

# *Algebra & Number Theory*

Volume 5

2011

No. 8



mathematical sciences publishers

# Algebra & Number Theory

msp.berkeley.edu/ant

## 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	Shigefumi Mori	RIMS, Kyoto University, Japan
Dave Benson	University of Aberdeen, Scotland	Raman Parimala	Emory University, USA
Richard E. Borcherds	University of California, Berkeley, USA	Jonathan Pila	University of Oxford, UK
John H. Coates	University of Cambridge, UK	Victor Reiner	University of Minnesota, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Karl Rubin	University of California, Irvine, USA
Brian D. Conrad	University of Michigan, USA	Peter Sarnak	Princeton University, USA
Hélène Esnault	Universität Duisburg-Essen, Germany	Joseph H. Silverman	Brown 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
Yuri Manin	Northwestern University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Barry Mazur	Harvard University, USA	Andrei Zelevinsky	Northeastern University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne	Efim Zelmanov	University of California, San Diego, USA
Susan Montgomery	University of Southern California, USA		

## PRODUCTION

contact@msp.org

Silvio Levy, Scientific Editor

---

See inside back cover or [www.jant.org](http://www.jant.org) for submission instructions.


The subscription price for 2011 is US \$150/year for the electronic version, and \$210/year (+\$35 shipping outside the US) for print and electronic. 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.

---

ANT peer review and production are managed by EditFLOW<sup>®</sup> from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**

<http://msp.org/>

A NON-PROFIT CORPORATION

Typeset in L<sup>A</sup>T<sub>E</sub>X

Copyright ©2011 by Mathematical Sciences Publishers

# The behavior of Hecke $L$ -functions of real quadratic fields at $s = 0$

Byungheup Jun and Jungyun Lee

For a family of real quadratic fields  $\{K_n = \mathbb{Q}(\sqrt{f(n)})\}_{n \in \mathbb{N}}$ , a Dirichlet character  $\chi$  modulo  $q$ , and prescribed ideals  $\{\mathfrak{b}_n \subset K_n\}$ , we investigate the linear behavior of the special value of the partial Hecke  $L$ -function  $L_{K_n}(s, \chi_n := \chi \circ N_{K_n}, \mathfrak{b}_n)$  at  $s = 0$ . We show that for  $n = qk + r$ ,  $L_{K_n}(0, \chi_n, \mathfrak{b}_n)$  can be written as

$$\frac{1}{12q^2}(A_\chi(r) + kB_\chi(r)),$$

where  $A_\chi(r), B_\chi(r) \in \mathbb{Z}[\chi(1), \chi(2), \dots, \chi(q)]$  if a certain condition on  $\mathfrak{b}_n$  in terms of its continued fraction is satisfied. Furthermore, we write  $A_\chi(r)$  and  $B_\chi(r)$  explicitly using values of the Bernoulli polynomials. We describe how the linearity is used in solving the class number one problem for some families and recover the proofs in some cases.

1. Introduction	1001
2. Partial Hecke $L$ -function	1005
3. Proof of the main theorem	1012
4. Biró's method	1023
5. A generalization	1025
Acknowledgment	1026
References	1026

## 1. Introduction

In this paper, we are mainly concerned with linear behavior of the special values of the Hecke  $L$ -function at  $s = 0$  for families of real quadratic fields.

Let  $\{K_n = \mathbb{Q}(\sqrt{f(n)})\}_{n \in \mathbb{N}}$  be a family of real quadratic fields where  $f(n)$  is a positive square free integer for each  $n$ . For example  $f(x)$  can be a polynomial with integer coefficients.

---

Work partially supported by KRF-2007-341-C00006 (Jun) and by the Basic Research Program through the National Foundation of Korea (NRF) funded by the ministry of Education, Science and Technology (Jun: 2012-007726; Lee: 2011-0023688).

*MSC2000:* 11M06.

*Keywords:* special values, Hecke  $L$ -functions, real quadratic fields, continued fractions.

For a Dirichlet character  $\chi$  modulo  $q$ , we have a ray class character  $\chi_n := \chi \circ N_{K_n}$  for each  $n$ . Fixing an ideal  $\mathfrak{b}_n$  in  $K_n$  for each  $n$ , one obtains an indexed family of partial Hecke  $L$ -functions  $\{L_{K_n}(s, \chi_n, \mathfrak{b}_n)\}$ , where the partial Hecke  $L$ -function for  $(K, \chi, \mathfrak{b})$  is defined as

$$L_K(s, \chi, \mathfrak{b}) := \sum_{\substack{\mathfrak{a} \sim \mathfrak{b} \text{ integral} \\ (q, \mathfrak{a})=1}} \chi(\mathfrak{a})N(\mathfrak{a})^{-s}.$$

and  $\mathfrak{a} \sim \mathfrak{b}$  means that  $\mathfrak{a} = \alpha\mathfrak{b}$  for totally positive  $\alpha \in K$ .

Roughly speaking, if  $L_{K_n}(0, \chi_n, \mathfrak{b}_n)$  can be written as linear polynomial in  $k$  with coefficients depending only on  $r$  for  $n = qk + r$ , we say that  $L_{K_n}(0, \chi_n, \mathfrak{b}_n)$  is linear.

**Definition 1.1** (linearity). When the special values of  $L_{K_n}(s, \chi_n, \mathfrak{b}_n)$  at  $s = 0$  are expressed as

$$L_{K_n}(0, \chi_n, \mathfrak{b}_n) = \frac{1}{12q^2}(A_\chi(r) + kB_\chi(r))$$

for  $n = qk + r$ ,  $A_\chi(r), B_\chi(r) \in \mathbb{Z}[\chi(1), \chi(2), \dots, \chi(q)]$ , we say that  $L_{K_n}(0, \chi_n, \mathfrak{b}_n)$  is linear.

Linearity was originally observed by Biró in his proof of Yokoi’s conjecture.

**Theorem 1.2** [Biró 2003b]. *If the class number of  $\mathbb{Q}(\sqrt{n^2 + 4})$  is 1, then  $n \leq 17$ .*

In Yokoi’s conjecture, we take  $K_n = \mathbb{Q}(\sqrt{n^2 + 4})$  and  $\mathfrak{b}_n = \mathcal{O}_{K_n}$ . Biró [2003b, pp. 88, 89] expressed the special value of the Hecke  $L$ -function for  $(K_n, \chi_n, \mathcal{O}_{K_n})$  at  $s = 0$  for  $n = qk + r$

$$L_{K_n}(0, \chi_n, \mathfrak{b}_n) = \frac{1}{q}(A_\chi(r) + kB_\chi(r)), \tag{1-1}$$

where

$$A_\chi(r) = \sum_{0 \leq C, D \leq q-1} \chi(D^2 - C^2 - rCD) \left\lceil \frac{rC - D}{q} \right\rceil (C - q),$$

$$B_\chi(r) = \sum_{0 \leq C, D \leq q-1} \chi(D^2 - C^2 - rCD) C(C - q).$$

When  $K_n$  is of class number 1, the unique ideal class can be represented by any ideal  $\mathfrak{b}_n$ . *A priori* the partial Hecke  $L$ -function equals the total Hecke  $L$ -function up to multiplication by 2 (that is,

$$L_{K_n}(0, \chi_n) = cL_{K_n}(0, \chi_n, \mathcal{O}_{K_n})$$

where  $c$  is the number of narrow ideal classes).

From this identification, one can find the residue of  $n$  by sufficiently many primes  $p$  for which the class number of  $\mathbb{Q}(\sqrt{n^2 + 4})$  is one. Moreover, by the linearity, this residue depends only on  $r$ . Consequently, one can tell whether or not  $p$  is inert in  $\mathbb{Q}(\sqrt{n^2 + 4})$ . As we have a bound for a smaller prime to inert depending on  $n$ , finally we have enough conditions to list all  $K_n$  of class number 1.

Other families  $(K_n, \chi_n, \mathfrak{b}_n)$  that have linearity were discovered in [Biró 2003a; Byeon et al. 2007; Byeon and Lee 2008; Lee 2009a; 2009b]. Similarly, developing Biro’s method, one can solve the associated class number one problems.

In this paper, we give a criterion on  $(K_n, \chi_n, \mathfrak{b}_n)$  for  $L_{K_n}(0, \chi_n, \mathfrak{b}_n)$  to be linear. The criterion is in terms of the continued fraction expression of  $\delta(n)$ , where  $\mathfrak{b}_n^{-1} = [1, \delta(n)] := \mathbb{Z} + \delta(n)\mathbb{Z}$ . Let  $[[a_0, a_1, \dots, a_n]]$  be the purely periodic continued fraction

$$[a_0, a_1, a_2, \dots, a_n, a_0, a_1, \dots],$$

where

$$[a_0, a_1, a_2, \dots] := a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

Our main theorem is as follows:

**Theorem 1.3** (linearity criterion). *Let  $\{K_n = \mathbb{Q}(\sqrt{f(n)})\}_{n \in \mathbb{N}}$  be a family of real quadratic fields where  $f(n)$  is a positive square free integer for each  $n$ . Let  $\chi$  be a Dirichlet character modulo  $q$  for a positive integer  $q$  and  $\chi_n$  be a ray class character modulo  $q$  defined by  $\chi \circ N_{K_n}$ . Suppose  $\mathfrak{b}_n$  is an integral ideal relatively prime to  $q$  such that  $\mathfrak{b}_n^{-1} = [1, \delta(n)]$ . Assume the continued fraction expansion of  $\delta(n) - 1$*

$$\delta(n) - 1 = [[a_0(n), a_1(n), \dots, a_{s-1}(n)]]$$

*is purely periodic and of a fixed length  $s$  independent of  $n$  and  $a_i(n) = \alpha_i n + \beta_i$  for some fixed  $\alpha_i, \beta_i \in \mathbb{Z}$ .*

*If  $N_{K_n}(\mathfrak{b}_n(C + D\delta(n)))$  modulo  $q$  is a function only depending on  $C, D$  and  $r$  for  $n = qk + r$ , then  $L_{K_n}(0, \chi_n, \mathfrak{b}_n)$  is linear.*

Furthermore, we give a precise description of  $A_\chi(r)$  and  $B_\chi(r)$  using values of the Bernoulli polynomials (Proposition 3.8). From this description, for  $n$  with  $h(K_n) = 1$ , as in Biró’s case, one can compute the residue of  $n$  modulo  $p$  depending on the mod- $q$  residue  $r$  of  $n$ . There are possibly many  $(q, p)$  pairs. The more pairs of  $(q, p)$  we have, the more we can restrict possible  $n$ . There are many known families for which the class number one problem can be solved in this way. Many known results can be recovered by using the continued fraction expansion to show linearity and finding enough  $(q, p)$ .

There are still other families of real quadratic fields with linearity whose class number one problems are not yet answered. Morally, once we obtain a reasonable class number one criterion, finding sufficiently many  $(q, p)$ -pairs should solve it.

This paper is composed as follows. In Section 2, we describe the special value at  $s = 0$  of the partial Hecke  $L$ -function in terms of values of the Bernoulli polynomials. Section 3 is devoted to the proof of our main theorem. In Section 4, Biró's method is sketched as a prototype to apply the linearity. Section 5 concludes the paper with a possible generalization of the linearity criterion to a polynomial of higher order.

**Notation and conventions.** Throughout this article, we keep the following general notation and conventions. If necessary, we rewrite the notation at the place where it is used.

- (1)  $K$  is a real quadratic field.
- (2) For a real quadratic field  $K$ , we fix an embedding  $\iota : K \rightarrow \mathbb{R}$ . If there is no danger of confusion, we denote  $\iota(\alpha)$  by an element  $\alpha \in K$ .  $\alpha'$  denotes the conjugate of  $\alpha$  as well as  $\iota(\alpha')$ .
- (3) For  $\alpha \in K$ ,  $N_K(\alpha)$  denotes the norm of  $\alpha$  over  $\mathbb{Q}$ . If there is no danger of confusion, we simply write  $N(\alpha)$  to denote  $N_K(\alpha)$ . For an integral ideal  $\mathfrak{a}$  of  $K$ , we let  $N(\mathfrak{a}) := [\mathfrak{o}_K, \mathfrak{a}]$  denote the norm of  $\mathfrak{a}$ .
- (4) For two linearly independent elements  $\alpha, \beta \in K$  viewed as a vector space over  $\mathbb{Q}$ ,  $[\alpha, \beta]$  denotes the lattice (ie. free abelian group) generated by  $\alpha$  and  $\beta$ . The lattice defined by a fractional ideal  $\mathfrak{a}$  of  $K$  is denoted by  $[\alpha, \beta]$  if  $\{\alpha, \beta\}$  is a free basis of  $\mathfrak{a}$ .
- (5) For a subset  $A$  of  $K$ , we denote by  $A^+$  the set of totally positive elements in  $A$ .
- (6)  $\chi$  is a fixed Dirichlet character of modulus  $q$ .
- (7) For a real number  $x$ ,

$$\langle x \rangle := \begin{cases} x - [x] & \text{for } x \notin \mathbb{Z}, \\ 1 & \text{for } x \in \mathbb{Z}. \end{cases}$$

Equivalently,  $\langle - \rangle$  is the composition  $\mathbb{R} \xrightarrow{\text{mod } \mathbb{Z}} \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}$ , where  $\mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}$  is the unique map so that the composition is the identity on  $(0, 1]$ .

- (8) For a real  $x$ ,  $[x]_1 := x - \langle x \rangle$ .
- (9) For an integer  $m$ ,  $\langle m \rangle_q$  denotes the residue of  $m$  by  $q$  taken in  $[1, q]$  (i.e.,  $m = qk + \langle m \rangle_q$  for  $k \in \mathbb{Z}$ ,  $\langle m \rangle_q \in [1, q] \cap \mathbb{Z}$ ).

(10) For positive integers  $a_i$ ,  $[a_0, a_1, a_2, \dots]$  denotes the usual continued fraction:

$$[a_0, a_1, a_2, \dots] := a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

$[a_0, a_1, \dots, a_{i-1}, \overline{a_i, a_{i+1}, \dots, a_{i+j}}]$  denotes the continued fraction with periodic part  $(a_i, a_{i+1}, \dots, a_{i+j})$ .

$[[a_0, a_1, \dots, a_n]]$  is the purely periodic continued fraction

$$[a_0, a_1, \dots, a_n, a_0, a_1, \dots].$$

(11)  $(a_0, a_1, a_2, \dots)$  denotes the minus continued fraction:

$$(a_0, a_1, a_2, \dots) := a_0 - \frac{1}{a_1 - \frac{1}{a_2 - \dots}}$$

$((a_0, a_1, \dots, a_n))$  is the purely periodic minus continued fraction:

$$(a_0, a_1, a_2, \dots, a_n, a_0, a_1, \dots)$$

(12) For an integer  $s$ ,  $\mu(s) = 1$  if  $s$  is odd and  $\mu(s) = \frac{1}{2}$  if  $s$  is even.

### 2. Partial Hecke $L$ -function

Throughout this section,  $K$  denotes a real quadratic field and  $\mathfrak{b}$  is a fixed integral ideal of  $K$  relatively prime to  $q$  such that  $\mathfrak{b}^{-1} = [1, \delta]$  for  $\delta \in K$  satisfying  $0 < \delta' < 1$  and  $\delta > 2$ .

A ray class character modulo  $q$  is a homomorphism

$$\chi : I_K(q) / P_K(q) \rightarrow \mathbb{C}^*$$

where  $I_K(q)$  is a group of fractional ideals of  $K$  which is relatively prime to  $q$  and  $P_K(q)$  is a subgroup of principal ideals  $(\alpha)$  for totally positive  $\alpha \equiv 1 \pmod{q}$ .

Define

$$F := \{(C, D) \in \mathbb{Z}^2 \mid 0 \leq C, D \leq q - 1, ((C + D\delta)\mathfrak{b}, q) = 1\}.$$

Let  $E^+$  be the set of totally positive units in  $K$ , and  $E_q^+$  the set of totally positive units congruent to 1 mod  $q$ . Then  $\epsilon \in E^+$  acts on the set  $F$  by the rule

$$\epsilon * (C + D\delta) = C' + D'\delta,$$

where  $C'$  and  $D'$  are given by

$$\epsilon \cdot (C + D\delta) + q\mathfrak{b}^{-1} = C' + D'\delta + q\mathfrak{b}^{-1} \quad \text{for } \epsilon \in E^+.$$

**Lemma 2.1.**  $(C, D)$  in  $F$  is fixed by the action of  $\epsilon$  if and only if  $\epsilon$  is in  $E_q^+$ .

*Proof.*  $(C, D)$  is fixed by  $\epsilon \in E^+$  if and only if  $(C + D\delta)(\epsilon - 1) \in q\mathfrak{b}^{-1}$ . Since  $(\mathfrak{b}(C + D\delta), q) = 1$ , the condition  $(C + D\delta)(\epsilon - 1) \in q\mathfrak{b}^{-1}$  is equivalent to

$$\epsilon \equiv 1 \pmod{q}. \quad \square$$

**Lemma 2.2.** Suppose  $0 \leq C, D \leq q - 1$ . Then the following are equivalent:

- (1)  $(C, D)$  is in  $F$ .
- (2) For every  $\alpha \in (C + D\delta)/q + \mathfrak{b}^{-1}$ , the ideal  $q\alpha\mathfrak{b}$  is relatively prime to  $q$ .
- (3) For a  $\alpha \in (C + D\delta)/q + \mathfrak{b}^{-1}$ , the ideal  $q\alpha\mathfrak{b}$  is relatively prime to  $q$ .

*Proof.* Suppose that  $(q, (C + D\delta)\mathfrak{b}) = 1$ .

We have

$$\frac{q\alpha}{C + D\delta} \in 1 + \frac{q}{C + D\delta}\mathfrak{b}^{-1}$$

for  $\alpha \in (C + D\delta)/q + \mathfrak{b}^{-1}$ . Thus  $(q, \mathfrak{b}(C + D\delta)) = 1$  implies that

$$\frac{q\alpha}{C + D\delta} \equiv 1 \pmod{q}.$$

Since

$$q\mathfrak{b}\alpha = \mathfrak{b}(C + D\delta)\frac{q\alpha}{C + D\delta},$$

we have

$$(q\mathfrak{b}\alpha, q) = 1.$$

If  $(q, (C + D\delta)\mathfrak{b}) \neq 1$ , then  $(q, q\mathfrak{b}\alpha) \neq 1$  for  $\alpha \in (C + D\delta)/q + \mathfrak{b}^{-1}$ , since for  $\alpha \in (C + D\delta)/q + \mathfrak{b}^{-1}$ , we have

$$q\mathfrak{b}\alpha \subset (C + D\delta)\mathfrak{b} + q\mathcal{O}_K. \quad \square$$

Let  $F' = F/E^+$  be the orbit space of the action of  $E^+$  on  $F$ . Let  $\tilde{F}'$  be a fundamental set of  $F'$ . Let  $\epsilon$  be the totally positive fundamental unit. The order of the action of  $\epsilon$  is  $\lambda := [E^+ : E_q^+]$  by Lemma 2.1. Then we can decompose  $F$  as follows:

$$F = \bigsqcup_{i=0}^{\lambda-1} \epsilon^i \tilde{F}'. \quad (2-1)$$

According to this decomposition of  $F$ , we can further decompose the partial Hecke  $L$ -function:



**Proposition 2.3.** *Let  $q$  be a positive integer. Given an ideal  $\mathfrak{b} \subset K$  as specified at the beginning of this section and a ray class character  $\chi$  modulo  $q$ , we have*

$$\begin{aligned} L_K(s, \chi, \mathfrak{b}) &= \sum_{\substack{\mathfrak{a} \sim \mathfrak{b} \text{ integral} \\ (q, \mathfrak{a})=1}} \chi(\mathfrak{a}) N(\mathfrak{a})^{-s} \\ &= \sum_{(C, D) \in \tilde{F}'} \chi((C + D\delta)\mathfrak{b}) \sum_{\alpha \in (\frac{C+D\delta}{q} + \mathfrak{b}^{-1})^+ / E_q^+} N(q\mathfrak{b}\alpha)^{-s}. \end{aligned}$$

*Proof.* For  $\alpha_1, \alpha_2 \in (q^{-1}\mathfrak{b}^{-1})^+$ ,  $q\alpha_1\mathfrak{b} = q\alpha_2\mathfrak{b}$  if and only if  $\alpha_1/\alpha_2 \in E^+$ .

So we have

$$\sum_{\substack{\mathfrak{a} \sim \mathfrak{b} \text{ integral} \\ (q, \mathfrak{a})=1}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \sum_{\substack{\mathfrak{a} \sim q\mathfrak{b} \text{ integral} \\ (q, \mathfrak{a})=1}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \sum_{\substack{\alpha \in (q^{-1}\mathfrak{b}^{-1})^+ / E^+ \\ (q, q\alpha\mathfrak{b})=1}} \frac{\chi(q\alpha\mathfrak{b})}{N(q\alpha\mathfrak{b})^s}$$

For a totally positive fundamental unit  $\epsilon > 1$ , we also have

$$\begin{aligned} \sum_{\substack{\alpha \in (q^{-1}\mathfrak{b}^{-1})^+ / E_q^+ \\ (q, q\mathfrak{b}\alpha)=1}} \frac{\chi(q\mathfrak{b}\alpha)}{N(q\mathfrak{b}\alpha)^s} &= \sum_{\substack{\alpha \in (q^{-1}\mathfrak{b}^{-1})^+ / E^+ \\ (q, q\mathfrak{b}\alpha)=1}} \sum_{i=0}^{\lambda-1} \frac{\chi(q\mathfrak{b}\alpha\epsilon^i)}{N(q\mathfrak{b}\alpha\epsilon^i)^s} \\ &= \lambda \cdot \sum_{\substack{\alpha \in (q^{-1}\mathfrak{b}^{-1})^+ / E^+ \\ (q, q\mathfrak{b}\alpha)=1}} \frac{\chi(q\mathfrak{b}\alpha)}{N(q\mathfrak{b}\alpha)^s}. \end{aligned}$$

And from Lemma 2.2, we have

$$\begin{aligned} \sum_{\substack{\alpha \in (q^{-1}\mathfrak{b}^{-1})^+ / E_q^+ \\ (q, q\mathfrak{b}\alpha)=1}} \frac{\chi(q\mathfrak{b}\alpha)}{N(q\mathfrak{b}\alpha)^s} &= \sum_{(C, D) \in F} \sum_{\substack{\alpha \in (\frac{C+D\delta}{q} + \mathfrak{b}^{-1})^+ / E_q^+ \\ (q, q\mathfrak{b}\alpha)=1}} \frac{\chi(q\mathfrak{b}\alpha)}{N(q\mathfrak{b}\alpha)^s} \\ &= \sum_{(C, D) \in F} \sum_{\alpha \in (\frac{C+D\delta}{q} + \mathfrak{b}^{-1})^+ / E_q^+} \frac{\chi(q\mathfrak{b}\alpha)}{N(q\mathfrak{b}\alpha)^s}. \end{aligned}$$

By equation (2), the above is equal to

$$\sum_{(C, D) \in \tilde{F}'} \sum_{i=0}^{\lambda-1} \sum_{\alpha \in (\frac{(C+D\delta)\epsilon^i}{q} + \mathfrak{b}^{-1})^+ / E_q^+} \frac{\chi(q\mathfrak{b}\alpha)}{N(q\mathfrak{b}\alpha)^s}.$$

Since

$$\sum_{\alpha \in (\frac{(C+D\delta)\epsilon^i}{q} + \mathfrak{b}^{-1})^+ / E_q^+} \frac{\chi(q\mathfrak{b}\alpha)}{N(q\mathfrak{b}\alpha)^s} = \sum_{\alpha \in (\frac{(C+D\delta)}{q} + \mathfrak{b}^{-1})^+ / E_q^+} \frac{\chi(q\mathfrak{b}\alpha\epsilon^i)}{N(q\mathfrak{b}\alpha\epsilon^i)^s},$$

the above also equal to

$$\lambda \cdot \sum_{(C,D) \in \tilde{F}'} \sum_{\alpha \in (\frac{C+D\delta}{q} + \mathfrak{b}^{-1})^+ / E_q^+} \frac{\chi(q\mathfrak{b}\alpha)}{N(q\mathfrak{b}\alpha)^s}.$$

Note that for  $\alpha \in (\frac{C+D\delta}{q} + \mathfrak{b}^{-1})^+$ ,  $q\mathfrak{b}\alpha$  and  $(C + D\delta)\mathfrak{b}$  are in the same ray class modulo  $q$ . Thus  $\chi(q\mathfrak{b}\alpha) = \chi((C + D\delta)\mathfrak{b})$ . This completes the proof.  $\square$

**Shintani–Zagier cone decomposition.** We review briefly the decomposition of  $(\mathbb{R}^2)^+$  into cones due to Shintani [1976] and Zagier [1975] (see also [van der Geer 1988]). This depends on a real quadratic field  $K$  and a fixed ideal  $\mathfrak{a}$  inside. Here for the sake of computation, we fix  $\mathfrak{a} = \mathfrak{b}^{-1}$  where  $\mathfrak{b}$  is set as in the beginning of this section.

$K$  is embedded into  $\mathbb{R}^2$  by  $\iota = (\tau_1, \tau_2)$ , where  $\tau_1, \tau_2$  are two real embeddings of  $K$ . In particular, the totally positive elements of  $K$  land on  $(\mathbb{R}^2)^+$ . We are going to describe the fundamental domain of  $(\frac{C+D\delta}{q} + \mathfrak{b}^{-1})^+ / E_q^+$  embedded into  $(\mathbb{R}^2)^+$ .

The multiplicative action of  $E_q^+$  on  $K^+$  induces an action on  $(\mathbb{R}^2)^+$  by coordinatewise multiplication:

$$\epsilon \circ (x, y) = (\tau_1(\epsilon)x, \tau_2(\epsilon)y).$$

A fundamental domain  $\mathfrak{D}_{\mathbb{R}}$  of  $(\mathbb{R}^2)^+ / E_q^+$  is given by

$$\mathfrak{D}_{\mathbb{R}} := \{x\iota(1) + y\iota(\epsilon^{-\lambda}) \mid x > 0, y \geq 0\} \subset (\mathbb{R}^2)^+ \tag{2-2}$$

where  $E_q^+ = \langle \epsilon^\lambda \rangle$  for an integer  $\lambda$  and  $\epsilon > 1$  is the unique totally positive fundamental unit.

If we take the convex hull of  $\iota(\mathfrak{b}^{-1}) \cap (\mathbb{R}^2)^+$  in  $(\mathbb{R}^2)^+$ , the vertices on the boundary are  $\{P_i\}_{i \in \mathbb{Z}}$  for  $P_i \in \iota(\mathfrak{b}^{-1})$ , and determined by the conditions  $P_0 = \iota(1)$ ,  $P_{-1} = \iota(\delta)$  and  $x(P_i) < x(P_{i-1})$  where  $x(P_k)$  denotes the first coordinate of  $P_k$  for  $k \in \mathbb{Z}$ . Since any two consecutive boundary points make a basis of  $\iota(\mathfrak{b}^{-1})$ , we find that

$$\begin{pmatrix} 0 & 1 \\ -1 & b_i \end{pmatrix} \begin{pmatrix} P_{i-1} \\ P_i \end{pmatrix} = \begin{pmatrix} P_i \\ P_{i+1} \end{pmatrix},$$

for an integer  $b_i$ . It is easy to see that  $b_i \geq 2$  from the convexity. Thus we obtain

$$x(P_{i-1}) + x(P_{i+1}) = b_i x(P_i). \tag{2-3}$$

Put  $\delta_i := \frac{x(P_{i-1})}{x(P_i)} > 1$ . Note that  $\delta_0 = \delta$ .  $\delta_i$  satisfies a recursion relation:

$$\delta_i = b_i - \frac{1}{\delta_{i+1}} \quad \text{for } i \in \mathbb{Z}.$$

Therefore

$$\delta_i = b_i - \frac{1}{b_{i+1} - \frac{1}{b_{i+2} - \dots}} = (b_i, b_{i+1}, b_{i+2}, \dots).$$

Let  $\epsilon > 1$  be the totally positive fundamental unit. Then  $\epsilon$  moves a boundary point to another boundary point, preserving the order. Thus, there exists a positive integer  $m$  so that for all  $i \in \mathbb{Z}$

$$\epsilon \circ P_i = P_{i-m}. \tag{2-4}$$

Therefore we obtain the following proposition.

**Proposition 2.4.** (1)  $\delta_{i+m} = \delta_i$  for all  $i \in \mathbb{Z}$ .

$$(2) \delta_i = ((b_i, b_{i+1}, \dots, b_{i+m-1})) = b_i - \frac{1}{b_{i+1} - \dots - \frac{1}{b_{i+m-1} - \frac{1}{b_i - \dots}}}.$$

$$(3) \iota(\epsilon^{-1}) = P_m.$$

$$(4) \epsilon^{-1} \circ P_i = P_{i+m}.$$

$$(5) \iota(\epsilon^{-\gamma}) = P_{\gamma m}.$$

*Proof.* (1)  $\delta_{i+m} = \frac{x(P_{i+m-1})}{x(P_{i+m})} = \frac{\epsilon x(P_{i-1})}{\epsilon x(P_i)} = \delta_i.$

(2) This is an immediate consequence of (1).

(3) From (2-4),

$$P_m = \epsilon^{-1} \circ P_0,$$

since  $P_0 = \iota(1)$  and  $\epsilon^{-1} \circ \iota(1) = \iota(\epsilon^{-1})$ .

(4) This is immediate from (2-4).

(5) This follows trivially from (3) and (4). □

Using (2-2) and Proposition 2.4(4), the fundamental domain  $\mathfrak{D}_{\mathbb{R}}$  of  $(\mathbb{R}^2)^+ / E_q^+$  is further decomposed into the disjoint union of  $\lambda m$  smaller cones:

$$\mathfrak{D}_{\mathbb{R}} = \bigsqcup_{i=1}^{\lambda m} \{xP_{i-1} + yP_i \mid x > 0, y \geq 0\}.$$

Clearly, the fundamental set of the quotient  $(\iota((C + D\delta)/q + \mathfrak{b}^{-1}) \cap (\mathbb{R}^2)^+) / E_q^+$  inside  $\mathfrak{D}_{\mathbb{R}}$ , which we denote by  $\mathfrak{D}$ , is given by a disjoint union:

$$\mathfrak{D} := \bigsqcup_{i=1}^{\lambda m} \left( \iota \left( \frac{C + D\delta}{q} + \mathfrak{b}^{-1} \right) \cap \{xP_{i-1} + yP_i \mid x > 0, y \geq 0\} \right).$$

Since  $\{P_{i-1}, P_i\}$  is a  $\mathbb{Z}$ -basis of  $\iota(\mathfrak{b}^{-1})$ , there is a unique  $(x_{C+D\delta}^i, y_{C+D\delta}^i) \in (0, 1] \times [0, 1)$  such that

$$x_{C+D\delta}^i P_{i-1} + y_{C+D\delta}^i P_i \in \iota\left(\frac{C+D\delta}{q} + \mathfrak{b}^{-1}\right),$$

for each  $i, C, D \in \mathbb{Z}$ . Thus

$$\begin{aligned} &\iota\left(\frac{C+D\delta}{q} + \mathfrak{b}^{-1}\right) \cap \{xP_{i-1} + yP_i \mid x > 0, y \geq 0\} \\ &= \{(x_{C+D\delta}^i + n_1)P_{i-1} + (y_{C+D\delta}^i + n_2)P_i \mid n_1, n_2 \in \mathbb{Z}_{\geq 0}\}. \end{aligned} \tag{2-5}$$

Yamamoto [2008, (2.1.3)] found that  $(x_{C+D\delta}^i, y_{C+D\delta}^i)$  satisfy the following recurrence relations:

$$\begin{aligned} x_{C+D\delta}^{i+1} &= \langle b_i x_{C+D\delta}^i + y_{C+D\delta}^i \rangle, \\ y_{C+D\delta}^{i+1} &= 1 - x_{C+D\delta}^i. \end{aligned} \tag{2-6}$$

Let  $A_i := x(P_i)$  for all  $i \in \mathbb{Z}$ . Then from (2-5), we obtain the following:

$$\begin{aligned} &\sum_{\alpha \in (\frac{C+D\delta}{q} + \mathfrak{b}^{-1}) + E_q^+} \frac{1}{N(\alpha)^s} \\ &= \sum_{i=1}^{\lambda m} \sum_{n_1, n_2 \geq 0} N((x_{C+D\delta}^i + n_1)A_{i-1} + (y_{C+D\delta}^i + n_2)A_i)^{-s} \\ &= \sum_{i=1}^{\lambda m} \sum_{n_1, n_2 \geq 0} N((x_{C+D\delta}^i + n_1)\delta_i + (y_{C+D\delta}^i + n_2))^{-s} A_i^{-s}. \end{aligned} \tag{2-7}$$

Shintani [1976] evaluated  $\sum_{n_1, n_2 \geq 0} N((x + n_1)\delta + (y + n_2))^{-s}$  for nonpositive integers  $s$ . In particular, the value at  $s = 0$  is expressed by first and second Bernoulli polynomials as follows:

**Lemma 2.5** (Shintani).

$$\begin{aligned} &\sum_{n_1, n_2 \geq 0} N((x + n_1)\delta + (y + n_2))^{-s} \Big|_{s=0} \\ &= \frac{\delta + \delta'}{4} B_2(x) + B_1(x)B_1(y) + \frac{1}{4} \left(\frac{1}{\delta} + \frac{1}{\delta'}\right) B_2(y). \end{aligned}$$

Using this, we have

$$\begin{aligned} & \sum_{\alpha \in (\frac{C+D\delta}{q} + \mathfrak{b}^{-1})^+ / E_q^+} \frac{1}{N(\alpha)^s} \Big|_{s=0} \\ &= \sum_{i=1}^{\lambda m} \frac{\delta_i + \delta'_i}{4} B_2(x_{C+D\delta}^i) + B_1(x_{C+D\delta}^i) B_1(y_{C+D\delta}^i) + \frac{1}{4} \left( \frac{1}{\delta_i} + \frac{1}{\delta'_i} \right) B_2(y_{C+D\delta}^i). \end{aligned} \quad (2-8)$$

This simplifies further:

**Lemma 2.6** [Yamamoto 2008, proof of Theorem 4.1.1].

$$\sum_{i=1}^{\lambda m} \frac{\delta_i + \delta'_i}{4} B_2(x_{C+D\delta}^i) + \frac{1}{4} \left( \frac{1}{\delta_i} + \frac{1}{\delta'_i} \right) B_2(y_{C+D\delta}^i) = \sum_{i=1}^{\lambda m} \frac{b_i}{2} B_2(x_{C+D\delta}^i).$$

Finally, we have

$$\sum_{\alpha \in (\frac{C+D\delta}{q} + \mathfrak{b}^{-1})^+ / E_q^+} \frac{1}{N(\alpha)^s} \Big|_{s=0} = \sum_{i=1}^{\lambda m} B_1(x_{C+D\delta}^i) B_1(y_{C+D\delta}^i) + \frac{b_i}{2} B_2(x_{C+D\delta}^i).$$

**Lemma 2.7.** *Let  $\epsilon$  be the totally positive fundamental unit of  $K$ . Then*

$$x_{C+D\delta}^{mi+j} = x_{\epsilon^i * (C+D\delta)}^j \quad \text{and} \quad y_{C+D\delta}^{mi+j} = y_{\epsilon^i * (C+D\delta)}^j$$

for  $j = 0, 1, 2, \dots, m - 1$ .

*Proof.* From (4) of Proposition 2.4, we have  $A_{mi+j} = \epsilon^{-i} A_j$ , for any integer  $i$ . Thus

$$x_{C+D\delta}^{mi+j} A_{mi+j-1} + y_{C+D\delta}^{mi+j} A_{mi+j} = x_{C+D\delta}^{mi+j} \epsilon^{-i} A_{j-1} + y_{C+D\delta}^{mi+j} \epsilon^{-i} A_j \in \frac{C + D\delta}{q} + \mathfrak{b}^{-1}.$$

Therefore,

$$x_{C+D\delta}^{mi+j} A_{j-1} + y_{C+D\delta}^{mi+j} A_j \in \frac{\epsilon^i \cdot (C + D\delta)}{q} + \mathfrak{b}^{-1}. \quad \square$$

From Lemma 2.7 and the periodicity of  $b_i$ , we have:

**Lemma 2.8.**

$$\begin{aligned} & \sum_{\alpha \in (\frac{C+D\delta}{q} + \mathfrak{b}^{-1})^+ / E_q^+} \frac{1}{N(\alpha)^s} \Big|_{s=0} \\ &= \sum_{i=1}^m \sum_{j=0}^{\lambda-1} B_1(x_{\epsilon^i * (C+D\delta)}^j) B_1(y_{\epsilon^i * (C+D\delta)}^j) + \frac{b_i}{2} B_2(x_{\epsilon^i * (C+D\delta)}^j). \end{aligned}$$

Finally, we have:

**Proposition 2.9.** *For a ray class character  $\chi$  modulo  $q$  and an ideal  $\mathfrak{b}$  of  $K$  such that*

$$\mathfrak{b}^{-1} = [1, \delta]$$

for  $\delta \in K$  with  $\delta > 2$  and  $0 < \delta' < 1$ , we have

$$L_K(0, \chi, \mathfrak{b}) = \sum_{1 \leq C, D \leq q} \chi((C + D\delta)\mathfrak{b}) \sum_{i=1}^m B_1(x_{(C+D\delta)}^i) B_1(y_{(C+D\delta)}^i) + \frac{b_i}{2} B_2(x_{(C+D\delta)}^i).$$

*Proof.* From Proposition 2.3, we obtain

$$L_K(0, \chi, \mathfrak{b}) = \sum_{(C,D) \in \tilde{F}'} \chi((C + D\delta)\mathfrak{b}) \sum_{\alpha \in (\frac{C+D\delta}{q} + \mathfrak{b}^{-1}) + / E_q^+} N(q\mathfrak{b}\alpha)^{-s} |_{s=0}.$$

Lemma 2.8 implies that this is equal to

$$\sum_{(C,D) \in \tilde{F}'} \chi((C + D\delta)\mathfrak{b}) \sum_{j=0}^{\lambda-1} \sum_{i=1}^m B_1(x_{\epsilon^{j*}(C+D\delta)}^i) B_1(y_{\epsilon^{j*}(C+D\delta)}^i) + \frac{b_i}{2} B_2(x_{\epsilon^{j*}(C+D\delta)}^i).$$

Since  $(C + D\delta)\epsilon\mathfrak{b} = (C + D\delta)\mathfrak{b}$ , this expression can be rewritten as

$$\sum_{(C,D) \in \tilde{F}'} \sum_{j=0}^{\lambda-1} \left( \chi((C + D\delta)\epsilon^j \mathfrak{b}) \times \sum_{i=1}^m B_1(x_{\epsilon^{j*}(C+D\delta)}^i) B_1(y_{\epsilon^{j*}(C+D\delta)}^i) + \frac{b_i}{2} B_2(x_{\epsilon^{j*}(C+D\delta)}^i) \right).$$

In view of the decomposition of  $F$  in (2-1), the preceding expression equals

$$\sum_{(C,D) \in F} \chi((C + D\delta)\mathfrak{b}) \sum_{i=1}^m B_1(x_{(C+D\delta)}^i) B_1(y_{(C+D\delta)}^i) + \frac{b_i}{2} B_2(x_{(C+D\delta)}^i).$$

If  $((C + D\delta)\mathfrak{b}, q) \neq 1$  then  $\chi((C + D\delta)\mathfrak{b}) = 0$ . Thus we complete the proof.  $\square$

**Remark 2.10.** The summation running over  $C, D \in [1, q]$  is actually supported on  $F$ . This is justified by the twist of the mod  $q$  Dirichlet character. Obviously,  $F$  depends on  $\delta$  in  $K$ , but the twisted sum has an invariant form of  $\delta$  and  $K$ . This is a subtle point in the proof of the main theorem where we deal with values of the Hecke  $L$ -function with respect to a family  $(K_n, \chi_n, \mathfrak{b})$ .

### 3. Proof of the main theorem

In this section, we compute special values of the Hecke  $L$ -function for a family of real quadratic fields. The computation is made using the expression for the  $L$ -value from the previous section. After the computation, it will be apparent that the

linearity property comes from the shape of the continued fractions in the family. This will complete the proof of Theorem 1.3.

This gives a criterion that will recover several approaches of class number problems for some families of real quadratic fields.

Consider a family of real quadratic fields  $K_n = \mathbb{Q}(\sqrt{d_n})$ , where  $d_n$  is a positive square free integer. For a fixed Dirichlet character  $\chi$  of modulus  $q$ , we associate a ray class character  $\chi_n := \chi \circ N_{K_n/\mathbb{Q}}$  for each  $n$ . Let us fix an ideal  $\mathfrak{b}_n$  of  $K_n$  for each  $n$ . Then we have a family of Hecke  $L$ -functions associated to  $(K_n, \chi_n, \mathfrak{b}_n)$ :

$$L_{K_n}(s, \chi_n, \mathfrak{b}_n) = \sum_{\mathfrak{a}} \frac{\chi_n(\mathfrak{a})}{N(\mathfrak{a})^s}$$

where  $\mathfrak{a}$  ranges over integral ideals in the ray class represented by  $\mathfrak{b}_n$ .

**Plan of the proof.** Assume that

$$\mathfrak{b}_n^{-1} = [1, \delta(n)]$$

with  $\delta(n) > 2, 0 < \delta(n)' < 1$ . As discussed in Proposition 2.4,  $\delta(n)$  has a purely periodic minus continued fraction expansion:

$$\begin{aligned} \delta(n) &= ((b_0(n), b_1(n), \dots, b_{m(n)-1}(n))) \\ &= b_0(n) - \frac{1}{b_1(n) - \dots - \frac{1}{b_{m(n)-1}(n) - \frac{1}{b_0(n) - \dots}}}, \end{aligned} \tag{3-1}$$

with  $b_k(n) \geq 2$ .

