{U}) \tag{3-13}$$

is an isomorphism.

(ii) *The map $\Lambda^* \rightarrow \Gamma(\tilde{U}, \mathbb{O}_{\tilde{U}}^*)$ is an isomorphism.*

Proof. Statement (ii) is immediate. Statement (i) follows from a very similar argument to the proof of [Proposition 3.1](#). The only new ingredient is that the polynomial c_4 is not irreducible over fields of characteristics 2 and 3 but it is a power of an irreducible polynomial (in characteristic 2 it is equal to a_1^4 and in characteristic 3 it is equal to $(a_1 + a_2)^2$). \square

Using this, one sees as before that the map

$$\text{Pic}(\Lambda) \times \text{Pic}(BG) \rightarrow \text{Pic}(\bar{\mathcal{M}}_{1,1,S}) \tag{3-14}$$

is an isomorphism with the character [Equation \(3-9\)](#) mapping to λ^{-1} .

4. The case when S is reduced

4.1. If S is an arbitrary scheme, and \mathcal{L} a line bundle on $\mathcal{M}_{1,1,S}$, then there is a unique function $s \mapsto l(s) \in \mathbb{Z}/(12)$ which associates to a point s the unique power $l(s)$ of λ such that $\mathcal{L}_s \otimes \lambda^{-l(s)}$ on $\mathcal{M}_{1,1,k(s)}$ descends to $\mathbb{A}_{k(s)}^1$ (and hence is trivial).

Lemma 4.2. *The function $s \mapsto l(s)$ is a locally constant function on S .*

Proof. The assertion is local on S so we may assume that S is affine. Furthermore, the assertion can be verified on each irreducible component so we may assume that S is integral. Finally, if $\tilde{S} \rightarrow S$ is the normalization then it suffices to verify the assertion for \tilde{S} . In this case the result follows from [Section 3](#). \square

4.3. In particular, if S is connected we obtain a homomorphism

$$\text{Pic}(\mathcal{M}_{1,1,S}) \rightarrow \mathbb{Z}/(12) \tag{4-1}$$

sending λ to 1. Thus, in general, to prove [Theorem 1.1](#) we need to show that the kernel of (4-1) is isomorphic to $\text{Pic}(\mathbb{A}_S^1)$.

4.4. To complete the proof of [Theorem 1.1](#) in the case when S is reduced, we make some general observations about the relationship between line bundles on a stack and line bundles on the coarse moduli space (Recall that by [Lemma 2.1](#), the j -invariant identifies \mathbb{A}_S^1 with the coarse moduli space of $\mathcal{M}_{1,1,S}$.)

Let S be a noetherian scheme and $\mathcal{X} \rightarrow S$ a Deligne–Mumford stack over S . Let $\pi : \mathcal{X} \rightarrow X$ be the coarse moduli space, and assume that the formation of the coarse space X commutes with arbitrary base change on S and that X is reduced (we just saw that this holds for $\mathcal{M}_{1,1}$ over a reduced scheme). For a field valued point $x : \text{Spec}(k) \rightarrow S$, let $\pi_x : \mathcal{X}_x \rightarrow X_x$ denote the base change $\mathcal{X} \times_{S,x} \rightarrow X \times_{S,x}$.

Proposition 4.5. *Let L be a line bundle on \mathcal{X} such that for every field valued point $x : \text{Spec}(k) \rightarrow S$, the sheaf $\pi_{x*}(L|_{\mathcal{X}_x})$ is locally free of rank 1 and $\pi_x^* \pi_{x*}(L|_{\mathcal{X}_x}) \rightarrow L|_{\mathcal{X}_x}$ is an isomorphism. If $\mathcal{X} \rightarrow X$ is flat, then the sheaf $\pi_* L$ is locally free of rank 1 on X and $\pi^* \pi_* L \rightarrow L$ is an isomorphism.*

Proof. One immediately reduces to the case when $X = \text{Spec}(R)$, $Y = \text{Spec}(B)$ is a finite flat R scheme, and Γ is a finite group acting on Y over X such that $\mathcal{X} = [Y/\Gamma]$ (see for example [\[Olsson 2006, 2.12\]](#)). Let M denote the B -module corresponding to L , so that M comes equipped with an action of Γ over the action on B . We can even assume that R is a local ring and that M is a free R -module (forgetting the B -module structure). We are then trying to compute the kernel of the map

$$M \rightarrow \prod_{\gamma \in \Gamma} M, \quad m \mapsto (\dots, \gamma(m) - m, \dots)_{\gamma \in \Gamma}.$$

We can also assume that $S = \text{Spec}(\Lambda)$ is affine. □

Lemma 4.6. *Let R be a reduced local Λ -algebra and let $A \in M_{n \times m}(R)$ be a matrix (which we view as a map $R^n \rightarrow R^m$) with the property that for every $x \in \text{Spec}(\Lambda)$, the matrix $A(x) \in M_{n \times m}(R \otimes_{\Lambda} k(x))$ has kernel a free $R \otimes_{\Lambda} k(x)$ -space of rank 1. Then $\text{Ker}(A)$ is a free rank 1 module over R and for every $x \in \text{Spec}(\Lambda)$, the natural map $\text{Ker}(A) \otimes_{\Lambda} k(x) \rightarrow \text{Ker}(A(x))$ is an isomorphism.*

Proof by induction on n . If $n = 1$, then the assertion is that A is a matrix with $A(x)$ the zero matrix for all $x \in \text{Spec}(\Lambda)$. Since R is reduced this implies that A is the zero matrix.

For the inductive step, consider the system of m equations

$$\sum_i a_{ij} X_i = 0$$

that we are trying to solve in R . If $x \in \text{Spec}(\Lambda)$ is the image of the closed point of $\text{Spec}(R)$, then $A(x)$ is not zero since $n \geq 2$. Since R is local, some a_{ij} is invertible and so we can solve for the variable X_j . This gives a system of $m - 1$ equations in $n - 1$ variables, which again has the property that for every point $x \in \text{Spec}(\Lambda)$, the image in $R \otimes k(x)$ has a unique line of solutions. By induction we obtain the result. \square

This completes the proof of [Theorem 1.1\(i\)](#).