We extend the definition of  $b_i(n)$  to all  $i \in \mathbb{Z}$  by requiring that  $b_{i+m(n)}(n) = b_i(n)$  for  $i \in \mathbb{Z}$ , and take  $\delta_k(n) = ((b_k(n), b_{k+1}(n), \dots, b_{k+m(n)-1}(n)))$ . We define  $\{A_k(n)\}_{k \in \mathbb{Z}}$  by

$$A_{-1}(n) = \delta(n), \quad A_0(n) = 1, \quad \dots, \quad A_{k+1}(n) = A_k(n)/\delta_{k+1}(n).$$

Then for fixed  $C, D$  and  $n$ , there is a unique  $(x_{C+D\delta(n)}^i, y_{C+D\delta(n)}^i)$  such that

$$0 < x_{C+D\delta(n)}^i \leq 1, \quad 0 \leq y_{C+D\delta(n)}^i < 1, \tag{3-2}$$

and

$$x_{C+D\delta(n)}^i A_{i-1}(n) + y_{C+D\delta(n)}^i A_i(n) \in \frac{C + D\delta(n)}{q} + \mathfrak{b}_n^{-1}, \tag{3-3}$$

for each  $i \in \mathbb{Z}$ , as described in the previous section. This  $(x_{C+D\delta(n)}^i, y_{C+D\delta(n)}^i)$  satisfies Yamamoto's recursive relation (2-6) as follows:

$$x_{C+D\delta(n)}^{i+1} = \langle b_i(n)x_{C+D\delta(n)}^i + y_{C+D\delta(n)}^i \rangle, \quad y_{C+D\delta(n)}^{i+1} = 1 - x_{C+D\delta(n)}^i. \tag{3-4}$$

Now recall a standard conversion formula from a continued fraction expansion to a minus continued fraction expansion:

**Lemma 3.1.** *Let  $\delta - 1$  be a purely periodic continued fraction:*

$$\llbracket a_0, a_1, \dots, a_{s-1} \rrbracket.$$

*Then the minus continued fraction expansion of  $\delta$  is*

$$((b_0, b_1, \dots, b_{m-1})),$$

*where*

$$b_i := \begin{cases} a_{2j} + 2 & \text{for } i = S_j, \\ 2 & \text{otherwise,} \end{cases}$$

*where*

$$S_j = \begin{cases} 0 & \text{for } j = 0, \\ S_{j-1} + a_{2j-1} & \text{for } j \geq 1, \end{cases}$$

*and the period  $m$  is given by*

$$m = \begin{cases} a_1 + a_3 + a_5 \cdots + a_{s-1} = S_{s/2} & \text{for even } s, \\ a_0 + a_1 + a_2 \cdots + a_{s-1} = S_s & \text{for odd } s. \end{cases}$$

*Proof.* (See [Zagier 1975, pp. 177, 178].) If  $s$  is an odd integer, the period  $m$  is

$$\sum_{i=1}^s a_{2i-1} = a_1 + a_3 + \cdots + a_{2s-1} = S_s.$$

Since  $a_i$  has period  $s$ , we find that

$$a_1 + a_3 + \cdots + a_{2s-1} = a_0 + a_1 + a_2 \cdots + a_{s-1} = \sum_{i=0}^{s-1} a_i. \quad \square$$

For the family of  $\delta(n) \in K$ , we assumed that

$$\delta(n) - 1 = \llbracket a_0(n), a_1(n), a_2(n), \dots, a_{s-1}(n) \rrbracket$$

has the same period for every  $n$ .

Then  $\delta(n)$  has a purely periodic minus continued fraction expansion

$$\delta(n) = ((b_0(n), b_1(n), \dots, b_{m(n)-1}(n))),$$

with  $b_i(n)$ ,  $S_j(n)$  and  $m(n)$  defined in the same manner as in the previous lemma.

One should be aware that  $m(n)$  varies with  $n$ , while the period  $s$  of the positive continued fraction is fixed.

From Proposition 2.9 and the recursion (3-4) for  $(x_{C+D\delta(n)}^i, y_{C+D\delta(n)}^i)$ , we have



$$L_{K_n}(0, \chi_n, \mathfrak{b}_n) = \sum_{1 \leq C, D \leq q} \left( \chi_n((C + D\delta(n))\mathfrak{b}_n) \times \sum_{i=1}^{m(n)} \left( B_1(x_{C+D\delta(n)}^i) B_1(y_{C+D\delta(n)}^i) + \frac{b_i(n)}{2} B_2(x_{C+D\delta(n)}^i) \right) \right). \quad (3-5)$$

To check the linear behavior, it suffices to show that

$$\sum_{i=1}^{m(n)} \left( B_1(x_{C+D\delta(n)}^i) B_1(y_{C+D\delta(n)}^i) + \frac{b_i(n)}{2} B_2(x_{C+D\delta(n)}^i) \right) \quad (3-6)$$

is linear in  $k$  with the coefficients depending only on  $r$ .

Because  $b_i(n) = 2$  if  $i \neq S_j(n)$  for every  $j$ , we can divide the sum above into two parts:

$$\sum_{l=1}^{s\mu(s)} \left( -B_1(x_{C+D\delta(n)}^{S_l(n)}) B_1(x_{C+D\delta(n)}^{S_l(n)-1}) + \frac{a_{2l}(n) + 2}{2} B_2(x_{C+D\delta(n)}^{S_l(n)}) \right) + \sum_{l=0}^{s\mu(s)-1} \sum_{i=S_l(n)+1}^{S_{l+1}(n)-1} F(x_{C+D\delta(n)}^i, x_{C+D\delta(n)}^{i-1}), \quad (3-7)$$

where  $\mu(s) = \frac{1}{2}$  or 1 for  $s$  even or odd, respectively, and

$$F(x, y) := -B_1(x) B_1(y) + B_2(x).$$

We will use the following fact to be proved later. Here and wherever there is no danger of misunderstanding,  $x_i(n)$  means  $x_{C+D\delta(n)}^i$  for fixed  $C, D$ .

**Claim.** *The sequence  $\{x_i(n)\}$  is a piecewise arithmetic progression, in the sense that it satisfies these properties:*

1.  $\{x_i(n)\}_{S_j(n) \leq i \leq S_{j+1}(n)}$  is an arithmetic progression mod  $\mathbb{Z}$  with common difference  $\langle x_{S_j(n)+1}(n) - x_{S_j(n)}(n) \rangle$ .
2.  $\{x_i(n)\}_{S_j(n) \leq i \leq S_{j+1}(n)}$  has period  $q$ .
3.  $x_{S_j(n)}(n), x_{S_j(n)-1}(n)$  and  $x_{S_j(n)+1}(n)$  are independent of  $k$ , where  $n = qk + r$ .

Because of the constraint  $a_i(n) = \alpha_i n + \beta_i$ , the value of  $\langle a_i(n) \rangle_q$  is independent of  $k$  for  $n = qk + r$  and depends only on  $i$  and  $r$ . We can thus set

$$\gamma_i(r) := \langle a_i(n) \rangle_q, \quad (3-8)$$

where  $n = qk + r$ . In particular,  $\gamma_i(r) = \langle a_i(r) \rangle_q$ .

Since  $\{F(x_i(n), x_{i-1}(n))\}_{S_l(n)+1 \leq i \leq S_{l+1}(n)-1}$  has period  $q$  (item 2 of the claim), we obtain

$$\begin{aligned} & \sum_{i=S_l(n)+1}^{S_{l+1}(n)-1} F(x_i(n), x_{i-1}(n)) \\ &= \sum_{i=S_l(n)+1}^{S_l(n)+\gamma_{2l+1}(r)-1} F(x_i(n), x_{i-1}(n)) + \kappa_{2l+1}(n) \sum_{i=S_l(n)+1}^{S_l(n)+q} F(x_i(n), x_{i-1}(n)), \end{aligned}$$

where  $a_i(n) = \kappa_i(n)q + \gamma_i(r)$  for an integer  $\kappa_i(n)$ . Written precisely,

$$\kappa_i(n) = \frac{a_i(n) - \gamma_i(r)}{q}. \tag{3-9}$$

Since

$$\alpha_i r + \beta_i = q\tau_i(r) + \gamma_i(r)$$

for some integer  $\tau_i(r)$ , we can write for  $n = qk + r$

$$\kappa_i(n) = k\alpha_i + \tau_i(r) \tag{3-10}$$

Using 3, we see that  $x_{S_l(n)}(n)$  and  $x_{S_l(n)+1}(n)$  are determined by the residue  $r$  of  $n$  by  $q$ . A priori the sums

$$\sum_{i=S_l(n)+1}^{S_l(n)+\gamma_{2l+1}(r)-1} F(x_i(n), x_{i-1}(n)) \quad \text{and} \quad \sum_{i=S_l(n)+1}^{S_l(n)+q} F(x_i(n), x_{i-1}(n))$$

are completely determined by  $x_{S_l(n)}(n)$  and  $x_{S_l(n)+1}(n)$  and remain unchanged while  $k$  varies.

Thus we conclude:

**Fact I.** For  $n = qk + r$ ,

$$\sum_{i=S_l(n)+1}^{S_{l+1}(n)-1} F(x_i(n), x_{i-1}(n))$$

is a linear function of  $k$ .

Using (3-9) and (3-10), we have

$$\begin{aligned} & -B_1(x_{S_l(n)}(n))B_1(x_{S_l(n)-1}(n)) + \frac{a_{2l}(n) + 2}{2} B_2(x_{S_l(n)}(n)) \\ &= -B_1(x_{S_l(n)}(n))B_1(x_{S_l(n)-1}(n)) + \frac{\alpha_{2l}qk + \tau_{2l}(r)q + \gamma_{2l}(r) + 2}{2} B_2(x_{S_l(n)}(n)). \end{aligned}$$

Again using item 3 of the Claim we conclude:

**Fact II.** For  $n = qk + r$ ,

$$-B_1(x_{S_l(n)}(n))B_1(x_{S_l(n)-1}(n)) + \frac{a_{2l}(n) + 2}{2}B_2(x_{S_l(n)}(n))$$

is a linear function of  $k$ .

Additionally, we have:

**Fact III.**  $s$  and  $\mu(s)$  are independent of  $n$ .

Together, Facts I, II and III imply that

$$\sum_{i=1}^{m(n)} -B_1(x_i(n))B_1(x_{i-1}(n)) + \frac{b_i(n)}{2}B_2(x_i(n)) \tag{3-11}$$

is linear in  $k$  and the coefficients are functions of  $r$  for fixed  $C, D$ .

There remains to prove properties 1, 2, and 3 of  $\{x_i(n)\}$ . We will also give a precise description of the expression (3-11) to finish the proof of Theorem 1.3.

**Periodicity and invariance.** We now prove the Claim above about the sequence  $\{x_i(n)\}$ .

**Proposition 3.2.** For  $j \geq 0$ ,  $\{x_i(n)\}_{S_j(n) \leq i \leq S_{j+1}(n)}$  is an arithmetic progression mod  $\mathbb{Z}$  with common difference  $\langle x_{S_j(n)+1}(n) - x_{S_j(n)}(n) \rangle$ .

*Proof.* Since  $b_i(n) = 2$  for  $S_j(n) + 1 \leq i \leq S_{j+1}(n) - 1$ , we have that

$$x_{i+1}(n) = \langle 2x_i(n) - x_{i-1}(n) \rangle.$$

This implies that for  $S_j(n) + 1 \leq i \leq S_{j+1}(n) - 1$ ,

$$\langle x_{i+1}(n) - x_i(n) \rangle = \langle \langle 2x_i(n) - x_{i-1}(n) \rangle - x_i(n) \rangle = \langle x_i(n) - x_{i-1}(n) \rangle. \quad \square$$

**Lemma 3.3.** For  $i \geq -1$ , we have  $qx_i(n) \in \mathbb{Z}$  and  $0 < x_i(n) \leq 1$ .

*Proof.* Since  $A_0(n) = 1$  and  $A_{-1}(n) = \delta(n)$ , we find from (3-2), (3-3), and (3-4) that

$$x_0(n) = \left\langle \frac{D}{q} \right\rangle, \quad x_{-1}(n) = 1 - \frac{C}{q}.$$

We also note that  $b_i(n) \in \mathbb{Z}$  for any  $i \geq 0$ . Thus (3-4) implies this lemma.  $\square$

**Proposition 3.4.** For  $j \geq 0$  and  $a_{2j+1}(n) \geq q$ ,  $\{x_i(n)\}_{S_j(n) \leq i \leq S_{j+1}(n)}$  has period  $q$ . Explicitly, we have

$$x_{S_j(n)+q+i}(n) = x_{S_j(n)+i}(n) \quad \text{for } 0 \leq i \leq a_{2j+1}(n) - q.$$

*Proof.* Note that  $\{x_i(n) \bmod 1\}_{S_j(n) \leq i \leq S_{j+1}(n)}$  is an arithmetic progression. Thus

$$x_{S_j(n)+q+i}(n) = \langle x_{S_j(n)+i}(n) + q \langle x_{S_j(n)+i}(n) - x_{S_j(n)+i-1}(n) \rangle \rangle,$$

for  $0 \leq i \leq a_{2j+1}(n) - q$ . From Lemma 3.3, we find that

$$q \langle x_{S_j(n)+i}(n) - x_{S_j(n)+i-1}(n) \rangle \in \mathbb{Z}.$$

Thus

$$\langle x_{S_j(n)+i}(n) + q \langle x_{S_j(n)+i}(n) - x_{S_j(n)+i-1}(n) \rangle \rangle = \langle x_{S_j(n)+i}(n) \rangle.$$

Since  $0 < x_{S_j(n)+i}(n) \leq 1$ , we finally have

$$\langle x_{S_j(n)+i}(n) \rangle = x_{S_j(n)+i}(n).$$

□

For  $0 \leq r \leq q - 1$ , we define

$$\Gamma_j(r) := \begin{cases} 0 & \text{for } j = 0, \\ \Gamma_j(r) + \gamma_{2j-1}(r) & \text{for } j \geq 1, \end{cases}$$

where  $\gamma_i(r)$  is defined as in (3-8). For  $i \geq 0$ , we put

$$c_i(r) = \begin{cases} \gamma_{2j}(r) + 2 & \text{for } i = \Gamma_j(r), \\ 2 & \text{otherwise.} \end{cases}$$

Consider a sequence  $\{v_{CD}^i(r)\}_{i \geq -1}$  with the initial value and the recursion relation as follows:

$$v_{CD}^{-1}(r) = \frac{q-C}{q}, \quad v_{CD}^0(r) = \left\langle \frac{D}{q} \right\rangle$$

and

$$v_{CD}^{i+1}(r) = \langle c_i(r)v_{CD}^i(r) - v_{CD}^{i-1}(r) \rangle.$$

If  $C, D$  are fixed and clear from the context, we omit the subscript and abbreviate  $v_{CD}^i(r)$  to  $v_i(r)$ .

**Proposition 3.5.** *Using the above notation, we have, for  $j \geq 0$  and  $n = qk + r$*

$$x_{S_j(n)+i}(n) = v_{\Gamma_j(r)+i}(r) \quad \text{for } 0 \leq i \leq \gamma_{2j+1}(r)$$

*Proof.* We use induction on  $j$ .

When  $j = 0$ ,  $S_0(n) = \Gamma_0(r) = 0$ . We need to show  $x_i(n) = v_i(r)$  for  $i \in [0, \gamma_1(r)]$ . As we saw in the proof of Lemma 3.3,

$$x_0(n) = \left\langle \frac{D}{q} \right\rangle = v_0(r), \quad x_{-1}(n) = 1 - \frac{C}{q} = v_{-1}(r).$$

Since  $a_0(n) - \gamma_0(r) \in q\mathbb{Z}$ , using (3-4) and the recursive relation of  $v_i(r)$ , one can easily check that

$$x_1(n) = \left\langle (a_0(n) + 2) \left\langle \frac{D}{q} \right\rangle + \frac{C}{q} \right\rangle = \langle (\gamma_0(r) + 2)v_0(r) - v_{-1}(r) \rangle = v_1(r).$$

For  $1 \leq i \leq \gamma_1(r) - 1$ ,  $x_i(n)$  and  $v_i(r)$  satisfy the same recursion relation

$$x_{i+1}(n) = \langle 2x_i(n) - x_{i-1}(n) \rangle, \quad v_{i+1}(r) = \langle 2v_i(r) - v_{i-1}(r) \rangle.$$

Thus we have  $x_i(n) = v_i(r)$  for  $0 \leq i \leq \gamma_1(r)$ .

Now assume that the proposition holds true for  $j < j_0$ . From Proposition 3.4, we find that if  $a_{2j_0-1}(n) \geq q$  then

$$x_{S_{j_0-1}(n)+q+i}(n) = x_{S_{j_0-1}(n)+i}(n) \text{ for } 0 \leq i \leq a_{2j_0-1}(n) - q. \tag{3-12}$$

Since  $a_{2j_0-1}(n) - \gamma_{2j_0-1}(r) \in q\mathbb{Z}$ , we obtain

$$\begin{aligned} x_{S_{j_0}(n)-1}(n) &= x_{S_{j_0-1}(n)+a_{2j_0-1}(n)-1}(n) = x_{S_{j_0-1}(n)+\gamma_{2j_0-1}(r)-1}(n) \\ &= v_{\Gamma_{j_0-1}(r)+\gamma_{2j_0-1}(r)-1}(r) = v_{\Gamma_{j_0}(r)-1}(r) \end{aligned}$$

and

$$\begin{aligned} x_{S_{j_0}(n)}(n) &= x_{S_{j_0-1}(n)+a_{2j_0-1}(n)}(n) \\ &= x_{S_{j_0-1}(n)+\gamma_{2j_0-1}(r)}(n) = v_{\Gamma_{j_0-1}(r)+\gamma_{2j_0-1}(r)}(r) = v_{\Gamma_{j_0}(r)}(r). \end{aligned}$$

Moreover from (3-4), we find that

$$\begin{aligned} x_{S_{j_0}(n)+1}(n) &= \langle (a_{2j_0}(n) + 2)x_{S_{j_0}(n)}(n) - x_{S_{j_0}(n)-1}(n) \rangle \\ &= \langle (\gamma_{2j_0}(r) + 2)v_{\Gamma_{j_0}(r)}(r) - v_{\Gamma_{j_0}(r)-1}(r) \rangle = v_{\Gamma_{j_0}(r)+1}(r). \end{aligned}$$

Since

$$x_{i+1}(n) = \langle 2x_i(n) - x_{i-1}(n) \rangle \text{ for } S_{j_0}(n) + 1 \leq i \leq S_{j_0+1}(n) - 1$$

and

$$v_{i+1}(r) = \langle 2v_i(r) - v_{i-1}(r) \rangle$$

for  $\Gamma_{j_0}(r) + 1 \leq i \leq \Gamma_{j_0}(r) + \gamma_{2j_0+1}(r) - 1 = \Gamma_{j_0+1}(r) - 1$ , we have

$$x_{S_{j_0}(n)+i}(n) = v_{\Gamma_{j_0}(r)+i}(r) \text{ for } 0 \leq i \leq \gamma_{2j_0+1}(r). \quad \square$$

**Summations.** Next we express (3-11), that is,

$$\sum_{i=1}^{m(n)} -B_1(x_{C+D\delta(n)}^i)B_1(x_{C+D\delta(n)}^{i-1}) + \frac{b_i(n)}{2}B_2(x_{C+D\delta(n)}^i)$$

in terms of  $\{v_{CD}^i(r)\}$ .

**Lemma 3.6.** *Let  $d_l(r) := \langle v_{\Gamma_l(r)+1}(r) - v_{\Gamma_l(r)}(r) \rangle$  and  $[x]_1 := x - \langle x \rangle$ . Then for  $1 \leq \gamma \leq q$  and  $n$  such that  $\gamma \leq a_{2l+1}(n)$  and  $n = qk + r$ , we have*

$$\sum_{i=S_l(n)+1}^{S_l(n)+\gamma} (x_i(n) - x_{i-1}(n))^2 = \gamma d_l(r)^2 + (1 - 2d_l(r))[v_{\Gamma_l(r)}(r) + d_l(r)\gamma]_1$$

*Proof.* Since  $0 < x_i(n) \leq 1$ , we have

$$-1 < x_i(n) - x_{i-1}(n) < 1.$$

Thus

$$x_i(n) - x_{i-1}(n) = \langle x_i(n) - x_{i-1}(n) \rangle + \psi_i(n),$$

where

$$\psi_i(n) = \begin{cases} -1 & \text{if } x_i(n) \leq x_{i-1}(n), \\ 0 & \text{if } x_i(n) > x_{i-1}(n). \end{cases}$$

Since

$$\langle x_{i+1}(n) - x_i(n) \rangle = \langle \langle 2x_i(n) - x_{i-1}(n) \rangle - x_i(n) \rangle = \langle x_i(n) - x_{i-1}(n) \rangle$$

for  $S_l(n) + 1 \leq i \leq S_{l+1}(n) - 1$ , we have

$$\langle x_i(n) - x_{i-1}(n) \rangle = \langle x_{S_l(n)+1}(n) - x_{S_l(n)}(n) \rangle = \langle v_{\Gamma_l(r)+1}(r) - v_{\Gamma_l(r)}(r) \rangle = d_l(r).$$

Hence we have

$$x_i(n) - x_{i-1}(n) = d_l(r) + \psi_i(n).$$

Thus we obtain

$$\sum_{i=S_l(n)+1}^{S_l(n)+\gamma} (x_i(n) - x_{i-1}(n))^2 = \gamma d_l(r)^2 + (1 - 2d_l(r)) \sum_{i=S_l(n)+1}^{S_l(n)+\gamma} \psi_i(n)^2.$$

Note that the sum on the right equals the number of  $i$ 's satisfying  $x_i(n) \leq x_{i-1}(n)$  for  $S_l(n) + 1 \leq i \leq S_l(n) + \gamma$ .

Therefore

$$\sum_{i=S_l(n)+1}^{S_l(n)+\gamma} \psi_i(n)^2 = [x_{S_l(n)}(n) + d_l(r)\gamma]_1 = [v_{\Gamma_l(r)}(r) + d_l(r)\gamma]_1. \quad \square$$

For simplicity, we let

$$F(x, y) := -B_1(x)B_1(y) + B_2(x) = \left(x - \frac{1}{2}\right)\left(\frac{1}{2} - y\right) + x^2 - x + \frac{1}{6}.$$

**Lemma 3.7.** *If  $l \geq 0$  and  $a_{2l+1}(n) \geq q$ , then*

$$\sum_{i=S_l(n)+1}^{S_l(n)+q} F(x_i(n), x_{i-1}(n)) = \frac{1}{12} [6(qd_l(r)^2 + (1 - 2d_l(r))[v_{\Gamma_l(r)}(r) + d_l(r)q]_1) - q].$$

And if  $1 \leq \gamma \leq q - 1$  and  $a_{2l+1}(n) \geq \gamma$ ,

$$\sum_{i=S_l(n)+1}^{S_l(n)+\gamma} F(x_i(n), x_{i-1}(n)) = \frac{1}{12} [6(\gamma d_l(r)^2 + (1 - 2d_l(r))[v_{\Gamma_l(r)}(r) + d_l(r)\gamma]_1 + B_2(x_{S_l(n)+\gamma}(n)) - B_2(x_{S_l(n)}(n))) - \gamma],$$

where  $B_2(x)$  is the second Bernoulli polynomial.

*Proof.* We note that

$$F(x, y) = \frac{1}{2}(x - y)^2 - \frac{1}{12} + \frac{1}{2}(B_2(x) - B_2(y)).$$

Thus

$$\begin{aligned} & \sum_{i=S_l(n)+1}^{S_l(n)+\gamma} F(x_i(n), x_{i-1}(n)) \\ &= \sum_{i=S_l(n)+1}^{S_l(n)+\gamma} \left[ \frac{1}{2}(x_i(n) - x_{i-1}(n))^2 - \frac{1}{12} + \frac{1}{2}(B_2(x_i(n)) - B_2(x_{i-1}(n))) \right]. \end{aligned}$$

We note that for  $1 \leq \gamma \leq q - 1$ ,

$$\sum_{i=S_l(n)+1}^{S_l(n)+\gamma} B_2(x_i(n)) - B_2(x_{i-1}(n)) = B_2(x_{S_l(n)+\gamma}(n)) - B_2(x_{S_l(n)}(n)).$$

and, from the periodicity of  $x_i(n)$ , we have that for  $\gamma = q$

$$\sum_{i=S_l(n)+1}^{S_l(n)+q} B_2(x_i(n)) - B_2(x_{i-1}(n)) = 0. \quad \square$$

**Proposition 3.8.** *Suppose  $\delta(n) - 1 = \llbracket a_0(n), a_2(n), \dots, a_{s-1}(n) \rrbracket$ ,  $a_i(n) = \alpha_i n + \beta_i$  for  $\alpha_i, \beta_i \in \mathbb{Z}$  and  $a_i(r) = q\tau_i(r) + \gamma_i(r)$  for  $\gamma_i(r) = \langle a_i(r) \rangle_q$ . Let  $d_{CD}^l(r) := \langle v_{CD}^{\Gamma_l(r)+1}(r) - v_{CD}^{\Gamma_l(r)}(r) \rangle$ . Then, for  $n = qk + r$ , we have*

$$\sum_{i=1}^{m(n)} -B_1(x_{C+D\delta(n)}^i) B_1(y_{C+D\delta(n)}^i) + \frac{b_i(n)}{2} B_2(x_{C+D\delta(n)}^i) = \frac{1}{12} (A_{CD}(r) + kB_{CD}(r)),$$

where

$$\begin{aligned}
 A_{CD}(r) &:= \sum_{l=1}^{s\mu(s)} -12B_1(v_{CD}^{\Gamma_l(r)}(r))B_1(v_{CD}^{\Gamma_l(r)-1}(r)) + 6(a_{2l}(r) + 2)B_2(v_{CD}^{\Gamma_l(r)}(r)) \\
 &+ \sum_{l=0}^{s\mu(s)-1} \left[ 6\left( (\gamma_{2l+1}(r) - 1)d_{CD}^l(r)^2 \right. \right. \\
 &\quad \left. \left. + (1 - 2d_{CD}^l(r))[v_{CD}^{\Gamma_l(r)}(r) + d_{CD}^l(r)(\gamma_{2l+1}(r) - 1)]_1 \right. \right. \\
 &\quad \left. \left. + B_2(v_{CD}^{\Gamma_{l+1}(r)-1}(r)) - B_2(v_{CD}^{\Gamma_l(r)}(r)) \right) - \gamma_{2l+1}(r) + 1 \right. \\
 &\quad \left. + \tau_{2l+1}(r)(6(qd_{CD}^l(r)^2 + (1 - 2d_{CD}^l(r))[v_{CD}^{\Gamma_l(r)}(r) + d_{CD}^l(r)q]_1) - q) \right]
 \end{aligned}$$

and

$$\begin{aligned}
 B_{CD}(r) &:= \sum_{l=1}^{s\mu(s)} 6q\alpha_{2l}B_2(v_{CD}^{\Gamma_l(r)}(r)) \\
 &+ \sum_{l=0}^{s\mu(s)-1} \alpha_{2l+1}(6(qd_{CD}^l(r)^2 + (1 - 2d_{CD}^l(r))[v_{CD}^{\Gamma_l(r)}(r) + d_{CD}^l(r)q]_1) - q).
 \end{aligned}$$

*Proof.* From (3-7), we have

$$\begin{aligned}
 &\sum_{i=1}^{m(n)} B_1(x_{C+D\delta(n)}^i)B_1(y_{C+D\delta(n)}^i) + \frac{b_i(n)}{2}B_2(x_{C+D\delta(n)}^i) \\
 &= \sum_{l=1}^{s\mu(s)} \left( -B_1(x_{C+D\delta(n)}^{S_l(n)})B_1(x_{C+D\delta(n)}^{S_l(n)-1}) + \frac{\alpha_{2l}qk + \tau_{2l}(r)q + \gamma_{2l}(r) + 2}{2}B_2(x_{C+D\delta(n)}^{S_l(n)}) \right) \\
 &\quad + \sum_{l=0}^{s\mu(s)-1} \sum_{i=S_l(n)+1}^{S_l(n)+q\alpha_{2l+1}k + q\tau_{2l+1}(r) + \gamma_{2l+1}(r) - 1} F(x_{C+D\delta(n)}^i, x_{C+D\delta(n)}^{i-1}).
 \end{aligned}$$

From Lemma 3.7, we have

$$\begin{aligned}
 &12 \sum_{i=S_l(n)+1}^{S_l(n)+q\alpha_{2l+1}k + q\tau_{2l+1}(r) + \gamma_{2l+1}(r) - 1} F(x_{C+D\delta(n)}^i, x_{C+D\delta(n)}^{i-1}) \\
 &= 12 \sum_{i=S_l(n)+1}^{S_l(n)+\gamma_{2l+1}(r) - 1} F(x_{C+D\delta(n)}^i, x_{C+D\delta(n)}^{i-1}) \\
 &\quad + 12(\alpha_{2l+1}k + \tau_{2l+1}(r)) \sum_{i=S_l(n)+1}^{S_l(n)+q} F(x_{C+D\delta(n)}^i, x_{C+D\delta(n)}^{i-1})
 \end{aligned}$$



$$\begin{aligned}
 &= 6 \left( (\gamma_{2l+1}(r) - 1) d_{CD}^l(r)^2 + (1 - 2d_{CD}^l(r)) [v_{CD}^{\Gamma_l(r)}(r) + d_{CD}^l(r)(\gamma_{2l+1}(r) - 1)]_1 \right. \\
 &\quad \left. + B_2(x_{C+D\delta(n)}^{S_l(n)+\gamma_{2l+1}-1}) - B_2(x_{C+D\delta(n)}^{S_l(n)}) \right) - (\gamma_{2l+1}(r) - 1) \\
 &\quad + (\alpha_{2l+1}k + \tau_{2l+1}(r)) (6(qd_{CD}^l(r)^2 + (1 - 2d_{CD}^l(r)) [v_{CD}^{\Gamma_l(r)}(r) + d_{CD}^l(r)q]_1) - q).
 \end{aligned}$$

Since

$$x_{C+D\delta(n)}^{S_l(n)} = v_{CD}^{\Gamma_l(r)}(r), \quad x_{C+D\delta(n)}^{S_l(n)-1} = v_{CD}^{\Gamma_l(r)-1}(r), \quad \text{and} \quad x_{C+D\delta(n)}^{S_l(n)+\gamma_{2l+1}(r)-1} = v_{CD}^{\Gamma_{l+1}(r)-1},$$

we complete the proof.  $\square$

*End of the proof.* Since  $v_{CD}^{\Gamma_l(r)}(r)$ ,  $v_{CD}^{\Gamma_l(r)-1}(r)$  and  $d_{CD}^l(r)$  are in  $\frac{1}{q}\mathbb{Z}$ , we find that

$$q^2 A_{CD}(r), q^2 B_{CD}(r) \in \mathbb{Z}.$$

Moreover, we have

$$L_{K_n}(0, \chi_n, \mathfrak{b}_n) = \frac{1}{12q^2} \sum_{C,D} \chi_n(C + D\delta(n)) (q^2 A_{CD}(r) + kq^2 B_{CD}(r)).$$

Since  $\chi$  is a Dirichlet character of modulus  $q$ , if  $n = qk + r$ , we can write

$$\chi_n(\mathfrak{b}_n(C + D\delta(n))) = F_{CD}(r)$$

for a function  $F_{CD}$ . Note that, if  $K_r$  is defined,

$$\chi_n(\mathfrak{b}_n(C + D\delta(n))) = \chi_r(\mathfrak{b}_r(C + D\delta(r))) = F_{CD}(r).$$

(This expression does not make sense if  $K_r$  and  $\delta(r)$  are undefined.)

If we set

$$A_\chi(r) := \sum_{C,D} F_{CD}(r) q^2 A_{CD}(r)$$

and

$$B_\chi(r) := \sum_{C,D} F_{CD}(r) q^2 B_{CD}(r),$$

we obtain the proof.  $\square$

#### 4. Biró's method

Let  $K_n$  be a family of real quadratic fields such that the special value of the Hecke  $L$ -function at  $s = 0$  has linearity. Biró [Biró 2003a; 2003b] developed a method using linearity to find the residue of  $n$  such that  $h(K_n) = 1$  by certain primes. In this section, we sketch Biró's method.

Let  $K_n = \mathbb{Q}(\sqrt{d})$  for a square free integer  $d = f(n)$  and  $D_n$  be the discriminant  $K_n$ . For an odd Dirichlet character  $\chi : \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{C}^*$ , let  $\chi_n$  denote the ray class

character defined as  $\chi_n = \chi \circ N_{K_n} : I_n(q)/P_n(q)^+ \rightarrow \mathbb{C}^*$ , and let  $\chi_D = (\frac{D}{\cdot})$  denote the Kronecker character. Then the special value of the Hecke  $L$ -function at  $s = 0$  has a factorization

$$L_{K_n}(0, \chi_n) = L(0, \chi)L(0, \chi\chi_{D_n}) = \left(\frac{1}{q} \sum_{a=1}^q a\chi(a)\right) \left(\frac{1}{qD_n} \sum_{b=1}^{qD_n} b\chi(b)\chi_{D_n}(b)\right).$$

Let  $\mathfrak{b}_n = \mathcal{O}_{K_n}$ . Suppose that  $L_{K_n}(0, \chi_n, \mathfrak{b}_n)$  is linear in the form

$$L_{K_n}(0, \chi_n, \mathfrak{b}_n) = \frac{1}{12q^2}(A_\chi(r) + kB_\chi(r))$$

for  $A_\chi(r), B_\chi(r) \in \mathbb{Z}[\chi(1), \chi(2) \cdots \chi(q)]$ . Let  $\epsilon_n$  be the fundamental unit of  $K_n$ . From Proposition 2.2 in [Byeon and Lee 2011], we find that  $L_{K_n}(0, \chi_n, \mathfrak{b}_n) = L_{K_n}(0, \chi_n, (\epsilon_n)\mathfrak{b}_n)$ . Thus if the class number of  $K_n$  is one, then we have for  $n = qk + r$

$$L_{K_n}(0, \chi_n) = \frac{c}{12q^2}(A_\chi(r) + kB_\chi(r))$$

where  $c$  is the number of narrow ideal classes.

Then we have

$$B_\chi(r)k + A_\chi(r) = \frac{12q}{c} \cdot \left(\sum_{a=1}^q a\chi(a)\right) \cdot \left(\frac{1}{qD_n} \sum_{b=1}^{qD_n} b\chi(b)\chi_{D_n}(b)\right).$$

Let  $L_\chi$  be the cyclotomic field generated by the values of  $\chi$ . Since

$$\frac{1}{qD_n} \sum_{b=1}^{qD_n} b\chi(b)\chi_{D_n}(b)$$

is integral in  $L_\chi$ , for a prime ideal  $I$  of  $L_\chi$  dividing  $\sum_{a=1}^q a\chi(a)$ , we have

$$B_\chi(r)k + A_\chi(r) \equiv 0 \pmod{I}.$$

And if  $I$  does not divide  $B_\chi(r)$ , then

$$k \equiv -\frac{A_\chi(r)}{B_\chi(r)} \pmod{I}.$$

Since  $n = qk + r$ , we have

$$n \equiv -q\frac{A_\chi(r)}{B_\chi(r)} + r \pmod{I}.$$

Moreover, if  $\mathcal{O}_{L_\chi}/I = \mathbb{Z}/p\mathbb{Z}$ , the residue of  $n$  modulo  $p$  is expressed only in terms of  $A_\chi(r), B_\chi(r)$ , and  $r$  as above.

We now list the necessary conditions on  $q$  and  $p$ :

**Condition (\*)**.  $q$  is an odd integer;  $p$  is an odd prime;  $\chi$  is a character with conductor  $q$ ;  $I$  is prime ideal in  $L_\chi$  lying over  $p$ , with  $I | (\sum_{a=1}^q a\chi(a))$  and  $O_{L_\chi}/I = \mathbb{Z}/p\mathbb{Z}$ .

When linearity holds, these conditions are independent of the family  $\{K_n\}$ .

Let  $S$  be the set of  $(q, p)$  satisfying Condition (\*). We partition  $S$  as follows:

$$S = \bigcup_{q \text{ odd integer}} S_q, \quad \text{where } S_q := \{(q, p) \in S\}.$$

Finally, for  $(q, p) \in S$ , we obtain the residue of  $n = qk + r$  modulo  $p$  for which the class number of  $K_n$  is 1.

The above method has been used to find an upper bound on the discriminant of real quadratic fields with class number 1 in some families of Richaud–Degerter type where the linearity criterion is satisfied [Biró 2003a; 2003b; Byeon et al. 2007; Lee 2009a]. This information, together with a properly developed class number one criteria for each case, could be used to solve the class number problems.

It is easily checked that the criterion is fulfilled by general families of Richaud–Degerter type. Furthermore, there are abundant examples of families of real quadratic fields satisfying the linearity criterion [McLaughlin 2003]. For these, we have controlled behavior of the special values of the Hecke  $L$ -function at  $s = 0$ , and Biro’s method is directly applicable in each case. We expect this method can be used to study many meaningful arithmetic problems for families of real quadratic fields, in addition to the class number problem.

### 5. A generalization

We conclude with a possible generalization of the linearity of the special value of the Hecke  $L$ -function. This generalization will be dealt in [Jun and Lee 2012].

As in the criterion for linearity, we set  $K_n = \mathbb{Q}(\sqrt{f(n)})$  and let  $\mathfrak{b}_n$  an integral ideal of  $K_n$ . We assume  $\mathfrak{b}_n^{-1} = [1, \delta(n)]$  for  $\delta(n) - 1 = [a_1(n), a_2(n), \dots, a_s(n)]$ , with  $a_i(x) \in \mathbb{Z}[x]$ .

For a given conductor  $q$ , write  $n = qk + r$  for  $r = 0, 1, 2, \dots, q - 1$ . Suppose  $N = \max_i \{\deg(a_i(x))\}$ . Then the special value of the partial  $\zeta$ -function of the ray class of  $\mathfrak{b}_n \pmod q$  at  $s = 0$  can be written as

$$\zeta_{K_n, q}(0, (C + D\delta(n))\mathfrak{b}_n) = \frac{1}{12q^2} (A_0(r) + A_1(r)k + \dots + A_N(r)k^N)$$

for some rational integers  $A_i$  depending only on  $r$ .

We have no application of this property in arithmetic, but it will be very interesting if one applies it in a similar fashion as Biró’s method.

### Acknowledgment

We would like to thank Prof. Dongho Byeon for helpful comments and discussions. We also thank the anonymous referee for careful reading and many invaluable suggestions. The first named author wishes to thank Prof. Bumsig Kim and Prof. Soon-Yi Kang for warm support and encouragement.

### References

- [Biró 2003a] A. Biró, “Chowla’s conjecture”, *Acta Arith.* **107**:2 (2003), 179–194. MR 2004a:11113 Zbl 1154.11339
- [Biró 2003b] A. Biró, “Yokoi’s conjecture”, *Acta Arith.* **106**:1 (2003), 85–104. MR 2003k:11162 Zbl 1154.11338
- [Byeon and Lee 2008] D. Byeon and J. Lee, “Class number 2 problem for certain real quadratic fields of Richaud–Degert type”, *J. Number Theory* **128**:4 (2008), 865–883. MR 2009a:11222 Zbl 1167.11036
- [Byeon and Lee 2011] D. Byeon and J. Lee, “A complete determination of Rabinowitsch polynomials”, *J. Number Theory* **131**:8 (2011), 1513–1529. MR 2012d:11210 Zbl 05899192
- [Byeon et al. 2007] D. Byeon, M. Kim, and J. Lee, “Mollin’s conjecture”, *Acta Arith.* **126**:2 (2007), 99–114. MR 2007j:11155 Zbl 1125.11059
- [van der Geer 1988] G. van der Geer, *Hilbert modular surfaces*, *Ergebnisse der Math.* (3) **16**, Springer, Berlin, 1988. MR 89c:11073 Zbl 0634.14022
- [Jun and Lee 2012] B. Jun and J. Lee, “Polynomial behavior of special values of partial zeta functions of real quadratic fields at  $s = 0$ ”, *Selecta Math. (N.S.)* (2012).
- [Lee 2009a] J. Lee, “The complete determination of wide Richaud–Degert types which are not 5 modulo 8 with class number one”, *Acta Arith.* **140**:1 (2009), 1–29. MR 2010j:11159 Zbl 05643768
- [Lee 2009b] J. Lee, “The complete determination of narrow Richaud–Degert type which is not 5 modulo 8 with class number two”, *J. Number Theory* **129**:3 (2009), 604–620. MR 2009k:11175 Zbl 1206.11135
- [McLaughlin 2003] J. McLaughlin, “Polynomial solutions of Pell’s equation and fundamental units in real quadratic fields”, *J. London Math. Soc.* (2) **67**:1 (2003), 16–28. MR 2004d:11017 Zbl 0846.11060
- [Shintani 1976] T. Shintani, “On evaluation of zeta functions of totally real algebraic number fields at non-positive integers”, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **23**:2 (1976), 393–417. MR 55 #266 Zbl 0349.12007
- [Yamamoto 2008] S. Yamamoto, “On Kronecker limit formulas for real quadratic fields”, *J. Number Theory* **128**:2 (2008), 426–450. MR 2009a:11233 Zbl 1185.11071
- [Zagier 1975] D. Zagier, “A Kronecker limit formula for real quadratic fields”, *Math. Ann.* **213** (1975), 153–184. MR 51 #3123 Zbl 0283.12004

Communicated by Andrew Granville

Received 2010-03-07    Revised 2011-03-24    Accepted 2011-05-08

byunghuep@gmail.com

*School of Mathematics, Korea Institute for Advanced Study,  
Hoegiro 87, Dongdaemun-gu, Seoul 130-722, South Korea*

lee9311@kias.re.kr

*School of Mathematics, Korea Institute for Advanced Study,  
Hoegiro 87, Dongdaemun-gu, Seoul 130-722, South Korea*

# The Picard group of a $K3$ surface and its reduction modulo $p$

Andreas-Stephan Elsenhans and Jörg Jahnel

We present a method to compute the geometric Picard rank of a  $K3$  surface over  $\mathbb{Q}$ . Contrary to a widely held belief, we show that it is possible to verify Picard rank 1 using reduction at a single prime.

## 1. Introduction

**1.1.** For complex, projective  $K3$  surfaces, the Picard group is a highly interesting invariant. In general, it is isomorphic to  $\mathbb{Z}^n$  for some  $n = 1, \dots, 20$ . A generic  $K3$  surface has Picard rank 1. Nevertheless, the first explicit examples of  $K3$  surfaces over  $\mathbb{Q}$  having geometric Picard rank 1 were constructed by R. van Luijk [2007] as late as 2004. Van Luijk's method is based on reduction modulo  $p$ . It works as follows.

**Approach 1.2** (van Luijk). Let  $S$  be a  $K3$  surface over  $\mathbb{Q}$ .

- (i) At a place  $p$  of good reduction, the Picard group  $\text{Pic}(S_{\overline{\mathbb{Q}}})$  of the surface injects into the Picard group  $\text{Pic}(S_{\overline{\mathbb{F}}_p})$  of its reduction modulo  $p$ .
- (ii) On its part, the group  $\text{Pic}(S_{\overline{\mathbb{F}}_p})$  injects into the second étale cohomology group  $H_{\text{ét}}^2(S_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l(1))$ .
- (iii) Only roots of unity can arise as eigenvalues of the Frobenius Frob on the image of  $\text{Pic}(S_{\overline{\mathbb{F}}_p})$  in  $H_{\text{ét}}^2(S_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l(1))$ . The number of eigenvalues of this form, counted with multiplicities, is therefore an upper bound for the Picard rank of  $S_{\overline{\mathbb{F}}_p}$ . One may compute the eigenvalues of Frob by counting the points on  $S$ , defined over  $\mathbb{F}_p$  and some finite extensions.

Doing this for one prime, one obtains an upper bound for  $\text{rk Pic}(S_{\overline{\mathbb{F}}_p})$ , which is always even. The Tate conjecture asserts that this bound is actually sharp.

---

Esenhans was supported in part by the Deutsche Forschungsgemeinschaft (DFG) through a funded research project.

*MSC2010:* primary 14C22; secondary 14D15, 14J28, 14Q10.

*Keywords:*  $K3$  surface, Picard group, Picard scheme, deformation, Artin approximation, Van Luijk's method.

Therefore, the best that could happen is to find a prime  $p$  that yields an upper bound of 2 for the rank of  $\text{Pic}(S_{\overline{\mathbb{Q}}})$ .

- (iv) In this case, the assumption that the surface has Picard rank 2 over  $\overline{\mathbb{Q}}$  implies that the discriminants of both Picard groups,  $\text{Pic}(S_{\overline{\mathbb{Q}}})$  and  $\text{Pic}(S_{\overline{\mathbb{F}}_p})$ , belong to the same square class. Note here that reduction modulo  $p$  respects the intersection pairing.
- (v) To obtain a contradiction, one combines information from two primes. It may happen that one has a rank bound of 2 at both places but that different square classes arise for the discriminants. Then, these data are incompatible with Picard rank 2 over  $\overline{\mathbb{Q}}$ . Geometric Picard rank 1 is proven.

**1.3. The improvement.** The idea behind Approach 1.2 is to consider the specialization  $\text{sp} : \text{Pic}(S_{\overline{\mathbb{Q}}}) \hookrightarrow \text{Pic}(S_{\overline{\mathbb{F}}_p})$  as an injection of lattices. Then, the two possibilities  $\text{rk Pic}(S_{\overline{\mathbb{Q}}}) < \text{rk Pic}(S_{\overline{\mathbb{F}}_p})$  and  $\text{rk Pic}(S_{\overline{\mathbb{Q}}}) = \text{rk Pic}(S_{\overline{\mathbb{F}}_p})$  are distinguished. In the latter, the standard fact is used that  $\text{disc Pic}(S_{\overline{\mathbb{Q}}}) / \text{disc Pic}(S_{\overline{\mathbb{F}}_p})$  is a perfect square.

We will show in this article that the assertion for the second case may be refined to  $\text{disc Pic}(S_{\overline{\mathbb{Q}}}) = \text{disc Pic}(S_{\overline{\mathbb{F}}_p})$ . More precisely, we shall prove that, at least for  $p \neq 2$ , the cokernel of  $\text{sp} : \text{Pic}(S_{\overline{\mathbb{Q}}}) \hookrightarrow \text{Pic}(S_{\overline{\mathbb{F}}_p})$  is always torsion-free. This is true actually in a by-far more general situation than just for  $K3$  surfaces.

**Theorem 1.4.** *Let  $R$  be a discrete valuation ring with quotient field  $K$  of characteristic 0 and residue field  $k$  of characteristic  $p > 0$ . Further, let  $\pi : X \rightarrow \text{Spec } R$  be a morphism of schemes that is proper and smooth.*

*Suppose that  $R$  is of ramification degree  $e < p - 1$  and that  $k$  is perfect. Then, the cokernel of the specialization homomorphism  $\text{sp}_{\overline{k}} : \text{Pic}(X_{\overline{k}}) \rightarrow \text{Pic}(X_{\overline{k}})$  is torsion-free.*

**Remarks 1.5.** (a) In the applications, we will have  $R = \mathbb{Z}_{(p)} \subset \mathbb{Q}$ . Then, the assumption simply means  $p \neq 2$ .

- (b) We will show this theorem in Section 3. As an application, one may prove  $\text{rk Pic}(S_{\overline{\mathbb{Q}}}) = 1$  for a  $K3$  surface  $S$  using its reduction at a single prime. This works as follows.

**Approach 1.6.** Let a  $K3$  surface  $S$  over  $\mathbb{Q}$  be given.

- (i) For a prime  $p \neq 2$  of good reduction, perform steps (i), (ii) and (iii) as in Approach 1.2. Thereby, the hope is to prove  $\text{rk Pic}(S_{\overline{\mathbb{F}}_p}) = 2$ . Further, compute the discriminant giving two explicit generators.

Alternatively, to determine the discriminant, one might use the Artin–Tate formula [Milne 1975]. In this case,  $\text{rk Pic}(S_{\overline{\mathbb{F}}_p}) = 2$  is shown only relative to the Tate conjecture. Observe, however, that a surface with  $\text{rk Pic}(S_{\overline{\mathbb{F}}_p}) = 1$ , due to a failure of the Tate conjecture, would serve our purposes as well.

- (ii) Assume  $\text{rk Pic}(S_{\overline{\mathbb{Q}}}) = 2$ . Then, according to Theorem 1.4, every invertible sheaf on  $S_{\overline{\mathbb{F}}_p}$  must lift to  $S_{\overline{\mathbb{Q}}}$ . Estimate the degree of a hypothetical effective divisor. Finally, use Gröbner bases to verify that such a divisor does not exist.

**Example 1.7.** Consider the K3 surface  $S$  over  $\mathbb{Q}$  given by

$$w^2 = x^5y + x^4y^2 + 2x^3y^3 + x^2y^4 + xy^5 + 4y^6 + 2x^5z + 2x^4z^2 + 4x^3z^3 + 2xz^5 + 4z^6.$$

Then,  $\text{rk Pic}(S_{\overline{\mathbb{Q}}}) = 1$ .

*Proof.* For the reduction of  $S$  at the prime 5, one sees that the branch locus has a tritangent line given by  $z - 2y = 0$ . It meets the branch locus at  $(1 : 0 : 0)$ ,  $(1 : 3 : 1)$ , and  $(0 : 1 : 2)$ .

The numbers of points on  $S$  over  $\mathbb{F}_{5^d}$  are, in this order, 41, 751, 15 626, 392 251, 9 759 376, 244 134 376, 6 103 312 501, 152 589 156 251, 3 814 704 296 876, and 95 367 474 609 376. Thus, the traces of Frob on  $H_{\text{ét}}^2(S_{\overline{\mathbb{F}}_5}, \overline{\mathbb{Q}}_l)$  are 15, 125, 0, 1 625,  $-6 250$ ,  $-6 250$ ,  $-203 125$ , 1 265 625, 7 031 250, and 42 968 750.

Elsenhans and Jahnel [2008a, Algorithm 23] show that the sign in the functional equation is positive. The characteristic polynomial of Frob is therefore completely determined. For its decomposition into prime polynomials, we find (after Tate twist to  $H_{\text{ét}}^2(S_{\overline{\mathbb{F}}_5}, \overline{\mathbb{Q}}_l(1))$ )

$$\begin{aligned} \frac{1}{5}(t - 1)^2(5t^{20} - 5t^{19} - 5t^{18} + 10t^{17} - 2t^{16} - 3t^{15} + 4t^{14} - 2t^{13} - 2t^{12} + t^{11} \\ + 3t^{10} + t^9 - 2t^8 - 2t^7 + 4t^6 - 3t^5 - 2t^4 + 10t^3 - 5t^2 - 5t + 5). \end{aligned}$$

This shows  $\text{rk Pic}(S_{\overline{\mathbb{F}}_5}) \leq 2$ .

The irreducible components of the pull-back of the tritangent line are explicit generators for  $\text{Pic}(S_{\overline{\mathbb{F}}_5})$ . Such a component  $l$ , because it is a projective line, has self-intersection number  $l^2 = -2$ . Further,  $lh = 1$  for  $h$  the pull-back of a line. If we had  $\text{rk Pic}(S_{\overline{\mathbb{Q}}}) = 2$ , then the invertible sheaf  $\mathcal{O}(l)$  would lift to  $S_{\overline{\mathbb{Q}}}$ . We would have a divisor  $L$  on  $S_{\overline{\mathbb{Q}}}$  such that  $HL = 1$  and  $L^2 = -2$ . By [Barth et al. 1984, Proposition VIII.3.6.i], such a divisor is automatically effective.

The equation  $HL = 1$  shows that  $L$  is obtained from a line on  $\mathbf{P}^2$ , the pull-back of which splits into two components. This is possible only for a line tritangent to the branch locus. Algorithm 8 of [Elsenhans and Jahnel 2008a] shows, however, using Gröbner bases, that such a tritangent line does not exist. □

## 2. The cokernel of the restriction map

**Notation 2.1.** (i) Let  $R$  be a discrete valuation ring of unequal characteristic. We will write  $K := \text{Quot}(R)$  for its quotient field,  $\mathfrak{p}$  for the maximal ideal,  $k := R/\mathfrak{p}$  for the residue field of characteristic  $p$ , and  $v : K \rightarrow \mathbb{Z}$  for the normalized valuation. Let  $e := v(p)$  denote the ramification degree of  $R$ .

- (ii) Let  $X$  be an  $R$ -scheme. Then, we will write  $X_{\mathfrak{p}}$  for the special fiber and  $X_{\eta}$  for the generic fiber of  $X$ . For  $L$  an extension of  $K$ , we will denote by  $X_L$  the base extension of  $X_{\eta}$  to  $L$ . Analogously, for  $l$  an extension of  $k$ , we will write  $X_l$  for the base extension of  $X_{\mathfrak{p}}$  to  $l$ . In the particular case that  $l = \mathbb{F}_q$ , the shortcut  $X_q$  shall be used for  $X_l$ .

**Proposition 2.2.** *Let  $\pi : X \rightarrow \text{Spec } R$  be a morphism of schemes that is proper and flat. Suppose that the special fiber  $X_{\mathfrak{p}}$  is normal.*

*If  $R$  is complete and satisfies the condition  $e < p - 1$ , then the cokernel of the restriction homomorphism  $\text{Pic}(X) \rightarrow \text{Pic}(X_{\mathfrak{p}})$  is torsion-free.*

*Proof.* This result was obtained by M. Raynaud in the course of his investigations on the Picard scheme [Raynaud 1979, Théorème 4.1.2.1]. □

**Remark 2.3.** Assume, also, that the restriction homomorphism  $H^1(X, \mathbb{C}_X) \rightarrow H^1(X_{\mathfrak{p}}, \mathbb{C}_{X_{\mathfrak{p}}})$  is surjective. Then, the assertion of Proposition 2.2 may be established using the following elementary argument, which is also due to M. Raynaud [1979, section 1].

Consider the functors  $T^i$  on the category of all finitely generated  $R$ -modules to finitely generated  $R$ -modules, given by  $T^i(M) := H^i(X, \pi^* \tilde{M})$ . Here,  $\tilde{M}$  denotes the coherent sheaf associated with the  $R$ -module  $M$ . According to [Grothendieck 1963, Proposition (7.7.10), p. 71], the functor  $T^1$  is right exact. Hence, by [ibid., Théorème (7.7.5.II), p. 68],  $T^2$  is left exact. This, in turn, immediately implies that  $H^2(X, \mathbb{C}_X)$  is torsion-free.

Further, the short exact sequence

$$0 \rightarrow \mathcal{U}_1 \rightarrow \mathbb{C}_X^* \rightarrow \mathbb{C}_{X_{\mathfrak{p}}}^* \rightarrow 0$$

shows that  $\text{coker}(\text{Pic}(X) \rightarrow \text{Pic}(X_{\mathfrak{p}}))$  injects into  $H^2(X, \mathcal{U}_1)$ . Finally, as  $e < p - 1$ , the exponential map provides us with an isomorphism

$$\mathbb{C}_X \xrightarrow{\cdot p} p\mathbb{C}_X \xrightarrow{\exp} \mathcal{U}_1.$$

**Remarks 2.4.** (i) The additional assumption of 2.3 is fulfilled in our applications.

- (ii) For prime-to- $p$  torsion, the assertion of Proposition 2.2 is true in a more general situation.

**Proposition 2.5.** *Let  $\pi : X \rightarrow \text{Spec } R$  be a proper morphism of schemes.*

*If  $R$  is Henselian, then the cokernel of the restriction homomorphism*

$$\text{Pic}(X) \rightarrow \text{Pic}(X_{\mathfrak{p}})$$

*has no prime-to- $p$  torsion.*



*Proof.* Let  $l \neq p$  be a prime number. We will show that there is no  $l$ -torsion. For this, we observe at first that, according to a consequence of the theorem on proper base change [Artin et al. 1973, Exp. XII, Corollaire 5.5.iii], the restriction morphism induces bijections

$$H_{\text{ét}}^1(X, \mu_l) \xrightarrow{\cong} H_{\text{ét}}^1(X_p, \mu_l) \quad \text{and} \quad H_{\text{ét}}^2(X, \mu_l) \xrightarrow{\cong} H_{\text{ét}}^2(X_p, \mu_l).$$

Because [Berthelot et al. 1971, Exp. X, diagramme (7.13.10)] the restriction homomorphisms on the Picard groups and étale cohomology commute with the Chern maps, we see that restriction induces a surjection  $\text{Pic}(X)_l \twoheadrightarrow \text{Pic}(X_p)_l$  and an injection  $\text{Pic}(X)/l \hookrightarrow \text{Pic}(X_p)/l$ .

Applied to the two commutative diagrams of short exact sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Pic}(X)_l & \longrightarrow & \text{Pic}(X) & \longrightarrow & P_X \longrightarrow 0 \\ & & \downarrow \twoheadrightarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Pic}(X_p)_l & \longrightarrow & \text{Pic}(X_p) & \longrightarrow & P_{X_p} \longrightarrow 0, \\ \\ 0 & \longrightarrow & P_X & \xrightarrow{\cdot l} & \text{Pic}(X) & \longrightarrow & \text{Pic}(X)/l \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \hookrightarrow \\ 0 & \longrightarrow & P_{X_p} & \xrightarrow{\cdot l} & \text{Pic}(X_p) & \longrightarrow & \text{Pic}(X_p)/l \longrightarrow 0, \end{array}$$

the snake lemma now shows that the induced homomorphism

$$\text{coker}(\text{Pic}(X) \rightarrow \text{Pic}(X_p)) \rightarrow \text{coker}(P_X \rightarrow P_{X_p})$$

is a bijection, while

$$\text{coker}(P_X \rightarrow P_{X_p}) \xrightarrow{\cdot l} \text{coker}(\text{Pic}(X) \rightarrow \text{Pic}(X_p))$$

is injective. Consequently,  $\text{coker}(\text{Pic}(X) \rightarrow \text{Pic}(X_p))$  has no  $l$ -torsion. □

### 3. The cokernel of the specialization map

**3.1.** In this section, we continue to use the notation from 2.1. Let  $\pi : X \rightarrow \text{Spec } R$  be a morphism of schemes that is proper and smooth. We have the restriction homomorphisms

$$\text{Pic}(X_\eta) \leftarrow \text{Pic}(X) \rightarrow \text{Pic}(X_p).$$

As  $\pi$  is smooth, the arrow to the left is a bijection [Berthelot et al. 1971, Exp. X, App. 7.8]. Consequently, there is a natural homomorphism  $\text{sp} : \text{Pic}(X_\eta) \rightarrow \text{Pic}(X_p)$ , which is called the *specialization*.

**Lemma 3.2.** *Let  $\pi : X \rightarrow \text{Spec } R$  be a morphism of schemes that is proper and smooth.*

*If  $R$  is complete and satisfies the condition  $e < p - 1$ , then the cokernel of the specialization homomorphism  $\text{sp} : \text{Pic}(X_\eta) \rightarrow \text{Pic}(X_{\mathfrak{p}})$  is torsion-free.*

*Proof.* The assertion follows directly from Proposition 2.2. □

**3.3.** Let  $K'/K$  be an extension field equipped with a discrete valuation extending that on  $K$ . Denote by  $R'$  the discrete valuation ring and by  $k'$  the residue field. The morphism  $X \times_{\text{Spec } R} \text{Spec } R' \rightarrow \text{Spec } R'$ , obtained by base change, induces a specialization homomorphism  $\text{sp}_{K'} : \text{Pic}(X_{K'}) \rightarrow \text{Pic}(X_{k'})$ .

There are the following two applications.

- (i) Suppose  $R$  to be complete. Then, for every finite extension  $K'/K$ , there is a unique [Serre 1968, Chap. II, §2, Proposition 3] discrete valuation extending the valuation on  $K$ . The direct limit of the homomorphisms  $\text{sp}_{K'} : \text{Pic}(X_{K'}) \rightarrow \text{Pic}(X_{k'})$  is a natural homomorphism  $\text{sp}_{\bar{K}} : \text{Pic}(X_{\bar{K}}) \rightarrow \text{Pic}(X_{\bar{k}})$ , again called the specialization.
- (ii) For general  $R$ , fix an embedding  $\bar{K} \hookrightarrow \widehat{\bar{K}}$  of the algebraic closure of  $K$  into that of its completion. By functoriality, this embedding induces a homomorphism  $\text{Pic}(X_{\bar{K}}) \rightarrow \text{Pic}(X_{\widehat{\bar{K}}})$ . Composing with  $\text{sp}_{\widehat{\bar{K}}}$ , constructed in (i), one has a specialization homomorphism  $\text{sp}_{\bar{K}} : \text{Pic}(X_{\bar{K}}) \rightarrow \text{Pic}(X_{\bar{k}})$ .

**Proposition 3.4.** *Let  $\pi : X \rightarrow \text{Spec } R$  be a morphism of schemes that is proper and smooth.*

*Suppose  $R$  is complete and satisfies the condition  $e < p - 1$ , and let  $k$  be perfect. Then, the cokernel of the specialization homomorphism  $\text{sp}_{\bar{K}} : \text{Pic}(X_{\bar{K}}) \rightarrow \text{Pic}(X_{\bar{k}})$  is torsion-free.*

*Proof.* By [Serre 1968, Chap. III, §5, Corollaire 1 du Théorème 3],  $K$  has a unique maximal unramified extension  $K^{\text{nr}}$ , which is actually the filtered direct limit of all finite unramified extensions  $K'/K$ .

An unramified extension does not change the ramification degree. Hence, by Lemma 3.2, the homomorphisms  $\text{sp}_{K'} : \text{Pic}(X_{K'}) \rightarrow \text{Pic}(X_{k'})$  have torsion-free cokernels. As the filtered direct limit is an exact functor, the same is true for  $\text{sp}_{K^{\text{nr}}} : \text{Pic}(X_{K^{\text{nr}}}) \rightarrow \text{Pic}(X_{\bar{k}})$ .

We claim that the specialization homomorphism  $\text{sp}_{\bar{K}}$  has the same image in  $\text{Pic}(X_{\bar{k}})$  as  $\text{sp}_{K^{\text{nr}}}$ . For this, let  $\mathcal{L} \in \text{Pic}(X_{\bar{K}})$ . The inertia group  $I := \text{Gal}(\bar{K}/K^{\text{nr}})$  sends  $\mathcal{L}$  to a finite orbit  $\{\mathcal{L}_1, \dots, \mathcal{L}_m\}$ . The specializations of  $\mathcal{L}_1, \dots, \mathcal{L}_m$  in  $\text{Pic}(X_{\bar{k}})$  are all the same. Therefore,

$$m \cdot \text{sp}_{\bar{K}}(\mathcal{L}) = \text{sp}_{\bar{K}}(\mathcal{L}^{\otimes m}) = \text{sp}_{\bar{K}}(\mathcal{L}_1 \otimes \dots \otimes \mathcal{L}_m) = \text{sp}_{K^{\text{nr}}}(\mathcal{L}_1 \otimes \dots \otimes \mathcal{L}_m),$$

since  $\mathcal{L}_1 \otimes \cdots \otimes \mathcal{L}_m$  is  $I$ -invariant. Hence,  $m \cdot \text{sp}_{\bar{K}}(\mathcal{L}) \in \text{im } \text{sp}_{K^{\text{nr}}}$ . As  $\text{sp}_{K^{\text{nr}}}$  has a torsion-free cokernel, we see that  $\text{sp}_{\bar{K}}(\mathcal{L}) \in \text{im } \text{sp}_{K^{\text{nr}}}$ , too. □

**Remark 3.5.** The argument above uses that  $\text{Pic}(X_L) = \text{Pic}(X_K)^{\text{Gal}(L/K)}$ . This equality is certainly not correct, in general. It is true as soon as  $Y(K) \neq \emptyset$  for every connected component  $Y$  of  $X$ .

As  $\pi$  is smooth, we indeed have  $Y(K^{\text{nr}}) \neq \emptyset$ . To see this, let  $s : \text{Spec } l \rightarrow Y_k$  be a point defined over a finite extension. By [Grothendieck 1967, Proposition (17.5.3), p. 68],  $s$  may be lifted to a morphism  $\text{Spf } S \rightarrow Y$  for  $S$  the corresponding unramified extension of  $R$ . Then [Grothendieck 1961, Théorème (5.4.1), p. 156] yields the desired point.

**Theorem 3.6.** *Let  $R$  be a discrete valuation ring with quotient field  $K$  of characteristic 0 and residue field  $k$  of characteristic  $p > 0$ . Further, let  $\pi : X \rightarrow \text{Spec } R$  be a morphism of schemes that is proper and smooth.*

*Suppose that  $R$  is of ramification degree  $e < p - 1$  and that  $k$  is perfect. Then, the cokernel of the specialization homomorphism  $\text{sp}_{\bar{K}} : \text{Pic}(X_{\bar{K}}) \rightarrow \text{Pic}(X_{\bar{k}})$  is torsion-free.*

**Corollary 3.7.** *Let  $p \neq 2$  be a prime number and  $X$  be a scheme proper and flat over  $\mathbb{Z}$ . Suppose that the special fiber  $X_p$  is nonsingular.*

*Then, the cokernel of the specialization homomorphism*

$$\text{sp}_{\bar{\mathbb{Q}}} : \text{Pic}(X_{\bar{\mathbb{Q}}}) \rightarrow \text{Pic}(X_{\bar{\mathbb{F}}_p})$$

*is torsion-free.*

**Remark 3.8.** The technical condition on the ramification degree cannot be omitted. In fact, D. Maulik and B. Poonen [2010, Example 3.12] constructed counterexamples to the assertion of Theorem 3.6 in the situation that  $e \geq p - 1$ .

**Remarks 3.9** (elementary reductions). (i) Let  $R'$  be a discrete valuation ring, finite and flat over  $R$ . Then, the assertion for  $\text{pr}_2 : X \times_{\text{Spec } R} \text{Spec } R' \rightarrow \text{Spec } R'$ , obtained by base-change, implies that for  $\pi$ .

(ii) In particular, we may suppose that  $\pi : X \rightarrow \text{Spec } R$  has a section.

(iii) We may suppose that the fibers of  $\pi$  are geometrically connected.

Indeed, as  $\pi : X \rightarrow \text{Spec } R$  is proper and smooth, one has  $\pi_* \mathcal{O}_X = \tilde{S}$  for  $S$  a finite étale  $R$ -algebra [Grothendieck 1963, Remarque (7.8.10.i), p. 75]. Hence, there exists a discrete valuation ring  $R'$ , étale over  $R$ , such that  $S \otimes_R R'$  is a direct product of finitely many copies of  $R'$ . This means that the connected components of  $X \times_{\text{Spec } R} \text{Spec } R'$  have geometrically connected fibers. Knowing the assertion for each component separately, the proof will be complete.

**Proposition 3.10.** *Let  $R$  be a discrete valuation ring of characteristic 0 and let  $\pi : X \rightarrow \text{Spec } R$  be a proper and smooth morphism of schemes. Suppose that  $\pi$  has a section and that the fibers of  $\pi$  are geometrically connected.*

*Then, the specialization homomorphisms*

$$\text{sp}_{\bar{K}} : \text{Pic}(X_{\bar{K}}) \rightarrow \text{Pic}(X_{\bar{k}}) \quad \text{and} \quad \text{sp}_{\bar{K}} : \text{Pic}(X_{\bar{K}}) \rightarrow \text{Pic}(X_{\bar{k}})$$

*have the same image.*

*Proof.* As  $\text{sp}_{\bar{K}}$  factors via  $\text{sp}_{\bar{K}}$ , we clearly have  $\text{im } \text{sp}_{\bar{K}} \subseteq \text{im } \text{sp}_{\bar{K}}$ . We will show the reverse inclusion in several steps. Let an invertible sheaf  $\mathcal{L} \in \text{Pic}(X_{\bar{K}})$  be given. We have to construct an invertible sheaf  $\mathcal{L}' \in \text{Pic}(X_{\bar{K}})$  having the same specialization as  $\mathcal{L}$ .

*First step (the Picard scheme).* Our assumptions on  $\pi$  imply that it is cohomologically flat in dimension zero [Grothendieck 1963, Proposition (7.8.6), p. 74]. Hence, by [Artin 1969b, Theorem 7.3], the Picard functor  $\text{Pic}_{X/R}$  is representable by an algebraic space  $P := \mathbf{Pic}_{X/R}$  that is locally of finite type over  $R$ . According to [Grothendieck 1962, Exp. 236, Théorème 2.1.i],  $P$  is separated. This is enough to ensure that  $P$  is actually a scheme [Raynaud 1970, Théorème (3.3.1)]. Further, every closed subset  $Z \subseteq P$ , being of finite type, is proper over  $R$ .

*Second step (the representing morphism).* The invertible sheaf  $\mathcal{L} \in \text{Pic}(X_{\bar{K}})$  is defined over a finite extension  $L$  of  $\hat{K}$ . Hence, it defines a morphism  $i : \text{Spec } L \rightarrow P$ . As  $\hat{K}$  is complete, there is a unique prolongation to  $L$  of the discrete valuation on  $\hat{K}$ . That is, we have a discrete valuation ring  $S \supseteq \hat{R}$ . There is a unique continuation  $j : \text{Spec } S \rightarrow P$  of  $i$ .

*Third step (Artin approximation).* By Lemma 3.12, we have  $S = \hat{S}$  for a discrete valuation ring  $\underline{S}$ , finite over  $R$ . Write  $\underline{L}$  for the quotient field of  $\underline{S}$ . This is a finite extension of  $K$ .

We now recall that discrete valuation rings of characteristic zero are excellent [Grothendieck 1965, Scholie (7.8.3.iii), p. 214]. In particular, Artin’s approximation results [1969a] are applicable. According to [1969a, Corollary (2.5)], there are an étale extension  $S'$  of  $\underline{S}$  and a morphism  $j' : \text{Spec } S' \rightarrow P$  of schemes that coincides, up to extensions of the base field, with  $j$  on the special fiber.

Corresponding to  $j'$ , there is some  $\xi \in \text{Pic}_{X/R}(\text{Spec } S')$ .

*Fourth step (an invertible sheaf).* As the fibers of  $X$  are geometrically connected, we have  $\pi_* \mathcal{O}_X = \mathcal{O}_{\text{Spec } R}$ . Further, since  $\pi$  has a section, one has [Grothendieck 1962, Exp. 232, Proposition 2.1]

$$\text{Pic}_{X/R}(T) = \text{Pic}(X \times_{\text{Spec } R} T) / \text{Pic}(T)$$

for every  $R$ -scheme  $T$ . In particular,

$$\begin{aligned} \text{Pic}_{X/R}(\text{Spec } S') &= \text{Pic}(X \times_{\text{Spec } R} \text{Spec } S') / \text{Pic}(\text{Spec } S') \\ &= \text{Pic}(X \times_{\text{Spec } R} \text{Spec } S'). \end{aligned}$$

Hence,  $\xi$  defines an invertible sheaf on  $X \times_{\text{Spec } R} \text{Spec } S'$ . Let  $\mathcal{L}' \in \text{Pic}(X_{\underline{L}})$  be its restriction to the generic fiber. Then, by construction,  $\mathcal{L}'$  has the same specialization as  $\mathcal{L}$ . The assertion follows. □

**Remark 3.11.** Suppose that  $H^1(X, \mathbb{O}_X) = 0$ . Then, Proposition 3.10 is significantly more elementary. In fact, the Picard scheme  $P_K$  is of dimension zero [Grothendieck 1962, Exp. 236, Proposition 2.10.iii] in this case. Hence, every point on  $P_K$  is defined over  $\bar{K}$ . No approximation argument is necessary.

Actually, the assumption  $H^1(X, \mathbb{O}_X) = 0$  is fulfilled in the examples, discussed in 1.7 and below in Section 4.

**Lemma 3.12.** *Let  $R$  be a discrete valuation ring with quotient field  $K$  of characteristic zero and  $L/\widehat{K}$  a finite field extension of its completion.*

*Then, there exists a subfield  $\underline{L} \subset L$ , finite over  $K$ , such that  $\widehat{\underline{L}} = L$ .*

*Proof.* Choose a primitive element  $x$  of  $L$  over  $\widehat{K}$  and let  $f \in \widehat{K}[X]$  be its minimal polynomial. Then, the assertion is an immediate consequence of [Serre 1968, Chapitre II, §2, Exercice 2]. □

**3.13. Proof of Theorem 3.6.** Consider the completion  $\widehat{R}$  of  $R$  and denote by  $\widehat{K}$  the corresponding quotient field. The ramification degree of  $\widehat{K}$  is the same as that of  $R$ . Therefore, Proposition 3.4 shows that the specialization homomorphism  $\text{sp}_{\widehat{K}}: \text{Pic}(X_{\widehat{K}}) \rightarrow \text{Pic}(X_{\bar{k}})$  has a torsion-free cokernel. Further, by Proposition 3.10,  $\text{sp}_{\widehat{K}}$  has the same image in  $\text{Pic}(X_{\bar{k}})$  as  $\text{sp}_{\bar{K}}$ . This implies the assertion. □

#### 4. The obstruction to first order deformations

The obstructions to lifting invertible sheaves were essential for the elementary proof of Proposition 2.2, as discussed in 2.3. In some cases, they can be made explicit.

**Proposition 4.1.** *Let  $S$  be a K3 surface of degree 2 over  $\mathbb{Q}$ , given explicitly by*

$$w^2 = f_6(x, y, z)$$

*for  $f_6 \in \mathbb{Z}[x, y, z]$  of degree 6. Suppose, for a prime  $p \neq 2$  of good reduction, there is an  $\mathbb{F}_p$ -rational line “ $\ell = 0$ ”, tritangent to the ramification locus of  $S_p$ . Write  $l$  for an irreducible component of the pull-back of the tritangent.*

*One has  $f_6 \equiv f_3^2 + \ell f_5 \pmod{p}$  for homogeneous forms  $f_3, f_5 \in \mathbb{Z}[x, y, z]$ . Put*

$$G(x, y, z) := (f_6 - f_3^2 - \ell f_5) / p.$$

Then,  $\mathcal{O}(l)$  lifts to  $S_{p^2}$  if and only if  $G$  vanishes in  $\mathbb{F}_p[x, y, z]/(\ell, f_3, f_5)$ .

*Proof.* Suppose that  $\mathcal{O}(l)$  has a lift  $\mathcal{L} \in \text{Pic}(X_{p^2})$ . Then,  $\mathcal{L}/p\mathcal{L} \cong \mathcal{O}(l)$ . Since multiplication by  $p$  induces an isomorphism  $\mathcal{L}/p\mathcal{L} \cong p\mathcal{L}$ , we automatically have a short exact sequence

$$0 \rightarrow \mathcal{O}(l) \rightarrow \mathcal{L} \rightarrow \mathcal{O}(l) \rightarrow 0.$$

As  $H^1(X_p, \mathcal{O}(l)) = 0$ , the restriction map  $H^0(X_{p^2}, \mathcal{L}) \rightarrow H^0(X_p, \mathcal{O}(l))$  is a surjection. That is, the divisor  $l$  on  $X_p$  necessarily lifts to an effective Cartier divisor on  $X_{p^2}$ .

This is possible only when the line defined by  $\ell$  may be lifted to  $\mathbf{P}_{p^2}^2$  in such a way that it is still a tritangent. On the other hand, if  $\ell$  may be lifted to  $\mathbf{P}_{p^2}^2$  such that it is still a tritangent, then clearly  $\mathcal{O}(l)$  lifts to  $X_{p^2}$ .

Explicitly, the condition means that  $f_6$  is a square modulo  $p^2$  and some lift of  $\ell$ . Writing

$$f_6 \equiv (f_3 + pf'_3)^2 + (\ell + p\ell')(f_5 + pf'_5) \pmod{p^2},$$

one immediately sees that this is equivalent to the assertion that  $G$  vanishes in  $\mathbb{F}_p[x, y, z]/(\ell, f_3, f_5)$ . □

**Remark 4.2.** There is another proof that consists of the determination of the cohomological obstruction to lifting  $\mathcal{O}(l)$ , that is, of the image of  $\mathcal{O}(l)$  under the connecting homomorphism  $d : \text{Pic}(X_p) \rightarrow H^2(X_p, \mathcal{O}_{X_p})$  that is induced by the short exact sequence

$$0 \rightarrow \mathcal{O}_{X_p} \rightarrow \mathcal{O}_{X_{p^2}}^* \rightarrow \mathcal{O}_{X_p}^* \rightarrow 0.$$

The obstruction may easily be computed in Čech cohomology for a suitable affine open covering of  $X_{p^2}$ . Via the corresponding isomorphism  $H^2(X_p, \mathcal{O}_{X_p}) \cong \mathbb{F}_p$ , our result is indeed  $((-G) \pmod{(p, \ell, f_3, f_5)})$ . The necessary calculations are, however, rather lengthy and shall not be reproduced here.

**4.3.** In the examples below, we will use the obstruction in its explicit form, as given in Proposition 4.1. The methods for point counting, which we apply, are explained in some detail in [Elsenhans and Jahnel 2008a; 2008b; 2010].

**Example 4.4.** Let  $S$  be a  $K3$  surface over  $\mathbb{Q}$  given by  $w^2 = f_6(x, y, z)$ . Suppose

$$\begin{aligned} f_6(x, y, z) \equiv & x^6 + 2x^5z + 2x^4y^2 + 2x^4z^2 + 2x^3y^3 + 2x^3z^3 \\ & + 2x^2y^4 + 2x^2y^3z + x^2z^4 + xy^3z^2 + 2xz^5 + y^6 \pmod{3}. \end{aligned}$$

Assume further that the coefficient of  $y^2z^4$  is not divisible by 9.

Then,  $\text{rk Pic}(S_{\overline{\mathbb{Q}}}) = 1$ .

*Proof.* A direct calculation shows that, modulo 3, the right hand side is  $f_3^2 + xf_5$  for  $f_3 = 2x^3 + 2x^2z + xz^2 + 2y^3$  and  $f_5 = 2x^3y^2 + x^2z^3 + 2xy^4 + 2z^5$ . Thus, the branch locus of  $S_3$  has a tritangent line given by  $x = 0$ .

The numbers of points over  $\mathbb{F}_{3^d}$  are, in this order, 19, 127, 676, 6751, 58564, 532414, 4791232, 43038703, 387383311, and 3486675052. For the decomposition of the characteristic polynomial of the Frobenius on  $H_{\text{ét}}^2(S_{\mathbb{F}_3}, \mathbb{Q}_l(1))$ , we find

$$\begin{aligned} \frac{1}{3}(t-1)^2(3t^{20} - 3t^{19} - 3t^{18} + 8t^{17} - 3t^{16} - 4t^{15} + 6t^{14} - 4t^{13} + 2t^{12} + 4t^{11} \\ - 7t^{10} + 4t^9 + 2t^8 - 4t^7 + 6t^6 - 4t^5 - 3t^4 + 8t^3 - 3t^2 - 3t + 3). \end{aligned}$$

This shows  $\text{rk Pic}(S_{\mathbb{F}_3}) \leq 2$ .

Let  $l$  be an irreducible component of the pull-back of the tritangent line. We have to show that the obstruction to lifting  $\mathbb{C}(l)$  is nonzero. For this, we observe that  $x$ ,  $f_3$ , and  $f_5$  do not generate the monomial  $y^2z^4$ . However,  $G$  contains this monomial by its very definition.  $\square$

**Example 4.5.** Consider the  $K3$  surface  $S$  over  $\mathbb{Q}$ , given by  $w^2 = f_6(x, y, z)$  for

$$\begin{aligned} f_6(x, y, z) = 4x^6 + 2x^5y + 12x^5z + 2x^4y^2 + 4x^4yz + 12x^4z^2 + 24x^3y^3 - 57x^3y^2z \\ - 9x^3yz^2 + 6x^3z^3 + 8x^2y^4 - 5x^2y^3z - 72x^2y^2z^2 + 7x^2yz^3 \\ + 4x^2z^4 + 20xy^4z - 52xy^3z^2 - 57xy^2z^3 + 7xyz^4 + 4y^5z \\ - 7y^4z^2 - 18y^3z^3 + 7y^2z^4 + 12yz^5 + 2z^6. \end{aligned}$$

Then,  $\text{rk Pic}(S_{\mathbb{Q}}) = 3$ .

*Proof.* We have

$$\begin{aligned} f_6 = (2x^3 + 2x^2z + 2y^2z + yz^2 + z^3)^2 \\ + (2x^2 + 2xz + yz + z^2)(x^3y + 2x^3z + x^2y^2 + x^2yz + 2x^2z^2 + 12xy^3 \\ - 34xy^2z - 9xyz^2 - 2xz^3 + 4y^4 - 15y^3z - 7y^2z^2 + 9yz^3 + z^4) \end{aligned}$$

and

$$\begin{aligned} f_6 = 4(x^3 + 2x^2y + 2x^2z + xy^2 + xyz + xz^2 + y^2z + yz^2 + z^3)^2 \\ - (x^2 + xz + yz + z^2)(14x^3y + 4x^3z + 22x^2y^2 + 22x^2yz + 8x^2z^2 - 8xy^3 \\ + 61xy^2z + 9xyz^2 + 6xz^3 - 4y^4 + 15y^3z + 11y^2z^2 - 6yz^3 + 2z^4). \end{aligned}$$

Hence, there are two conics  $C_1$  and  $C_2$ , each of which is six times tangent to the ramification locus of  $S$ . The irreducible components of their pull-backs yield the

intersection matrix

$$\begin{pmatrix} -2 & 6 & 1 & 3 \\ 6 & -2 & 3 & 1 \\ 1 & 3 & -2 & 6 \\ 3 & 1 & 6 & -2 \end{pmatrix},$$

which is of rank 3. Hence,  $\text{rk Pic}(S_{\overline{\mathbb{Q}}}) \geq 3$ .

On the other hand,  $S$  has good reduction at the prime  $p = 3$ . Point counting over extensions of  $\mathbb{F}_3$  shows that the characteristic polynomial of the Frobenius operating on  $H_{\text{ét}}^2(S_{\overline{\mathbb{F}_3}}, \mathbb{Q}_l(1))$  is

$$\begin{aligned} \frac{1}{3}(t-1)^4(3t^{18} + 3t^{17} + 2t^{16} + 2t^{15} + 4t^{14} + 5t^{13} + 4t^{12} + 3t^{11} + 6t^{10} + 8t^9 \\ + 6t^8 + 3t^7 + 4t^6 + 5t^5 + 4t^4 + 2t^3 + 2t^2 + 3t + 3). \end{aligned}$$

Consequently, we have  $\text{rk Pic}(S_{\overline{\mathbb{F}_3}}) \leq 4$ .

In particular, the assumption  $\text{rk Pic}(S_{\overline{\mathbb{Q}}}) > 3$  implies  $\text{rk Pic}(S_{\overline{\mathbb{Q}}}) = \text{rk Pic}(S_{\overline{\mathbb{F}_3}})$ . Theorem 3.6 guarantees that the specialization map  $\text{sp}_{\overline{\mathbb{Q}}} : \text{Pic}(S_{\overline{\mathbb{Q}}}) \rightarrow \text{Pic}(S_{\overline{\mathbb{F}_3}})$  must be bijective. Giving one invertible sheaf  $\mathcal{L} \in \text{Pic}(S_{\overline{\mathbb{F}_3}})$  with a nontrivial obstruction will be enough to yield a contradiction.