5. Proof of [Theorem 1.1\(ii\)](#)

Proposition 5.1. *For any scheme S over $\mathbb{Z}[1/2]$, with $\pi : \mathcal{M}_{1,1,S} \rightarrow \mathbb{A}_{j,S}^1$ the projection, and any coherent \mathcal{O}_S -module M , the sheaf $R^1\pi_*(\mathcal{O}_{\mathcal{M}_{1,1,S}} \otimes_{\mathcal{O}_S} M)$ is zero.*

Proof. Using the theorem of formal functions one is reduced to the case when S is the spectrum of a field. Furthermore, if the characteristic is not 3, the result is immediate, as $\mathcal{M}_{1,1,S}$ is tame in this case (see, for example, the proof of [[Abramovich and Vistoli 2002](#), 2.3.4]), so it suffices to consider $S = \text{Spec}(k)$ with $\text{char}(k) = 3$, and $M = k$. We may further assume that k is algebraically closed.

The coherent sheaf $R^1\pi_*(\mathcal{O}_{\mathcal{M}_{1,1,k}})$ restricts to the zero sheaf on $\mathbb{A}_k^1 - \{0\}$, since over this open subset of \mathbb{A}_k^1 the stack $\mathcal{M}_{1,1,k}$ is tame (the automorphism groups are $\{\pm 1\}$). Let $\bar{x} \rightarrow \mathcal{M}_{1,1,k}$ be a geometric point mapping to 0 in \mathbb{A}_k^1 , and let A denote the completion of $\mathcal{O}_{\mathcal{M}_{1,1,k},\bar{x}}$ along the maximal ideal. Let $\Gamma_{\bar{x}}$ denote the stabilizer group scheme of \bar{x} , so that $\Gamma_{\bar{x}}$ acts on A . The ring of invariants $B := A^{\Gamma_{\bar{x}}}$ is equal to the completion of \mathbb{A}_k^1 at the origin. Let F denote the finite type B -module obtained by pulling back $R^1\pi_*(\mathcal{O}_{\mathcal{M}_{1,1,k}})$ to $\text{Spec}(B)$. Then F is equal to the cohomology group $H^1(\Gamma_{\bar{x}}, A)$. We show that this group is zero. Since F is supported on the closed point of $\text{Spec}(B)$, there exists an integer n such that $j^n F = 0$ (where $j \in B$ is the uniformizer defined by the standard coordinate on \mathbb{A}^1). To prove the proposition it therefore suffices to show that F is j -torsion-free.

For this we use an explicit description of A and $\Gamma_{\bar{x}}$ given by the Legendre family. Let

$$V = \text{Spec}(k[\lambda][1/\lambda(\lambda - 1)]), \quad (5-1)$$

and let $E_V \rightarrow V$ be the elliptic curve

$$E_V : Y^2 Z = X(X - Z)(X - \lambda Z). \quad (5-2)$$

If μ denotes $\lambda + 1$, then the j -invariant of E_V is equal to $\mu^6/(\mu^4 - 1)$ (Recall that $\text{char}(k) = 3$.) The map $V \rightarrow \mathcal{M}_{1,1,k}$ defined by E_V is étale (see for example [[Katz](#)

and Mazur 1985, 2.2.8]), so this defines an isomorphism $A \simeq k[[\mu]]$. The group $\Gamma_{\bar{x}}$ sits in an exact sequence

$$1 \rightarrow \{\pm 1\} \rightarrow \Gamma_{\bar{x}} \rightarrow S_3 \rightarrow 1, \quad (5-3)$$

and the action of $\Gamma_{\bar{x}}$ on $A \simeq k[[\mu]]$ factors through the action of S_3 on $k[[\mu]]$ given by the two automorphisms

$$\alpha : \mu \mapsto -\mu \quad (5-4)$$

and

$$\beta : \mu \mapsto \mu/(1 - \mu) = \mu(1 + \mu + \mu^2 + \dots). \quad (5-5)$$

Also note that the Leray spectral sequence

$$E_2^{pq} = H^p(S_3, H^q(\{\pm 1\}, A)) \implies H^{p+q}(\Gamma_{\bar{x}}, A) \quad (5-6)$$

and the fact that $H^q(\{\pm 1\}, A) = 0$ for $q > 0$ (since 2 is invertible in k) imply that $H^1(\Gamma_{\bar{x}}, A) = H^1(S_3, A)$.

An element in $H^1(S_3, A)$ can be represented by a set map $\zeta : S_3 \rightarrow k[[\mu]]$ (written $\sigma \mapsto \zeta_\sigma$) such that for $\sigma, \tau \in S_3$ we have (recall the action is a right action)

$$\zeta_{\sigma\tau} = \zeta_\sigma^\tau + \zeta_\tau. \quad (5-7)$$

The class of ζ is trivial if there exists an element $g \in k[[\mu]]$ such that $\zeta_\sigma = g^\sigma - g$ for all $\sigma \in S_e$. Note that (5-7) implies that it suffices to check the equalities $\zeta_\sigma = g^\sigma - g$ for a set of generators $\sigma \in S_3$.

If ζ represents a class in $H^1(S_3, A)$ annihilated by j , there exists an element $g \in k[[\mu]]$ such that

$$\frac{\mu^6}{\mu^4 - 1} \zeta_\sigma = g^\sigma - g \quad (5-8)$$

for all $\sigma \in S_3$. To prove that $H^1(S_3, A)$ is j -torsion-free, it therefore suffices to show that for such a ζ , we can choose g to have μ -adic valuation ≥ 6 (since A is j -torsion-free).