For this, observe that the ramification locus of  $S_3$  has a tritangent line given by  $x + y + z = 0$ . Indeed,

$$\begin{aligned} f_6(x, y, z) \equiv (x^3 + x^2y + xy^2 + y^3)^2 + (x + y + z)(2x^3y^2 + x^3yz + 2x^2yz^2 + 2xy^4 \\ + xy^3z + xy^2z^2 + 2xyz^3 + xz^4 + 2y^5 + 2y^4z + yz^4 + 2z^5) \pmod{3}. \end{aligned}$$

Modulo the ideal  $(3, x + y + z)$ , we have

$$\begin{aligned} f_3 \equiv x^3 + x^2y + xy^2 + y^3, \\ f_5 \equiv -(x^5 + x^3y^2 + x^2y^3 + xy^4 + y^5), \quad G \equiv x^6 + 2x^5y + x^4y^2 + 2xy^5 + y^6. \end{aligned}$$

Trying to generate  $G$  by  $3, x + y + z, f_3,$  and  $f_5$  now leads to a system of seven linear equations in six unknowns that is easily seen to be unsolvable.  $\square$

**Remarks 4.6.** (i) It is not at all hard to generate more examples similar to 1.7 and 4.4. Choosing the coefficients in  $\mathbb{F}_p$  at random, one usually finds Picard rank 2 over  $\overline{\mathbb{F}_p}$  after a few trials. One may work with small primes, only, say  $p \leq 7$ .

Clearly, for our arguments, it is of importance to have explicit generators for  $\text{Pic}(S_{\overline{\mathbb{F}_p}})$ . In practice, it turns out that a second generator may often be found. We have no formal reason for this. However, [Kovács 1994] might give an indication.

In Example 4.4, we applied a linear transform in order to make the obstruction depend only on a single coefficient. In general, one would have a linear form in the coefficients.



(ii) Example 4.5 is a bit more particular. Both conics, which are six times tangent to the ramification sextic, simultaneously lift to  $\mathbb{Q}$ . This is not at all the generic behavior.

(iii) It seems to be substantially more difficult to construct examples for which  $\text{rk Pic}(X) \leq \text{rk Pic}(X_p) - 2$  may be shown. To understand the problem, recall the obstruction homomorphism  $\delta : \text{Pic}(X_p) \rightarrow H^2(X, \mathbb{O}_X)$ , introduced in Remark 2.3. In Proposition 4.1, we calculated  $\delta(\mathbb{O}(l))$  at a precision of one  $p$ -adic digit.

In order to verify  $\text{rk Pic}(X) \leq \text{rk Pic}(X_p) - 2$ , one would have to ensure that  $\text{rk}_{\mathbb{Z}}(\text{im } \delta) \geq 2$ . This, however, is impossible as long as only  $p$ -adic approximations of finitely many values  $\delta(\mathcal{L})$  are known.

There are methods known to show

$$\text{rk Pic}(X) \leq \text{rk Pic}(X_{p_1}) - 2 \quad \text{and} \quad \text{rk Pic}(X) \leq \text{rk Pic}(X_{p_2}) - 2$$

when one works with two primes [Elsenhans and Jahnel 2011].

## References

- [Artin 1969a] M. Artin, “Algebraic approximation of structures over complete local rings”, *Inst. Hautes Études Sci. Publ. Math.* 36 (1969), 23–58. MR 42 #3087 Zbl 0181.48802
- [Artin 1969b] M. Artin, “Algebraization of formal moduli, I”, pp. 21–71 in *Global Analysis: Papers in Honor of K. Kodaira*, Univ. Tokyo Press, Tokyo, 1969. MR 41 #5369 Zbl 0205.50402
- [Artin et al. 1973] M. Artin, A. Grothendieck, and J. L. Verdier (editors), *Théorie des topos et cohomologie étale des schémas, Tome 3*, Lecture Notes in Mathematics **305**, Springer, Berlin, 1973. MR 50 #7132 Zbl an:0245.00002
- [Barth et al. 1984] W. Barth, C. Peters, and A. Van de Ven, *Compact complex surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **4**, Springer, Berlin, 1984. MR 86c:32026 Zbl 0718.14023
- [Berthelot et al. 1971] P. Berthelot, A. Grothendieck, and L. Illusie (editors), *Théorie des intersections et théorème de Riemann–Roch (SGA 6)*, Lecture Notes in Mathematics **225**, Springer, Berlin, 1971. MR 50 #7133 Zbl 0218.14001
- [Elsenhans and Jahnel 2008a] A.-S. Elsenhans and J. Jahnel, “ $K3$  surfaces of Picard rank one and degree two”, pp. 212–225 in *Algorithmic number theory*, edited by A. J. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011**, Springer, Berlin, 2008. MR 2010h:11102 Zbl 1205.11073
- [Elsenhans and Jahnel 2008b] A.-S. Elsenhans and J. Jahnel, “ $K3$  surfaces of Picard rank one which are double covers of the projective plane”, pp. 63–77 in *Higher-dimensional geometry over finite fields*, edited by D. Kaledin and Y. Tschinkel, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. **16**, IOS, Amsterdam, 2008. MR 2009j:14047 Zbl 1182.14036
- [Elsenhans and Jahnel 2010] A.-S. Elsenhans and J. Jahnel, “On Weil polynomials of  $K3$  surfaces”, pp. 126–141 in *Algorithmic number theory*, edited by G. Hanrot et al., Lecture Notes in Comput. Sci. **6197**, Springer, Berlin, 2010. MR 2011m:11130 Zbl 05793676
- [Elsenhans and Jahnel 2011] A.-S. Elsenhans and J. Jahnel, “On the computation of the Picard group for  $K3$  surfaces”, *Math. Proc. Cambridge Philos. Soc.* **151**:2 (2011), 263–270. MR 2823134 Zbl 1223.14044

- [Grothendieck 1961] A. Grothendieck, *Étude cohomologique des faisceaux cohérents, I (EGA III)*, Inst. Hautes Études Sci. Publ. Math. **11**, 1961. MR 29 #1209 Zbl 0118.36206
- [Grothendieck 1962] A. Grothendieck, *Fondements de la géométrie algébrique: Extraits du Séminaire Bourbaki, 1957–1962*, Secrétariat mathématique, Paris, 1962. MR 26 #3566 Zbl 0239.14002
- [Grothendieck 1963] A. Grothendieck, *Étude cohomologique des faisceaux cohérents, II (EGA III)*, Inst. Hautes Études Sci. Publ. Math. **17**, 1963. MR 29 #1210 Zbl 0122.16102
- [Grothendieck 1965] A. Grothendieck, *Étude locale des schémas et des morphismes de schémas, II (EGA IV)*, Publications Mathématiques **24**, Institut des Hautes Études Scientifiques, Paris, 1965. MR 33 #7330 Zbl 0135.39701
- [Grothendieck 1967] A. Grothendieck, *Étude locale des schémas et des morphismes de schémas, IV (EGA IV)*, Publications Mathématiques **32**, Institut des Hautes Études Scientifiques, Paris, 1967. MR 39 #220 Zbl 0153.22301
- [Kovács 1994] S. J. Kovács, “The cone of curves of a  $K3$  surface”, *Math. Ann.* **300**:4 (1994), 681–691. MR 96a:14044 Zbl 0813.14026
- [van Luijk 2007] R. van Luijk, “ $K3$  surfaces with Picard number one and infinitely many rational points”, *Algebra Number Theory* **1**:1 (2007), 1–15. MR 2008d:14058 Zbl 1123.14022
- [Maulik and Poonen 2010] D. Maulik and B. Poonen, “Néron–Severi groups under specialization”, preprint, version 3, 2010. arXiv 0907.4781v3
- [Milne 1975] J. S. Milne, “On a conjecture of Artin and Tate”, *Ann. of Math. (2)* **102**:3 (1975), 517–533. MR 54 #2659 Zbl 0343.14005
- [Raynaud 1970] M. Raynaud, “Spécialisation du foncteur de Picard”, *Inst. Hautes Études Sci. Publ. Math.* **38** (1970), 27–76. MR 44 #227 Zbl 0207.51602
- [Raynaud 1979] M. Raynaud, “‘ $p$ -torsion’ du schéma de Picard”, pp. 87–148 in *Journées de Géométrie Algébrique de Rennes* (Rennes, 1978), vol. 2, Astérisque **64**, Soc. Math. France, Paris, 1979. MR 81f:14026 Zbl 0434.14024
- [Serre 1968] J.-P. Serre, *Corps locaux*, 2nd ed., Publications de l’Université de Nancago **8**, Hermann, Paris, 1968. MR 50 #7096

Communicated by János Kollár

Received 2010-03-31    Revised 2011-03-01    Accepted 2011-04-01

stephan.elsenhans@uni-bayreuth.de

*Mathematisches Institut, Universität Bayreuth,  
Universitätsstraße 30, D-95440 Bayreuth, Germany  
<http://www.staff.uni-bayreuth.de/~btm216>*

jahnel@mathematik.uni-siegen.de

*Fachbereich 6 Mathematik, Universität Siegen,  
Walter-Flex-Straße 3, D-57068 Siegen, Germany  
<http://www.uni-math.gwdg.de/jahnel>*

# Linear determinantal equations for all projective schemes

Jessica Sidman and Gregory G. Smith

We prove that every projective embedding of a connected scheme determined by the complete linear series of a sufficiently ample line bundle is defined by the  $2 \times 2$  minors of a 1-generic matrix of linear forms. Extending the work of Eisenbud, Koh and Stillman for integral curves, we also provide effective descriptions for such determinantly presented ample line bundles on products of projective spaces, Gorenstein toric varieties, and smooth varieties.

## 1. Introduction

Relating the geometric properties of a variety to the structural features of its defining equations is a fundamental challenge in algebraic geometry. Describing generators for the homogeneous ideal associated to a projective scheme is a basic form of this problem. For a rational normal curve, a Segre variety, or a quadratic Veronese variety, the homogeneous ideal is conveniently expressed as the 2-minors (that is, the determinants of all  $2 \times 2$  submatrices) of a generic Hankel matrix, a generic matrix, or a generic symmetric matrix respectively. These determinantal representations lead to a description of the minimal graded free resolution of the homogeneous ideal of the variety and equations for higher secant varieties. Mumford's "somewhat startling observation" [Mumford 1970, p. 31] is that a suitable multiple of every projective embedding is the intersection of a quadratic Veronese variety with a linear space and, hence, is defined by the 2-minors of a matrix of linear forms. Exercise 6.10 in [Eisenbud 2005] rephrases this as a "(vague) principle that embeddings of varieties by sufficiently positive bundles are often defined by ideals of  $2 \times 2$  minors". Our primary goal is to provide a precise form of this principle.

---

Sidman was partially supported by NSF grant DMS-0600471 and the Clare Boothe Luce program. Smith was partially supported by NSERC and grant KAW 2005.0098 from the Knut and Alice Wallenberg Foundation.

*MSC2000*: primary 14A25; secondary 14F05, 13D02.

*Keywords*: determinantly presented, linear free resolution, Castelnuovo–Mumford regularity.

To be more explicit, consider a scheme  $X$  embedded in  $\mathbb{P}^r$  by the complete linear series of a line bundle  $L$ . As in [Eisenbud et al. 1988, p. 514], the line bundle  $L$  is called *determinantly presented* if the homogeneous ideal  $I_{X|\mathbb{P}^r}$  of  $X$  in  $\mathbb{P}^r$  is generated by the 2-minors of a 1-generic matrix (that is, no conjugate matrix has a zero entry) of linear forms. Definition 3.1 in [Green 1984b] states that a property holds for a *sufficiently ample* line bundle on  $X$  if there exists a line bundle  $A$  such that the property holds for all  $L \in \text{Pic}(X)$  for which  $L \otimes A^{-1}$  is ample. Our main result is this:

**Theorem 1.1.** *Every sufficiently ample line bundle on a connected scheme is determinantly presented.*

We also describe, in terms of Castelnuovo–Mumford regularity, a set of determinantly presented line bundles on an arbitrary projective scheme; see Corollary 3.3.

This theorem is a new incarnation of a well-known phenomenon—roughly speaking, the complexity of the first few syzygies of a projective subscheme is inversely related to the positivity of the corresponding linear series. Nevertheless, Theorem 1.1 counterintuitively implies that most projective embeddings by a complete linear series are simply the intersection of a Segre variety with a linear subspace. More precisely, if we fix the Euclidean metric on the ample cone  $\text{Amp}(X)$  that it inherits from the finite-dimensional real vector space  $N^1(X) \otimes \mathbb{R}$ , then the fraction of determinantly presented ample classes within distance  $\rho$  of the trivial class approaches 1 as  $\rho$  tends to  $\infty$ .

Theorem 1.1 also has consequences beyond showing that the homogeneous ideal is generated by quadrics of rank at least 2. Proposition 6.13 in [Eisenbud 2005] shows that an Eagon–Northcott complex is a direct summand of the minimal graded free resolution of the ideal. Despite the classic examples, being able to give a complete description of this resolution in the general setting seems overly optimistic. However, a determinantal presentation provides many equations for higher secant varieties; see [Eisenbud et al. 1988, Proposition 1.3]. For a scheme  $X \subset \mathbb{P}^r$ , let  $\text{Sec}^k(X)$  be the Zariski closure of the union of the linear spaces spanned by collections of  $k + 1$  points on  $X$ . A natural generalization of Theorem 1.1 would be as follows:

**Conjecture 1.2.** *Let  $k$  be a positive integer. If  $X \subset \mathbb{P}^r$  is embedded by the complete linear series of a sufficiently ample line bundle, then the homogeneous ideal of  $\text{Sec}^k(X)$  is generated by the  $(k + 2)$ -minors of a 1-generic matrix of linear forms.*

This conjecture holds for rational normal curves [Eisenbud 1988, Proposition 4.3], rational normal scrolls [Catalano-Johnson 1996, Proposition 2.2], Segre varieties, and quadratic Veronese varieties [Sturmfels and Sullivant 2006, Section 4]. It also extends the conjecture for curves appearing in [Eisenbud et al. 1988, p. 518] for which [Ravi 1994] proves a set-theoretic version and for which [Ginensky

2010, Section 7] proves a scheme-theoretic version. Although Theorem 1.1.4 in [Buczyński et al. 2010] produces counterexamples to this conjecture for some singular  $X$ , Corollary 1.2.4 therein provides supporting evidence when  $X$  is smooth. Theorem 1.3 in [Buczyński and Buczyński 2010] suggests that the secant varieties in Conjecture 1.2 should be replaced by cactus varieties.

The secondary goal of this article is to effectively bound the determinantly presented line bundles on specific schemes. For an integral curve of genus  $g$ , Theorem 1 in [Eisenbud et al. 1988] shows that a line bundle is determinantly presented when its degree is at least  $4g + 2$  and this bound is sharp. We provide the analogous result on smooth varieties and Gorenstein toric varieties:

**Theorem 1.3.** *Let  $X$  be a smooth variety of dimension  $n$  or an  $n$ -dimensional Gorenstein toric variety and let  $A$  be a very ample line bundle on  $X$  such that  $(X, A) \neq (\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(1))$ . If  $B$  is a nef line bundle,  $K_X$  is the dualizing bundle on  $X$ , and  $L := K_X^2 \otimes A^j \otimes B$  with  $j \geq 2n + 2$ , then  $L$  is determinantly presented.*

As an application of our methods, we describe determinantly presented ample line bundles on products of projective spaces; see Theorem 4.1.

To prove these theorems, we need a source of appropriate matrices. Composition of linear series (also known as multiplication in the total coordinate ring or the Cox ring) traditionally supply the required matrices. If  $X \subset \mathbb{P}^r$  is embedded by the complete linear series for a line bundle  $L$ , then  $H^0(X, L)$  is the space of linear forms on  $\mathbb{P}^r$ . Factoring  $L$  as  $L = E \otimes E'$  for some  $E, E' \in \text{Pic}(X)$  yields a natural map

$$\mu : H^0(X, E) \otimes H^0(X, E') \rightarrow H^0(X, E \otimes E') = H^0(X, L).$$

By choosing ordered bases  $y_1, \dots, y_s \in H^0(X, E)$  and  $z_1, \dots, z_t \in H^0(X, E')$ , we obtain an associated  $(s \times t)$ -matrix  $\Omega := [\mu(y_i \otimes z_j)]$  of linear forms. The matrix  $\Omega$  is 1-generic and its ideal  $I_2(\Omega)$  of 2-minors vanishes on  $X$ ; see [Eisenbud 2005, Proposition 6.10]. Numerous classical examples of this construction can be found in [Room 1938].

With these preliminaries, the problem reduces to finding conditions on  $E$  and  $E'$  that guarantee that  $I_{X|\mathbb{P}^r} = I_2(\Omega)$ . Inspired by the approach in [Eisenbud et al. 1988], Theorem 3.2 achieves this by placing restrictions on certain modules arising from the line bundles  $L, E$ , and  $E'$ . The key hypotheses require these modules to have a *linear free presentation*; the generators of the  $\mathbb{N}$ -graded modules have degree 0 and their first syzygies must have degree 1. Methods introduced by Green and Lazarsfeld [Green 1984a; Green and Lazarsfeld 1985] — for an expository account see [Eisenbud 2005, Section 8; Green 1989; Lazarsfeld 1989, Section 1] — yield a cohomological criterion for our modules to have a linear free presentation. Hence, we can prove Theorem 1.1 by combining this with uniform vanishing results derived from Castelnuovo–Mumford regularity. Building on known conditions (that

is, sufficient conditions for a line bundle to satisfy  $N_1$ ), we obtain effective criteria for the appropriate modules to have a linear free presentation on Gorenstein toric varieties, and smooth varieties.

Rather than focusing exclusively on a single factorization of the line bundle  $L$ , we set up the apparatus to handle multiple factorizations; see Lemma 3.1. Multiple factorizations of a line bundle were used in [Graf v. Bothmer and Hulek 2004] to study the equations and syzygies of elliptic normal curves and their secant varieties. They also provide a geometric interpretation for the *flattenings* appearing in [Garcia et al. 2005, Section 7] and [Catalisano et al. 2008, p. 1915]. Using this more general setup, we are able to describe the homogeneous ideal for every embedding of a product of projective spaces by a very ample line bundle as the 2-minors of appropriate 1-generic matrices of linear forms; see Proposition 4.4.

**Conventions.** In this paper,  $\mathbb{N}$  is the set of nonnegative integers,  $\mathbb{1}_W \in \text{Hom}(W, W)$  is the identity map, and  $\mathbf{1} := (1, \dots, 1)$  is the vector in which every entry is 1. We work over an algebraically closed field  $\mathbb{k}$  of characteristic zero. A variety is always irreducible and all of our toric varieties are normal. For a vector bundle  $U$ , we write  $U^j$  for the  $j$ -fold tensor product  $U^{\otimes j} = U \otimes \dots \otimes U$ .

### 2. Linear free presentations

This section collects the criteria needed to show that certain modules arising from line bundles have a linear free presentation. While accomplishing this, we also establish some notation and nomenclature used throughout the document.

Let  $X$  be a projective scheme over  $\mathbb{k}$ , let  $\mathcal{F}$  be a coherent  $\mathcal{O}_X$ -module, and let  $L$  be a line bundle on  $X$ . We write  $\Gamma(L) := H^0(X, L)$  for the  $\mathbb{k}$ -vector space of global sections and  $S := \text{Sym}(\Gamma(L))$  for the homogeneous coordinate ring of  $\mathbb{P}^r := \mathbb{P}(\Gamma(L))$ . Consider the  $\mathbb{N}$ -graded  $S$ -module  $F := \bigoplus_{j \geq 0} H^0(X, \mathcal{F} \otimes L^j)$ . When  $\mathcal{F} = \mathcal{O}_X$ ,  $F$  is the section ring of  $L$ . However, when  $\mathcal{F} = L$ , the module  $F$  is the truncation of the section ring omitting the zeroth graded piece and shifting degrees by  $-1$ . Let  $P_\bullet$  be a minimal graded free resolution of  $F$ :

$$\begin{array}{ccccccc} \dots & \longrightarrow & \bigoplus S(-a_{i,j}) & \longrightarrow & \dots & \longrightarrow & \bigoplus S(-a_{0,j}) \longrightarrow F \longrightarrow 0. \\ & & \parallel & & & & \parallel \\ & & P_i & & & & P_0 \end{array}$$

Following [Eisenbud et al. 1988, p. 515], we say that, for  $p \in \mathbb{N}$ ,  $\mathcal{F}$  has a *linear free resolution to stage  $p$  with respect to  $L$*  or  $F$  has a *linear free resolution to stage  $p$*  if  $P_i = \bigoplus S(-i)$  for all  $0 \leq i \leq p$ . Thus,  $F$  has a linear free resolution to stage 0 if and only if it is generated in degree 0. Since having a linear free resolution to stage 1 implies that the relations among the generators (also known as first syzygies) are linear, the module  $F$  has a linear free resolution to stage 1 if and only if it has a

linear free presentation. In this case, we say that  $\mathcal{F}$  has a *linear free presentation with respect to  $L$* . More generally, having a linear free resolution to stage  $p$  is the module-theoretic analogue of the  $N_p$ -property introduced in [Green and Lazarsfeld 1985, Section 3]. If  $X$  is connected, then the line bundle  $L$  satisfies  $N_1$  precisely when  $L$  has a linear free presentation with respect to itself and satisfies  $N_p$  when  $L$  has a linear free resolution to stage  $p$ . Following [Ein and Lazarsfeld 1993, Convention 0.4], we do not assume that  $X$  is normal.

Henceforth, we assume that  $L$  is globally generated. In other words, the natural evaluation map  $ev_L : \Gamma(L) \otimes_{\mathbb{k}} \mathcal{O}_X \rightarrow L$  is surjective. If  $M_L := \text{Ker}(ev_L)$ , then  $M_L$  is a vector bundle of rank  $r := \dim_{\mathbb{k}} \Gamma(L) - 1$  that sits in the short exact sequence

$$0 \rightarrow M_L \rightarrow \Gamma(L) \otimes_{\mathbb{k}} \mathcal{O}_X \rightarrow L \rightarrow 0. \tag{*}$$

For convenience, we record the following cohomological criteria, which is a minor variant of [Eisenbud 2005, Theorem 5.6], [Green 1989, Proposition 2.4], or [Ein and Lazarsfeld 1993, Lemma 1.6].

**Lemma 2.1.** *If  $H^1(X, \bigwedge^i M_L \otimes \mathcal{F} \otimes L^j) = 0$  for all  $1 \leq i \leq p + 1$  and all  $j \geq 0$ , then the coherent  $\mathcal{O}_X$ -module  $\mathcal{F}$  has a linear free resolution to stage  $p$  with respect to  $L$ . In characteristic zero,  $\bigwedge^i M_L$  is a direct summand of  $M_L^i$ , so it suffices to show  $H^1(X, M_L^i \otimes \mathcal{F} \otimes L^j) = 0$  for all  $1 \leq i \leq p + 1$  and all  $j \geq 0$ .  $\square$*

*Sketch of proof.* The key observation is that the graded Betti numbers for the minimal free resolution of  $F$  can be computed via Koszul cohomology. If  $L$  is globally generated and  $\mathbb{P}^r = \mathbb{P}(H^0(X, L))$ , then there is a morphism  $\varphi_L : X \rightarrow \mathbb{P}^r$  with  $\varphi_L^*(\mathcal{O}_{\mathbb{P}^r}(1)) = L$ . Since the pullback by  $\varphi_L^*$  of  $0 \rightarrow M_{\mathcal{O}_{\mathbb{P}^r}(1)} \rightarrow \Gamma(\mathcal{O}_{\mathbb{P}^r}(1)) \otimes_{\mathbb{k}} \mathcal{O}_{\mathbb{P}^r} \rightarrow \mathcal{O}_{\mathbb{P}^r}(1) \rightarrow 0$  is just  $(*)$ , the proof of [Eisenbud 2005, Theorem 5.6] goes through working on  $X$  instead of  $\mathbb{P}^r$ .  $\square$

Multigraded Castelnuovo–Mumford regularity, as developed in [Maclagan and Smith 2004, Section 6] or [Hering et al. 2006, Section 2], allows us to exploit this criteria. To be more precise, fix a list  $B_1, \dots, B_\ell$  of globally generated line bundles on  $X$ . For a vector  $\mathbf{u} := (u_1, \dots, u_\ell) \in \mathbb{Z}^\ell$ , we set  $\mathbf{B}^{\mathbf{u}} := B_1^{u_1} \otimes \dots \otimes B_\ell^{u_\ell}$  and we write  $\mathfrak{B} := \{\mathbf{B}^{\mathbf{u}} : \mathbf{u} \in \mathbb{N}^\ell\} \subset \text{Pic}(X)$  for the submonoid generated by these line bundles. If  $\mathbf{e}_1, \dots, \mathbf{e}_\ell$  is the standard basis for  $\mathbb{Z}^\ell$  then  $\mathbf{B}^{\mathbf{e}_j} = B_j$ . A coherent  $\mathcal{O}_X$ -module  $\mathcal{F}$  is said to be *regular with respect to  $B_1, \dots, B_\ell$*  if  $H^i(X, \mathcal{F} \otimes \mathbf{B}^{-\mathbf{u}}) = 0$  for all  $i > 0$  and all  $\mathbf{u} \in \mathbb{N}^\ell$  satisfying  $|\mathbf{u}| := u_1 + \dots + u_\ell = i$ . When  $\ell = 1$ , we recover the version of Castelnuovo–Mumford regularity found in [Lazarsfeld 2004, Section 1.8].

Although the definition may not be intuitive, the next result shows that regular line bundles are at least ubiquitous.

**Lemma 2.2.** *Let  $X$  be a scheme and let  $B_1, \dots, B_\ell$  be globally generated line bundles on  $X$ . If there is a positive vector  $\mathbf{w} \in \mathbb{Z}^\ell$  such that  $\mathbf{B}^{\mathbf{w}}$  is ample, then a sufficiently ample line bundle on  $X$  is regular with respect to  $B_1, \dots, B_\ell$ .*

The hypothesis on  $\mathbf{w}$  means that the cone  $\text{pos}(B_1, \dots, B_\ell)$  generated by  $B_1, \dots, B_\ell$  contains an ample line bundle. In other words, the subcone  $\text{pos}(B_1, \dots, B_\ell)$  of  $\text{Nef}(X)$  has a nonempty intersection with the interior of  $\text{Nef}(X)$ .

*Proof.* It suffices to find a line bundle  $A$  on  $X$  such that, for any nef line bundle  $C$ ,  $A \otimes C$  is regular with respect to  $B_1, \dots, B_\ell$ . Because  $\mathbf{B}^{\mathbf{w}}$  is ample, Fujita’s vanishing theorem (for example, [Fujita 1983, Theorem 1]) implies that there is  $k \in \mathbb{N}$  such that, for any nef line bundle  $C$ , we have  $H^i(X, \mathbf{B}^{j\mathbf{w}} \otimes C) = 0$  for all  $i > 0$  and all  $j \geq k$ . Let  $n := \dim X$  and consider  $A := \mathbf{B}^{(k+n)\mathbf{w}}$ . Since  $\mathbf{w}$  is positive, the line bundle  $\mathbf{B}^{n\mathbf{w}-\mathbf{u}}$  is nef for all  $\mathbf{u} \in \mathbb{N}^\ell$  with  $0 \leq |\mathbf{u}| \leq n$ . Therefore, we have  $H^i(X, (A \otimes C) \otimes \mathbf{B}^{-\mathbf{u}}) = H^i(X, \mathbf{B}^{k\mathbf{w}} \otimes (\mathbf{B}^{n\mathbf{w}-\mathbf{u}} \otimes C)) = 0$  for all  $i > 0$  and all  $\mathbf{u} \in \mathbb{N}^\ell$  satisfying  $|\mathbf{u}| = i$ . □

Before describing the pivotal results in this section, we record a technical lemma bounding the regularity of certain tensor products. Our approach is a hybrid of [Lazarsfeld 2004, Proposition 1.8.9 and Remark 1.8.16].

**Lemma 2.3.** *Let  $X$  be a scheme of dimension  $n$  and  $\mathcal{F}$  be a coherent  $\mathcal{O}_X$ -module. Fix a vector bundle  $V$  and a globally generated ample line bundle  $B$  on  $X$ . If  $m$  is positive integer such that  $\mathcal{F}$ ,  $V$ , and  $B^m$  are all regular with respect to  $B$ , then  $\mathcal{F} \otimes V \otimes B^w$  is also regular with respect to  $B$  for all  $w \geq (m - 1)(n - 1)$ .*

*Proof.* Since  $\mathcal{F}$  and  $B^m$  are regular with respect to  $B$ , either [Arapura 2004, Corollary 3.2] or [Maclagan and Smith 2004, Theorem 7.8] (also compare with [Lazarsfeld 2004, Proposition 1.8.8]) produces a locally free resolution of  $\mathcal{F}$  of the form

$$\dots \longrightarrow \bigoplus B^{-jm} \longrightarrow \dots \longrightarrow \bigoplus B^{-m} \longrightarrow \bigoplus \mathcal{O}_X \longrightarrow \mathcal{F} \rightarrow 0.$$

Tensoring by a locally free sheaf preserves exactness, so we get the exact complex

$$\dots \longrightarrow \bigoplus V \otimes B^{w-jm} \longrightarrow \dots \longrightarrow \bigoplus V \otimes B^w \longrightarrow \mathcal{F} \otimes V \otimes B^w \rightarrow 0.$$

Since  $V$  is also regular with respect to  $B$ , Mumford’s lemma (see for example [Lazarsfeld 2004, Theorem 1.8.5]) implies that  $H^{i+j}(X, V \otimes B^{w-jm-i}) = 0$  for  $i \geq 1$  provided we have  $w - jm - i \geq -i - j$ . Chasing through the complex (see [Lazarsfeld 2004, Proposition B.1.2]), we conclude that  $\mathcal{F} \otimes V \otimes B^w$  is also regular with respect to  $B$  when  $w \geq (m - 1)(n - 1)$ . □

The next three propositions each provide sufficient conditions for an appropriate line bundle to have a linear free presentation with respect to another line bundle.



**Proposition 2.4.** *Fix a positive integer  $m$  and a scheme  $X$  of dimension  $n$ . Let  $L$  be a line bundle on  $X$  and let  $B$  be a globally generated ample line bundle on  $X$ . If  $L^j$  and  $B^m$  are regular with respect to  $B$  for all  $j \geq 1$ , then  $B^w$  has a linear free presentation with respect to  $L$  for all  $w \geq 2(m - 1)n + 1$ .*

*Proof.* We first prove that  $M_L \otimes B^m$  is regular with respect to  $B$ . Tensoring (\*) with  $B^{m-i}$  and taking the associated long exact sequence gives

$$\begin{aligned} \Gamma(L) \otimes H^0(X, B^{m-i}) &\longrightarrow H^0(X, L \otimes B^{m-i}) \longrightarrow H^1(X, M_L \otimes B^{m-i}) \longrightarrow \dots \\ &\longrightarrow H^{i-1}(X, L \otimes B^{m-i}) \longrightarrow H^i(X, M_L \otimes B^{m-i}) \longrightarrow \Gamma(L) \otimes H^i(X, B^{m-i}). \end{aligned}$$

Since  $L$  is regular with respect to  $B$ , Mumford’s lemma shows that, for all  $k \in \mathbb{N}$ , the map  $\Gamma(L) \otimes H^0(X, B^k) \rightarrow H^0(X, L \otimes B^k)$  is surjective and, for all  $i > 0$  and all  $k \in \mathbb{N}$ , we have  $H^i(X, L \otimes B^{k-i}) = 0$ . As  $m$  is a positive integer, the map  $\Gamma(L) \otimes H^0(X, B^{m-1}) \rightarrow H^0(X, L \otimes B^{m-1})$  is surjective and  $H^{i-1}(X, L \otimes B^{m-i}) = 0$  for all  $i > 1$ . Since  $B^m$  is also regular with respect to  $B$ , we have  $H^i(X, B^{m-i}) = 0$  for all  $i > 0$ . It follows that  $H^i(X, M_L \otimes B^{m-i}) = 0$  for all  $i > 0$ .

By Lemma 2.1, it suffices to show that

$$H^1(X, M_L \otimes B^w \otimes L^j) = 0 \quad \text{and} \quad H^1(X, M_L^2 \otimes B^w \otimes L^j) = 0$$

for all  $j \in \mathbb{N}$ . Thus, it suffices to show that the vector bundles  $M_L \otimes B^{w+1} \otimes L^j$  and  $M_L^2 \otimes B^{w+1} \otimes L^j$  are both regular with respect to  $B$ . If  $w \geq (m - 1)n$ , then Lemma 2.3 implies that  $(M_L \otimes B^m) \otimes L^j \otimes B^{w+1-m} = M_L \otimes B^{w+1} \otimes L^j$  is regular with respect to  $B$ . Similarly, if  $w \geq 2(m - 1)n + 1$ , then using Lemma 2.3 twice establishes that the vector bundle

$$((M_L \otimes B^m) \otimes (M_L \otimes B^m) \otimes B^{(m-1)(n-1)}) \otimes L^j \otimes B^{w-mn-m+n} = M_L^2 \otimes B^{w+1} \otimes L^j$$

is also regular with respect to  $B$ . □

By adapting the proof of [Hering et al. 2006, Theorem 1.1], we obtain the second proposition.

**Proposition 2.5.** *Let  $\mathbf{m} \in \mathbb{N}^\ell$  be a vector satisfying  $\mathbf{B}^{m-e_j} \in \mathfrak{B}$  for all  $1 \leq j \leq \ell$  and let the coherent  $\mathcal{O}_X$ -module  $\mathcal{F}$  be regular with respect to  $B_1, \dots, B_\ell$ . If  $L := \mathbf{B}^{\mathbf{m}}$  and the map*

$$\Gamma(L) \otimes H^0(X, \mathcal{F} \otimes \mathbf{B}^{-e_j}) \rightarrow H^0(X, \mathcal{F} \otimes \mathbf{B}^{m-e_j})$$

*is surjective for all  $1 \leq j \leq \ell$ , then  $\mathcal{F}$  has a linear presentation with respect to  $L$ .*

The condition that  $\mathbf{B}^{m-e_j} \in \mathfrak{B}$  for all  $1 \leq j \leq \ell$  implies that  $L = \mathbf{B}^{\mathbf{m}}$  lies in the interior of the cone  $\text{pos}(B_1, \dots, B_\ell)$ .

*Proof.* We first prove that  $M_L \otimes \mathcal{F}$  is regular with respect to  $B_1, \dots, B_\ell$ . Tensoring  $(*)$  with  $\mathcal{F} \otimes \mathbf{B}^{-u}$  and taking the associated long exact sequence gives

$$\begin{aligned} \Gamma(L) \otimes H^0(X, \mathcal{F} \otimes \mathbf{B}^{-u}) &\longrightarrow H^0(X, \mathcal{F} \otimes \mathbf{B}^{m-u}) \\ &\longrightarrow H^1(X, M_L \otimes \mathcal{F} \otimes \mathbf{B}^{-u}) \longrightarrow \dots \longrightarrow H^{i-1}(X, \mathcal{F} \otimes \mathbf{B}^{m-u}) \\ &\longrightarrow H^i(X, M_L \otimes \mathcal{F} \otimes \mathbf{B}^{-u}) \longrightarrow \Gamma(L) \otimes H^i(X, \mathcal{F} \otimes \mathbf{B}^{-u}). \end{aligned}$$

Since  $\mathcal{F}$  is regular with respect to  $B_1, \dots, B_\ell$ , Theorem 2.1 in [Hering et al. 2006] shows that, for all  $i > 0$  and all  $\mathbf{u}, \mathbf{v} \in \mathbb{N}^\ell$  with  $|\mathbf{u}| = i$ ,  $H^i(X, \mathcal{F} \otimes \mathbf{B}^{\mathbf{v}-\mathbf{u}}) = 0$ . As  $\mathbf{B}^{m-e_j} \in \mathfrak{B}$  for  $1 \leq j \leq \ell$ , we see that  $H^{i-1}(X, \mathcal{F} \otimes \mathbf{B}^{m-u}) = 0$  for all  $i > 1$  and all  $\mathbf{u} \in \mathbb{N}^\ell$  satisfying  $|\mathbf{u}| = i$ . By hypothesis, the map

$$\Gamma(L) \otimes H^0(X, \mathcal{F} \otimes \mathbf{B}^{-e_j}) \rightarrow H^0(X, \mathcal{F} \otimes \mathbf{B}^{m-e_j})$$

is surjective for all  $1 \leq j \leq \ell$ . It follows that  $H^i(X, M_L \otimes \mathcal{F} \otimes \mathbf{B}^{-u}) = 0$  for all  $i > 0$  and all  $\mathbf{u} \in \mathbb{N}^\ell$  such that  $|\mathbf{u}| = i$ .

By Lemma 2.1, it suffices to show that

$$H^1(X, M_L \otimes \mathcal{F} \otimes L^j) \quad \text{and} \quad H^1(X, M_L^2 \otimes \mathcal{F} \otimes L^j)$$

are zero for  $j \in \mathbb{N}$ . Since  $M_L \otimes \mathcal{F}$  is regular with respect to  $B_1, \dots, B_\ell$ , the vanishing of the first group follows from Theorem 2.1 [ibid.]. For the second, tensoring  $(*)$  with  $M_L \otimes \mathcal{F} \otimes L^j$  gives the exact sequence

$$\begin{aligned} \Gamma(L) \otimes H^0(X, M_L \otimes \mathcal{F} \otimes L^j) &\longrightarrow H^0(X, M_L \otimes \mathcal{F} \otimes L^{j+1}) \\ &\longrightarrow H^1(X, M_L^2 \otimes \mathcal{F} \otimes L^j) \rightarrow 0. \end{aligned}$$

Because  $M_L \otimes \mathcal{F}$  is regular with respect to  $B_1, \dots, B_\ell$ , Theorem 2.1 [ibid.] also shows that the left map is surjective for all  $j \geq 0$ . □

Our third proposition is a variant of [Ein and Lazarsfeld 1993, Proposition 3.1].

**Proposition 2.6.** *Let  $X$  be a smooth variety of dimension  $n$ , let  $K_X$  be its canonical bundle, and let  $A$  be a very ample line bundle on  $X$  such that  $(X, A) \neq (\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(1))$ . Suppose that  $B$  and  $C$  are nef line bundles on  $X$ . If the integers  $w$  and  $m$  are both greater than  $n$ , then the line bundle  $K_X \otimes A^w \otimes B$  has a linear free presentation with respect to  $K_X \otimes A^m \otimes C$ .*

*Proof.* Let  $\mathcal{F} := K_X \otimes A^w \otimes B$  and  $L := K_X \otimes A^m \otimes C$ . Since [Ein and Lazarsfeld 1993, Proposition 3.1] shows that  $L$  satisfies  $N_0$  and [Ein and Lazarsfeld 1993, Equation 3.2] shows that  $H^1(X, M_L^i \otimes \mathcal{F} \otimes L^j) = 0$  for all  $1 \leq i \leq 2$  and all  $j \geq 0$ , Lemma 2.1 completes the proof. □

### 3. Determinantly presented line bundles

The goal of this section is to prove Theorem 1.1. We realize this goal by developing general methods for showing that a line bundle is determinantly presented; see Theorem 3.2.

Suppose  $X \subset \mathbb{P}^r$  is embedded by the complete linear series for a line bundle  $L$ . Factor  $L$  as  $L = E \otimes E'$  for some  $E, E' \in \text{Pic}(X)$  and denote by

$$\mu_{E,E'} : H^0(X, E) \otimes H^0(X, E') \rightarrow H^0(X, L)$$

the natural multiplication map. Choose ordered bases  $y_1, \dots, y_s$  and  $z_1, \dots, z_t$  for the  $\mathbb{k}$ -vector spaces  $H^0(X, E)$  and  $H^0(X, E')$ , respectively. Define  $\Omega = \Omega(E, E')$  to be the associated  $(s \times t)$ -matrix  $[\mu_{E,E'}(y_i \otimes z_j)]$  of linear forms. Its ideal  $I_2(\Omega)$  of 2-minors is independent of the choice of bases. Then [Eisenbud 2005, Proposition 6.10] shows that  $\Omega$  is 1-generic and that  $I_2(\Omega)$  vanishes on  $X$ .

Our key technical result is inspired by [Eisenbud et al. 1988, Section 2].

**Lemma 3.1.** *If  $L$  is a very ample line bundle on  $X$  satisfying  $N_1$  and  $\{(E_i, E'_i)\}$  is a family of factorizations for  $L$ , then the commutative diagram  $(\star)$  has exact rows and columns. Moreover, if  $\varphi_2$  is surjective, then the homogeneous ideal  $I_{X|\mathbb{P}^r}$  is generated by the 2-minors of the matrices  $\Omega(E_i, E'_i)$  if and only if  $Q_2$  surjects onto  $Q_1$ .*

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 & & \bigoplus_i \wedge^2 \Gamma(E_i) \otimes \wedge^2 \Gamma(E'_i) & \xrightarrow{\varphi} & (I_{X|\mathbb{P}^r})_2 & & \\
 & & \downarrow & & \downarrow & & \\
 0 \longrightarrow & Q_2 & \longrightarrow & \bigoplus_i \text{Sym}_2(\Gamma(E_i) \otimes \Gamma(E'_i)) & \xrightarrow{\varphi_2} & \text{Sym}_2(\Gamma(L)) & (\star) \\
 & \downarrow \psi & & \downarrow & & \downarrow & \\
 0 \longrightarrow & Q_1 & \longrightarrow & \bigoplus_i \text{Sym}_2(\Gamma(E_i)) \otimes \text{Sym}_2(\Gamma(E'_i)) & \xrightarrow{\varphi_1} & \Gamma(L^2) & \\
 & & & \downarrow & & \downarrow & \\
 & & & 0 & & 0 & 
 \end{array}$$

*Proof.* To begin, we prove the columns are exact. Since  $L$  satisfies  $N_0$  (that is, the natural maps  $\text{Sym}_j(\Gamma(L)) \rightarrow H^0(X, L^j)$  are surjective for all  $j \in \mathbb{N}$ ), the ideal  $I_{X|\mathbb{P}^r}$  is the kernel of the map from the homogeneous coordinate ring of  $\mathbb{P}^r$  to the section ring of  $L$ . By taking the quadratic components, we obtain the right column.