For this, note that we can assume without loss of generality that g has no constant term, and then write

$$g = a_1\mu + a_2\mu^2 + a_3\mu^3 + a_4\mu^4 + a_5\mu^5 + g_{\geq 6}, \quad (5-9)$$

where $g_{\geq 6}$ has μ -adic valuation ≥ 6 . We have

$$\frac{\mu^6}{\mu^4 - 1} \zeta_\alpha = 2a_1\mu + 2a_3\mu^3 + 2a_5\mu^5 + (g_{\geq 6}^\alpha - g_{\geq 6}), \quad (5-10)$$

which implies that $a_1 = a_3 = a_5 = 0$. Then

$$\frac{\mu^6}{\mu^4 - 1} \zeta_\beta = 2a_2\mu^3 + (\text{higher order terms}), \quad (5-11)$$

which gives $a_2 = 0$. Finally, using this, we see that

$$\frac{\mu^6}{\mu^4 - 1} \zeta_\beta = a_4 \mu^5 + (\text{higher order terms}), \quad (5-12)$$

which implies that $a_4 = 0$ as desired. This completes the proof of [Proposition 5.1](#). \square

5.2. Now let us prove [Theorem 1.1](#) for a connected $\mathbb{Z}[1/2]$ -scheme S . We need to show that if L is a line bundle on $\mathcal{M}_{1,1,S}$ such that for any field-valued point $s \in S$ the fiber L_s on $\mathcal{M}_{1,1,s}$ descends to $\mathbb{A}_{j,s}^1$, then L descends to $\mathbb{A}_{j,S}^1$. By a standard limit argument it suffices to consider the case when S is noetherian and even affine, say $S = \text{Spec}(\Lambda)$. Let $J \subset \Lambda$ denote the nilradical. By the reduced case already treated in [Section 4](#), it suffices to show inductively that if the result holds for Λ/J^r then it also holds for Λ/J^{r+1} . In other words, let L_0 denote a line bundle on $\mathbb{A}_{j,\Lambda/J^r}^1$ and \tilde{L} a lifting of π^*L_0 to $\mathcal{M}_{1,1,\Lambda/J^{r+1}}$. Then we want to show that \tilde{L} is pulled back from a lifting of L_0 to $\mathbb{A}_{j,\Lambda/J^{r+1}}^1$. By standard deformation theory this is equivalent to showing that the map

$$0 = H^1(\mathbb{A}_\Lambda^1, J^r/J^{r+1}) \rightarrow H^1(\mathcal{M}_{1,1,\Lambda}, J^r/J^{r+1})$$

is an isomorphism; or, equivalently, that $H^1(\mathcal{M}_{1,1,\Lambda}, J^r/J^{r+1})$ is zero. Since $\mathbb{A}_{j,\Lambda}^1$ is affine, the group $H^1(\mathcal{M}_{1,1,\Lambda}, J^r/J^{r+1})$ is zero if and only if the sheaf $R^1\pi_*(J^r/J^{r+1} \otimes \mathcal{O}_{\mathcal{M}_{1,1,\Lambda}})$ is zero on $\mathbb{A}_{j,\Lambda}^1$, which follows from [Proposition 5.1](#). This completes the proof of [Theorem 1.1](#). \square

6. Computations in characteristic 2

Proposition 6.1. *Let k be a field of characteristic 2, and let $\pi : \overline{\mathcal{M}}_{1,1,k} \rightarrow \mathbb{P}_k^1$ be the morphism defined by the j -invariant. Then $R^1\pi_*\mathcal{O}_{\overline{\mathcal{M}}_{1,1,k}}$ is a line bundle on \mathbb{P}_k^1 of negative degree.*

Proof. We may without loss of generality assume that k is algebraically closed.

Let $\mathcal{U}_\infty \subset \overline{\mathcal{M}}_{1,1,k}$ denote the open substack $\overline{\mathcal{M}}_{1,1,k} \times_{\mathbb{P}_j^1} \mathbb{A}_{1/j}^1$ (the complement of $j = 0$), and let $\mathcal{U}_0 = \mathcal{M}_{1,1,k} \subset \overline{\mathcal{M}}_{1,1,k}$ denote the complement of $j = \infty$. Let $U_\infty, U_0 \subset \mathbb{P}_j^1$ be the coarse moduli spaces (the standard open cover of \mathbb{P}_j^1).

The stack \mathcal{U}_∞ is a $\mathbb{Z}/(2)$ -gerbe over U_∞ . Now in general, if $f : \mathcal{G} \rightarrow X$ is a $\mathbb{Z}/(2)$ -gerbe in characteristic 2, the sheaf $R^1f_*\mathcal{O}_{\mathcal{G}}$ is locally free of rank 1 and in fact canonically trivialized. This can be seen as follows. Étale locally on X , we have $\mathcal{G} = X \times B(\mathbb{Z}/(2))$. Computing in this local situation, one sees that $R^1f_*(\mathbb{Z}/(2))$ is a locally constant sheaf of groups étale locally isomorphic to $\mathbb{Z}/(2)$, and the natural map $R^1f_*(\mathbb{Z}/(2)) \otimes_{\mathbb{Z}/(2)} \mathcal{O}_X \rightarrow R^1f_*\mathcal{O}_{\mathcal{G}}$ (which exists since we are in characteristic 2) is an isomorphism. Since a group of order 2 admits no nontrivial automorphisms, there is a canonical isomorphism $\mathbb{Z}/(2) \simeq R^1f_*(\mathbb{Z}/(2))$ which induces a canonical

trivialization of $R^1 f_* \mathbb{O}_{\mathcal{G}}$. In the case of $\mathcal{G} = X \times B(\mathbb{Z}/(2))$ and $X = \text{Spec}(A)$ we have

$$H^1({}^c\mathcal{G}, \mathbb{O}_{\mathcal{G}}) \simeq \text{Hom}_{\text{Gp}}(\mathbb{Z}/(2), A),$$

and the trivialization is given by the homomorphism sending $1 \in \mathbb{Z}/(2)$ to $1 \in A$.