The middle column is the direct sum of the complexes:

$$0 \rightarrow \wedge^2 \Gamma(E_i) \otimes \wedge^2 \Gamma(E'_i) \longrightarrow \text{Sym}_2(\Gamma(E_i) \otimes \Gamma(E'_i)) \\ \longrightarrow \text{Sym}_2(\Gamma(E_i)) \otimes \text{Sym}_2(\Gamma(E'_i)) \rightarrow 0.$$

The map  $\wedge^2 \Gamma(E_i) \otimes \wedge^2 \Gamma(E'_i) \rightarrow \text{Sym}_2(\Gamma(E_i) \otimes \Gamma(E'_i))$ , defined by

$$e \wedge f \otimes e' \wedge f' \mapsto (e \otimes e') \cdot (f \otimes f') - (e \otimes f') \cdot (f \otimes e'), \tag{†}$$

is simply the inclusion map determined by the 2-minors of the generic matrix. The map  $\text{Sym}_2(\Gamma(E_i) \otimes \Gamma(E'_i)) \rightarrow \text{Sym}_2(\Gamma(E_i)) \otimes \text{Sym}_2(\Gamma(E'_i))$  is  $(e \otimes e') \cdot (f \otimes f') \mapsto ef \otimes e'f'$ . Hence, each of these complexes is exact, so the middle column also is. By definition,  $Q_1$  and  $Q_2$  are the kernels of the  $\varphi_1$  and  $\varphi_2$  respectively, and  $\psi$  is the induced map between them.

We next identify the horizontal maps. By applying the functor  $\text{Sym}_2$  to  $\mu_{E_i, E'_i}$ , we obtain a map from  $\text{Sym}_2(\Gamma(E_i) \otimes \Gamma(E'_i))$  to  $\text{Sym}_2(\Gamma(L))$  for each  $i$ , and  $\varphi_2$  is their direct sum. The composite map

$$\mu_{L,L} \circ (\mu_{E_i, E'_i} \otimes \mu_{E_i, E'_i}) : \Gamma(E_i) \otimes \Gamma(E'_i) \otimes \Gamma(E_i) \otimes \Gamma(E'_i) \rightarrow \Gamma(L^2)$$

factors through  $\text{Sym}_2(\Gamma(E_i)) \otimes \text{Sym}_2(\Gamma(E'_i))$ , and  $\varphi_1$  is the direct sum of the associated maps from  $\text{Sym}_2(\Gamma(E_i)) \otimes \text{Sym}_2(\Gamma(E'_i))$  to  $\Gamma(L^2)$ . The map  $\varphi$  is induced by  $\varphi_2$ . From (†), we see that the image of  $\varphi$  is generated by the 2-minors of the matrices  $\Omega(E_i, E'_i)$ .

Finally, the line bundle  $L$  satisfies  $N_1$ , so the quadratic component  $(I_{X|\mathbb{P}^r})_2$  generates the entire ideal  $I_{X|\mathbb{P}^r}$ . Hence, the image of  $\varphi$  generates the ideal  $I_{X|\mathbb{P}^r}$  if and only if  $\varphi$  is surjective. Since  $\varphi_2$  is surjective, the snake lemma (for example, [Weibel 1994, Lemma 1.3.2]) shows that the surjectivity of  $\varphi$  is equivalent to the surjectivity of  $\psi$ . □

Our main application for Lemma 3.1 focuses on a single factorization of the line bundle  $L$ . The proof follows the strategy in [Eisenbud et al. 1988, Section 2].

**Theorem 3.2.** *Let  $L$  be a very ample line bundle on a scheme  $X$  satisfying  $N_1$ . If  $L = E \otimes E'$  for some nontrivial  $E, E' \in \text{Pic}(X)$  and the conditions*

- (a)  $E$  has a linear presentation with respect to  $E'$ ,
- (b)  $E'$  has a linear presentation with respect to  $E$ ,
- (c)  $E^2$  has a linear presentation with respect to  $E'$ , and
- (d) both  $E$  and  $E'$  satisfy  $N_0$

*hold, then the 2-minors of the matrix  $\Omega(E, E')$  generate the homogeneous ideal of  $X$  in  $\mathbb{P}(\Gamma(L))$ . In particular, the line bundle  $L$  is determinantly presented.*

*Proof.* Given Lemma 3.1, it suffices to show that the map  $\psi : Q_2 \rightarrow Q_1$  is surjective. To accomplish this, we reinterpret both modules. Since condition (a) or (b) implies that the map  $\mu_{E,E'} : \Gamma(E) \otimes \Gamma(E') \rightarrow \Gamma(L)$  is surjective, we get an exact sequence

$$\text{Ker}(\mu_{E,E'}) \otimes \Gamma(E) \otimes \Gamma(E') \rightarrow \text{Sym}_2(\Gamma(E) \otimes \Gamma(E')) \rightarrow \text{Sym}_2(\Gamma(L)) \rightarrow 0,$$

so the image of  $\text{Ker}(\mu_{E,E'}) \otimes \Gamma(E) \otimes \Gamma(E')$  generates  $Q_2$  in  $\text{Sym}_2(\Gamma(E) \otimes \Gamma(E'))$ . The maps  $\mu_{E,E}$  and  $\mu_{E',E'}$  factor through  $\text{Sym}_2(\Gamma(E))$  and  $\text{Sym}_2(\Gamma(E'))$  and thus induce maps  $\eta : \text{Sym}_2(\Gamma(E)) \rightarrow \Gamma(E^2)$  and  $\eta' : \text{Sym}_2(\Gamma(E')) \rightarrow \Gamma(E'^2)$ , respectively. It follows that  $\varphi_1$  is the composition

$$\mu_{E^2,E'^2} \circ (\eta \otimes \eta') : \text{Sym}_2(\Gamma(E)) \otimes \text{Sym}_2(\Gamma(E')) \rightarrow \Gamma(E^2 \otimes E'^2) = \Gamma(L^2).$$

Hence,  $Q_1$  is the sum of the images of

$$\text{Ker}(\eta) \otimes \Gamma(E') \otimes \Gamma(E') \quad \text{and} \quad \Gamma(E) \otimes \Gamma(E) \otimes \text{Ker}(\eta'),$$

and the pullback to  $\text{Sym}_2(\Gamma(E)) \otimes \text{Sym}_2(\Gamma(E'))$  of  $\text{Ker}(\mu_{E^2,E'^2})$ .

We now break the proof that  $Q_2$  surjects onto  $Q_1$  into four steps:

- (i) The image of  $\text{Ker}(\mu_{E^2,E'}) \otimes \Gamma(E')$  in  $\Gamma(E^2) \otimes \Gamma(E'^2)$  contains  $\text{Ker}(\mu_{E^2,E'^2})$ .
- (ii) The image of  $\text{Ker}(\mu_{E,E'}) \otimes \Gamma(E)$  in  $\Gamma(E^2) \otimes \Gamma(E')$  contains  $\text{Ker}(\mu_{E^2,E'})$ .
- (iii) The image of  $\text{Ker}(\mu_{E,E'}) \otimes \Gamma(E)$  in  $\text{Sym}_2(\Gamma(E)) \otimes \Gamma(E')$  contains  $\text{Ker}(\eta) \otimes \Gamma(E')$ .
- (iv) The image of  $\text{Ker}(\mu_{E,E'}) \otimes \Gamma(E')$  in  $\Gamma(E) \otimes \text{Sym}_2(\Gamma(E'))$  contains  $\Gamma(E) \otimes \text{Ker}(\eta')$ .

By tensoring with the  $\mathbb{k}$ -vector space  $\Gamma(E')$ , step (ii) yields a surjective map

$$\text{Ker}(\mu_{E,E'}) \otimes \Gamma(E) \otimes \Gamma(E') \rightarrow \text{Ker}(\mu_{E^2,E'}) \otimes \Gamma(E').$$

Combining this with step (i) shows that  $\text{Ker}(\mu_{E,E'}) \otimes \Gamma(E) \otimes \Gamma(E') \rightarrow \text{Ker}(\mu_{E^2,E'^2})$  is surjective. Again by tensoring with  $\mathbb{k}$ -vector space  $\Gamma(E')$ , step (iii) gives a surjective map  $\text{Ker}(\mu_{E,E'}) \otimes \Gamma(E) \otimes \Gamma(E') \rightarrow \text{Ker}(\eta) \otimes \Gamma(E') \otimes \Gamma(E')$ . Similarly, step (iv) implies that the map  $\text{Ker}(\mu_{E,E'}) \otimes \Gamma(E) \otimes \Gamma(E') \rightarrow \Gamma(E) \otimes \Gamma(E) \otimes \text{Ker}(\eta')$  is surjective. Therefore, it is enough to establish the four steps.

For step (i), condition (c) implies that  $\text{Ker}(\mu_{E^2,E'})$ , the span of the linear relations on  $\bigoplus_{j \geq 0} H^0(X, E^2 \otimes E'^j)$  regarded as a  $\text{Sym}(\Gamma(E'))$ -module, generates the relations in higher degrees as well. Hence,  $\text{Ker}(\mu_{E^2,E'}) \otimes \Gamma(E')$  maps onto the quadratic relations that are the kernel of the composite map  $\mu_{E^2,E'^2} \circ (\mathbb{1}_{\Gamma(E^2)} \otimes \eta')$ . Since this kernel is generated by  $\Gamma(E^2) \otimes \text{Ker}(\eta')$  and the pullback of  $\text{Ker}(\mu_{E^2,E'^2})$ , Condition (d) implies that  $\eta'$  is surjective, and we have established step (i).

To complete the proof, we simultaneously establish steps (ii) and (iii); the symmetric argument yields step (iv). Condition (b) implies that  $\text{Ker}(\mu_{E,E'})$  generates

all the relations on  $\bigoplus_{j \geq 0} H^0(X, E' \otimes E^j)$  regarded as a  $\text{Sym}(\Gamma(E))$ -module. In particular, the vector space  $\text{Ker}(\mu_{E,E'}) \otimes \Gamma(E)$  maps onto the quadratic relations that are the kernel of the composite map  $\mu_{E^2,E'} \circ (\eta \otimes \mathbb{1}_{\Gamma(E')})$ . This kernel is generated by  $\text{Ker}(\eta) \otimes \Gamma(E')$  and the pullback of  $\text{Ker}(\mu_{E^2,E'})$ . Condition (d) implies that  $\eta$  is surjective, so step (ii) and step (iii) follow.  $\square$

As the proof indicates, Theorem 3.2 holds under a weaker version of condition (d), in that it is only necessary that  $\eta$  and  $\eta'$  are surjective. Nevertheless, in all of our applications, a stronger condition is satisfied: Both  $E$  and  $E'$  satisfy  $N_1$ .

This theorem leads to a description, given in terms of Castelnuovo–Mumford regularity, for certain determinantly presented line bundles on any projective scheme.

**Corollary 3.3.** *Let  $X$  be a connected scheme and let  $B_1, \dots, B_\ell$  be globally generated line bundles on  $X$  for which there exists  $\mathbf{w} \in \mathbb{N}^\ell$  such that  $\mathbf{B}^{\mathbf{w}}$  is ample. If  $\mathbf{B}^{\mathbf{m}}$  is regular with respect to  $B_1, \dots, B_\ell$  for  $\mathbf{m} \in \mathbb{N}^\ell$  and  $\mathbf{B}^{2\mathbf{m}}$  is very ample, then the line bundle  $\mathbf{B}^{2\mathbf{m}+\mathbf{u}}$  is determinantly presented for any  $\mathbf{u} \in \mathbb{N}^\ell$ .*

*Proof.* Factor  $L := \mathbf{B}^{2\mathbf{m}+\mathbf{u}}$  as  $L = E \otimes E'$  where  $E := \mathbf{B}^{\mathbf{m}}$  and  $E' := \mathbf{B}^{\mathbf{m}+\mathbf{u}}$ . Theorem 2.1 in [Hering et al. 2006] shows that  $L, E, E^2$ , and  $E'$  are all regular with respect to  $B_1, \dots, B_\ell$ . Hence, Proposition 2.5 together with [ibid., Theorem 2.1] imply that  $L, E$ , and  $E'$  satisfy  $N_1$ , that  $E'$  has a linear free presentation with respect to  $E$ , and that both  $E$  and  $E^2$  have a linear free presentation with respect to  $E'$ . Therefore, Theorem 3.2 proves that  $L$  is determinantly presented.  $\square$

Theorem 3.2, combined with results from Section 2, also yields a proof for our main theorem.

*Proof of Theorem 1.1.* Let  $X$  be a connected scheme of dimension  $n$  and let  $B$  be a globally generated ample line bundle on  $X$ . Choose a positive integer  $m \in \mathbb{N}$  such that  $B^m$  is regular with respect to  $B$ . Lemma 2.2 implies that there exists a line bundle  $E$ , which we may assume is very ample, such that, for any nef line bundle  $C$ ,  $E \otimes C$  is regular with respect to  $B$ . By replacing  $E$  with  $E \otimes B$  if necessary, we may assume that the map  $\Gamma(B) \otimes H^0(X, E \otimes B^{-1}) \rightarrow H^0(X, E)$  is surjective. Since a sufficiently ample line bundle on  $X$  satisfies  $N_1$  (combine [Inamdar 1997, Lemmas 1.1–1.3] with Fujita’s vanishing theorem), we may also assume that  $E \otimes C$  satisfies  $N_1$  for any nef line bundle  $C$ .

Consider the line bundle  $A := E \otimes B^{2(m-1)n+1}$ . If  $L$  is a line bundle on  $X$  such that  $L \otimes A^{-1}$  is nef, then  $L = A \otimes C = (E \otimes C) \otimes B^{2(m-1)n+1}$  for some nef line bundle  $C$ . Our choice of  $E$  guarantees that,  $(E \otimes C)^j$  is regular with respect to  $B$  for all  $j \geq 1$ , and that  $L$  satisfies  $N_1$ . Hence, Proposition 2.4 implies that  $B^{2(m-1)n+1}$  has a linear free presentation with respect to  $E \otimes C$ . Proposition 2.5 together with Mumford’s lemma (for example, [Lazarsfeld 2004, Theorem 1.8.5])

imply that both  $E \otimes C$  and  $(E \otimes C)^2$  have a linear free presentation with respect to  $B^{2(m-1)n+1}$ . Via Lemma 2.3 and Proposition 2.5, we see  $B^{2(m-1)n+1}$  satisfies  $N_1$ . Therefore, Theorem 3.2 proves that  $L$  is determinantly presented.  $\square$

### 4. Effective bounds

In this section, we give effective bounds for determinantly presented line bundles. As a basic philosophy, one can convert explicit conditions for line bundles to satisfy  $N_2$  into effective descriptions for determinantly presented line bundles. The three subsections demonstrate this philosophy for products of projective spaces, projective Gorenstein toric varieties, and smooth varieties. Despite not developing them here, we expect similar results for general surfaces and abelian varieties following [Gallego and Purnaprajna 1999] and [Rubei 2000; Pareschi and Popa 2004], respectively.

**4.1. Products of projective space.** The tools from Section 3 lead to a description of the determinantly presented ample line bundles on a product of projective spaces. In contrast with [Bernardi 2008, Theorem 3.11], which proves that Segre–Veronese varieties are defined by 2-minors of an appropriate hypermatrix, our classification shows that a Segre–Veronese variety is typically generated by the 2-minors of a single matrix. In particular, we recover the Segre–Veronese ideals considered in [Sullivant 2008, Section 6.2].

To study the product of projective spaces  $X = \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_\ell}$ , we first introduce some notation. Let  $R := \mathbb{k}[x_{i,j} : 1 \leq i \leq \ell, 0 \leq j \leq n_i]$  be the total coordinate ring (also known as Cox ring) of  $X$ ; this polynomial ring has the  $\mathbb{Z}^\ell$ -grading induced by  $\deg(x_{i,j}) := \mathbf{e}_i \in \mathbb{Z}^\ell$ . Hence, we have  $R_{\mathbf{d}} = \Gamma(\mathcal{O}_X(\mathbf{d}))$  for all  $\mathbf{d} \in \mathbb{Z}^\ell$ , and a torus-invariant global section of  $\mathcal{O}_X(\mathbf{d})$  is identified with a monomial  $\mathbf{x}^{\mathbf{w}} \in R_{\mathbf{d}}$ , where  $\mathbf{w} \in \mathbb{N}^r$  and  $r := \sum_{i=1}^\ell (n_i + 1)$ . We write  $\mathbf{e}_{i,j}$  for the standard basis of  $\mathbb{Z}^r$ ; in particular  $\mathbf{x}^{\mathbf{e}_{i,j}} = x_{i,j}$ .

**Theorem 4.1.** *Let  $X = \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_\ell}$ . An ample line bundle  $\mathcal{O}_X(\mathbf{m})$  is determinantly presented if at least  $\ell - 2$  of the entries in the vector  $\mathbf{m}$  are at least 2.*

When  $\ell = 2$ , this theorem shows that all of the Segre–Veronese embeddings are determinantly presented. We note that Corollary 3.3 establishes that  $\mathcal{O}_X(\mathbf{m})$  is determinantly presented when  $m_j \geq 2$  for all  $1 \leq j \leq \ell$ .

*Proof.* Since a line bundle  $\mathcal{O}_X(\mathbf{v})$  is ample (and very ample) if and only if  $v_j \geq 1$  for all  $1 \leq j \leq \ell$ , Corollary 1.5 in [Hering et al. 2006] shows that  $\mathcal{O}_X(\mathbf{m})$  satisfies  $N_1$ . Without loss of generality, we may assume that  $m_j \geq 2$  for  $1 \leq j \leq \ell - 2$ . Factor  $\mathcal{O}_X(\mathbf{m})$  as  $\mathcal{O}_X(\mathbf{m}) = E \otimes E'$ , where  $\mathbf{u} := \mathbf{e}_1 + \mathbf{e}_2 + \dots + \mathbf{e}_{\ell-1} = (1, 1, \dots, 1, 0)$ ,  $E := \mathcal{O}_X(\mathbf{u})$ , and  $E' := \mathcal{O}_X(\mathbf{m} - \mathbf{u})$ . The canonical surjection  $\Gamma(E) \otimes \Gamma(E') \rightarrow \Gamma(\mathcal{O}_X(\mathbf{m}))$  implies that the map  $\varphi_2$  in  $(\mathfrak{X})$  is surjective. By Lemma 3.1, it suffices

prove that the map  $\psi : Q_2 \rightarrow Q_1$  is surjective. A slight modification to the proof of [Sturmfels 1996, Lemma 4.1] shows that  $Q_1 = \text{Ker}(\varphi_1)$  is generated by “binomial” elements in  $\text{Sym}_2(\Gamma(E)) \otimes \text{Sym}_2(\Gamma(E'))$  of the form

$$\mathbf{x}^a \mathbf{x}^b \otimes \mathbf{x}^c \mathbf{x}^d - \mathbf{x}^{a'} \mathbf{x}^{b'} \otimes \mathbf{x}^{c'} \mathbf{x}^{d'},$$

where  $\mathbf{x}^a, \mathbf{x}^b, \mathbf{x}^{a'}, \mathbf{x}^{b'} \in \Gamma(E)$ ,  $\mathbf{x}^c, \mathbf{x}^d, \mathbf{x}^{c'}, \mathbf{x}^{d'} \in \Gamma(E')$ , and  $\mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d} = \mathbf{a}' + \mathbf{b}' + \mathbf{c}' + \mathbf{d}'$ . Thus, the two terms in each such binomial differ by exchanging variables among the various factors. Since every such binomial element is the sum of binomials that each exchange a single pair of variables, it suffices to consider the following two cases.

In the first case, the pair of variables are exchanged between a section of  $E$  and a section  $E'$ . In particular, there exists some  $1 \leq k \leq \ell - 1$  such that the binomial element has the form

$$\mathbf{x}^a \mathbf{x}^b \otimes \mathbf{x}^c \mathbf{x}^d - \mathbf{x}^{a-e_{k,\alpha}+e_{k,\gamma}} \mathbf{x}^b \otimes \mathbf{x}^{c+e_{k,\alpha}-e_{k,\gamma}} \mathbf{x}^d,$$

where  $\mathbf{a} - \mathbf{e}_{k,\alpha}$  and  $\mathbf{c} - \mathbf{e}_{k,\gamma}$  are nonnegative. This element is the image of

$$(\mathbf{x}^a \otimes \mathbf{x}^c)(\mathbf{x}^b \otimes \mathbf{x}^d) - (\mathbf{x}^{a-e_{k,\alpha}+e_{k,\gamma}} \otimes \mathbf{x}^{c+e_{k,\alpha}-e_{k,\gamma}})(\mathbf{x}^b \otimes \mathbf{x}^d),$$

which lies in  $Q_2 = \text{Ker}(\varphi_2) \subset \text{Sym}_2(\Gamma(E) \otimes \Gamma(E'))$ .

In the second case, we may assume that the pair of variables are exchanged between two sections of  $E'$ , as exchanging variables between two sections of  $E$  is analogous. More precisely, let  $x_{k,\gamma}$  and  $x_{k,\delta}$  for some  $1 \leq k \leq \ell$  denote the exchanged variables and consider the binomial element

$$\mathbf{x}^a \mathbf{x}^b \otimes \mathbf{x}^c \mathbf{x}^d - \mathbf{x}^a \mathbf{x}^b \otimes \mathbf{x}^{c-e_{k,\gamma}+e_{k,\delta}} \mathbf{x}^{d+e_{k,\gamma}-e_{k,\delta}}$$

where  $\mathbf{c} - \mathbf{e}_{k,\gamma}$  and  $\mathbf{d} - \mathbf{e}_{k,\delta}$  are nonnegative. Since  $\mathbf{x}^a \mathbf{x}^b \otimes \mathbf{x}^c \mathbf{x}^d = \mathbf{x}^a \mathbf{x}^b \otimes \mathbf{x}^d \mathbf{x}^c$  in  $\text{Sym}_2(\Gamma(E)) \otimes \text{Sym}_2(\Gamma(E'))$ , we may also assume that  $k < \ell$ . Hence, there is a variable  $x_{k,\alpha}$  such that  $\mathbf{a} - \mathbf{e}_{k,\alpha}$  is nonnegative and

$$\begin{aligned} &\mathbf{x}^a \mathbf{x}^b \otimes \mathbf{x}^c \mathbf{x}^d - \mathbf{x}^a \mathbf{x}^b \otimes \mathbf{x}^{c-e_{k,\gamma}+e_{k,\delta}} \mathbf{x}^{d+e_{k,\gamma}-e_{k,\delta}} \\ &= \mathbf{x}^a \mathbf{x}^b \otimes \mathbf{x}^c \mathbf{x}^d - \mathbf{x}^{a-e_{k,\alpha}+e_{k,\delta}} \mathbf{x}^b \otimes \mathbf{x}^{c+e_{k,\alpha}-e_{k,\delta}} \\ &\quad + \mathbf{x}^{a-e_{k,\alpha}+e_{k,\delta}} \mathbf{x}^b \otimes \mathbf{x}^c \mathbf{x}^{d+e_{k,\alpha}-e_{k,\delta}} - \mathbf{x}^{a-e_{k,\alpha}+e_{k,\gamma}} \mathbf{x}^b \otimes \mathbf{x}^{c-e_{k,\gamma}+e_{k,\delta}} \mathbf{x}^{d+e_{k,\alpha}-e_{k,\delta}} \\ &\quad + \mathbf{x}^{a-e_{k,\alpha}+e_{k,\gamma}} \mathbf{x}^b \otimes \mathbf{x}^{c-e_{k,\gamma}+e_{k,\delta}} \mathbf{x}^{d+e_{k,\alpha}-e_{k,\delta}} - \mathbf{x}^a \mathbf{x}^b \otimes \mathbf{x}^{c-e_{k,\gamma}+e_{k,\delta}} \mathbf{x}^{d+e_{k,\gamma}-e_{k,\delta}}. \end{aligned}$$

In other words, the binomial element under consideration is a sum of binomials in which variables are exchanged between sections of  $E$  and  $E'$ . Hence, the first case shows that this binomial element lies in the image of  $Q_2$ .

We conclude that  $\psi$  is surjective and  $\mathbb{O}_X(\mathbf{m})$  is determinantly presented.  $\square$



The next proposition shows that Theorem 4.1 is optimal when  $\ell = 3$ . In fact, our experiments in Macaulay2 [Grayson and Stillman 2010] suggest that Theorem 4.1 is always sharp.

**Proposition 4.2.** *If  $X = \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_\ell}$  with  $\ell \geq 3$ , then the ample line bundle  $\mathcal{O}_X(\mathbf{1})$  is not determinantly presented.*

*Proof.* Any nontrivial factorization of  $\mathcal{O}_X(\mathbf{1})$  has the form  $E \otimes E'$ , where  $E := \mathcal{O}_X(\mathbf{u})$  for some  $\mathbf{u} \in \{0, 1\}^\ell$  and  $E' := \mathcal{O}_X(\mathbf{1} - \mathbf{u})$ . For a suitable choice of bases for  $\Gamma(\mathcal{O}_X(\mathbf{u}))$  and  $\Gamma(\mathcal{O}_X(\mathbf{1} - \mathbf{u}))$ , the associated matrix  $\Omega(\mathcal{O}_X(\mathbf{u}), \mathcal{O}_X(\mathbf{1} - \mathbf{u}))$  is the generic  $(s \times t)$ -matrix with  $s := \sum_{u_i \neq 0} (n_i + 1)$  and  $t := \sum_{i=0}^\ell (n_i + 1) - s$ . Since the 2-minors of a generic  $(s \times t)$ -matrix define  $\mathbb{P}^{s-1} \times \mathbb{P}^{t-1}$  in its Segre embedding, we see that  $\mathcal{O}_X(\mathbf{1})$  is not determinantly presented when  $\ell \geq 3$ .  $\square$

**Example 4.3.** Consider the variety  $X = \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$  embedded in

$$\mathbb{P}^{11} = \text{Proj}(\mathbb{k}[y_0, \dots, y_{11}])$$

by the complete linear series of  $\mathcal{O}_X(2, 1, 1)$ . If  $R = \mathbb{k}[x_{1,0}, x_{1,1}, x_{2,0}, x_{2,1}, x_{3,0}, x_{3,1}]$  is the total coordinate ring of  $X$ , then the twelve monomials

$$\left\{ \begin{array}{cccc} x_{1,0}^2 x_{2,0} x_{3,0}, & x_{1,0}^2 x_{2,0} x_{3,1}, & x_{1,0}^2 x_{2,1} x_{3,0}, & x_{1,0}^2 x_{2,1} x_{3,1}, \\ x_{1,0} x_{1,1} x_{2,0} x_{3,0}, & x_{1,0} x_{1,1} x_{2,0} x_{3,1}, & x_{1,0} x_{1,1} x_{2,1} x_{3,0}, & x_{1,0} x_{1,1} x_{2,1} x_{3,1}, \\ x_{1,1}^2 x_{2,0} x_{3,0}, & x_{1,1}^2 x_{2,0} x_{3,1}, & x_{1,1}^2 x_{2,1} x_{3,0}, & x_{1,1}^2 x_{2,1} x_{3,1} \end{array} \right\}$$

give an ordered basis for  $\Gamma(\mathcal{O}_X(2, 1, 1))$ . The homogeneous ideal  $I_{X|\mathbb{P}^{11}}$  is the toric ideal associated to these monomials and is minimally generated by thirty three quadrics. Choosing  $\{x_{1,0}x_{2,0}, x_{1,0}x_{2,1}, x_{1,1}x_{2,0}, x_{1,1}x_{2,1}\}$  as ordered basis for  $\Gamma(\mathcal{O}_X(1, 1, 0))$  and  $\{x_{1,0}x_{3,0}, x_{1,0}x_{3,1}, x_{1,1}x_{3,0}, x_{1,1}x_{3,1}\}$  for  $\Gamma(\mathcal{O}_X(1, 0, 1))$ , we find  $\Omega(\mathcal{O}_X(1, 1, 0), \mathcal{O}_X(1, 0, 1))$  is

$$\begin{bmatrix} y_0 & y_1 & y_4 & y_5 \\ y_2 & y_3 & y_6 & y_7 \\ y_4 & y_5 & y_8 & y_9 \\ y_6 & y_7 & y_{10} & y_{11} \end{bmatrix}$$

and one may verify that the 2-minors of this matrix generates the ideal of  $X$ , so  $\mathcal{O}_X(2, 1, 1)$  is determinantly presented.  $\diamond$

However, if we consider multiple factorizations of a very ample line bundle on a product of projective spaces, then we do obtain a convenient expression of the homogeneous ideal as the 2-minors of matrices. This perspective give a conceptual explanation for both [Hà 2002, Theorem 2.6] and [Bernardi 2008, Theorem 3.11].

**Proposition 4.4.** *If  $X = \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_\ell}$ , then the homogeneous ideal of  $X$  in  $\mathbb{P}(\mathcal{O}_X(\mathbf{d}))$  is generated by the 2-minors of the matrices  $\Omega(\mathcal{O}_X(\mathbf{e}_i), \mathcal{O}_X(\mathbf{d} - \mathbf{e}_i))$ , where  $1 \leq i \leq \ell$ .*

*Proof.* Given Theorem 4.1, we may assume that  $\ell \geq 3$ . For brevity, set  $E_i := \mathbb{O}_X(\mathbf{e}_i)$  and  $E'_i := \mathbb{O}_X(\mathbf{d} - \mathbf{e}_i)$ , where  $1 \leq i \leq \ell$ . Since  $\Gamma(E_i) \otimes \Gamma(E'_i)$  surjects onto  $\Gamma(\mathbb{O}_X(\mathbf{d}))$ , the map  $\varphi_2$  in  $(\mathfrak{X})$  is surjective, and it suffices to prove that the map  $\psi : Q_2 \rightarrow Q_1$  is surjective. By an abuse of notation, we use  $\epsilon_i$  to denote the canonical inclusion map onto the  $i$ -th summand for all three of the direct sums appearing in the middle column of  $(\mathfrak{X})$ . As in the proof of Theorem 4.1,  $Q_1$  is generated by binomial elements in  $\bigoplus_{k=1}^{\ell} \text{Sym}_2(\Gamma(E_k)) \otimes \text{Sym}_2(\Gamma(E'_k))$ . Generators have the form

$$\epsilon_i(x_{i,\alpha}x_{i,\beta} \otimes \mathbf{x}^c \mathbf{x}^d) - \epsilon_j(x_{j,\gamma}x_{j,\delta} \otimes \mathbf{x}^a \mathbf{x}^b),$$

where  $x_{i,\alpha}, x_{i,\beta} \in \Gamma(E_i)$ ,  $\mathbf{x}^c, \mathbf{x}^d \in \Gamma(E'_i)$ ,  $x_{j,\gamma}, x_{j,\delta} \in \Gamma(E_j)$ ,  $\mathbf{x}^a, \mathbf{x}^b \in \Gamma(E'_j)$  and  $\mathbf{e}_{i,\alpha} + \mathbf{e}_{i,\beta} + \mathbf{c} + \mathbf{d} = \mathbf{a} + \mathbf{b} + \mathbf{e}_{j,\gamma} + \mathbf{e}_{j,\delta}$ . We consider the following two cases.

In the first case, we have  $i = j$ . Since every binomial element is the sum of binomials that each exchange a single pair of variables, it suffices to consider an element of the form

$$\epsilon_i(x_{i,\alpha}x_{i,\beta} \otimes \mathbf{x}^c \mathbf{x}^d - x_{i,\alpha}x_{i,\beta} \otimes \mathbf{x}^{c - \mathbf{e}_{k,\gamma} + \mathbf{e}_{k,\delta}} \mathbf{x}^{d + \mathbf{e}_{k,\gamma} - \mathbf{e}_{k,\delta}}),$$

where  $1 \leq k \leq \ell$  and both  $\mathbf{c} - \mathbf{e}_{k,\gamma}$  and  $\mathbf{d} - \mathbf{e}_{k,\delta}$  are nonnegative. This element is the image of

$$\begin{aligned} \epsilon_i((x_{i,\alpha} \otimes \mathbf{x}^c)(x_{i,\beta} \otimes \mathbf{x}^d) \\ - (x_{i,\alpha} \otimes \mathbf{x}^{c - \mathbf{e}_{k,\gamma} + \mathbf{e}_{k,\delta}})(x_{i,\beta} \otimes \mathbf{x}^{d + \mathbf{e}_{k,\gamma} - \mathbf{e}_{k,\delta}})) \\ - \epsilon_k((x_{k,\gamma} \otimes \mathbf{x}^{c + \mathbf{e}_{i,\alpha} - \mathbf{e}_{k,\gamma}})(x_{k,\delta} \otimes \mathbf{x}^{d + \mathbf{e}_{i,\beta} - \mathbf{e}_{k,\delta}}) \\ - (x_{k,\delta} \otimes \mathbf{x}^{c + \mathbf{e}_{i,\alpha} - \mathbf{e}_{k,\gamma}})(x_{k,\gamma} \otimes \mathbf{x}^{d + \mathbf{e}_{i,\beta} - \mathbf{e}_{k,\delta}})), \end{aligned}$$

which lies in  $Q_2 = \text{Ker}(\varphi_2)$ .

For the second case, we have  $i \neq j$ . We may assume that the binomial element has the form  $\epsilon_i(x_{i,\alpha}x_{i,\beta} \otimes \mathbf{x}^c \mathbf{x}^d) - \epsilon_j(x_{j,\gamma}x_{j,\delta} \otimes \mathbf{x}^{c + \mathbf{e}_{i,\alpha} - \mathbf{e}_{j,\gamma}} \mathbf{x}^{d + \mathbf{e}_{i,\beta} - \mathbf{e}_{j,\delta}})$ , where  $\mathbf{c} - \mathbf{e}_{j,\gamma}$  and  $\mathbf{d} - \mathbf{e}_{j,\delta}$  are nonnegative, because any additional exchanges of variables can be obtained by adding elements from the first case. This element is the image of

$$\epsilon_i((x_{i,\alpha} \otimes \mathbf{x}^c)(x_{i,\beta} \otimes \mathbf{x}^d)) - \epsilon_j((x_{j,\gamma} \otimes \mathbf{x}^{c + \mathbf{e}_{i,\alpha} - \mathbf{e}_{j,\gamma}})(x_{j,\delta} \otimes \mathbf{x}^{d + \mathbf{e}_{i,\beta} - \mathbf{e}_{j,\delta}})),$$

which lies in  $Q_2 = \text{Ker}(\varphi_2)$ . □

**Example 4.5.** We consider the variety  $X = \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$  embedded in  $\mathbb{P}^7 = \text{Proj}(\mathbb{k}[y_0, \dots, y_7])$  by the complete linear series of the line bundle  $\mathbb{O}_X(1, 1, 1)$ . The homogeneous ideal  $I_X|_{\mathbb{P}^7}$  is the toric ideal associated to the monomial list

$$\left\{ \begin{array}{cccc} x_{1,0}x_{2,0}x_{3,0}, & x_{1,0}x_{2,0}x_{3,1}, & x_{1,0}x_{2,1}x_{3,0}, & x_{1,0}x_{2,1}x_{3,1}, \\ x_{1,1}x_{2,0}x_{3,0}, & x_{1,1}x_{2,0}x_{3,1}, & x_{1,1}x_{2,1}x_{3,0}, & x_{1,1}x_{2,1}x_{3,1} \end{array} \right\}$$

and is minimally generated by nine quadrics. Choosing appropriate monomials for the ordered bases of the global sections, we obtain

$$\begin{aligned} \Omega(\mathbb{O}_X(1, 0, 0), \mathbb{O}_X(0, 1, 1)) &= \begin{bmatrix} y_0 & y_1 & y_2 & y_3 \\ y_4 & y_5 & y_6 & y_7 \end{bmatrix}, \\ \Omega(\mathbb{O}_X(0, 1, 0), \mathbb{O}_X(1, 0, 1)) &= \begin{bmatrix} y_0 & y_1 & y_4 & y_5 \\ y_2 & y_3 & y_6 & y_7 \end{bmatrix}, \\ \Omega(\mathbb{O}_X(0, 0, 1), \mathbb{O}_X(1, 1, 0)) &= \begin{bmatrix} y_0 & y_2 & y_4 & y_6 \\ y_1 & y_3 & y_5 & y_7 \end{bmatrix}. \end{aligned}$$

It follows that  $\mathbb{O}_X(1, 1, 1)$  is not determinantly presented, but one easily verifies that the ideal  $I_X|_{\mathbb{P}^7}$  is generated by the 2-minors of all three matrices.  $\diamond$

Multiple factorizations of a very ample line bundle allow one to describe a larger number of homogeneous ideals via 2-minors. With this in mind, it would be interesting to write down the analogue of Theorem 3.2 for multiple factorizations of the line bundle.

**4.2. Toric varieties.** In addition to the bound given in Corollary 3.3, there is an effective bound for toric varieties involving adjoint bundles for toric varieties; see [Hering et al. 2006, Corollary 1.6]. Recall that a line bundle on a toric variety  $X$  is nef if and only if it is globally generated, and the dualizing sheaf  $K_X$  is a line bundle if and only if  $X$  is Gorenstein.

**Proposition 4.6.** *Let  $X$  be a projective  $n$ -dimensional Gorenstein toric variety with dualizing sheaf  $K_X$ , and let  $B_1, \dots, B_\ell$  be the minimal generators of its nef cone  $\text{Nef}(X)$ . Suppose that  $\mathbf{m}, \mathbf{m}' \in \mathbb{N}^\ell$  satisfy  $\mathbf{B}^{\mathbf{m}-\mathbf{u}}, \mathbf{B}^{\mathbf{m}'-\mathbf{u}} \in \mathfrak{B}$  for all  $\mathbf{u} \in \mathbb{N}^\ell$  with  $|\mathbf{u}| \leq n + 1$ . If  $X \neq \mathbb{P}^n$  and  $\mathbf{w} \in \mathbb{N}^\ell$ , then  $L = K_X^2 \otimes \mathbf{B}^{\mathbf{m}+\mathbf{m}'+\mathbf{w}}$  is determinantly presented.*

*Proof.* Factor  $L$  as  $L = E \otimes E'$ , where  $E := K_X \otimes \mathbf{B}^{\mathbf{m}+\mathbf{w}}$  and  $E' := K_X \otimes \mathbf{B}^{\mathbf{m}'}$ . Since  $\mathbf{B}^{\mathbf{m}-(n+1)\mathbf{e}_j}, \mathbf{B}^{\mathbf{m}'-(n+1)\mathbf{e}_j} \in \mathfrak{B}$ , Corollary 0.2 in [Fujino 2003] implies that  $E \otimes \mathbf{B}^{-\mathbf{e}_j}$  and  $E' \otimes \mathbf{B}^{-\mathbf{e}_j}$  belong to  $\mathfrak{B}$  for all  $1 \leq j \leq \ell$ . For any torus-invariant curve  $Y$ , there is a  $\mathbf{B}^{\mathbf{e}_j}$  such that  $\mathbf{B}^{\mathbf{e}_j} \cdot Y > 0$ . Theorem 3.4 in [Mustață 2002] implies that  $E, E^2$  and  $E'$  are regular with respect to  $B_1, \dots, B_\ell$ . Hence, Proposition 2.5 shows that  $L, E$ , and  $E'$  satisfy  $N_1$ , and that  $E$  has a linear free presentation with respect to  $E'$ , that  $E'$  has a linear free presentation with respect to  $E$ , and that  $E^2$  has a linear free presentation with respect to  $E'$ . Therefore, Theorem 3.2 shows that  $L$  is determinantly presented.  $\square$

*Proof of Theorem 1.3 for toric varieties.* This is a special case of Proposition 4.6.  $\square$

We give an example showing that Theorem 1.3 is not sharp for all toric varieties.

**Example 4.7.** Consider the toric del Pezzo surface  $X$  obtained by blowing up  $\mathbb{P}^2$  at the three torus-fixed points. Let  $R := \mathbb{k}[x_0, \dots, x_5]$  be the total coordinate ring of  $X$ . The anticanonical bundle  $K_X^{-1}$  is very ample and corresponds to polygon

$$P := \text{conv}\{(1, 0), (1, 1), (0, 1), (-1, 0), (-1, -1), (0, -1)\}.$$

It is easy to see that the polygon  $P$  is the smallest lattice polygon with its inner normal fan. The polygon  $2P$  contains 19 lattice points. The corresponding monomials

$$\left\{ \begin{array}{cccccc} x_0^4 x_1^4 x_2^2 x_5^2, & x_0^4 x_1^3 x_2 x_4 x_5^3, & x_0^4 x_1^2 x_2^2 x_4^2, & x_0^3 x_1^4 x_2^3 x_3 x_5, & x_0^3 x_1^3 x_2^2 x_3 x_4 x_5^2, \\ x_0^3 x_1^2 x_2 x_3 x_4^2 x_5^3, & x_0^3 x_1 x_2 x_3^3 x_4^4, & x_0^2 x_1^4 x_2^4 x_3^2, & x_0^2 x_1^3 x_2^3 x_3^2 x_4 x_5, & x_0^2 x_1^2 x_2^2 x_3^2 x_4^2 x_5^2, \\ x_0^2 x_1 x_2 x_3^2 x_4^3 x_5^3, & x_0^2 x_3^2 x_4^4 x_5^4, & x_0 x_1^3 x_2^4 x_3^3 x_4, & x_0 x_1^2 x_2^3 x_3^3 x_4^2 x_5, & x_0 x_1 x_2^2 x_3^3 x_4^3 x_5^2, \\ x_0 x_2 x_3^3 x_4^4 x_5^3, & x_1^2 x_2^4 x_3^4 x_4^2, & x_1 x_2^3 x_3^4 x_4^3 x_5, & x_2^2 x_3^4 x_4^4 x_5^2 \end{array} \right\}$$

embed  $X$  into  $\mathbb{P}^{18} = \text{Proj}(\mathbb{k}[y_0, \dots, y_{18}])$ . The homogeneous ideal  $I_{X|\mathbb{P}^{18}}$  is the toric ideal associated to these monomials and it is minimally generated by 129 quadrics. Choosing

$$\{x_0^2 x_1^2 x_2 x_5, x_0^2 x_1 x_4 x_5^2, x_0 x_1^2 x_2^2 x_3, x_0 x_1 x_2 x_3 x_4 x_5, x_0 x_3 x_4^2 x_5^2, x_1 x_2^2 x_3^2 x_4, x_2 x_3^2 x_4^2 x_5\}$$

as an ordered basis for  $\Gamma(K_X^{-1})$ , the matrix  $\Omega(K_X^{-1}, K_X^{-1})$  is

$$\begin{bmatrix} y_0 & y_1 & y_3 & y_4 & y_5 & y_8 & y_9 \\ y_1 & y_2 & y_4 & y_5 & y_6 & y_9 & y_{10} \\ y_3 & y_4 & y_7 & y_8 & y_9 & y_{12} & y_{13} \\ y_4 & y_5 & y_8 & y_9 & y_{10} & y_{13} & y_{14} \\ y_5 & y_6 & y_9 & y_{10} & y_{11} & y_{14} & y_{15} \\ y_8 & y_9 & y_{12} & y_{13} & y_{14} & y_{16} & y_{17} \\ y_9 & y_{10} & y_{13} & y_{14} & y_{15} & y_{17} & y_{18} \end{bmatrix},$$

and its 2-minors generate  $I_{X|\mathbb{P}^{18}}$ . However, Theorem 1.3 only establishes that the line bundle  $K_X^{-4} = K_X^2 \otimes (K_X^{-1})^{2 \cdot 2 + 2}$  is determinantly presented.  $\diamond$

**4.3. Smooth varieties.** For smooth varieties, we also have an effective bound for adjoint bundles; see Theorem 1.3.

*Proof of Theorem 1.3 for smooth varieties.* Factor the line bundle  $L$  as  $L = E \otimes E'$  where  $E := K_X \otimes A^{n+1}$  and  $E' := K_X \otimes A^{j-n-1} \otimes B$ . Since  $j \geq 2n + 2$  and  $E$  is nef (see [Lazarsfeld 2004, Example 1.5.35]), Proposition 2.6 implies that  $L$ ,  $E$ , and  $E'$  satisfy  $N_1$ ,  $E$  has a linear free presentation with respect to  $E'$ , that  $E'$  has a linear free presentation with respect to  $E$ , and that  $E^2$  has a linear free presentation with respect to  $E'$ . Thus, Theorem 3.2 shows that  $L$  is determinantly presented.  $\square$

We end with an example showing that the hypotheses in Theorem 1.3 are optimal without further restrictions on the varieties under consideration.

**Example 4.8.** Let  $X = \text{Gr}(2, 4)$  be the Grassmannian parametrizing all two-dimensional subspaces of the vector space  $\mathbb{k}^4$ . Let  $\mathcal{O}_X(1)$  denote the determinant of the universal rank 2 subbundle on  $X$ . The associated complete linear series determines the Plücker embedding of  $X$  into  $\mathbb{P}^5 = \text{Proj}(\mathbb{k}[x_{1,2}, x_{1,3}, x_{1,4}, x_{2,3}, x_{2,4}, x_{3,4}])$ . As  $I_{X|\mathbb{P}^5} = \langle x_{1,2}x_{3,4} - x_{1,3}x_{2,4} + x_{2,3}x_{1,4} \rangle$ , it follows that  $\mathcal{O}_X(1)$  is not determinantly presented. On the other hand, the monomials

$$\left\{ \begin{array}{cccccc} x_{1,2}^2, & x_{1,2}x_{1,3}, & x_{1,2}x_{1,4}, & x_{1,2}x_{2,3}, & x_{1,2}x_{2,4}, & x_{1,2}x_{3,4}, & x_{1,3}^2, \\ x_{1,3}x_{1,4}, & x_{1,3}x_{2,3}, & & x_{1,3}x_{3,4}, & x_{1,4}^2, & x_{1,4}x_{2,3}, & x_{1,4}x_{2,4}, \\ x_{1,4}x_{3,4}, & x_{2,3}^2, & x_{2,3}x_{2,4}, & x_{2,3}x_{3,4}, & x_{2,4}^2, & x_{2,4}x_{3,4}, & x_{3,4}^2 \end{array} \right\}$$

form an ordered basis for  $\Gamma(\mathcal{O}_X(2))$ , so the complete linear series of  $\mathcal{O}_X(2)$  embeds  $X$  into  $\mathbb{P}^{19} = \text{Proj}(\mathbb{k}[y_0, \dots, y_{19}])$ . The matrix  $\Omega(\mathcal{O}_X(1), \mathcal{O}_X(1))$  is

$$\begin{bmatrix} y_0 & y_1 & y_2 & y_3 & y_4 & y_5 \\ y_1 & y_6 & y_7 & y_8 & y_5 + y_{11} & y_9 \\ y_2 & y_7 & y_{10} & y_{11} & y_{12} & y_{13} \\ y_3 & y_8 & y_{11} & y_{14} & y_{15} & y_{16} \\ y_4 & y_5 + y_{11} & y_{12} & y_{15} & y_{17} & y_{18} \\ y_5 & y_9 & y_{13} & y_{16} & y_{18} & y_{19} \end{bmatrix}$$

and the 2-minors of this matrix generated  $I_{X|\mathbb{P}^{19}}$  (indeed, this is the second Veronese of the Plücker embedding). Since  $K_X = \mathcal{O}_X(-4)$  and  $\mathcal{O}_X(2) = K_X^2 \otimes \mathcal{O}_X(1)^{2 \cdot 4 + 2}$ , we see that the bound in Theorem 1.3 is sharp in this case.  $\diamond$

### Acknowledgements

We thank David Eisenbud, Tony Geramita, Rob Lazarsfeld, and Pete Vermeire for helpful discussions. The computer software Macaulay2 [Grayson and Stillman 2010] was useful for generating examples. We are grateful to the referee for the careful reading.

### References

[Arapura 2004] D. Arapura, “Frobenius amplitude and strong vanishing theorems for vector bundles”, *Duke Math. J.* **121**:2 (2004), 231–267. MR 2005d:14025 Zbl 1067.14018

[Bernardi 2008] A. Bernardi, “Ideals of varieties parameterized by certain symmetric tensors”, *J. Pure Appl. Algebra* **212**:6 (2008), 1542–1559. MR 2009c:14106 Zbl 1131.14055

[Graf v. Bothmer and Hulek 2004] H.-C. Graf v. Bothmer and K. Hulek, “Geometric syzygies of elliptic normal curves and their secant varieties”, *Manuscripta Math.* **113**:1 (2004), 35–68. MR 2006b:14009 Zbl 1053.14032

- [Buczyński and Buczyński 2010] W. Buczyński and J. Buczyński, “Secant varieties to high degree Veronese reembeddings, catalecticant matrices and smoothable Gorenstein schemes”, preprint, version 2, 2010. arXiv 1012.3563v2
- [Buczyński et al. 2010] J. Buczyński, A. Ginensky, and J. Landsberg, “Determinantal equations for secant varieties and the Eisenbud–Koh–Stillman conjecture”, preprint, 2010. arXiv 1007.0192
- [Catalano-Johnson 1996] M. L. Catalano-Johnson, “The possible dimensions of the higher secant varieties”, *Amer. J. Math.* **118**:2 (1996), 355–361. MR 97a:14058 Zbl 0871.14043
- [Catalisano et al. 2008] M. V. Catalisano, A. V. Geramita, and A. Gimigliano, “On the ideals of secant varieties to certain rational varieties”, *J. Algebra* **319**:5 (2008), 1913–1931. MR 2009g:14068 Zbl 1142.14035
- [Ein and Lazarsfeld 1993] L. Ein and R. Lazarsfeld, “Syzygies and Koszul cohomology of smooth projective varieties of arbitrary dimension”, *Invent. Math.* **111**:1 (1993), 51–67. MR 93m:13006 Zbl 0814.14040
- [Eisenbud 1988] D. Eisenbud, “Linear sections of determinantal varieties”, *Amer. J. Math.* **110**:3 (1988), 541–575. MR 89h:14041 Zbl 0681.14028
- [Eisenbud 2005] D. Eisenbud, *The geometry of syzygies*, Graduate Texts in Math. **229**, Springer, New York, 2005. MR 2005h:13021 Zbl 1086.14044
- [Eisenbud et al. 1988] D. Eisenbud, J. Koh, and M. Stillman, “Determinantal equations for curves of high degree”, *Amer. J. Math.* **110**:3 (1988), 513–539. MR 89g:14023 Zbl 0681.14027
- [Fujino 2003] O. Fujino, “Notes on toric varieties from Mori theoretic viewpoint”, *Tohoku Math. J.* (2) **55**:4 (2003), 551–564. MR 2004j:14059 Zbl 1078.14077
- [Fujita 1983] T. Fujita, “Vanishing theorems for semipositive line bundles”, pp. 519–528 in *Algebraic geometry* (Tokyo/Kyoto, 1982), Lecture Notes in Math. **1016**, Springer, Berlin, 1983. MR 85g:14023 Zbl 0522.14010
- [Gallego and Purnaprajna 1999] F. J. Gallego and B. P. Purnaprajna, “Syzygies of projective surfaces: an overview”, *J. Ramanujan Math. Soc.* **14** (1999), 65–93. MR 2000f:14019 Zbl 1058.14025
- [Garcia et al. 2005] L. D. Garcia, M. Stillman, and B. Sturmfels, “Algebraic geometry of Bayesian networks”, *J. Symbolic Comput.* **39**:3-4 (2005), 331–355. MR 2006g:68242 Zbl 1126.68102
- [Ginensky 2010] A. Ginensky, “A generalization of the Clifford index and determinantal equations for curves and their secant varieties”, preprint, 2010. arXiv 1002.2023
- [Grayson and Stillman 2010] D. Grayson and M. Stillman, *Macaulay2, a software system for research in algebraic geometry*, 2010, available at <http://www.math.uiuc.edu/Macaulay2/>.
- [Green 1984a] M. L. Green, “Koszul cohomology and the geometry of projective varieties”, *J. Differential Geom.* **19**:1 (1984), 125–171. MR 85e:14022 Zbl 0559.14008
- [Green 1984b] M. L. Green, “Koszul cohomology and the geometry of projective varieties, II”, *J. Differential Geom.* **20**:1 (1984), 279–289. MR 86j:14011 Zbl 0559.14009
- [Green 1989] M. L. Green, “Koszul cohomology and geometry”, pp. 177–200 in *Lectures on Riemann surfaces* (Trieste, 1987), edited by M. Raynaud and T. Shioda, World Sci. Publ., Teaneck, NJ, 1989. MR 91k:14012 Zbl 0800.14004
- [Green and Lazarsfeld 1985] M. Green and R. Lazarsfeld, “On the projective normality of complete linear series on an algebraic curve”, *Invent. Math.* **83**:1 (1985), 73–90. MR 87g:14022 Zbl 0594.14010
- [Hà 2002] H. T. Hà, “Box-shaped matrices and the defining ideal of certain blowup surfaces”, *J. Pure Appl. Algebra* **167**:2-3 (2002), 203–224. MR 2002h:13020 Zbl 1044.13004

- [Hering et al. 2006] M. Hering, H. Schenck, and G. G. Smith, “Syzygies, multigraded regularity and toric varieties”, *Compos. Math.* **142**:6 (2006), 1499–1506. MR 2007k:13025 Zbl 1111.14052
- [Inamdar 1997] S. P. Inamdar, “On syzygies of projective varieties”, *Pacific J. Math.* **177**:1 (1997), 71–76. MR 98a:14010 Zbl 0898.14015
- [Lazarsfeld 1989] R. Lazarsfeld, “A sampling of vector bundle techniques in the study of linear series”, pp. 500–559 in *Lectures on Riemann surfaces* (Trieste, 1987), edited by M. Raynaud and T. Shioda, World Sci. Publ., Teaneck, NJ, 1989. MR 92f:14006 Zbl 0800.14003
- [Lazarsfeld 2004] R. Lazarsfeld, *Positivity in algebraic geometry, I: Classical setting: line bundles and linear series*, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)* **48**, Springer, Berlin, 2004. MR 2005k:14001a Zbl 1093.14501
- [Maclagan and Smith 2004] D. Maclagan and G. G. Smith, “Multigraded Castelnuovo–Mumford regularity”, *J. Reine Angew. Math.* **571** (2004), 179–212. MR 2005g:13027 Zbl 1062.13004
- [Mumford 1970] D. Mumford, “Varieties defined by quadratic equations”, pp. 29–100 in *Questions on Algebraic Varieties (C.I.M.E., III)* (Ciclo, Varenna, 1969), Edizioni Cremonese, Rome, 1970. MR 44 #209 Zbl 0198.25801
- [Mustață 2002] M. Mustață, “Vanishing theorems on toric varieties”, *Tohoku Math. J. (2)* **54**:3 (2002), 451–470. MR 2003e:14013 Zbl 1092.14064
- [Pareschi and Popa 2004] G. Pareschi and M. Popa, “Regularity on abelian varieties, II: Basic results on linear series and defining equations”, *J. Algebraic Geom.* **13** (2004), 167–193. MR 2005a:14059 Zbl 1073.14061
- [Ravi 1994] M. S. Ravi, “Determinantal equations for secant varieties of curves”, *Comm. Algebra* **22**:8 (1994), 3103–3106. MR 95c:14029 Zbl 0809.14038
- [Room 1938] T. G. Room, *The Geometry of Determinantal Loci*, Cambridge University Press, 1938. Zbl 0020.05402 JFM 64.0693.04
- [Rubei 2000] E. Rubei, “On syzygies of abelian varieties”, *Trans. Amer. Math. Soc.* **352**:6 (2000), 2569–2579. MR 2000j:14071 Zbl 0967.14013
- [Sturmfels 1996] B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series **8**, American Mathematical Society, Providence, RI, 1996. MR 97b:13034 Zbl 0856.13020
- [Sturmfels and Sullivant 2006] B. Sturmfels and S. Sullivant, “Combinatorial secant varieties”, *Pure Appl. Math. Q.* **2**:3 (2006), 867–891. MR 2007h:14082 Zbl 1107.14045
- [Sullivant 2008] S. Sullivant, “Combinatorial symbolic powers”, *J. Algebra* **319**:1 (2008), 115–142. MR 2009c:13005 Zbl 1133.13027
- [Weibel 1994] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics **38**, Cambridge University Press, 1994. MR 95f:18001 Zbl 0797.18001

Communicated by Kei-Ichi Watanabe

Received 2010-05-20

Revised 2011-05-31

Accepted 2011-06-30

jsidman@mtholyoke.edu

*Department of Mathematics and Statistics,  
Mount Holyoke College, 415A Clapp Lab,  
South Hadley, MA 01075, United States  
<http://www.mtholyoke.edu/~jsidman/>*

ggsmith@mast.queensu.ca

*Department of Mathematics and Statistics,  
Queen's University, 512 Jeffery Hall, University Avenue,  
Kingston, ON K7L 3N6, Canada  
<http://www.mast.queensu.ca/~ggsmith/>*





# Involutions, weights and $p$ -local structure

Geoffrey R. Robinson

We prove that for an odd prime  $p$ , a finite group  $G$  with no element of order  $2p$  has a  $p$ -block of defect zero if it has a non-Abelian Sylow  $p$ -subgroup or more than one conjugacy class of involutions. For  $p=2$ , we prove similar results using elements of order 3 in place of involutions. We also illustrate (for an arbitrary prime  $p$ ) that certain pairs  $(Q, y)$ , with a  $p$ -regular element  $y$  and  $Q$  a maximal  $y$ -invariant  $p$ -subgroup, give rise to  $p$ -blocks of defect zero of  $N_G(Q)/Q$ , and we give lower bounds for the number of such blocks which arise. This relates to the weight conjecture of J. L. Alperin.

## Introduction

Involutions have played a crucial role in finite group theory for many decades. They also figure prominently in representation theory, both ordinary and modular. Examples of the former include their occurrence in finite reflection groups, and an example of the latter is that in characteristic 2, J. Murray proved in [2006] that the projective summands of the (characteristic 2) permutation module (under conjugation action) on the solutions of  $x^2 = 1$  in  $G$  are (in bijection with) the real 2-blocks of defect zero.

Involutions also influence representation theory in odd characteristic. It was proved by Brauer and Fowler in [1955] that when  $p$  is an odd prime,  $G$  has a  $p$ -block of defect zero if there is an involution  $t \in G$  that neither inverts nor centralizes any nontrivial  $p$ -element of  $G$ . This result was extended by T. Wada [1977], who proved that if there are  $r$  mutually nonconjugate involutions of  $G$  that neither invert nor centralize any nontrivial  $p$ -element of  $G$ , then  $G$  has at least  $r$  distinct  $p$ -blocks of defect zero. We prove here that when  $p = 2$ , elements of order 3 can play a role analogous to that played when  $p$  is odd by involutions in the results above: We prove that the number of 2-blocks of defect zero of  $G$  is at least as great as the number of conjugacy classes of elements of order 3 that normalize no nontrivial 2-subgroup of  $G$ .

We also point out here that results of this nature can be combined with local group-theoretic analysis to prove that if  $p$  is an odd prime and  $G$  is a group without

---

*MSC2010:* 20C20.

*Keywords:* block, involution.

elements of order  $2p$ , then  $G$  has a  $p$ -block of defect zero if it has more than one conjugacy class of involutions (we prove a more precise result without using the classification of finite simple groups, which could be sharpened even further by using that classification).

In a different direction, the celebrated weight conjecture of J. L. Alperin (in its nonblockwise version) defines (for a fixed prime  $p$ ) a *weight* of  $G$  (up to conjugacy) as a pair  $(Q, S)$ , where  $Q$  is a  $p$ -subgroup of  $G$  and  $S$  is an absolutely simple projective  $N_G(Q)/Q$  module in characteristic  $p$ . Alperin's weight conjecture then asserts that the number of nonconjugate weights of  $G$  for  $p$  should be the number of conjugacy classes of  $p$ -regular elements of  $G$  (which is also the number of isomorphism types of absolutely simple modules for  $G$  in characteristic  $p$ ). At present, there seems to be no reason to expect a natural bijection between weights and  $p$ -regular conjugacy classes, or between weights and characteristic  $p$  simple modules for  $G$  (though it is impossible to preclude the possibility that one or the other might emerge in future). Relatively few purely group-theoretic criteria are known to date that place nonconjectural bounds on the number of weights. We give some group-theoretic conditions of this nature that place lower bounds on the number of weights, using sharpenings of results of Brauer and Fowler [1955], Tsushima [1977] and Wada [1977], going somewhat further than my results in [Robinson 1983], and incorporating the result about 2-blocks of defect zero and elements of order 3 that normalize no nontrivial 2-subgroup of  $G$ .

A naïve attempt at associating  $p$ -regular classes with weights of  $G$  might be to consider a  $p$ -regular element  $y$  and a maximal  $y$ -invariant  $p$ -subgroup  $Q$ . Then  $y$  normalizes no nontrivial  $p$ -subgroup of  $N_G(Q)/Q$  and it might be hoped that a  $p$ -block of defect zero of  $N_G(Q)/Q$  could be naturally associated to  $y$  (or  $yQ$ ). More ambitiously, it might be hoped that weights could be parametrized in terms of conjugacy classes of pairs  $(Q, y)$ , where  $y$  is a  $p$ -regular element of  $G$  and  $Q$  is a maximal  $y$ -invariant  $p$ -subgroup of  $G$ .

However, there are usually more conjugacy classes of such pairs  $(Q, y)$  than there are simple modules. The number of conjugacy classes of such pairs  $(Q, y)$  is equal to the number of simple modules precisely when  $C_G(y)$  transitively permutes the maximal  $y$ -invariant  $p$ -subgroups of  $G$  for each  $p$ -regular  $y \in G$ . In general, this need not be the case. For example, when  $p = 3$  and  $G \cong \text{PSL}(2, 11)$  we may take  $y$  to be an involution. There is a Sylow 3-subgroup  $Q$  of  $G$  that is centralized by  $y$ , and there is another Sylow 3-subgroup  $R$  of  $G$  whose nonidentity elements are inverted by  $y$ . Clearly  $Q$  and  $R$  are not conjugate via an element of  $C_G(y)$ .

We are nevertheless interested in pairs  $(Q, y)$ , where  $y$  is  $p$ -regular and  $Q$  is a maximal  $y$ -invariant  $p$ -subgroup, and we will point out some instances where they give rise to weights.

- Lemma 1.** (i) Let  $Q$  be a  $p$ -subgroup of  $G$  and  $y$  be a  $p$ -regular element of  $N_G(Q)$  such that  $yQ \in O_{p'}(N_G(Q)/Q)$ . Then  $Q$  is a maximal  $y$ -invariant  $p$ -subgroup of  $G$  if and only if  $C_Q(y) \in \text{Syl}_p(N_G(Q) \cap C_G(y))$ .
- (ii) Suppose that  $p$  is odd, and let  $Q$  be a  $p$ -subgroup of  $G$  and  $y$  be an involution of  $N_G(Q)$ . Then  $Q$  is a maximal  $y$ -invariant  $p$ -subgroup of  $G$  if and only if  $yQ$  neither inverts nor centralizes any element of order  $p$  in  $N_G(Q)/Q$ .
- (iii) Suppose that  $p = 2$ , and let  $Q$  be a 2-subgroup of  $G$  and  $y$  be an element of order 3 in  $N_G(Q)$ . Then  $Q$  is a maximal  $y$ -invariant 2-subgroup of  $G$  if and only if  $yQ$  is not contained in any subgroup isomorphic to  $A_4$  of  $N_G(Q)/Q$ , and  $yQ$  does not centralize any involution of  $N_G(Q)/Q$ .

*Proof.* (i) Notice that  $Q$  is a maximal  $y$ -invariant  $p$ -subgroup of  $G$  if and only if  $Q$  is a maximal  $y$ -invariant  $p$ -subgroup of  $N_G(Q)$ , for if  $Q < R$  and  $R$  is another  $y$ -invariant  $p$ -subgroup of  $G$ , then  $Q < N_R(Q)$  and  $N_R(Q)$  is  $y$ -invariant. Hence we may suppose that  $Q \triangleleft G$ , and do so. Set  $\bar{G} = G/Q$ , and so on. Then  $\overline{C_G(y)} = C_{\bar{G}}(\bar{y})$  since  $y$  is  $p$ -regular and  $Q$  is a  $p$ -group. Since  $\bar{y} \in O_{p'}(\bar{G})$ , we see that  $\bar{y}$  centralizes any  $p$ -subgroup of  $\bar{G}$  that it normalizes. Hence  $Q$  is a maximal  $y$ -invariant  $p$ -subgroup of  $G$  if and only if  $\bar{y}$  normalizes no nontrivial  $p$ -subgroup of  $\bar{G}$ , if and only if  $\bar{y}$  centralizes no nontrivial  $p$ -subgroup of  $\bar{G}$ , if and only if  $C_Q(y) \in \text{Syl}_p(C_G(y))$ .

(ii) Again we may suppose that  $Q \triangleleft G$  and we set  $\bar{G} = G/Q$ . If  $\bar{y}$  inverts or centralizes an element of order  $p$  in  $\bar{G}$ , then  $Q$  is clearly not a maximal  $y$ -invariant  $p$ -subgroup of  $G$ . On the other hand, if  $\bar{y}$  normalizes a nontrivial  $p$ -subgroup of  $\bar{G}$ , then  $\bar{y}$  normalizes a nontrivial Abelian  $p$ -subgroup  $\bar{A}$ , say. We have  $\bar{A} = [\bar{A}, \bar{y}] \times C_{\bar{A}}(\bar{y})$ , so that  $\bar{y}$  must either centralize or invert a nonidentity element of  $\bar{A}$ .

(iii) The proof of this part is analogous to part (ii), except that in the final step,  $\bar{A}$  may be chosen to be elementary Abelian, and  $[\bar{A}, \bar{y}]$  is a direct product of  $\bar{y}$ -invariant Klein 4-groups, each acted on by  $\bar{y}$  without nontrivial fixed points.  $\square$

**Definition.** When  $p$  is a prime and  $G$  is a finite group, a pair  $(Q, x)$  is called a *pseudoweight* for  $G$  if  $x$  is a  $p$ -regular element of  $G$ ,  $Q$  is a maximal  $x$ -invariant  $p$ -subgroup of  $G$ , and one or more of the following occurs:

- (i)  $xQ \in O_{p'}(N_G(Q)/Q)$ .
- (ii)  $p$  is odd and  $x$  is an involution.
- (iii)  $p = 2$  and  $x$  has order 3.

**Remark.** It is easy to check that  $(Q, 1)$  is a pseudoweight for  $G$  if and only if  $Q \in \text{Syl}_p(G)$ , so there is a unique conjugacy class of pseudoweights with second component  $1_G$ . When  $Q$  is a Sylow  $p$ -subgroup of  $G$ , notice that the number of

nonconjugate pseudoweights with first component  $Q$  is the number of conjugacy classes of  $p$ -regular elements of  $N_G(Q)$ , since  $N_G(Q)/Q$  is a  $p'$ -group. If  $p$  is odd, every involution occurs as the second component of at least one pseudoweight, since whenever  $t$  is an involution, there is at least one maximal  $t$ -invariant  $p$ -subgroup of  $G$  (which may be trivial). Similarly, if  $p = 2$ , then every element of order 3 occurs as the second component of at least one pseudoweight.

Before our first result, we recall some results of [Murray 1999; Robinson 1983]. Let  $P$  be a Sylow  $p$ -subgroup of  $G$ . In [Robinson 1983], it is proved that the number of  $p$ -blocks of defect zero is the rank of a matrix  $S$  with entries in  $\text{GF}(p)$  defined as follows: The rows and columns of  $S$  are indexed by the conjugacy classes of  $p$ -regular elements  $y$  of  $G$  such that  $C_G(y)$  is a  $p'$ -group. The  $(i, j)$ -entry of  $S$  is  $s_{ij}$ , which is the residue (mod  $p$ ) of  $|\Omega_{ij}|/|P|$ , where  $\Omega_{ij}$  is the set of  $(u, v) \in C_i \times C_j$  such that  $u^{-1}v \in P$ , where  $C_i$  is the  $i$ -th conjugacy class of  $p$ -regular elements of  $p$ -defect zero. This is refined by [Murray 1999, 6.3], which shows that  $\Omega_{ij}$  may be replaced by  $\tilde{\Omega}_{ij}$ , which is obtained by only counting ordered pairs  $(u, v)$  such that  $u^{-1}v$  is an element of  $P$  of order at most  $p$ , and we may use  $\tilde{S}$  in place of  $S$ , where  $\tilde{s}_{ij}$  is the residue (mod  $p$ ) of  $|\tilde{\Omega}_{ij}|/|P|$ . We will see that, when  $p = 2$ , this refinement is advantageous.

**Theorem 2.** *For each  $p$ -subgroup  $Q$  of  $G$ , the number of conjugacy classes of weights of  $G$  with first component conjugate to  $Q$  is greater than or equal to the number of conjugacy classes of pseudoweights of  $G$  with first component conjugate to  $Q$ .*

*Proof.* First note that  $G$  permutes its pseudoweights by conjugation. For each  $p$ -subgroup of  $G$ , the  $G$ -conjugate pseudoweights with first component  $Q$  correspond bijectively to the  $N_G(Q)/Q$ -conjugacy classes of pseudoweights with trivial first component, since there is a bijection between  $p$ -regular conjugacy classes of  $N = N_G(Q)$  and  $p$ -regular conjugacy classes of  $N/Q$ . Hence it suffices to prove that the number of  $p$ -blocks of defect zero is at least the number of conjugacy classes of pseudoweights with trivial first component.

Let  $(1, x_1), \dots, (1, x_d)$  be representatives for the conjugacy classes of pseudoweights of  $G$  with trivial first component. Then no  $x_i$  normalizes any nontrivial  $p$ -subgroup of  $G$ .

Let us label so that  $x_i \in C_i$  for  $1 \leq i \leq d$ . We show that the first  $d \times d$  minor of  $\tilde{S}$  is an invertible diagonal matrix, so that  $\tilde{S}$  has rank at least  $d$ . For if  $1 \leq i, j \leq d$ , and  $u$  is conjugate to  $x_i$  and  $v$  is conjugate to  $x_j$  with  $u^{-1}v \in P$  of order at most  $p$ , then  $u^{-1}v$  is  $p$ -regular (if  $u$  or  $v$  is in  $O_{p'}(G)$  this is clear). If  $p$  is odd and  $u$  and  $v$  are both involutions that invert no element of order  $p$ , then  $u^{-1}v$  must be  $p$ -regular. If  $p = 2$  and  $u$  and  $v$  are both elements of order 3 that normalize no nontrivial 2-subgroup of  $G$  and  $u^{-1}v$  is an involution, then  $\langle u, v \rangle \cong A_4$  and  $u$  is

conjugate to  $v$  within  $\langle u, v \rangle$ , a contradiction. Hence  $u^{-1}v$  is  $p$ -regular in all cases, (so is the identity, as  $P$  is a  $p$ -group). Thus  $\tilde{s}_{ij} = 0$  for  $i \neq j$  and  $1 \leq i, j \leq d$ . Also,  $\tilde{s}_{ii}$  is the residue (mod  $p$ ) of  $|C_i|/|P|$  for  $1 \leq i \leq d$ . Thus  $\tilde{s}_{ii} \neq 0$  for  $1 \leq i \leq d$ , as required to complete the proof.  $\square$

Because of its analogy with the result of Brauer and Fowler [1955] mentioned previously, we single out for special mention this:

**Corollary 3.** *Let  $G$  be a finite group of order divisible by 6. If  $G$  contains an element of order 3 that normalizes no nontrivial 2-subgroup of  $G$ , then  $G$  has a 2-block of defect zero. More precisely, the number of 2-blocks of defect zero is greater than or equal to the number of conjugacy class of elements of order 3 of  $G$  that normalize no nontrivial 2-subgroup of  $G$ .*

We now combine some local-group theoretic analysis with the block-theoretic results we have used.

**Theorem 4.** *Let  $G$  be a finite group of even order that contains no element of order  $2p$  for some odd prime  $p$ . Then either  $G$  has a  $p$ -block of defect zero or else  $G$  has Abelian Sylow  $p$ -subgroups and a unique conjugacy class of involutions. Furthermore, if  $G$  has no  $p$ -block of defect zero, and has Sylow  $p$ -subgroups of rank at least 3, then either  $G/O_{\{2,p\}}(G)$  has a normal Sylow  $p$ -subgroup or else  $G$  has a strongly  $p$ -embedded subgroup.*

*Proof.* Suppose that  $G$  has no  $p$ -block of defect zero. Set  $\pi = \{2, p\}$ . To prove the theorem, it suffices to consider the case that  $O_{\pi'}(G) = 1$ . By the result of Brauer and Fowler mentioned earlier, every involution of  $G$  inverts an element of order  $p$ , as  $G$  has no element of order  $2p$ . Also, since  $G$  contains no element of order  $2p$ , no section of  $G$  is isomorphic to  $SL(2, p)$ , so that, by a theorem of Glauberman [1968],  $N = N_G(ZJ(P))$  controls strong fusion in  $G$  for  $P \in \text{Syl}_p(G)$ . Thus  $N$  must have even order, as some element of order  $p$  is conjugate to its inverse in  $G$ .

Since  $G$  contains no element of order  $2p$ , the Sylow 2-subgroups of  $N$  must be cyclic or generalized quaternion, since if there were a Klein 4-subgroup,  $V$  say, of  $N$ , then each involution of  $V$  would invert every element of  $ZJ(P)$ , which is a contradiction since the product of any two involutions that invert all of  $ZJ(P)$  centralizes  $ZJ(P)$ . Hence  $N$  has a unique conjugacy class of involutions and, by the Brauer–Suzuki theorem,  $N = O_{2'}(N)C_N(t)$  for  $t$  any involution of  $N$ . Thus  $O_{2'}(N)$  contains  $P$  as  $C_N(t)$  is a  $p'$ -group. We may suppose that  $P$  is  $t$ -invariant, so that  $P$  is Abelian as  $t$  acts without nontrivial fixed-points on  $P$ . We wish to prove that  $G$  has a unique conjugacy class of involutions. Let  $u$  be an involution of  $G$ . Then, replacing  $u$  by a conjugate if necessary, we may suppose that  $u$  inverts an element  $h$  of order  $p$  in  $P$ . Then  $N_G(\langle h \rangle) = C_G(h)N_N(\langle h \rangle)$  so that  $u$  is conjugate within  $N_G(\langle h \rangle)$  to an involution of  $N_N(\langle h \rangle)$  since  $C_G(h)$  has odd order. In particular,  $u$  is

conjugate in  $G$  to an involution of  $N$ . This completes the proof of the first claim, as  $N$  has one conjugacy class of involutions.

For the second claim, set  $A = \Omega_1(P)$ , and suppose that  $|A| \geq p^3$ . For each  $a \in A^\#$ , we know that  $C_G(a)$  has odd order by hypothesis, and so is solvable. Thus  $C_G(a) = C_N(a)O_{p'}(C_G(a))$  for each such  $a$ . If  $O_{p'}(C_G(a)) = 1$  for each such  $a$ , then either  $N$  is strongly  $p$ -embedded in  $G$  or else  $P \triangleleft G$  (for if  $O_p(G) \neq 1$ , then  $G = O_{2'}(G)C_G(t)$  for  $t$  an involution, and  $O_{2'}(G)$  has a normal Sylow  $p$ -subgroup since  $O_{\pi'}(G) = 1$ ). Otherwise, by the solvable signalizer functor theorem [Glauberman 1976],

$$\theta(A) = \langle O_{p'}(C_G(a)) : a \in A^\# \rangle$$

is a solvable  $\pi'$ -group. Then  $M = N_G(\theta(A)) < G$ . Now

$$N = N_G(P) \leq N_G(A) \leq M.$$

Also, for each  $a \in A^\#$ , we have  $C_G(a) = C_N(a)O_{p'}(C_G(a)) \leq M$ . For each non-trivial subgroup  $B$  of  $P$ , we have

$$N_G(B) \leq N_G(\Omega_1(B)) = C_G(\Omega_1(B))N_N(\Omega_1(B)) \leq M.$$

Thus  $M$  is strongly  $p$ -embedded in this case. □

## References

- [Brauer and Fowler 1955] R. Brauer and K. A. Fowler, "On groups of even order", *Ann. of Math.* (2) **62** (1955), 565–583. MR 17,580e Zbl 0067.01004
- [Glauberman 1968] G. Glauberman, "A characteristic subgroup of a  $p$ -stable group", *Canad. J. Math.* **20** (1968), 1101–1135. MR 37 #6365 Zbl 0164.02202
- [Glauberman 1976] G. Glauberman, "On solvable signalizer functors in finite groups", *Proc. London Math. Soc.* (3) **33**:1 (1976), 1–27. MR 54 #5341 Zbl 0342.20008
- [Murray 1999] J. C. Murray, "Blocks of defect zero and products of elements of order  $p$ ", *J. Algebra* **214**:2 (1999), 385–399. MR 2000e:20010 Zbl 0929.20007
- [Murray 2006] J. Murray, "Projective modules and involutions", *J. Algebra* **299**:2 (2006), 616–622. MR 2007b:16057 Zbl 1101.20005
- [Robinson 1983] G. R. Robinson, "The number of blocks with a given defect group", *J. Algebra* **84**:2 (1983), 493–502. MR 85c:20009 Zbl 0519.20011
- [Tsushima 1977] Y. Tsushima, "On the weakly regular  $p$ -blocks with respect to  $O_{p'}(G)$ ", *Osaka J. Math.* **14**:3 (1977), 465–470. MR 57 #438 Zbl 0373.20022
- [Wada 1977] T. Wada, "On the existence of  $p$ -blocks with given defect groups", *Hokkaido Math. J.* **6**:2 (1977), 243–248. MR 56 #3111 Zbl 0372.20014

Communicated by Ronald Mark Solomon

Received 2010-06-09

Revised 2010-12-22

Accepted 2011-06-07

g.r.robinson@abdn.ac.uk

*Institute of Mathematics, University of Aberdeen,  
Fraser Noble Building, Aberdeen AB24 3UE, Scotland*

# Parametrizing quartic algebras over an arbitrary base

Melanie Matchett Wood

We parametrize quartic commutative algebras over any base ring or scheme (equivalently finite, flat degree-4  $S$ -schemes), with their cubic resolvents, by pairs of ternary quadratic forms over the base. This generalizes Bhargava's parametrization of quartic rings with their cubic resolvent rings over  $\mathbb{Z}$  by pairs of integral ternary quadratic forms, as well as Casnati and Ekedahl's construction of Gorenstein quartic covers by certain rank-2 families of ternary quadratic forms. We give a geometric construction of a quartic algebra from any pair of ternary quadratic forms, and prove this construction commutes with base change and also agrees with Bhargava's explicit construction over  $\mathbb{Z}$ .

## 1. Introduction

**Definitions and main result.** A  $n$ -ic algebra  $Q$  over a scheme  $S$  is an  $\mathcal{O}_S$ -algebra  $Q$  that is a locally free rank- $n$   $\mathcal{O}_S$ -module, or equivalently  $\text{Spec } Q$  is a finite, flat degree- $n$   $S$ -scheme. For  $n = 3, 4$ , we call such algebras *cubic* and *quartic* respectively. Given a quartic algebra, we can define a cubic resolvent which is a model over  $S$  of the classical cubic resolvent field of a quartic field (but which is not always determined uniquely by the quartic algebra). For a quartic algebra  $Q$  over  $S$ , a *cubic resolvent*  $C$  of  $Q$  is a cubic algebra  $C$  over  $S$ , with a quadratic map  $\phi : Q/\mathcal{O}_S \rightarrow C/\mathcal{O}_S$  and an isomorphism  $\delta : \wedge^4 Q \xrightarrow{\sim} \wedge^3 C$ , such that for any sections  $x, y$  of  $Q$  we have  $\delta(1 \wedge x \wedge y \wedge xy) = 1 \wedge \phi(x) \wedge \phi(y)$  and also  $C$  is the cubic algebra corresponding to  $\text{Det}(\phi)$  (see Section 3 for more details). An isomorphism from a pair  $(Q, C)$  of a quartic algebra and cubic resolvent to a pair  $(Q', C')$  is given by isomorphisms of the respective algebras that respect  $\phi$  and  $\delta$ .

A *double ternary quadratic form* over  $S$  is a locally free rank-3  $\mathcal{O}_S$ -module  $W$ , a locally free rank-2  $\mathcal{O}_S$ -module  $U$ , and a global section  $p \in \text{Sym}^2 W \otimes U$ , and an isomorphism  $\wedge^3 W \otimes \wedge^2 U \xrightarrow{\sim} \mathcal{O}_S$  which is called an *orientation*. An isomorphism

---

*MSC2000:* primary 11R16; secondary 11E20.

*Keywords:* quartic algebras, cubic resolvents, pairs of ternary quadratic forms, degree-4 covers, quartic covers.

of double ternary quadratic forms  $(W, U, p)$  and  $(W', U', p')$  is given by isomorphisms  $W \xrightarrow{\sim} W'$  and  $U \xrightarrow{\sim} U'$  that send  $p$  to  $p'$  and respect the orientations.

The main theorem of this paper is the following.

**Theorem 1.1.** *There is an isomorphism between the moduli stack for quartic algebras with cubic resolvents and the moduli stack for double ternary quadratic forms. In other words, for a scheme  $S$  there is an equivalence between the category of quartic algebras with cubic resolvents and the category of double ternary quadratic forms (with morphisms given by isomorphisms in both categories), and this natural equivalence commutes with base change in  $S$ .*

The moduli stack of double ternary quadratic forms is simply  $[\mathbb{A}^{12}/\Gamma]$ , where  $\Gamma$  is the sub-group scheme of  $\mathrm{GL}_2 \times \mathrm{GL}_3$  of elements  $(g, h)$  such that  $\det g \det h = 1$ . The action of  $\Gamma$  on  $\mathbb{A}^{12}$  is given by viewing  $\mathbb{A}^{12}$  as the space  $\mathrm{Sym}^2 \mathbb{Z}^3 \otimes \mathbb{Z}^2$ , where  $\mathrm{GL}_3$  has the standard action on the  $\mathbb{Z}^3$  (and the thereby induced action on  $\mathrm{Sym}^2 \mathbb{Z}^3$ ) and acts trivially on the  $\mathbb{Z}^2$  and  $\mathrm{GL}_2$  acts trivially on the  $\mathrm{Sym}^2 \mathbb{Z}^3$  and with the standard action on  $\mathbb{Z}^2$ . In particular, we have a parametrization of quartic algebras with cubic resolvents.

**Corollary 1.2.** *Over a scheme  $S$ , there is a bijection between isomorphism classes of double ternary quadratic forms over  $S$  and isomorphism classes of pairs  $(Q, C)$  where  $Q$  is a quartic algebra over  $S$  and  $C$  is a cubic resolvent of  $Q$ .*

**Remark 1.3.** The geometric language of this paper makes it more natural to work over a scheme  $S$ , but all of our work includes the case  $S = \mathrm{Spec} R$ , in which case we are simply working over a ring  $R$ . The reader mainly interested in a base ring can replace  $\mathcal{O}_S$  with  $R$  and “global section” with “element” throughout the paper.