Lemma 6.2. *The sheaf $R^1 \pi_* \mathbb{O}_{\overline{\mathcal{M}}_{1,1,k}}$ is locally free of rank 1 on \mathbb{P}^1_j .*

Proof. By finiteness of coherent cohomology for stacks, the sheaf is in any case coherent. Since \mathbb{P}^1_j is a smooth curve it therefore suffices to show that it is torsion-free. Furthermore, the only issue is at the point $j = 0$. Since the formation of cohomology commutes with flat base change, it suffices to show that

$$H^1(\overline{\mathcal{M}}_{1,1,k} \times_{\mathbb{P}^1_j} \text{Spec}(k[[j]]), \mathbb{O}_{\overline{\mathcal{M}}_{1,1,k} \times_{\mathbb{P}^1_j} \text{Spec}(k[[j]])}) \tag{6-1}$$

is j -torsion-free.

For this we use the so-called Hesse presentation of $\mathcal{M}_{1,1,k}$. Let

$$V = \text{Spec}(k[\mu, \omega][1/(\mu^3 - 1)]/(\omega^2 + \omega + 1)), \tag{6-2}$$

and let $E_V \rightarrow V$ be the elliptic curve given by the equation

$$X^3 + Y^3 + Z^3 = \mu XYZ. \tag{6-3}$$

This elliptic curve has a basis for its three-torsion group given by the points $[1 : 0 : -1]$ and $[-1 : \omega : 0]$. In fact, this is the universal elliptic curve with full level three structure. The j -invariant of E_V is $\mu^{12}/(\mu^3 - 1)^3$ (since we are in characteristic 2). In particular, the fiber over $j = 0$ is the curve $X^3 + Y^3 + Z^3 = 0$.

Changing the choice of basis for the 3-torsion subgroup defines an action of $GL_2(\mathbb{F}_3)$ on V such that $\mathcal{M}_{1,1,k} \simeq [V/GL_2(\mathbb{F}_3)]$. A calculation shows that this action is described as follows:

- (1) $(\mu, \omega) * \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = (\omega\mu, \omega)$.
- (2) $(\mu, \omega) * \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (\mu/(\mu-1), \omega)$.
- (3) $(\mu, \omega) * \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = (\mu, \omega^2)$.

Putting this together one finds that

$$\overline{\mathcal{M}}_{1,1,k} \times_{\mathbb{P}^1_j} \text{Spec}(k[[j]]) \simeq [\text{Spec}(k[[\mu]])/\text{SL}_2(\mathbb{F}_3)], \tag{6-4}$$

where $\alpha = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ acts by $\mu \mapsto \zeta \mu$ (for some fixed primitive cube root of unity ζ) and $\beta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ acts by $\mu \mapsto \mu/(\mu-1)$.

As in the proof of [Proposition 5.1](#), an element of (6-1) is given by a set map $\zeta : \text{SL}_2(\mathbb{F}_3) \rightarrow k[[\mu]]$ (written $\sigma \mapsto \zeta_\sigma$) such that for any two elements $\sigma, \tau \in \text{SL}_2(\mathbb{F}_3)$ we have

$$\zeta_{\sigma\tau} = \zeta_\sigma^\zeta + \zeta_\tau,$$

and the class of ζ is trivial if there exists an element $g \in k[[\mu]]$ such that for every σ we have $\zeta_\sigma = g^\sigma - g$.

Now if (6-1) has j -torsion there exists a set map ζ as above and an element $g \in k[[\mu]]$ such that for all σ we have

$$\frac{\mu^{12}}{\mu^3 - 1} \zeta_\sigma = g^\sigma - g.$$

To prove that (6-1) is torsion-free, it suffices to show that we can choose g to be divisible by μ^{12} . For since $k[[\mu]]$ is an integral domain we then have

$$\zeta_\sigma = \left(\frac{\mu^3 - 1}{\mu^{12}} g \right)^\sigma - \left(\frac{\mu^3 - 1}{\mu^{12}} g \right).$$

We can without loss of generality assume that g has no constant term. Write

$$g = a_1\mu + a_2\mu^2 + \cdots + a_{11}\mu^{11} + g_{\geq 12}.$$

Then $g^\alpha - g$ has μ -adic valuation ≥ 12 (recall that $\alpha = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$). Looking at the coefficients a_i , this implies that all but a_3, a_6 , and a_9 are zero, so

$$g = a_3\mu^3 + a_6\mu^6 + a_9\mu^9 + g_{\geq 12}.$$

Similarly, $g^\beta - g$ has μ -adic valuation ≥ 12 . Looking at the coefficient of μ^4 in $g^\beta - g$ one sees that $a_3 = 0$. Then looking at the coefficient of μ^8 one sees that $a_6 = 0$, and finally looking at the coefficient of μ^{10} one sees that $a_9 = 0$. \square

Let M denote the cohomology group (6-1) (a $k[[j]]$ -module) and let M_η denote $M \otimes_{k[[j]]} k[[j]][1/j]$. Let $e_\infty \in M_\eta$ denote the basis element defined by the canonical trivialization of $R^1\pi_* \mathcal{O}_{\overline{\mathcal{M}}_{1,1,k}}$ over \mathcal{U}_∞ . The lattice $M \subset M_\eta$ defines a valuation ν on M_η and it suffices to show that $\nu(e_\infty) < 0$. Equivalently, we have to show that for any element $m \in M$, if we write $m = he_\infty$ in M_η then the j -adic valuation of h is positive.

For this we again use the presentation (6-4). An element $m \in M$ is then represented by a map $\zeta : \mathrm{SL}_2(\mathbb{F}_3) \rightarrow k[[\mu]]$. The corresponding element in M_η can be described in terms of the basis e_∞ as follows. First of all, the element $\zeta_{\beta^2} \in k[[\mu]]$ is $\mathrm{SL}_2(\mathbb{F}_3)$ -invariant, since for any other element σ we have

$$\zeta_{\beta^2}^\sigma + \zeta_\sigma = \zeta_{\beta^2\sigma} = \zeta_\sigma\beta^2 = \zeta_\sigma^{\beta^2} + \zeta_{\beta^2},$$

and β^2 acts trivially on $k[[\mu]]$. Therefore, ζ_{β^2} is actually an element in $k[[j]]$. The image of ζ in $M_\eta \simeq \mathrm{Hom}(\mathbb{Z}/(2), k[[j]][1/j])$ is then equal to the homomorphism

$$\mathbb{Z}/(2) \rightarrow k[[j]][1/j], \quad 1 \mapsto \zeta_{\beta^2}.$$

The class e_∞ corresponds to the homomorphism sending 1 to 1, so we have to show that the j -adic valuation of ξ_{β^2} is positive. For this, let $f = \xi_\beta$. Then

$$\xi_{\beta^2} = f^\beta + f = f(\mu(1 + \mu + \mu^2 + \cdots)) + f(\mu).$$

Since we are in characteristic 2, it follows that the μ -adic valuation of ξ_{β^2} is at least 2, and therefore the j -adic valuation of ξ_{β^2} is also positive. \square

Corollary 6.3. *For any field k , we have $H^1(\overline{\mathcal{M}}_{1,1,k}, \mathbb{O}_{\overline{\mathcal{M}}_{1,1,k}}) = 0$.*

Proof. We have $R^1\pi_*\mathbb{O}_{\overline{\mathcal{M}}_{1,1,k}} = 0$ when $\text{char}(k) \neq 2$ (When $\text{char}(k) = 3$, this follows from [Proposition 5.1](#).) It follows that

$$H^0(\mathbb{P}_k^1, R^1\pi_*\mathbb{O}_{\overline{\mathcal{M}}_{1,1,k}}) = 0 \tag{6-5}$$

in all characteristics. From the Leray spectral sequence we obtain

$$H^1(\overline{\mathcal{M}}_{1,1,k}, \mathbb{O}_{\overline{\mathcal{M}}_{1,1,k}}) = H^1(\mathbb{P}_k^1, \mathbb{O}_{\mathbb{P}_k^1}) = 0. \tag{6-6}$$

This concludes the proof. \square

Remark 6.4. Note that if $\text{char}(k) = 2$, then the restriction of $R^1\pi_*\mathbb{O}_{\mathcal{M}_{1,1,k}}$ to $\mathbb{A}_k^1 \subset \mathbb{P}_k^1$ is nonzero. From the Leray spectral sequence it follows that the map

$$0 = H^1(\mathbb{A}_k^1, \mathbb{O}_{\mathbb{A}_k^1}) \rightarrow H^1(\mathcal{M}_{1,1,k}, \mathbb{O}_{\mathcal{M}_{1,1,k}}) \tag{6-7}$$

is *not* an isomorphism. Since the group $H^1(\mathcal{M}_{1,1,k}, \mathbb{O}_{\mathcal{M}_{1,1,k}})$ classifies deformations of the structure sheaf to $\mathcal{M}_{1,1,k[\epsilon]/(\epsilon^2)}$, this implies that there are line bundles on $\mathcal{M}_{1,1,k[\epsilon]/(\epsilon^2)}$ which are in the kernel of (4-1) but are nontrivial. This implies that [Theorem 1.1](#) fails for $S = \text{Spec}(k[\epsilon]/(\epsilon^2))$. More generally, [Theorem 1.1](#) fails for any nonreduced affine scheme over \mathbb{F}_2 .

7. Proof of [Theorem 1.3](#)

7.1. In order to prove [Theorem 1.3](#) it is easiest to prove a stronger statement that implies it. Let $\text{Pic}(\overline{\mathcal{M}}_{1,1,S})$ denote the Picard stack over S which to any S -scheme T associates the group of line bundles on $\overline{\mathcal{M}}_{1,1,T}$. By [[Aoki 2006](#), 5.1], the stack $\text{Pic}(\overline{\mathcal{M}}_{1,1,S})$ is an algebraic stack (an Artin stack) over S . There is a morphism of stacks

$$\mathbb{Z} \times B\mathbb{G}_{m,S} \rightarrow \text{Pic}(\overline{\mathcal{M}}_{1,1,S}) \tag{7-1}$$

sending a pair (n, L) consisting of $n \in \mathbb{Z}$ and L a line bundle on S to $\lambda^n \otimes_{\mathbb{O}_S} L$ on $\overline{\mathcal{M}}_{1,1,S}$. The following theorem implies [Theorem 1.3](#) by evaluation of both sides of (7-1) on S and passing to isomorphism classes.

Theorem 7.2. *The morphism (7-1) is an isomorphism.*

Proof. Note first that if n and n' are integers and L and L' are line bundles on S , then $\lambda^n \otimes L$ and $\lambda^{n'} \otimes L'$ on $\overline{\mathcal{M}}_{1,1,S}$ are isomorphic if and only if $n = n'$ and $L \simeq L'$. Indeed, if these two sheaves are isomorphic, then this implies that $\lambda^{n-n'}$ descends to \mathbb{P}_j^1 . By the case of a field, this implies that $n = n'$. In this case we recover L and L' from their pullbacks to $\overline{\mathcal{M}}_{1,1,S}$ by pushing back down to S . Therefore, the functor (7-1) is fully faithful. It therefore suffices to show that for any cartesian diagram

$$\begin{array}{ccc}
 P & \longrightarrow & S \\
 \downarrow & & \downarrow L \\
 \mathbb{Z} \times B\mathbb{G}_m & \longrightarrow & \text{Pic}_{\overline{\mathcal{M}}_{1,1,S}}
 \end{array}
 \tag{7-2}$$

the morphism of algebraic spaces $P \rightarrow S$ is an isomorphism. For this it suffices to consider the case when S is artinian local. Furthermore, we know the result in the case when S is the spectrum of a field by Section 3. Since a line bundle on the spectrum of an artinian local ring is trivial, what we therefore need to show is that if S is an artinian local ring, then any line bundle on $\overline{\mathcal{M}}_{1,1,S}$ is isomorphic to λ^n for some n . Proceeding by induction on the length of S , it further suffices to consider the following. Let $S = \text{Spec}(A)$, k the residue field of A , and let $J \subset A$ be a square-zero ideal annihilated by the maximal ideal of A , and set $A_0 = A/J$. Then any deformation of λ^n over $\overline{\mathcal{M}}_{1,1,A_0}$ to $\overline{\mathcal{M}}_{1,1,A}$ is isomorphic to λ^n . Using the exponential sequence

$$0 \rightarrow J \otimes \mathcal{O}_{\overline{\mathcal{M}}_{1,1,k}} \rightarrow \mathcal{O}_{\overline{\mathcal{M}}_{1,1,A}}^* \rightarrow \mathcal{O}_{\overline{\mathcal{M}}_{1,1,A_0}}^* \rightarrow 0,$$

one sees that this amounts exactly to $H^1(\overline{\mathcal{M}}_{1,1,k}, \mathcal{O}_{\overline{\mathcal{M}}_{1,1,k}}) = 0$. □