**Background and previous work.** It has been known since [Delone and Faddeev 1940] (see also Section 2 of this paper and [Davenport and Heilbronn 1971; Gan et al. 2002; Bhargava 2004b]) that cubic rings are parametrized by binary cubic forms. A *cubic ring* is a ring whose additive structure is a free rank-3  $\mathbb{Z}$ -module, and a *binary cubic form* is a polynomial

$$f = ax^3 + bx^2y + cxy^2 + dy^3$$

with  $a, b, c, d \in \mathbb{Z}$ . Cubic rings, up to isomorphism, are in natural discriminant-preserving bijection with  $\mathrm{GL}_2(\mathbb{Z})$ -classes of binary cubic forms. If we prefer to think geometrically, a cubic ring is a finite, flat degree-3 cover of  $\mathrm{Spec} \mathbb{Z}$ . A parametrization analogous to that of [Delone and Faddeev 1940] was proven in [Miranda 1985] for finite, flat degree-3 covers of an irreducible scheme over an algebraically closed field of characteristic not 2 or 3. Though these correspondences were originally given by writing down a multiplication table for the cubic ring (or sheaf of functions on the cubic cover), when  $f$  is a non-zero integral binary



cubic form, the associated cubic ring is simply the ring of global functions of the subscheme of  $\mathbb{P}_{\mathbb{Z}}^1$  cut out by  $f$ ; see [Deligne 2000; Wood 2011b, Theorem 2.4; Casnati and Ekedahl 1996].

In this paper, we study quartic (commutative) algebras, or equivalently, finite, flat degree-4 covers of a base scheme. Casnati and Ekedahl [1996] found that finite, flat degree-4 Gorenstein covers of an integral base scheme are given by global sections of certain double ternary quadratic forms, with a codimension condition on the section at every point of the base. (See also [Hahn and Miranda 1999] on quartic covers of algebraic varieties in characteristic not 2.) Recently, quartic algebras over  $\mathbb{Z}$  have been parametrized in [Bhargava 2004b]. More precisely, Bhargava proved that isomorphism classes of pairs  $(Q, C)$ , where  $Q$  is a quartic ring (i.e., isomorphic to  $\mathbb{Z}^4$  as a  $\mathbb{Z}$ -module) and  $C$  is a cubic resolvent of  $Q$ , are in natural bijection with  $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ -classes of pairs of integral ternary quadratic forms. (We could view a pair of ternary quadratic forms over  $\mathbb{Z}$  as a double ternary quadratic form  $\sum_{1 \leq i \leq j \leq 3} a_{ij} x_i x_j y + \sum_{1 \leq i \leq j \leq 3} b_{ij} x_i x_j z$ .) Bhargava [2004b] introduced cubic resolvents as models of the classical cubic resolvent field of a quartic field. All quartic rings over  $\mathbb{Z}$  have at least one cubic resolvent, and many quartic rings (for example, maximal quartic rings over  $\mathbb{Z}$ ) have a unique cubic resolvent [Bhargava 2004b, Corollary 4]. This has allowed Bhargava [2005] to count asymptotically the number of  $S_4$  number fields of discriminant less than  $X$  (as well as the number of orders in  $S_4$  number fields). Casnati [1998] has also given a construction of a finite, flat degree-3 “discriminant cover” corresponding to a finite, flat degree-4 Gorenstein cover of an integral scheme over an algebraically closed field of characteristic not equal to 2, but since he was only considering quartic covers that turn out to have unique cubic resolvents, the importance of the cubic resolvent to the moduli problem was not apparent. Bhargava [2004b] realized that to obtain a nice parametrization of quartic rings over  $\mathbb{Z}$ , one must parametrize them along with their cubic resolvents.

In this paper, we generalize the results of [Bhargava 2004b] from  $\mathbb{Z}$  to an arbitrary scheme, and those of [Casnati and Ekedahl 1996] from the case of Gorenstein covers and special forms to all quartic covers and forms, as well as to an arbitrary base scheme. Moreover, we prove our correspondence between quartic algebras with resolvents and double ternary quadratic forms commutes with base change.

Bhargava [2004b] describes the relationship between quartic rings with cubic resolvents and pairs of ternary quadratic forms by giving the multiplication tables for the quartic and cubic rings explicitly in terms of the coefficients of the forms. In this paper, we give a geometric, coordinate-free description of a quartic ring  $Q$  given by a pair of integral ternary quadratic forms. For the nicest forms, the pair of ternary quadratic forms gives a pencil of conics in  $\mathbb{P}_{\mathbb{Z}}^2$  and the quartic ring is given by the global functions of the degree-4 subscheme cut out by the pencil. In Section 4, we

give a global, geometric, coordinate-free construction over a quartic algebra from a double ternary quadratic form over any scheme  $S$ . The construction that works for all forms is taking the degree-0 hypercohomology of the Koszul complex of the double ternary quadratic form. This agrees with the intuitive geometric description given above for nice cases, but unlike the above description, always gives a quartic algebra. Casnati and Ekedahl [1996] have given an analogous geometric construction over an arbitrary scheme in the case when the quartic algebra is Gorenstein. Deligne, in a letter to Bhargava [2004], gives an analogous geometric construction when the generic conic in the pencil is non-singular over each geometric point, and proves that it extends (without giving a geometric construction in the extended case) to all pairs of ternary quadratic forms. The geometric construction in this paper works for all double ternary quadratic forms, for example when the form is identically 0 in some fiber, when the conics given by the ternary quadratic forms share a component, or even when both forms are identically 0!

In Section 5, we explain how the quartic algebra associated to a double ternary quadratic form over  $S$  can be defined locally in terms of the multiplication tables given in [Bhargava 2004b], and prove that these constructions agree. The calculations showing this agreement are not straightforward and are given in Theorem 5.1.

In Section 2, we review the parametrization of cubic algebras. This is not only motivation for our study of quartic algebras, but also is important background for the results in this paper because the cubic resolvent  $C$  is a cubic algebra. In Section 3 we give the definition of a cubic resolvent in more detail. In Section 6, we give the construction of a cubic resolvent from a double ternary quadratic form. In Section 7, we prove Theorem 1.1.

**Notation.** If  $\mathcal{F}$  is a sheaf, we use  $s \in \overline{\mathcal{F}}$  to denote that  $s$  is a global section of  $\overline{\mathcal{F}}$ . If  $V$  is a locally free  $\mathcal{O}_S$ -module, we use  $V^*$  to denote the  $\mathcal{O}_S$ -module  $\mathcal{H}om_{\mathcal{O}_S}(V, \mathcal{O}_S)$ . We use  $\text{Sym}^n V$  to denote the usual quotient of  $V^{\otimes n}$ , and  $\text{Sym}_n V$  to denote the submodule of symmetric elements of  $V^{\otimes n}$ . Note that when  $V$  is locally free we have  $\text{Sym}_n V = (\text{Sym}^n V^*)^*$  (see Lemma A.4). We define  $\mathbb{P}(V) = \text{Proj Sym}^* V$ .

Normally, in the language of algebra, one says that an  $R$ -module  $M$  is locally free of rank  $n$  if for all prime ideals  $\mathfrak{p}$  of  $R$ , the localization  $M_{\mathfrak{p}}$  is free of rank  $n$ . However, if we have a scheme  $S$  and an  $\mathcal{O}_S$ -module  $M$ , we normally say that  $M$  is locally free of rank  $n$  if on some open cover of  $S$  it is free of rank  $n$ ; in the algebraic language this is equivalent to saying that for every prime ideal  $\mathfrak{p}$  of  $R$ , there is an  $f \in R \setminus \mathfrak{p}$  such that the localization  $M_f$  is free of rank  $n$ . In this paper we shall use the geometric sense of the term *locally free of rank  $n$* . The geometric condition of locally free of rank  $n$  is equivalent to being finitely generated and having the algebraic condition of locally free of rank  $n$ .

## 2. The parametrization of cubic algebras

In this section, we review the parametrization of cubic algebras. A *binary cubic form* over a scheme  $S$  is a locally free rank-2  $\mathbb{O}_S$ -module  $V$  and an  $f \in \text{Sym}^3 V \otimes \wedge^2 V^*$ . An isomorphism of binary cubic forms  $(V, f) \cong (V', f')$  is given by an isomorphism  $V \cong V'$  that takes  $f$  to  $f'$ . (Normally, we would call these *twisted binary cubic forms* but since they are the only binary cubic forms in this paper, we will use the shorter name for simplicity.) Of course, if  $V$  is the free rank-2  $\mathbb{O}_S$ -module  $\mathbb{O}_S x \oplus \mathbb{O}_S y$ , then the binary cubic forms  $f \in \text{Sym}^3 V \otimes \wedge^2 V^*$  are just polynomials  $(ax^3 + bx^2y + cxy^2 + dy^3) \otimes (x \wedge y)^*$ , where  $a, b, c, d \in \mathbb{O}_S$ .

Over an arbitrary base, we have the following theorem of Deligne, also proved by Poonen.

**Theorem 2.1** [Deligne 2000; Poonen 2008, Proposition 5.1]. *There is an isomorphism between the moduli stack for cubic algebras and the moduli stack for binary cubic forms. That is, there is an equivalence of categories between the category of cubic algebras over  $S$  where morphisms are given by isomorphisms and the category of binary cubic forms over  $S$  where morphisms are given by isomorphisms, and this equivalence commutes with base change in  $S$ . Thus, over a scheme  $S$ , there is a bijection between isomorphism classes of cubic algebras and isomorphism classes of binary cubic forms. If a cubic algebra  $C$  corresponds to a binary cubic form  $(V, f)$ , then as  $\mathbb{O}_S$ -modules, we have  $C/\mathbb{O}_S \cong V^*$ .*

Miranda [1985] gives the bijection between isomorphism classes over a base which is an irreducible scheme over an algebraically closed field of characteristic not equal to 2 or 3. Also, this isomorphism of stacks is studied and proven as part of a series of such isomorphisms involving binary forms of any degree in [Wood 2011b].

In [Bhargava 2004a, Footnote 3], the following algebraic, global, coordinate free description of the construction of a binary cubic form from a cubic algebra is mentioned. Given a cubic algebra  $C$ , we can define an  $\mathbb{O}_S$ -module  $V = (C/\mathbb{O}_S)^*$ . (Note that  $V$  is a locally free rank-2  $\mathbb{O}_S$ -module; see [Voight 2010, Lemma 1.3], for example.) We can then define an  $\mathbb{O}_S$ -module homomorphism  $\text{Sym}_3 C/\mathbb{O}_S \rightarrow \wedge^2 C/\mathbb{O}_S$  given by  $xyz \mapsto x \wedge yz$ . One can check that this map is well-defined, and so it gives a binary cubic form  $f \in (\text{Sym}_3 C/\mathbb{O}_S)^* \otimes \wedge^2 C/\mathbb{O}_S \cong \text{Sym}^3 V \otimes \wedge^2 V^*$ . Deligne [2000] gives a different, geometric construction in the case when  $C$  is Gorenstein and then argues that the construction extends across the non-Gorenstein locus.

It is often useful to also have the following local, explicit version of the construction. Where  $C$  is a free  $\mathbb{O}_S$ -module, we can choose a basis  $1, \omega, \theta$  for  $C$  and then shift  $\omega$  and  $\theta$  by elements of  $\mathbb{O}_S$  so that  $\omega\theta \in \mathbb{O}_S$ . Then, the associative law

implies that we have a multiplication table

$$\begin{aligned} \omega\theta &= -ad, \\ \omega^2 &= -ac + b\omega - a\theta, \\ \theta^2 &= -bd + d\omega - c\theta, \end{aligned} \tag{1}$$

where  $a, b, c, d \in \mathbb{C}_S$ . Let  $x, y$  be the basis of  $V$  dual to  $\omega, \theta$ . Then we can define a form  $(ax^3 + bx^2y + cxy^2 + dy^3) \otimes (x \wedge y)^* \in \text{Sym}^3 V \otimes \wedge^2 V^*$ . We can check that if we pick another basis  $1, \omega', \theta'$  (also normalized so that  $\omega'\theta' \in \mathbb{C}_S$ ) and another corresponding  $x'$  and  $y'$  we would define the same form in  $\text{Sym}^3 V \otimes \wedge^2 V^*$ . Thus the form is defined everywhere locally in a way that agrees on overlapping open sets, and we have constructed a global binary cubic form  $(V, f)$ .

One construction of a cubic algebra from a form (i.e., the inverse to the above construction) simply gives the cubic algebra locally by the above multiplication table. This gives the bijection locally in terms of bases with explicit formulas. However, it is hard to see where the formula for the multiplication table came from or why the local constructions are invariant under change of basis. The following global description is given by Deligne in his letter [Deligne 2000]. Given a binary form  $f \in \text{Sym}^3 V \otimes \wedge^2 V^*$  over a base scheme  $S$ , the form  $f$  determines a subscheme  $S_f$  of  $\mathbb{P}(V)$ . Let  $\pi : \mathbb{P}(V) \rightarrow S$ . Let  $\mathbb{C}(k)$  denote the usual sheaf on  $\mathbb{P}(V)$  and  $\mathbb{C}_{S_f}(k)$  denote the pullback of  $\mathbb{C}(k)$  to  $S_f$ . Then we can define the  $\mathbb{C}_S$ -algebra by the hypercohomology

$$C := H^0 R\pi_*(\mathbb{C}(-3) \otimes \pi^* \wedge^2 V \xrightarrow{f} \mathbb{C}), \tag{2}$$

where  $\mathbb{C}(-3) \otimes \pi^* \wedge^2 V \xrightarrow{f} \mathbb{C}$  is a complex in degrees  $-1$  and  $0$ . The product on  $C$  is given by the product on the Koszul complex  $\mathbb{C}(-3) \otimes \pi^* \wedge^2 V \xrightarrow{f} \mathbb{C}$  with itself and the  $\mathbb{C}_S$ -algebra structure is induced from the map of  $\mathbb{C}$  as a complex in degree  $0$  to the complex  $\mathbb{C}(-3) \xrightarrow{f} \mathbb{C}$  (see Section B for more details on the inheritance of the algebra structure). (Note that  $H^0 R\pi_*(\mathbb{C}) = \mathbb{C}_S$ .)

Given a map of schemes  $X \xrightarrow{\pi} S$ , the construction of global functions of  $X$  relative to  $S$  is just the pushforward  $\pi_*(\mathbb{C}_X)$ . So the natural notion of global functions of  $S_f$  relative to  $S$  would be  $\pi_*$  of  $\mathbb{C}_{S_f}$ . We have that  $\mathbb{C}_{S_f} = \mathbb{C}_S/f(\mathbb{C}(-3) \otimes \pi^* \wedge^2 V)$ . When  $f$  is injective, then  $\mathbb{C}_{S_f} = \mathbb{C}_S/f(\mathbb{C}(-3) \otimes \pi^* \wedge^2 V)$  as a complex in degree  $0$  has the same hypercohomology as  $\mathbb{C}(-3) \otimes \pi^* \wedge^2 V \xrightarrow{f} \mathbb{C}$  as a complex in degrees  $-1$  and  $0$ . Thus we see when  $f$  is injective that  $C$  is just  $\pi_*(\mathbb{C}_{S_f})$ . When  $f$  gives an injective map and  $S = \text{Spec } R$  then  $C$  is just the ring of global functions of  $S_f$ . Unfortunately, this simpler construction does not give a cubic algebra when  $f \equiv 0$ . When  $f \equiv 0$ , then  $S_f = \mathbb{P}^1$  and the global functions are a rank-1  $\mathbb{C}_S$ -algebra, i.e.,  $\mathbb{C}_S$  itself. Hypercohomology is exactly the machinery we need to naturally extend the construction to all  $f$ .

### 3. Cubic resolvents

We now give the definition of a cubic resolvent, given first in [Bhargava 2004b, Definition 20] over  $\mathbb{Z}$ . The definition might seem complicated at first, but we will explain each aspect of it.

**Definition.** Given a quartic algebra  $Q$  over a base scheme  $S$ , a cubic resolvent  $C$  of  $Q$  is

- a cubic algebra  $C$  over  $S$ ,
- a quadratic map  $\phi : Q/\mathbb{O}_S \rightarrow C/\mathbb{O}_S$ , and
- an isomorphism  $\delta : \wedge^4 Q \xrightarrow{\sim} \wedge^3 C$  (or equivalently  $\bar{\delta} : \wedge^3 Q/\mathbb{O}_S \xrightarrow{\sim} \wedge^2 C/\mathbb{O}_S$ ), which we call the *orientation*,

such that

- (1) for any open set  $U \subset S$  and for all  $x, y \in Q(U)$ , we have  $\delta(1 \wedge x \wedge y \wedge xy) = 1 \wedge \phi(x) \wedge \phi(y)$ , and
- (2)  $C$  is the cubic algebra corresponding to  $\text{Det}(\phi)$ .

Note that  $Q/\mathbb{O}_S$  and  $C/\mathbb{O}_S$  are locally free  $\mathbb{O}_S$ -modules of ranks 3 and 2, respectively (see [Voight 2010, Lemma 1.3], for example). A *quadratic map* from  $A$  to  $B$  is given by an  $\mathbb{O}_S$ -module homomorphism  $\text{Sym}_2 A \rightarrow B$  evaluated on the diagonal (see Section A.i in Appendix A). (In [Wood 2011a, Proposition 6.1] it is shown this is equivalent to the more classical notion of a quadratic map.) The map  $\phi$  models the map from quartic fields to their resolvent fields given by  $x \mapsto xx' + x''x'''$ , where  $x, x', x'', x'''$  are the conjugates of an element  $x$ . In [Bhargava 2004b, Lemma 9] it is shown that condition 1 above holds for such classical resolvent maps, and it turns out that condition 1 is the key property of resolvent maps that allows them to be useful in the parametrization of quartic algebras. So the definition of resolvent allows all quadratic maps that have this key property.

Another important property of the cubic resolvent over  $\mathbb{Z}$  is that the discriminant of the cubic resolvent is equal to the discriminant of the quartic ring. In [Bhargava 2004b], this is a crucial part of the definition of a cubic resolvent over the integers. With the above formulation of the definition of a cubic resolvent, the equality of discriminants follows as a corollary of properties 1 and 2. However, since the discriminant of an algebra  $R$  of rank  $n$  lies in  $(\wedge^n R)^{\otimes -2}$ , we need the orientation isomorphism to even state the question of the equality of discriminants. The orientation is a phenomenon that it is hard to recognize the importance of over  $\mathbb{Z}$  because  $\text{GL}_1(\mathbb{Z})$  is so small, however it appears in Bhargava’s choice of bases for a quartic ring and its cubic resolvent.

The quadratic map  $\phi$  is equivalent to a double ternary quadratic form in the module  $\text{Sym}^2(Q/\mathbb{O}_S)^* \otimes C/\mathbb{O}_S$ . The determinant of a double ternary quadratic

form is given by a natural cubic map from  $\text{Sym}^2 W \otimes V$  to  $(\wedge^3 W)^{\otimes 2} \otimes \text{Sym}^3 V$ . We have a natural cubic determinant map from  $\text{Sym}^2 W$  to  $(\wedge^3 W)^{\otimes 2}$ . For free  $W$  and an element of  $\text{Sym}^2 W$  represented by the matrix

$$A = \begin{pmatrix} a_{11} & \frac{1}{2}a_{12} & \frac{1}{2}a_{13} \\ \frac{1}{2}a_{12} & a_{22} & \frac{1}{2}a_{23} \\ \frac{1}{2}a_{13} & \frac{1}{2}a_{23} & a_{33} \end{pmatrix},$$

the map is given by the polynomial  $4 \text{Det}(A)$ , and since this is invariant under  $\text{GL}_3$  change of basis, it defines a determinant map for all locally free  $W$ . We use 2's in the denominator of our expression for  $A$  because it allows us a convenient way to express the polynomial  $4 \text{Det}(A)$ , but note that the polynomial given by  $4 \text{Det}(A)$  does not have any denominators, and thus we do not need to require that 2 is invertible to construct the determinant of a double ternary quadratic form. We can extend to a cubic determinant map from  $\text{Sym}^2 W \otimes V$  to  $(\wedge^3 W)^{\otimes 2} \otimes \text{Sym}^3 V$  by using the elements of  $V$  as coefficients (see Section A.ii). Thus the determinant of  $\phi$  lies in  $(\wedge^3 Q/\mathcal{O}_S)^{\otimes -2} \otimes \text{Sym}^3(C/\mathcal{O}_S)$ , which is isomorphic to  $(\wedge^2 C/\mathcal{O}_S) \otimes \text{Sym}^3(C/\mathcal{O}_S)^*$  by the orientation isomorphism (see also Corollary A.3). From Theorem 2.1, we have that  $C$  corresponds to a global section of  $(\wedge^2 C/\mathcal{O}_S) \otimes \text{Sym}^3(C/\mathcal{O}_S)^*$ , and condition (2) above is that  $C$  corresponds to the section  $\text{Det}(\phi)$ .

When we speak of a pair  $(Q, C)$  of a quartic algebra  $Q$  and a cubic resolvent  $C$  of  $Q$ , the maps  $\phi$  and  $\delta$  are implicit. An isomorphism of pairs is given by isomorphisms of the respective algebras that respect  $\phi$  and  $\delta$ .

#### 4. The geometric construction

In this section, we will construct a quartic algebra from a double ternary quadratic form  $p \in \text{Sym}^2 W \otimes U$  over a base  $S$ . We consider the map  $\pi : \mathbb{P}(W) \rightarrow S$ , and the usual line bundles  $\mathcal{O}(k)$  on  $\mathbb{P}(W)$ . We can view  $p$  as a two-dimensional family of quadratic forms on  $\mathbb{P}(W)$  (the two dimensions being given by  $U$ ). More precisely, since  $p$  is equivalent to a map  $U^* \rightarrow \text{Sym}^2 W$ , we have a naturally induced map  $\pi^*U^* \rightarrow \mathcal{O}(2)$ , which is equivalent to a map  $p_1 : \pi^*U^* \otimes \mathcal{O}(-2) \rightarrow \mathcal{O}$ . The image of  $p_1$  is functions that are zero on the space cut out by the forms of  $p$ . The regular functions on the scheme cut out by  $p$  are just given by  $\mathcal{O}/\text{im}(p_1)$ . From  $p$  we can construct one more map to make the Koszul complex of  $p$ , given as follows

$$\mathcal{H}_p : \quad \wedge^2 \pi^*U^* \otimes \mathcal{O}(-4) \xrightarrow{p_2} \pi^*U^* \otimes \mathcal{O}(-2) \xrightarrow{p_1} \mathcal{O}.$$

The complex  $\mathcal{H}_p$  has  $\mathcal{O}$  in degree 0, and the other two terms in degrees  $-1$  and  $-2$ . We can construct  $p_2$  similarly to  $p_1$  since  $p$  is also equivalent to a map  $\wedge^2 U^* \otimes U \rightarrow \text{Sym}^2 W$ . (Recall that  $\wedge^2 U^* \otimes U \cong U^*$ ; see Lemma A.2.) One can

read about the construction of all the maps in the Koszul complex in [Eisenbud 2005, Appendices A2F and A2H].

**Example 4.1.** Suppose  $U$  is free with basis  $x, y$ , and dual basis  $\dot{x}$  and  $\dot{y}$ . Then we can write  $p = f_1 \otimes x + f_2 \otimes y$ . The map  $p_1$  just sends  $\dot{x} \otimes g \mapsto f_1 g$  and  $\dot{y} \otimes g \mapsto f_2 g$ . We can write how  $p_1$  acts on a general element as  $a \otimes g \mapsto gp(a)$ , where  $p$  acts on an element of  $U^*$  by evaluating the  $U$  components of  $p$  at the given element of  $U^*$ . The map  $p_2$  sends  $\dot{x} \wedge \dot{y} \otimes g \mapsto gf_1 \otimes \dot{y} - gf_2 \otimes \dot{x}$ . We can write how  $p_2$  acts on a general element as  $a \wedge b \otimes g \mapsto b \otimes gp(a) - a \otimes gp(b)$ . From this we see that  $\mathcal{K}_p$  is a complex.

For sufficiently nice  $p$  the Koszul complex will be exact in all places except the last and thus give a resolution of  $\mathbb{O}/\text{im}(p_1)$ . For example, this is true when  $p$  is the universal double ternary quadratic form over the polynomial ring in twelve variables. In this well-behaved case,  $p$  will cut out four (relative) points in  $\mathbb{P}(W)$  (i.e., a finite, flat degree four  $S$ -scheme) and the pushforward of the global functions of those points will give us a quadratic algebra over the base  $S$ .

When the Koszul complex of  $p$  is not a resolution, instead of taking the pushforward of the global functions of the scheme cut out by  $p$ , we will take the 0th hypercohomology of the complex  $\mathcal{K}_p$ . We define  $Q_p$  to be  $H^0 R\pi_*(\mathcal{K}_p)$ , where  $R\pi_*$  denotes the pushforward of the complex in the derived category. Alternatively, we can view the construction as the hypercohomological derived functor of  $\pi_*$ , where the hypercohomology is necessary since we are operating on a complex and not just a single sheaf. If  $p$  is nice enough that its Koszul complex  $\mathcal{K}_p$  is a resolution of  $\mathbb{O}/\text{im}(p_1)$ , then  $Q_p$  will just be  $\pi_*(\mathbb{O}/\text{im}(p_1))$ . However, what is convenient about the hypercohomology construction is that  $Q_p$  will be a quartic algebra even when  $\mathcal{K}_p$  is not a resolution (as we'll see in Section 4.ii). So far we have constructed  $Q_p$  as an  $\mathbb{O}_S$ -module, however, the Koszul complex has a natural differential graded algebra structure, and that gives the cohomology an inherited algebra structure (see Section B for more details on the inheritance of the algebra structure). The map from  $\mathbb{O}$  as a complex in degree 0 to the complex  $\mathcal{K}_p$  induces a map from  $H^0 R\pi_*(\mathbb{O}) = \mathbb{O}_S \rightarrow Q_p$ . This gives  $Q_p$  the structure of an  $\mathbb{O}_S$ -algebra.

**4.i. Examples when  $\mathcal{K}_p$  is not a resolution.** When constructing the cubic algebra from a binary cubic form, we took

$$H^0 R\pi_*(\mathbb{O}(-3) \xrightarrow{f} \mathbb{O})$$

on  $\mathbb{P}(V)$ , which, as long as the cubic form  $f$  gives an injective map above is the same as  $\pi_*(\mathbb{O}/\text{im } f)$ . For example, when the base  $S$  is integral, whenever  $f \neq 0$  then  $\mathbb{O}(-3) \xrightarrow{f} \mathbb{O}$  is injective. However, when  $f \equiv 0$ , of course  $\mathbb{O}(-3) \xrightarrow{f} \mathbb{O}$  is not

injective, and  $H^0 R\pi_*(\mathbb{O}(-3) \xrightarrow{f} \mathbb{O})$  is not the same as  $\pi_*(\mathbb{O}/\text{im } f)$ . When  $f \equiv 0$ , the latter is an  $\mathbb{O}_S$ -module of rank 1.

Again, when constructing our quartic algebra as  $H^0 R\pi_*(\mathcal{H}_p)$ , if  $p \equiv 0$  the complex will not be a resolution and  $H^0 R\pi_*(\mathcal{H}_p)$  won't agree with  $\pi_*(\mathbb{O}/\text{im } p_1)$ . This is the case when both ‘‘conics’’ are given by the 0 form. However, even over an integral base, there are now more situations on which the complex  $\mathcal{H}_p$  is not a resolution. The geometric constructions of [Casnati and Ekedahl 1996] and [Deligne 2004] for certain nice quartic algebras are in cases when  $\pi_*(\mathbb{O}/\text{im } p_1)$  simply gives the quartic algebra.

We now give several examples in which  $\mathcal{H}_p$  is not a resolution.

**Example 4.2.** Let  $p \equiv 0$ . Then  $Q_p = \mathbb{O}_S \oplus W^*$ , with the multiplication given by  $W^* \otimes_{\mathbb{O}_S} W^* \rightarrow 0$ .

Let  $U$  be free with the notation of Example 4.1.

**Example 4.3.** If  $f_2 \equiv 0$ , then  $Q_p = \mathbb{O}_S \oplus W^*$ , with the multiplication given by  $W^* \otimes_{\mathbb{O}_S} W^* \rightarrow 0$ .

Now, let  $W$  be free on  $w_1, w_2, w_3$ .

**Example 4.4.** If  $f_1 = w_1 w_2$  and  $f_2 = w_1 w_3$ , then  $Q_p \cong \mathbb{O}_S \oplus \mathbb{O}_S[z_1, z_2]/(z_1, z_2)^2$ . This is the case where the two conics share a linear component, and the pencil of second lines all go through a point not on the shared line.

**Example 4.5.** If  $f_1 = w_1 w_2$  and  $f_2 = w_1^2$ , then  $Q_p \cong \mathbb{O}_S[z_1, z_2]/(z_1^3, z_1 z_2, z_2^2)$ . This is the case where the two conics share a linear component, and the pencil of second lines all go through a point on the shared line.

**Example 4.6.** If  $f_1 = w_1^2 + w_1 w_3$  and  $f_2 = w_2^2 + w_2 w_3$ , then  $\mathcal{H}_p$  is a resolution and  $Q_p \cong R := \mathbb{O}_S \oplus \mathbb{O}_S \oplus \mathbb{O}_S \oplus \mathbb{O}_S$ . However, unlike in the case of binary cubic forms, we can change  $p$  in just one closed fiber and  $\mathcal{H}_p$  will no longer be a resolution. For simplicity, let  $S = \text{Spec } \mathbb{Z}$ , and let  $q$  be a prime. Then if  $f_1 = q(w_1^2 + w_1 w_3)$  and  $f_2 = q(w_2^2 + w_2 w_3)$ , the global functions of the subscheme cut out by  $p$  are isomorphic to  $\mathbb{Z} \oplus pR \subset R$  (a quartic  $\mathbb{Z}$ -algebra) but  $Q_p \cong \mathbb{Z} \oplus p^2 R \subset R$ .

**4.ii. Module structure of  $Q_p$ .** In this section, we determine the  $\mathbb{O}_S$ -module structure of  $Q_p$ . We consider the short exact sequence of complexes  $\mathcal{O} \rightarrow \mathcal{A} \rightarrow \mathcal{H}_p \rightarrow \mathcal{D} \rightarrow 0$ , where

$$\begin{array}{lcl}
 \mathcal{A} : & 0 & \longrightarrow \pi^* U^* \otimes \mathbb{O}(-2) \xrightarrow{p_1} \mathbb{O} \\
 \mathcal{H}_p : & \bigwedge^2 \pi^* U^* \otimes \mathbb{O}(-4) & \xrightarrow{p_2} \pi^* U^* \otimes \mathbb{O}(-2) \xrightarrow{p_1} \mathbb{O} \\
 \mathcal{B} : & \bigwedge^2 \pi^* U^* \otimes \mathbb{O}(-4) & \longrightarrow 0 \longrightarrow 0.
 \end{array}$$



From this short exact sequence we obtain a long exact sequence of hypercohomology sheaves on  $S$ , of which we consider the following part:

$$H^{-1}R\pi_*(\mathcal{B}) \rightarrow H^0R\pi_*(\mathcal{A}) \rightarrow H^0R\pi_*(\mathcal{A}_p) \rightarrow H^0R\pi_*(\mathcal{B}) \rightarrow H^1R\pi_*(\mathcal{A}).$$

$$\parallel$$

$$Q_p$$

This sequence will allow us to determine the module structure of  $Q_p$  once we compute the other terms. It is natural to shift the term in  $\mathcal{B}$  to degree 0 and obtain

$$R^1\pi_*(\wedge^2\pi^*U^* \otimes \mathbb{C}(-4))$$

$$\parallel$$

$$0 \rightarrow H^0R\pi_*(\mathcal{A}) \rightarrow Q_p \rightarrow R^2\pi_*(\wedge^2\pi^*U^* \otimes \mathbb{C}(-4)) \rightarrow H^1R\pi_*(\mathcal{A}).$$

$$\parallel$$

$$W^* \otimes \wedge^3W^* \otimes \wedge^2U^*$$

$$\downarrow \cong$$

$$W^*$$

We can analyze the  $\mathcal{A}$  terms by putting the complex  $\mathcal{A}$  in its own short exact sequence of complexes  $0 \rightarrow \mathcal{D} \rightarrow \mathcal{A} \rightarrow \mathcal{E} \rightarrow 0$ , given by the following

$$\mathcal{D} : \quad 0 \longrightarrow \mathbb{C}$$

$$\mathcal{A} : \quad \pi^*U^* \otimes \mathbb{C}(-2) \xrightarrow{p_1} \mathbb{C}$$

$$\mathcal{E} : \quad \pi^*U^* \otimes \mathbb{C}(-2) \longrightarrow 0.$$

Taking the long exact sequence for this short exact sequence of complexes gives

$$H^{-1}R\pi_*(\mathcal{E}) \rightarrow H^0R\pi_*(\mathcal{D}) \rightarrow H^0R\pi_*(\mathcal{A}) \rightarrow H^0R\pi_*(\mathcal{E})$$

$$\rightarrow H^1R\pi_*(\mathcal{D}) \rightarrow H^1R\pi_*(\mathcal{A}) \rightarrow H^1R\pi_*(\mathcal{E}),$$

or

$$R^0\pi_*(\pi^*U^* \otimes \mathbb{C}(-2)) \rightarrow R^0\pi_*(\mathbb{C}) \rightarrow H^0R\pi_*(\mathcal{A}) \rightarrow R^1\pi_*(\pi^*U^* \otimes \mathbb{C}(-2))$$

$$\parallel \quad \parallel \quad \parallel$$

$$0 \quad \mathbb{C}_S \quad 0$$

and

$$R^1\pi_*(\mathbb{C}) \rightarrow H^1R\pi_*(\mathcal{A}) \rightarrow R^2\pi_*(\pi^*U^* \otimes \mathbb{C}(-2)).$$

$$\parallel \quad \parallel$$

$$0 \quad 0$$

Thus, we conclude that  $H^0R\pi_*(\mathcal{A}) \cong \mathbb{C}_S$  and  $H^1R\pi_*(\mathcal{A}) = 0$ .

Going back to our original long exact sequence, we have

$$0 \rightarrow \mathbb{C}_S \rightarrow Q_p \rightarrow W^* \rightarrow 0.$$

This proves that  $Q_p$  is a locally free rank-4  $\mathbb{O}_S$ -module. Also, it gives us the necessary map  $\mathbb{O}_S \rightarrow Q_p$  for our algebra to have a unit. (We can check this map respects the algebra structures because it is induced from the map of complexes  $\mathcal{D} \rightarrow \mathcal{H}_p$  that respects the differential graded algebra structures on  $\mathcal{D}$  and  $\mathcal{H}_p$ .)

**Theorem 4.7.** *The construction of  $Q_p$  commutes with base change in  $S$ .*

*Proof.* To prove this theorem, we will compute all of the cohomology of  $\mathcal{H}_p$ . The complex  $\mathcal{H}_p$  has no cohomology in degrees other than 0. We have  $R^k\pi_*(\mathbb{O}(-4)) = 0$  for  $k \neq 2$ , and  $R^k\pi_*(\mathbb{O}(-2)) = 0$  for all  $k$ , and  $R^k\pi_*(\mathbb{O}) = 0$  for  $k \neq 0$ . Thus  $H^k R\pi_*(\mathcal{H}_p) = 0$  for  $k \neq 0$ . We have just seen that  $H^0 R\pi_*(\mathcal{H}_p)$  is locally free. Thus since all  $H^i R\pi_*(\mathcal{H}_p)$  are flat, by [EGA III.2 1963, corollaire 6.9.9], we have that cohomology and base change commute.  $\square$

### 5. Local construction by multiplication table

Given a double ternary quadratic form  $p \in \text{Sym}^2 W \otimes U$  (with a given  $\wedge^3 W \cong \wedge^2 U^*$ ), now that we know that there is a natural quartic algebra  $Q_p$  we could define the structure locally where  $W$  and  $U$  are free by giving multiplication tables, as in the case of cubic algebras from binary cubic forms.

For a double ternary quadratic form over  $\mathbb{Z}$  (and therefore with  $W$  and  $U$  necessarily free), Bhargava [2004b, Equations (15) and (21)] gives a ring structure on  $\mathbb{Z}^4$  whose multiplication table is given in terms of the coefficients of  $p$ . Each entry in the multiplication table is a polynomial in the coefficients of  $p$ . This, of course, is the multiplication table we would impose for free  $W$  and  $U$  in the above local construction. We will now see that this local construction agrees with the geometric construction we have given in Section 4. We will show this by working over the universal algebra  $R = \mathbb{Z}[\{a_{ij}, b_{ij}\}_{1 \leq i \leq j \leq 3}]$  for double ternary quadratic forms, and with the universal free form  $u = \sum_{1 \leq i \leq j \leq 3} a_{ij}x_i x_j y_1 + b_{ij}x_i x_j y_2$ .

**Theorem 5.1.** *For the universal form  $u$ , the quartic algebra  $Q_u$  is isomorphic to the quartic algebra over  $R$  that is constructed above using Bhargava’s multiplication tables.*

In particular, since our geometric construction of  $Q_u$  is invariant under change of basis of  $W$  and  $U$  (respecting  $\wedge^3 W \cong \wedge^2 U^*$ ), this gives a proof of the invariance of Bhargava’s multiplication table under change of basis, as long as the correct  $\text{GL}_3 \times \text{GL}_2$  action is used. Since all double ternary quadratic forms are locally pull-backs from the universal form, and both the local construction by multiplication tables and the global geometric construction of Section 4 respect base change, Theorem 5.1 implies that the two constructions of quartic algebras from double ternary quadratic forms agree. We now prove Theorem 5.1.

*Proof.* For the universal form  $u$ , the complex  $\mathcal{H}_u$  used to define  $Q_u$  is exact, and therefore  $Q_u$  is just the global functions on the scheme  $S_u$  in  $\mathbb{P}_R^2$  cut out by

$$A = \sum_{1 \leq i \leq j \leq 3} a_{ij} x_i x_j \quad \text{and} \quad B = \sum_{1 \leq i \leq j \leq 3} b_{ij} x_i x_j.$$

(We can just work in terms of global functions instead of the pushforward to the base since the base  $\text{Spec } R$  is affine. Moreover, the multiplicative structure of the global functions of  $S_u$  is the same as the induced multiplicative structure on the hypercohomological construction of  $Q_u$ .) We cover  $S_u$  with open sets  $\mathcal{U}_{x_i}$  coming from the usual open sets in  $\mathbb{P}_R^2$ . As a first step, we will find  $(f, g) \in \Gamma(\mathcal{U}_{x_i}) \times \Gamma(\mathcal{U}_{x_j})$  such that  $f = g$  in  $\Gamma(\mathcal{U}_{x_i} \cap \mathcal{U}_{x_j})$ . This will find all regular functions on  $\mathcal{U}_{x_i} \cup \mathcal{U}_{x_j}$ , and it will turn out that they all extend uniquely to global functions on  $S_u$ . Thus, we will have found all the regular functions on  $S_u$ . We will identify these regular functions with the basis in Bhargava’s quartic ring construction, and then it can be checked that the multiplication tables agree.

Let  $i, j, k$  be some permutation of 1, 2, 3. We have that

$$\Gamma(\mathcal{U}_{x_i}) = R[x_j/x_i, x_k/x_i]/(A/x_i^2, B/x_i^2).$$

Let  $I_i$  be the ideal  $(A/x_i^2, B/x_i^2)$  of  $R[x_j/x_i, x_k/x_i]$ , and similarly for  $I_j$ . Also,

$$\Gamma(\mathcal{U}_{x_i} \cap \mathcal{U}_{x_j}) = R[x_j/x_i, x_k/x_i, x_i/x_j]/(A/x_i^2, B/x_i^2).$$

If we have  $(f, g) \in \Gamma(\mathcal{U}_{x_i}) \times \Gamma(\mathcal{U}_{x_j})$  such that  $f = g$  in  $\Gamma(\mathcal{U}_{x_i} \cap \mathcal{U}_{x_j})$ , then  $f$  and  $g$  are represented by polynomials  $\tilde{f} \in R[x_j/x_i, x_k/x_i]$  and  $\tilde{g} \in R[x_i/x_j, x_k/x_j]$  such the element  $\tilde{f} - \tilde{g} \in R[x_j/x_i, x_k/x_i, x_i/x_j]$  is in the ideal  $I = (A/x_i^2, B/x_i^2)$ . However,  $\tilde{f} - \tilde{g}$  will not have any terms with an  $x_i$  and an  $x_j$  in the denominator. We define  $T_1$  to be the sub  $R$ -module of  $I$  of elements that do not have any terms with both an  $x_i$  and an  $x_j$  in the denominator. The set  $T_1$  gives all the relations between polynomials representing elements in  $\Gamma(\mathcal{U}_{x_i})$  and polynomials representing elements in  $\Gamma(\mathcal{U}_{x_j})$ . We define  $T_2$  to be the sub  $R$ -module of  $T_1$  generated by the images of  $I_i$  and  $I_j$  under their natural inclusion into  $R[x_j/x_i, x_k/x_i, x_i/x_j]$ . The set  $T_2$  gives all the relations of  $T_1$  that come from relations already in  $\mathcal{U}_{x_i}$  and already in  $\mathcal{U}_{x_j}$ . We now seek to determine  $T_1/T_2$ , which gives rise to all pairs  $(f, g) \in \Gamma(\mathcal{U}_{x_i}) \times \Gamma(\mathcal{U}_{x_j})$  such that  $f = g$  in  $\Gamma(\mathcal{U}_{x_i} \cap \mathcal{U}_{x_j})$  that are not functions on the base  $\text{Spec } R$ .

We first define some notation to help us write down elements of  $T_1/T_2$ . Let

$$A_{i^m j^n} = A \frac{x_k^{m+n-2}}{x_i^m x_j^n},$$

where the subscript  $i^m j^n$  is a product of formal symbols, where a missing exponent denotes an exponent of 1. We define  $B_{i^m j^n}$  analogously.