References

[Abramovich and Vistoli 2002] D. Abramovich and A. Vistoli, “Compactifying the space of stable maps”, *J. Amer. Math. Soc.* **15**:1 (2002), 27–75. [MR 2002i:14030](#) [Zbl 0991.14007](#)

[Aoki 2006] M. Aoki, “Hom stacks”, *Manuscripta Math.* **119**:1 (2006), 37–56. [MR 2007a:14003](#) [Zbl 1094.14001](#)

[Deligne 1975] P. Deligne, “Courbes elliptiques: formulaire d’après J. Tate”, pp. 53–73 in *Modular functions of one variable* (Antwerp, 1972), vol. IV, edited by B. J. Birch and W. Kuyk, Lecture Notes in Math. **476**, Springer, Berlin, 1975. [MR 52 #8135](#)

[Fulton 1998] W. Fulton, *Intersection theory*, vol. 2, 2nd ed., Springer, Berlin, 1998. [MR 99d:14003](#) [Zbl 0885.14002](#)

[Ischebeck 1979] F. Ischebeck, “Über die Abbildung $\text{Pic}A \rightarrow \text{Pic}A_f$ ”, *Math. Ann.* **243**:3 (1979), 237–245. [MR 80k:14015](#) [Zbl 0418.14008](#)

[Katz and Mazur 1985] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, vol. 108, Princeton University Press, 1985. [MR 86i:11024](#) [Zbl 0576.14026](#)

- [Keel and Mori 1997] S. Keel and S. Mori, “Quotients by groupoids”, *Ann. of Math. (2)* **145**:1 (1997), 193–213. [MR 97m:14014](#) [Zbl 0881.14018](#)
- [Mumford 1965] D. Mumford, “Picard groups of moduli problems”, pp. 33–81 in *Arithmetical Algebraic Geometry* (West Lafayette, IN), edited by O. F. G. Schilling, Harper & Row, New York, 1965. [MR 34 #1327](#) [Zbl 0187.42801](#)
- [Olsson 2005] M. C. Olsson, “On proper coverings of Artin stacks”, *Adv. Math.* **198**:1 (2005), 93–106. [MR 2006h:14003](#) [Zbl 1084.14004](#)
- [Olsson 2006] M. C. Olsson, “Hom-stacks and restriction of scalars”, *Duke Math. J.* **134**:1 (2006), 139–164. [MR 2007f:14002](#) [Zbl 1114.14002](#)
- [Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009. [MR 2514094](#) [Zbl 05549721](#)

Communicated by Ravi Vakil

Received 2009-05-15

Revised 2009-09-30

Accepted 2009-11-30

wfulton@umich.edu

*Department of Mathematics, University of Michigan,
Ann Arbor, MI 48109-1043, United States*

molsson@math.berkeley.edu

*Department of Mathematics, University of California,
Berkeley, CA 94720-3840, United States*

Positive motivic measures are counting measures

Jordan S. Ellenberg and Michael Larsen

A *motivic measure* is a ring homomorphism from the Grothendieck group of a field K (with multiplication coming from the fiber product over $\text{Spec } K$) to some field. We show that if a real-valued motivic measure μ satisfies $\mu([V]) \geq 0$ for all K -varieties V , then μ is a counting measure; that is, there exists a finite field L containing K such that $\mu([V]) = |V(L)|$ for all K -varieties V .

Let K be a field. By a K -variety, we mean a geometrically reduced, separated scheme of finite type over K . Let $K_0(\text{Var}_K)$ denote the Grothendieck group of K , that is, the free abelian group generated by isomorphism classes $[V]$ of K -varieties, with the scissors relations $[V] = [W] - [V \setminus W]$ whenever W is a closed K -subvariety of V . There is a unique product on $K_0(\text{Var}_K)$ characterized by the relation

$$[V] \cdot [W] = [V \times W],$$

where \times denotes the fiber product over $\text{Spec } K$. This product gives $K_0(\text{Var}_K)$ a commutative ring structure with identity $[\text{Spec } K]$. For every extension L of K , extension of scalars gives a natural ring homomorphism $K_0(\text{Var}_K) \rightarrow K_0(\text{Var}_L)$. The map $K \mapsto K_0(\text{Var}_K)$ can be regarded as a functor from fields to commutative rings. Throughout the paper, we follow the usual convention of writing \mathbb{L} for $[\mathbb{A}_K^1]$.

Following the terminology of [Larsen and Lunts 2003], we call a ring homomorphism from $K_0(\text{Var}_K)$ to a field F a *motivic measure*. Note that the original meaning of this term [Hales 2005; Looijenga 2002] is different (though related). If K is a finite field, the map $[V] \mapsto |V(K)|$ extends to a homomorphism $\mu_K : K_0(\text{Var}_K) \rightarrow \mathbb{Z}$, and therefore to an F -valued measure for any field F . More generally, if L is an extension of K which is also a finite field, the composition of μ_L with the natural map $K_0(\text{Var}_K) \rightarrow K_0(\text{Var}_L)$ gives for each F a motivic measure. We will call all such measures *counting measures*.

In this paper, we consider *positive* motivic measures, by which we mean \mathbb{R} -valued measures μ such that $\mu([V]) \geq 0$ for all K -varieties V . We now state our main result.

MSC2000: primary 14F43; secondary 14G15.

Keywords: motives, motivic measures, finite fields.

Theorem 1. *Every positive motivic measure is a counting measure. In other words, if K is any field and $\mu: K_0(\text{Var}_K) \rightarrow \mathbb{R}$ is positive, there exists a finite field L containing K such that $\mu([V]) = |V(L)|$ for all K -varieties V .*

Of course, for other choices of F there may still be motivic measures such that $\mu([V])$ lies in some interesting semiring of F for all K -varieties V . For example, if F is $\mathbb{C}(u, v)$ and $K = \mathbb{C}$, the measure sending V to its Hodge–Deligne polynomial takes values in the semiring of polynomials in u, v whose term of highest total degree is a positive multiple of a power of uv .

We begin with a direct proof of the following obvious corollary of [Theorem 1](#).

Proposition 2. *If K is infinite, there are no positive motivic measures on $K_0(\text{Var}_K)$.*

Proof. Let μ be such a measure. For any finite subset S of K , which we regard as a zero-dimensional subvariety of \mathbb{A}^1 ,

$$0 \leq \mu(\mathbb{A}^1 \setminus S) = \mu(\mathbb{L}) - |S|.$$

Thus, $\mu(\mathbb{L}) \geq |S|$ for all subsets S of K , which proves the proposition. □

For the remainder of the paper we may and do assume that K is finite, of cardinality q . We write \mathbb{F}_{q^n} for the degree n extension of K .

Proposition 3. *Let Ω^n denote the variety obtained from \mathbb{A}^n by removing all proper affine-linear subspaces defined over \mathbb{F}_q . Then*

$$[\Omega^n] = (\mathbb{L} - q)(\mathbb{L} - q^2) \cdots (\mathbb{L} - q^n).$$

Proof. For any \mathbb{F}_q -rational affine-linear subspace A of \mathbb{A}^n , let A° denote the open subvariety of A which is the complement of all proper \mathbb{F}_q -rational affine-linear subspaces of A . Then $[A^\circ] = [\Omega^{\dim A}]$, and one can write recursively

$$[\Omega^n] = \mathbb{L}^n - \sum_{i=1}^{n-1} a_{n,i} [\Omega^i],$$

where $a_{n,i}$ is the number of \mathbb{F}_q -rational i -dimensional affine linear subspaces of \mathbb{A}^n . Thus, $[\Omega^n]$ can be expressed as $P_n(\mathbb{L})$, where $P_n \in \mathbb{Z}[x]$ is monic and of degree n . It suffices to prove that q^d is a root of $P_n(x)$ for all integers $d \in \{1, 2, \dots, n\}$.

For any d in this range $\Omega^n(\mathbb{F}_{q^d})$ is empty. Indeed, if $x \in \mathbb{A}^n(\mathbb{F}_{q^d})$, then the n coordinates of x together with 1 cannot be linearly independent over \mathbb{F}_q , which implies that x lies in a proper \mathbb{F}_q -rational affine-linear subspace of \mathbb{A}^n . Thus,

$$0 = \mu_{\mathbb{F}_{q^d}}(\Omega^n) = P_n(q^d). \quad \square$$

Corollary 4. *If μ is a positive measure on $K_0(\text{Var}_{\mathbb{F}_q})$, there exists a positive integer n such that $\mu(\mathbb{L}) = q^n$.*

Proof. If $q^{n-1} < \mu(\mathbb{L}) < q^n$ for some integer n , then $\mu(\Omega^n) < 0$, contrary to positivity. \square

Our goal is then to prove that $\mu(\mathbb{L}) = q^n$ implies $\mu = \mu_{\mathbb{F}_{q^n}}$. We prove first that these measures coincide for varieties of the form $\text{Spec } \mathbb{F}_{q^d}$ and deduce that they coincide for all affine varieties. As $K_0(\text{Var}_{\mathbb{F}_q})$ is generated by the classes of affine varieties, this implies [Theorem 1](#).

Lemma 5. *Let μ be a real-valued motivic measure of $K_0(\text{Var}_{\mathbb{F}_q})$ and m a positive integer. Then*

$$\mu(\text{Spec } \mathbb{F}_{q^m}) \in \{0, m\}.$$

If $\text{Spec } \mathbb{F}_{q^m}$ has measure m , then $\text{Spec } \mathbb{F}_{q^d}$ has measure d whenever d divides m .

Proof. As

$$\mathbb{F}_{q^m} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} = \mathbb{F}_{q^m}^m,$$

the class x of $\text{Spec } \mathbb{F}_{q^m}$ satisfies $x^2 = mx$. If d divides m ,

$$\mathbb{F}_{q^d} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} = \mathbb{F}_{q^d}^m,$$

so $\mu(\text{Spec } \mathbb{F}_{q^m}) = m$ implies $\mu(\text{Spec } \mathbb{F}_{q^d}) = d$. \square

Of course,

$$\mu_{\mathbb{F}_{q^n}}(\text{Spec } \mathbb{F}_{q^m}) = \begin{cases} m & \text{if } m \mid n, \\ 0 & \text{otherwise.} \end{cases}$$

We will prove the same thing for the values of $\mu(\text{Spec } \mathbb{F}_{q^m})$. We begin with:

Proposition 6. *If $\mu(\mathbb{L}) = q^n$ and $\mu(\text{Spec } (\mathbb{F}_{q^k})) = k$ for some $k \geq n$, then*

$$\mu(\text{Spec } \mathbb{F}_{q^m}) = \begin{cases} m & \text{if } m \mid n, \\ 0 & \text{otherwise.} \end{cases} \quad (1)$$

For any integer k , we denote by X_k the complement in \mathbb{A}^1 of the set of all points with residue field contained in \mathbb{F}_{q^k} .

Proof. By [Lemma 5](#), $\mu(\text{Spec } \mathbb{F}_{q^d}) = d$ when d divides k . Choose an m not dividing k , and let $Y_{k,m}$ denote the complement in X_k of the set of points with residue field \mathbb{F}_{q^m} . Then

$$\mu([Y_{k,m}]) = \mu(\mathbb{L}) - \sum_{d \mid k} c_d d - c_m \mu(\text{Spec } \mathbb{F}_{q^m}),$$

where c_i is the number of points in \mathbb{A}^1 with residue field \mathbb{F}_{q^i} . From the positivity of $\mu([Y_{k,m}])$ and the fact that

$$0 = \mu_{\mathbb{F}_{q^k}}([Y_{k,m}]) = q^k - \sum_{d \mid k} c_d d,$$

we see that $\mu(\mathbb{L}) - q^k = q^n - q^k$ must be nonnegative, which is to say $k = n$, and that $\mu(\text{Spec } \mathbb{F}_{q^m}) = 0$. \square

Proposition 7. *If $\mu(\mathbb{L}) = q^n$, then $\mu(\text{Spec } \mathbb{F}_{q^n}) = n$.*

Proof. The assertion is clear for $n = 1$, so we assume $n > 1$. Let c_i denote the number of points in \mathbb{A}^1 with residue field \mathbb{F}_{q^i} . Thus $ic_i \leq q^i - 1$ for all $i > 1$. If $\mu(\text{Spec } \mathbb{F}_{q^n}) = 0$, then $\mu(\text{Spec } (\mathbb{F}_{q^i})) = 0$ for all $i \geq n$, so for all $k > 0$ we have

$$\mu([X_k]) \geq q^n - q - \sum_{i=2}^{n-1} (q^i - 1) \geq 2.$$

Now we consider all curves in \mathbb{A}^2 of the form $y = P(x)$ where $P(x) \in \mathbb{F}_q[x]$ has degree $\leq 2n$. The total number of such curves is greater than q^{2n} , and for any intersection point (α, β) of any two distinct curves of this family, α satisfies a polynomial equation of degree $\leq 2n$ over \mathbb{F}_q . Therefore, the open curves

$$C_P := \{(x, P(x)) \mid x \notin \mathbb{F}_{q^{(2n)!}}\},$$

indexed by polynomials P of degree $\leq 2n$, each isomorphic to $X_{(2n)!}$, are mutually disjoint. If C denotes the closure of the union of the C_P in \mathbb{A}^2 , it follows that

$$\mu([C]) > q^{2n} \mu([X_{(2n)!}]) > q^{2n},$$

so $\mu([\mathbb{A}^2 \setminus C]) < 0$, which is absurd. □

Together, the two preceding propositions imply (1).

We can now prove [Theorem 1](#). We assume $\mu(\mathbb{L}) = q^n$. It suffices to check that $\mu([V]) = |V(\mathbb{F}_{q^n})|$ for all affine \mathbb{F}_q -varieties V .

Each closed point of V with residue field \mathbb{F}_{q^d} corresponds to a d -element Galois orbit in $V(\mathbb{F}_{q^d})$. If d divides n , it gives a d -element subset of $V(\mathbb{F}_{q^n})$ and the subsets arising from different closed points are mutually disjoint. Since $V(\mathbb{F}_{q^n})$ is the union of all these subsets, and $\mu(\text{Spec } \mathbb{F}_{q^d}) = d$, we have

$$\mu([V]) \geq |V(\mathbb{F}_{q^n})| \tag{2}$$

for each \mathbb{F}_q -variety V . However, embedding V as a closed subvariety of \mathbb{A}^m for some m , the complement $W = \mathbb{A}^m \setminus V$ is again a variety, so

$$\mu([W]) \geq |W(\mathbb{F}_{q^n})|. \tag{3}$$

Since

$$\begin{aligned} q^{mn} &= \mu([\mathbb{A}^m]) = \mu([V]) + \mu([W]) \\ &\geq |V(\mathbb{F}_{q^n})| + |W(\mathbb{F}_{q^n})| \\ &= |\mathbb{A}^m(\mathbb{F}_{q^n})| = q^{mn}, \end{aligned}$$

we must have equality in (2) and (3).

References

- [Hales 2005] T. C. Hales, “What is motivic measure?”, *Bull. Amer. Math. Soc. (N.S.)* **42**:2 (2005), 119–135. [MR 2006h:14031](#) [Zbl 1081.14033](#)
- [Larsen and Lunts 2003] M. Larsen and V. A. Lunts, “Motivic measures and stable birational geometry”, *Mosc. Math. J.* **3**:1 (2003), 85–95, 259. [MR 2005a:14026](#) [Zbl 1056.14015](#)
- [Looijenga 2002] E. Looijenga, “Motivic measures”, pp. 267–297 in *Séminaire Bourbaki, 1999/2000*, Astérisque **276**, Soc. Math. de France, Paris, 2002. [MR 2003k:14010](#) [Zbl 0996.14011](#)

Communicated by Bjorn Poonen

Received 2009-07-10 Accepted 2009-08-10

ellenber@math.wisc.edu

*Department of Mathematics, University of Wisconsin,
480 Lincoln Drive, Madison, WI 53706, United States*
<http://math.wisc.edu/~ellenber>

mjlarsen@indiana.edu

*Department of Mathematics, Indiana University,
Bloomington, IN 47405, United States*
<http://mlarsen.math.indiana.edu/~larsen/>

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the [ANT website](#).

Originality. Submission of a manuscript acknowledges that the manuscript is original and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in ANT are usually in English, but articles written in other languages are welcome.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use \LaTeX but submissions in other varieties of \TeX , and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of Bib \TeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@mathscipub.org with details about how your graphics were generated.

White Space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 4 No. 1 2010

| | |
|--|-----|
| Density of rational points on diagonal quartic surfaces | 1 |
| ADAM LOGAN, DAVID MCKINNON and RONALD VAN LUIJK | |
| An Euler–Poincaré bound for equicharacteristic étale sheaves | 21 |
| CARL A. MILLER | |
| Reflexivity and rigidity for complexes, I: Commutative rings | 47 |
| LUCHEZAR L. AVRAMOV, SRIKANTH B. IYENGAR and JOSEPH LIPMAN | |
| The Picard group of $\mathfrak{M}_{1,1}$ | 87 |
| WILLIAM FULTON and MARTIN OLSSON | |
| Positive motivic measures are counting measures | 105 |
| JORDAN S. ELLENBERG and MICHAEL LARSEN | |