**Lemma 5.2.** *Let  $t \in T_1/T_2$ . We can write*

$$t = \sum_{\substack{m,n \geq 1 \\ m+n \leq 3}} c_{m,n} A_i^m x_j^n + d_{m,n} B_i^m x_j^n \quad \text{with } c_{m,n}, d_{m,n} \in R.$$

*Proof.* Clearly we can write any  $t$  in  $I$  as such as sum over  $m, n \in \mathbb{Z}$  with  $m+n \geq 2$ . Any term with  $m \leq 0$  is in the image of  $I_j$  and thus in  $T_2$ , and any term with  $n \leq 0$  is in the image of  $I_i$  and thus in  $T_2$ . It remains to show that we do not need terms with  $m+n \geq 4$  in order to represent  $t$ .

We suppose for the sake of contradiction that a term with  $m+n \geq 4$  was required, and we take a  $t$  with  $m+n$  maximal for this condition, and  $m$  maximal given that. Then  $c_{m,n} A_i^m x_j^n$  contributes a  $x_k^{m+n}/x_i^m x_j^n$  term with coefficient  $c_{m,n} a_{kk}$  and  $d_{m,n} B_i^m x_j^n$  contributes  $x_k^{m+n}/x_i^m x_j^n$  term with coefficient  $d_{m,n} b_{kk}$ . No other terms of the summand for  $t$  can contribute a term with  $x_i^m x_j^n$  in the denominator, and so we must have  $c_{m,n} = r b_{kk}$  and  $d_{m,n} = -r a_{kk}$  for some element  $r \in R$ .

Now we claim we did not need to use the terms  $r b_{kk} A_i^m x_j^n - r a_{kk} B_i^m x_j^n$  in the sum that represents  $t$ . To prove this claim, we use the following identity

$$\begin{aligned} b_{kk} A_i^m x_j^n - a_{kk} B_i^m x_j^n \\ = -b_{ik} A_{i^{m-1} j^n} + a_{ik} B_{i^{m-1} j^n} - b_{jk} A_{i^m j^{n-1}} + a_{jk} B_{i^m j^{n-1}} + a_{ij} B_{i^{m-1} j^{n-1}} \\ - b_{ij} A_{i^{m-1} j^{n-1}} - b_{jj} A_{i^m j^{n-2}} + a_{jj} B_{i^m j^{n-2}} - b_{i,i} A_{i^{m-2} j^n} + a_{ii} B_{i^{m-2} j^n}. \end{aligned}$$

This proves the lemma.  $\square$

The above lemma tells us that every element of  $T_1/T_2$  can be written as an  $R$ -linear combination of  $A_{ij}$ ,  $B_{ij}$ ,  $A_{i^2 j}$ ,  $B_{i^2 j}$ ,  $A_{ij^2}$ , and  $B_{ij^2}$ . Since only  $A_{i^2 j}$  and  $B_{i^2 j}$  have terms with  $x_i^2 x_j$  in the denominator, we must have that  $A_{i^2 j}$  and  $B_{i^2 j}$  appear with coefficients  $c_{2,1}$  and  $d_{2,1}$  so as to cancel those terms out. We can argue similarly for  $A_{ij^2}$  and  $B_{ij^2}$ . Thus, every element of  $T_1/T_2$  can be written as a  $R$  linear combination of  $A_{ij}$ ,  $B_{ij}$ ,  $b_{kk} A_{i^2 j} - a_{kk} B_{i^2 j}$ , and  $b_{kk} A_{ij^2} - a_{kk} B_{ij^2}$ . We note that all four of  $A_{ij}$ ,  $B_{ij}$ ,  $b_{kk} A_{i^2 j} - a_{kk} B_{i^2 j}$ , and  $b_{kk} A_{ij^2} - a_{kk} B_{ij^2}$  have terms with a  $x_i x_j$  denominator.

We define some notation so we can write combinations of these elements down more easily. For  $i < j$ , let  $a_{ji} = a_{ij}$ . Let  $\lambda_{\ell_3 \ell_4}^{\ell_1 \ell_2} = a_{\ell_1 \ell_2} b_{\ell_3 \ell_4} - b_{\ell_1 \ell_2} a_{\ell_3 \ell_4}$ . We note that

$$\begin{aligned} H_{i,j} &= b_{kk} A_{i^2 j} - a_{kk} B_{i^2 j} + b_{ik} A_{ij} - a_{ik} B_{ij} \\ &= \lambda_{kk}^{jj} \frac{x_j x_k}{x_i^2} + \lambda_{kk}^{ij} \frac{x_k}{x_i} + \lambda_{kk}^{ii} \frac{x_k}{x_j} + \lambda_{kk}^{jk} \frac{x_k^2}{x_i^2} + \lambda_{ik}^{jj} \frac{x_j}{x_i} + \lambda_{ik}^{ij} + \lambda_{ik}^{ii} \frac{x_i}{x_j} + \lambda_{ik}^{jk} \frac{x_k}{x_i} \end{aligned}$$

and

$$H_{j,i} = b_{kk} A_{ij^2} - a_{kk} B_{ij^2} + b_{jk} A_{ij} - a_{jk} B_{ij}$$

do not have any terms with both  $x_i$  and  $x_j$  in the denominator. Every element of  $T_1/T_2$  can be written as a  $R$  linear combination of  $A_{ij}$ ,  $B_{ij}$ ,  $H_{i,j}$  and  $H_{j,i}$ , because this is just a unipotent triangular transformation of the last list of four generators. We have seen that  $H_{i,j}$  and  $H_{j,i}$  have no  $x_k^2/x_i x_j$  terms, and  $A_{ij}$  and  $B_{ij}$  have  $x_k^2/x_i x_j$  terms with coefficients  $a_{kk}$  and  $b_{kk}$  respectively. Since an element of  $t$  does not have a term with  $x_i x_j$  in the denominator, it can be written as a linear combination of  $H_{i,j}$ ,  $H_{j,i}$  and  $F_{ij} = F_{ji} = b_{kk}A_{ij} - a_{kk}B_{ij}$ . Moreover,  $H_{i,j}$ ,  $H_{j,i}$  and  $F_{ij}$  are all in  $T_1$ . We now define  $h_{i,j}$  to be the sum of terms in  $H_{i,j}$  that do not have an  $x_j$  in the denominator, and  $h_{i,j} = H_{i,j} - h_{i,j}$ . We define  $f_{ij} = f_{ji}$  to be the sum of terms in  $F_{ij}$  with  $x_i$  in the denominator, so that  $f_{ij} + f_{ji} + \lambda_{kk}^{ij} = F_{ij}$ .

We have now found that the pairs  $(f, g) \in \Gamma(\mathcal{O}_{x_i}) \times \Gamma(\mathcal{O}_{x_j})$  such that  $f = g$  in  $\Gamma(\mathcal{O}_{x_i} \cap \mathcal{O}_{x_j})$  can be written in terms of four  $R$ -module generators:

$$(1, 1), (h_{i,j}, -h_{i,j}), (h_{j,i}, -h_{j,i}), (f_{ij}, -f_{ji} + \lambda_{ij}^{kk}).$$

Letting  $i$  and  $j$  vary, this information is enough to determine the global functions on  $S_u$ . In this case, it turns out that the regular functions on  $\mathcal{O}_{x_i}$  that can be extended to  $\mathcal{O}_{x_j}$  are exactly the same as the regular functions on  $\mathcal{O}_{x_i}$  that can be extended to  $\mathcal{O}_{x_k}$ . In particular, in the polynomial ring  $R[x_j/x_i, x_k/x_i]$ , we can compute that

$$h_{i,j} + h_{i,k} = \lambda_{jk}^{ii} + a_{jk}B/x_i^2 - b_{jk}A/x_i^2$$

and

$$h_{j,i} = -f_{ik}.$$

Moreover, it will turn out that the extensions to  $\mathcal{O}_{x_j}$  and  $\mathcal{O}_{x_k}$  agree on their intersection. We see that the global functions of  $S_u$  are generated as a  $R$ -module by four generators  $g_1, g_2, g_3, g_4 \in \Gamma(\mathcal{O}_{x_1}) \times \Gamma(\mathcal{O}_{x_2}) \times \Gamma(\mathcal{O}_{x_3})$ , whose components are:

	$\Gamma(\mathcal{O}_{x_1})$	$\Gamma(\mathcal{O}_{x_2})$	$\Gamma(\mathcal{O}_{x_3})$
$g_1$	1	1	1
$g_2$	$h_{1,2} = -h_{1,3} + \lambda_{23}^{11}$	$-h_{1,2} = f_{23}$	$-f_{32} + \lambda_{23}^{11} = h_{1,3} + \lambda_{23}^{11}$
$g_3$	$h_{2,1} = -f_{13}$	$-h_{2,1} = h_{2,3} + \lambda_{22}^{13}$	$-h_{2,3} + \lambda_{22}^{13} = f_{31} + \lambda_{22}^{13}$
$g_4$	$f_{12} = -h_{3,1}$	$-f_{21} + \lambda_{12}^{33} = h_{3,2} + \lambda_{12}^{33}$	$-h_{3,2} + \lambda_{12}^{33} = h_{3,1}$

We now show that the  $g_i$  are generators for a free  $R$ -module of rank 4. Suppose for the sake of contradiction that there was a relation among these generators. Then over the generic point of  $R$  the global functions of  $S_u$  would be a vector space of at most dimension 3. But we have seen (top of page 1080) that the global functions of  $S_u$  form a locally free four-dimensional  $R$  module, and thus will be a

four-dimensional vector space over the generic point of  $\text{Spec } R$ .

To construct the multiplication table on our four generators  $g_i$  of the global functions on  $S_u$ , we can reduce to finding a multiplication table in the  $\Gamma(\mathcal{O}_{x_1})$  component, since the  $g_i$  are  $R$ -linearly independent even in this component. We can further reduce to finding the multiplication table over the generic point of  $\text{Spec } R$ . We first construct a multiplication table on  $1, x_2/x_1, x_3/x_1, x_2x_3/x_1^2$  over the generic point of  $\text{Spec } R$ . To do this, we replace  $A$  and  $B$  by linear combinations of  $A$  and  $B$ , one of which has no  $(x_2/x_1)^2$  term, and one of which has no  $(x_3/x_1)^2$  term. Then on  $\mathcal{O}_{x_1}$  over the generic point of  $\text{Spec } R$ , we can write all functions in terms of  $1, x_2/x_1, x_3/x_1, x_2x_3/x_1^2$ . We can then also write the  $g_i$  in terms of  $1, x_2/x_1, x_3/x_1, x_2x_3/x_1^2$ , and just apply this change of basis to the multiplication table to obtain a multiplication table for the  $g_i$ . If we take  $\alpha_1 = -g_2, \alpha_2 = -g_3,$  and  $\alpha_3 = -g_4$ , we obtain exactly the multiplication tables in [Bhargava 2004b, (15) and (21)].  $\square$

In Section 4.ii, we found that  $Q_p/\mathbb{C}_S$  is canonically isomorphic to  $W^*$ . However, we also have explicit basis for  $Q_p/\mathbb{C}_S$  when we have a basis for  $W$ . We see how these bases are related.

**Theorem 5.3.** *For the universal form  $u$ , in the map  $Q_p \rightarrow W^*$  from Section 4.ii, we have*

$$g_2 \mapsto x_1^*, \quad g_3 \mapsto x_3^*, \quad g_4 \mapsto x_2^*.$$

*Proof.* We compute the map in two steps. We first find the map

$$R^0\pi_*(\mathbb{C}/u(\mathbb{C}(-2)^{\oplus 2})) \rightarrow R^1\pi_*(\mathbb{C}(-2)^{\oplus 2}/u(\mathbb{C}(-4)))$$

and then the map

$$R^1\pi_*(\mathbb{C}(-2)^{\oplus 2}/u(\mathbb{C}(-4))) \rightarrow R^2\pi_*(\mathbb{C}(-4)).$$

We compute each of the individual maps by using the snake lemma on the Čech complex with the usual affine cover of  $\mathbb{P}^2$ . The charts on pages 1085–1087, which should be read from upper right to lower left, summarize the computation.  $\square$

### 6. Construction of the cubic resolvent

In Section 2, we have already given a geometric construction of a cubic algebra from a binary cubic form. In Section 3, we defined the determinant of a double ternary quadratic form  $p$  to be a binary cubic form  $\det(p) \in \text{Sym}^3 U^* \otimes (\wedge^2 U)$ . The cubic algebra  $C$  of this binary cubic form can be constructed as described in Section 2, and is the desired cubic resolvent.

We have  $C/\mathbb{C}_S \cong U$  (see [Wood 2011b, Section 3.1] for a similar, but simpler argument to the one in Section 4.ii). Thus,  $p$  gives the required quadratic map

	$\mathbb{C}(-4)$	$\mathbb{C}(-2)^{\oplus 2}$	$\mathbb{C}(-2)^{\oplus 2}/u(\mathbb{C}(-4))$	$\mathbb{C}$	$\mathbb{C}/u(\mathbb{C}(-2)^{\oplus 2})$
$\Gamma(\mathcal{U}_{x_1})$ $\times \Gamma(\mathcal{U}_{x_2})$ $\times \Gamma(\mathcal{U}_{x_3})$				$h_{1,2}$ $-h_{1,2}$ $-f_{3,2} + \lambda_{23}^{11}$	$g_2$
$\Gamma(\mathcal{U}_{x_1x_2})$			$\left(\frac{a_{33}x_3}{x_1^2x_2} + \frac{a_{13}}{x_1x_2}, \frac{b_{33}x_3}{x_1^2x_2} + \frac{b_{13}}{x_1x_2}\right)$	$h_{1,2} + h_{1,\bar{2}} = H_{1,2}$ ..... $-h_{1,2} + f_{\bar{3},2} - \lambda_{23}^{11}$ $= f_{2,3} + f_{\bar{3},2} - \lambda_{23}^{11}$ $= F_{23}$ .....	
$\times \Gamma(\mathcal{U}_{x_2x_3})$			$\left(\frac{a_{11}}{x_2x_3}, \frac{b_{11}}{x_2x_3}\right)$	$h_{1,2} + f_{\bar{3},2} - \lambda_{23}^{11}$ $= -h_{1,3} - h_{1,\bar{3}} + a_{23}\frac{A}{x_1^2} - b_{23}\frac{A}{x_1^2}$ $= -H_{1,3}$	
$\times \Gamma(\mathcal{U}_{x_3x_1})$			$-\left(\frac{a_{22}x_2}{x_1^2x_3} + \frac{a_{12}}{x_1x_3}, \frac{b_{22}x_2}{x_1^2x_3} + \frac{b_{12}}{x_1x_3}\right)$  $-\left(\frac{a_{23}}{x_1^2}, \frac{b_{23}}{x_1^2}\right)$	$+ \frac{B}{a_{23}\frac{A}{x_1^2}} - b_{23}\frac{A}{x_1^2}$	
$\Gamma(\mathcal{U}_{x_1x_2x_3})$	$\frac{1}{x_1^2x_2x_3}$	$\frac{A+B}{x_1^2x_2x_3}$			

Calculation of the image of  $g_2$  under the map  $Q_p \rightarrow W^*$ .

	$\mathbb{O}(-4)$	$\mathbb{O}(-2)^{\oplus 2}$	$\mathbb{O}(-2)^{\oplus 2}/u(\mathbb{O}(-4))$	$\mathbb{O}$	$\mathbb{O}/u(\mathbb{O}(-2)^{\oplus 2})$
$\Gamma(\mathcal{O}_{x_1})$ $\times \Gamma(\mathcal{O}_{x_2})$ $\times \Gamma(\mathcal{O}_{x_3})$				$h_{2,1}$ $-h_{2,1}$ $f_{3,1} + \lambda_{22}^{13}$	$g_3$
$\Gamma(\mathcal{O}_{x_1x_2})$  $\times \Gamma(\mathcal{O}_{x_2x_3})$			$\left(\frac{a_{33}x_3}{x_1x_2^2} + \frac{a_{23}}{x_1x_2}, \frac{b_{33}x_3}{x_1x_2^2} + \frac{b_{23}}{x_1x_2}\right)$  $\left(\frac{a_{11}x_1}{x_3x_2^2} + \frac{a_{12}}{x_3x_2}, \frac{b_{11}x_1}{x_3x_2^2} + \frac{b_{12}}{x_3x_2}\right)$  $+ \left(\frac{a_{13}}{x_2^2}, \frac{b_{13}}{x_2}\right)$	$h_{2,1} + h_{2,1} = H_{2,1}$ ..... $-h_{2,1} - f_{3,1} - \lambda_{22}^{13}$ $= h_{2,3} + h_{2,3} - a_{13}\frac{B}{x_2^2} + b_{13}\frac{A}{x_2^2}$ $= H_{2,3}$  $+ \quad -a_{13}\frac{B}{x_2^2} + b_{13}\frac{A}{x_2^2}$ ..... $h_{2,1} - f_{3,1} - \lambda_{22}^{13}$ $= -f_{1,3} - f_{3,1} - \lambda_{22}^{13}$ $= -F_{13}$	
$\times \Gamma(\mathcal{O}_{x_3x_1})$			$- \left(\frac{a_{22}}{x_1x_3}, \frac{b_{22}}{x_1x_3}\right)$		
$\Gamma(\mathcal{O}_{x_1x_2x_3})$	$\frac{1}{x_1x_2^2x_3}$	$\frac{A+B}{x_1x_2^2x_3}$			

Calculation of the image of  $g_3$  under the map  $Q_p \rightarrow W^*$ .



	$\mathbb{O}(-4)$	$\mathbb{O}(-2)^{\oplus 2}$	$\mathbb{O}(-2)^{\oplus 2}/u(\mathbb{O}(-4))$	$\mathbb{O}$	$\mathbb{O}/u(\mathbb{O}(-2)^{\oplus 2})$
$\Gamma(\mathcal{O}_{x_1})$ $\times \Gamma(\mathcal{O}_{x_2})$ $\times \Gamma(\mathcal{O}_{x_3})$				$h_{3,\bar{1}}$ $-f_{\bar{2},1} + \lambda_{12}^{33}$ $h_{\bar{3},1}$	$g_4$
$\Gamma(\mathcal{O}_{x_1x_2})$			$\left( \frac{a_{33}}{x_1x_2}, \frac{b_{33}}{x_1x_2} \right)$	$-h_{3,\bar{1}} + f_{\bar{2},1} - \lambda_{12}^{33}$ $= f_{\bar{2},1} + f_{\bar{1},2} + \lambda_{33}^{12}$ $= F_{12}$ .....	
$\times \Gamma(\mathcal{O}_{x_2x_3})$			$\left( \frac{a_{11}x_1}{x_1x_3^2} + \frac{a_{13}}{x_2x_3}, \frac{b_{11}x_1}{x_1x_3^2} + \frac{b_{13}}{x_2x_3} \right)$ $+ \left( \frac{a_{12}}{x_3^2}, \frac{b_{12}}{x_3^2} \right)$	$-h_{\bar{3},1} - f_{\bar{2},1} + \lambda_{12}^{33}$ $= h_{\bar{3},2} + h_{2,\bar{3}} - a_{12} \frac{A}{x_3^2} + b_{12} \frac{A}{x_3^2}$ $= H_{3,2}$  $+ -a_{12} \frac{B}{x_3^2} + b_{12} \frac{A}{x_3^2}$ .....	
$\times \Gamma(\mathcal{O}_{x_3x_1})$			$- \left( \frac{a_{22}x_2}{x_3^2x_1} + \frac{a_{23}}{x_1x_3}, \frac{b_{22}x_2}{x_3^2x_1} + \frac{b_{23}}{x_1x_3} \right)$	$-h_{\bar{3},1} - h_{3,\bar{1}} = -H_{3,1}$ .....	
$\Gamma(\mathcal{O}_{x_1x_2x_3})$	$\frac{1}{x_1x_2x_3^2}$	$\frac{A+B}{x_1x_2x_3^2}$			

Calculation of the image of  $g_4$  under the map  $Q_p \rightarrow W^*$ .

from  $Q/\mathbb{O}_S$  to  $C/\mathbb{O}_S$ . The orientation isomorphism  $\delta : \wedge^3 Q/\mathbb{O}_S \xrightarrow{\sim} \wedge^2 C/\mathbb{O}_S$  comes from the orientation on the double ternary quadratic form. On any open set, we can check that  $\delta(x \wedge y \wedge xy) = p(x) \wedge p(y)$  by looking on a open subcover on which  $W$  and  $U$  are trivial and pulling back from the universal form on each open set in that subcover. It remains to check that  $\delta(x \wedge y \wedge xy) = p(x) \wedge p(y)$  when  $p$  is the universal ternary quadratic form, which can be checked explicitly given the multiplication table of  $Q_p$ . In particular, at the end of the proof of the main theorem in Section 7, we lay out a plan to determine the multiplication table of  $Q_p$  in terms of  $p$ . The result agrees with the multiplication table given explicitly in [Bhargava 2004b, Equations (15) and (21)]. The expressions  $\delta(x \wedge y \wedge xy)$  and  $p(x) \wedge p(y)$  both represent linear maps from  $\text{Sym}_2(Q_p/\mathbb{O}_S) \otimes \text{Sym}_2(Q_p/\mathbb{O}_S)$  to  $\wedge^4 Q_p$ . Thus it suffices to check that these maps agree on a basis of global sections of  $\text{Sym}_2(Q_p/\mathbb{O}_S) \otimes \text{Sym}_2(Q_p/\mathbb{O}_S)$ , since in this case  $Q_p/\mathbb{O}_S$  is a free  $\mathbb{O}_S$  module. This is easily checked, especially exploiting the symmetry of the situation.

## 7. Main theorem

In this section, we prove the main theorem of this paper.

**Theorem 7.1.** *There is an isomorphism between the moduli stack for quartic algebras with cubic resolvents and the moduli stack for double ternary quadratic forms. In other words, for a scheme  $S$  there is an equivalence between the category of quartic algebras with cubic resolvents and the category of double ternary quadratic forms (with morphisms given by isomorphisms in both categories), and this natural equivalence commutes with base change in  $S$ .*

*Proof.* Given a double ternary quadratic form  $p$  over a base  $S$ , we have shown how to construct a pair  $(Q_p, C_p)$ , and all aspects of the construction commute with base change in  $S$ . Given a pair  $(Q, C)$  over  $S$ , we can just take the quadratic map  $\phi$  from  $Q/\mathbb{O}_S$  to  $C/\mathbb{O}_S$  to be our double ternary quadratic form with  $W = (Q/\mathbb{O}_S)^*$  and  $U = C/\mathbb{O}_S$  (using the orientation  $\wedge^3 Q/\mathbb{O}_S \xrightarrow{\sim} \wedge^2 C/\mathbb{O}_S$ ). This construction clearly commutes with base change.

It remains to prove that the compositions of these two constructions (in either order) are the identity. To prove this, we rigidify the moduli problems. A *based double ternary quadratic form* is a ternary quadratic form  $p \in \text{Sym}^2 W \otimes U$  and a choice of bases  $w_1, w_2, w_3$  and  $u_1, u_2$  for  $W$  and  $U$  respectively as free  $\mathbb{O}_S$ -modules, such that  $(w_1 \wedge w_2 \wedge w_3) \otimes (u_1 \wedge u_2)$  corresponds to the identity under the orientation isomorphism. A *based pair  $(Q, C)$  of a quadratic algebra and cubic resolvent* is a pair  $(Q, C)$  of quadratic algebra and cubic resolvent and choices of basis  $q_1, q_2, q_3$  and  $c_1, c_2$  for  $Q/\mathbb{O}_S$  and  $C/\mathbb{O}_S$  as free  $\mathbb{O}_S$ -modules, such that  $(q_1 \wedge q_2 \wedge q_3)$  corresponds to  $(c_1 \wedge c_2)$  under the orientation isomorphism. We see that our constructions above extend to the moduli stacks for these rigidified moduli

problems. In particular, we obtain a basis for  $Q/\mathbb{O}_S$  as a dual basis for the basis of  $W$  and vice versa.

It now suffices to show that these constructions compose to the identity on the rigidified moduli stacks. If we start with a double ternary quadratic form  $p \in \text{Sym}^2 W \otimes U$ , we obtain a pair  $(Q, C)$  whose quadratic map is given exactly by the form, and then the construction of a form from  $(Q, C)$  gives back exactly our original form. The choices of bases for  $W$  and  $U$  and the orientation are clearly preserved under this composition.

We can start with a based pair  $(Q, C)$ , then build another based pair  $(Q_\phi, C_\phi)$  from the quadratic map  $\phi$  of  $(Q, C)$ , and we wish to show that  $(Q, C)$  and  $(Q_\phi, C_\phi)$  are equal. (We can use the notion of equal instead of isomorphic since all of the objects are based.) We have that  $C$  and  $C_\phi$  are both given as the cubic algebra corresponding to  $\text{Det}(\phi)$  and thus are equal. The quadratic resolvent maps are the same, since  $\phi$  carries through the two constructions. The orientation isomorphism are clearly the same since they also carry through the constructions. It remains to show that the multiplication on  $Q$  agrees with the multiplication on  $Q_\phi$ . To do this, we will show that the condition  $\delta(1 \wedge x \wedge y \wedge xy) = \phi(x) \wedge \phi(y)$  determines the multiplication table on  $Q$  from the resolvent map  $\phi$ . Since  $Q$  and  $Q_\phi$  have the same resolvent map, this will show that they are isomorphic as  $\mathbb{O}_S$ -algebras.

Let the quadratic map  $\phi$  be written as  $Ac_2 + Bc_1$ , where  $A = \sum_{1 \leq i \leq j \leq 3} a_{ij}x_i x_j$  and  $B = \sum_{1 \leq i \leq j \leq 3} b_{ij}x_i x_j$ , and the  $x_i$  are a dual basis for  $q_i$  in  $Q/\mathbb{O}_S$ . We recall the notation

$$\lambda_{\ell_3 \ell_4}^{\ell_1 \ell_2} = a_{\ell_1 \ell_2} b_{\ell_3 \ell_4} - b_{\ell_1 \ell_2} a_{\ell_3 \ell_4}.$$

We lift the basis  $q_i$  of  $Q/\mathbb{O}_S$  to a basis of  $Q$  uniquely so that  $q_1 q_2$  has no  $q_1$  or  $q_2$  term and so that  $q_1 q_3$  has no  $q_1$  term. Let  $m_{ij}^k$  be the coefficient of  $q_k$  in the  $q_i q_j$ . From Equation (23) in [Bhargava 2004b], we know that the constant coefficient of  $q_i q_j$  is given as a polynomial in the various  $m$  coefficients. Thus, it remains to show that the  $m_{ij}^k$  are determined by  $\phi$ . We plug various  $x$  and  $y$  into  $\delta(1 \wedge x \wedge y \wedge xy) = \phi(x) \wedge \phi(y)$ . In the below, we always let  $i, j, k$  be a permutation of 1, 2, 3 and let  $\pm$  be the sign of this permutation. First, letting  $x = q_i$  and  $y = q_j$  gives  $m_{ij}^k = \pm \lambda_{ii}^{jj}$ . Then, letting  $x = q_i + q_j$  and  $y = q_i$  gives  $m_{ii}^k = \pm \lambda_{ii}^{ij}$ . Next, letting  $x = q_i + q_k$  and  $y = q_j$  gives  $m_{jk}^k - m_{ij}^i = \pm \lambda_{ik}^{jj}$ . Using the choice of lift, which gives  $m_{12}^1 = m_{21}^2 = m_{13}^1 = 0$ , this determines all  $m_{ij}^i$ . Finally, letting  $x = q_i + q_k$  and  $y = q_i + q_j$  determines  $m_{ii}^i$  in terms of the  $\lambda$ 's and the  $m$ 's that we have already determined. □

### Appendix A. Maps between locally free $\mathbb{O}_S$ -modules

Let  $S$  be a scheme. In this appendix we will give several basic facts about maps between locally free  $\mathbb{O}_S$ -modules.

**Lemma A.1.** *If  $L$  is a locally free  $\mathbb{O}_S$ -module and  $V$  is a locally free rank- $n$   $\mathbb{O}_S$ -module, then  $\text{Sym}^k(V \otimes L) \cong \text{Sym}^k V \otimes L^{\otimes k}$ .*

*Proof.* We have the canonical map

$$\begin{aligned} \text{Sym}^k(V \otimes L) &\rightarrow \text{Sym}^k V \otimes \text{Sym}^k L, \\ (v_1 \otimes \ell_1) \cdots (v_k \otimes \ell_k) &\mapsto v_1 \cdots v_k \otimes \ell_1 \cdots \ell_k, \end{aligned}$$

which we can check is an isomorphism on free modules and thus is an isomorphism on locally free modules. Moreover, we have that  $L^{\otimes k} \cong \text{Sym}^k L$ . We have the canonical quotient map  $L^{\otimes k} \rightarrow \text{Sym}^k L$ , which is clearly an isomorphism for  $L$  free of rank 1 and thus locally free of rank 1.  $\square$

**Lemma A.2.** *If  $V$  is a locally free  $\mathbb{O}_S$ -module of rank 2 then  $V \otimes \wedge^2 V^* \cong V^*$ .*

*Proof.* We have

$$\begin{aligned} V \otimes \wedge^2 V^* &\rightarrow V^*, \\ v \otimes (\mathcal{V}_1 \wedge \mathcal{V}_2) &\mapsto \mathcal{V}_1(v)\mathcal{V}_2 - \mathcal{V}_2(v)\mathcal{V}_1. \end{aligned}$$

We can define the canonical map which is an isomorphism for free and thus locally free modules of rank 2.  $\square$

We combine these two lemmas to obtain a corollary that is used throughout this paper.

**Corollary A.3.** *If  $V$  is a locally free  $\mathbb{O}_S$ -module of rank 2 then*

$$\text{Sym}^3 V \otimes (\wedge^2 V)^{\otimes -2} \cong \text{Sym}^3 V^* \otimes (\wedge^2 V^*)^{\otimes -1}.$$

**Lemma A.4.** *If  $V$  is a locally free  $\mathbb{O}_S$ -module, we have  $(\text{Sym}_n V)^* \cong \text{Sym}^n V^*$ .*

*Proof.* We give a map from  $\text{Sym}^n V^*$  to  $(\text{Sym}_n V)^*$  as follows:

$$\mathcal{V}_1 \mathcal{V}_2 \cdots \mathcal{V}_n \mapsto (v_1 \otimes \cdots \otimes v_n \mapsto \mathcal{V}_1(v_1)\mathcal{V}_2(v_2) \cdots \mathcal{V}_n(v_n)).$$

If we permute the  $\mathcal{V}_i$  factors, we see the result does not change because the elements of  $\text{Sym}_n V$  that we evaluate on are invariant with respect to this permutation. When  $V$  is free, we can explicitly see that this map is an isomorphism.  $\square$

**A.i. Degree- $k$  maps.** Let  $M$  and  $N$  be locally free  $\mathbb{O}_S$ -modules. A linear map from  $M$  to  $N$  is equivalent to a global section of  $M^*$ . In other words, sections of  $M^*$  are the degree-1 functions on  $M$ . We define the degree- $n$  functions on  $M$  as the global sections of  $\text{Sym}^n M^*$ , symmetric polynomials in linear functions on  $M$ .

**Definition.** A degree- $n$  map from  $M$  to  $N$  is a global section of

$$\text{Sym}^n M^* \otimes N \cong \mathcal{H}om(\text{Sym}_n M, N).$$

Note that the identity map on  $\text{Sym}_n M$  gives a canonical degree- $n$  map from  $M$  to  $\text{Sym}_n M$ .

The language “degree- $n$  map from  $M$  to  $N$ ” suggests that we should be able to evaluate such a thing on elements of  $M$ .

**Definition.** Let a degree- $n$  map from  $M$  to  $N$  be given, and regarded as an element  $f \in \text{Hom}(\text{Sym}_n M, N)$ , the *evaluation* of  $f$  on an element of  $M$  is  $f(m \otimes \cdots \otimes m)$ .

When  $M$  is free, say with generators  $m_1, \dots, m_k$  and dual basis  $m_1, \dots, m_k$  of  $M^*$ , then we defined a degree- $n$  map  $f$  from  $M$  to  $R$  to be a homogeneous polynomial of degree- $n$  in the  $m_1, \dots, m_k$ . If we evaluate  $f$  on  $(c_1 m_1 + \cdots + c_k m_k)$  for arbitrary sections  $c_i$  of  $\mathcal{O}_S$ , we will have a degree- $n$  polynomial in the  $c_i$ . Replacing the  $c_i$  in this polynomial by  $m_i$  we obtain the homogeneous polynomial of degree  $n$  in the  $m_1, \dots, m_k$  which is the realization of  $f$  as an element of  $\text{Sym}^n M^*$ .

When  $M$  is free, we may have a non-linear map  $\rho : M \rightarrow \mathcal{O}_S$  (or  $\rho : M \rightarrow N$ , but we take  $N = \mathcal{O}_S$  for simplicity) and wish to realize it as the evaluation of a degree- $n$  map. We can consider  $\rho(c_1 m_1 + \cdots + c_k m_k)$  for arbitrary  $c_i \in R$  and if  $\rho(c_1 m_1 + \cdots + c_k m_k)$  is a degree- $n$  polynomial in the  $c_i$ , we have an  $f \in \text{Sym}^n M^*$  (given by replacing the  $c_i$  by  $m_i$ ) of which  $\rho$  is the evaluation).

Since  $M$  is locally free, we locally have  $f \in \text{Sym}^n M^*$  and see that the above recipe is invariant under change of basis and so we have a global  $f \in \text{Sym}^n M^*$  (as long as everywhere locally where  $M$  is free  $\rho(c_1 m_1 + \cdots + c_k m_k)$  is a degree- $n$  polynomial in the  $c_i$ ).

As an example, we explicitly realize the determinant as a distinguished element of

$$\text{Hom}(\text{Sym}_n \text{Hom}(M, N), \text{Hom}(\wedge^n M, \wedge^n N)).$$

Let  $\phi_1 \otimes \cdots \otimes \phi_n \in \text{Hom}(M, N)^{\otimes n}$ . Then we can map  $\phi_1 \otimes \cdots \otimes \phi_n$  to the element of  $\text{Hom}(\wedge^n M, \wedge^n N)$  which sends  $m_1 \wedge \cdots \wedge m_n$  to  $\phi_1(m_1) \wedge \cdots \wedge \phi_n(m_n)$ . This will not be well-defined for  $\phi_1 \otimes \cdots \otimes \phi_n \in \text{Hom}(M, N)^{\otimes n}$ , but it will be well-defined when restricted to  $\text{Sym}_n \text{Hom}(M, N)$ .

$$\begin{aligned} \text{Sym}_n \text{Hom}(M, N) &\rightarrow \text{Hom}(\wedge^n M, \wedge^n N), \\ \phi_1 \otimes \cdots \otimes \phi_n &\mapsto (m_1 \wedge \cdots \wedge m_n \mapsto \phi_1(m_1) \wedge \cdots \wedge \phi_n(m_n)). \end{aligned} \tag{3}$$

This is our realization of the determinant function (as opposed to the determinant of a specific homomorphism) as an element of

$$\text{Hom}(\text{Sym}_n \text{Hom}(M, N), \text{Hom}(\wedge^n M, \wedge^n N)).$$

When we evaluate the determinant on a map  $\phi \in \text{Hom}(M, N)$ , we have  $\phi(m_1) \wedge \cdots \wedge \phi(m_n)$ . For example, let  $N$  and  $M$  be free of rank 2. Evaluating our degree-2 determinant map on a generic element of  $\text{Hom}(M, N)$  that sends  $m_1$  to  $an_1 + cn_2$

and  $m_2$  to  $bn_1 + dn_2$ , we see that we obtain the element of  $\text{Hom}(\wedge^2 M, \wedge^2 N)$  that sends  $m_1 \wedge m_2$  to  $(an_1 + cn_2) \wedge (bn_1 + dn_2) = (ad - bc)n_1 \wedge n_2$ .

**A.ii. Degree- $k$  maps with coefficients.** Recall that we have defined a degree- $k$  map from a locally free  $\mathbb{O}_S$ -module  $M$  to a locally free  $\mathbb{O}_S$ -module  $V$  to be a linear map from  $\text{Sym}_k M$  to  $V$ . This is equivalent to a global section of  $\text{Sym}^k M^* \otimes V$ . We use the following proposition to show that we can “add coefficients” to a degree- $k$  map.

**Proposition A.5.** In the natural map

$$\text{Sym}_k(M \otimes N) \rightarrow M^{\otimes k} \otimes \text{Sym}^k N,$$

the image of  $\text{Sym}_k(M \otimes N)$  is inside  $\text{Sym}_k M \otimes \text{Sym}^k N$ .

*Proof.* We prove this proposition by checking the statement locally where the modules are free. If we symmetrize a pure tensor of basis elements in  $(M \otimes N)^{\otimes k}$ , we see that when we forget the terms from  $N$  we still obtain an element of  $\text{Sym}_k M$ . Since all of the terms in the symmetrization will have the same factor in  $\text{Sym}^k N$ , this completes the proof.  $\square$

Thus, given a degree- $k$  map from  $M$  to  $V$ , we naturally obtain a degree- $k$  map from  $M \otimes N$  to  $V \otimes \text{Sym}^k N$  (by composing  $\text{Sym}_k(M \otimes N) \rightarrow \text{Sym}_k M \otimes \text{Sym}^k N \rightarrow V \otimes \text{Sym}^k N$ ). We call this construction *using  $V$  as coefficients*, because it is as if we treat the elements of  $V$  as formal ring elements.

## Appendix B. Inherited algebra structure

Let  $X$  be a scheme. A *multiplication* on a chain complex  $C$  of  $\mathbb{O}_X$ -modules is given by a map  $C \otimes C \rightarrow C$ . (See [Weibel 1994, 2.7.1] for the definition of the tensor product of two chain complexes.) Associativity and commutativity of the multiplication are given by the commutativity of the expected diagrams built out of the multiplication map. A unit is given by a map  $\mathbb{O}_X \rightarrow C$  that satisfies the expected properties with respect to the multiplication.

If  $\pi : X \rightarrow Y$  is a morphism of schemes, such a multiplication on  $C$  is inherited by  $R\pi_* C$  in the derived category of  $Y$ . To be more precise, we let  $Q$  be the localization functor that maps complexes of  $\mathbb{O}_X$ -modules to the associated objects in the derived category of  $X$ . From the universal property of the derived tensor (see, [Weibel 1994, 10.5.1], for instance), we have a morphism

$$Q(C) \otimes Q(C) \rightarrow Q(C \otimes C), \tag{4}$$

where the  $\otimes$  of the left side denotes the total tensor in the derived category (see [Weibel 1994, 10.6] or [Hartshorne 1966, II.4]). From Equation (4) composed with

$Q(C \otimes C) \rightarrow Q(C)$  from the multiplication map, we see that the multiplication on  $C$  is inherited by  $Q(C)$  in the derived category of  $X$ .

Next we see there is a map

$$R\pi_*Q(C) \otimes R\pi_*Q(C) \rightarrow R\pi_*(Q(C) \otimes Q(C)) \quad (5)$$

which can be obtained from the morphism  $R\pi_*Q(C) \otimes R\pi_*Q(C) \rightarrow R\pi_*(Q(C) \otimes L\pi^*R\pi_*Q(C))$  of the projection formula (see [Weibel 1994, 10.8.1] [Hartshorne 1966, II.5.6]) and the morphism  $L\pi^*R\pi_*Q(C) \rightarrow Q(C)$  that comes from the adjointness of  $L\pi^*$  and  $R\pi_*$  and the identity map  $R\pi_* \rightarrow R\pi_*$ ; see [Weibel 1994, 10.7.1; Hartshorne 1966, II.5.10, II.5.11]. Thus the multiplication is inherited by  $R\pi_*Q(C)$ . Finally, the natural map

$$H^0(R\pi_*Q(C)) \otimes H^0(R\pi_*Q(C)) \rightarrow H^0(R\pi_*Q(C) \otimes R\pi_*Q(C)) \quad (6)$$

shows how the multiplication is inherited by  $H^0(R\pi_*Q(C))$ . If the original multiplication on  $C$  is associative and commutative, one can follow the diagrams to see that the inherited multiplication on  $H^0(R\pi_*Q(C))$  will also be associative and commutative. Moreover, if we have a unit  $\mathbb{O}_X \rightarrow C$ , and  $\pi_*\mathbb{O}_X = \mathbb{O}_Y$ , then one can similarly follow diagrams to see that the inherited map  $\mathbb{O}_Y = H^0(R\pi_*Q(\mathbb{O}_X)) \rightarrow H^0(R\pi_*Q(C))$  is a unit. Thus if  $C$  has a commutative, associative multiplication and a unit and  $\pi_*\mathbb{O}_X = \mathbb{O}_Y$ , then  $H^0(R\pi_*Q(C))$  is an  $\mathbb{O}_Y$ -algebra.

### Acknowledgements

The author would like to thank Manjul Bhargava for asking the questions that inspired this research, guidance along the way, and helpful feedback both on the ideas and the exposition in this paper. She would also like to thank Lenny Taelman for suggestions for improvements to the paper. This work was done as part of the author's Ph.D. thesis at Princeton University, and during the work she was supported by an NSF Graduate Fellowship, an NDSEG Fellowship, an AAUW Dissertation Fellowship, and a Josephine De Kármán Fellowship. This paper was prepared for submission while the author was supported by an American Institute of Mathematics Five-Year Fellowship. The author would also like to thank the referee for making many suggestions that improved the paper.

### References

- [Bhargava 2004a] M. Bhargava, "Higher composition laws, II: On cubic analogues of Gauss composition", *Ann. of Math. (2)* **159**:2 (2004), 865–886. MR 2005f:11062b
- [Bhargava 2004b] M. Bhargava, "Higher composition laws, III: The parametrization of quartic rings", *Ann. of Math. (2)* **159**:3 (2004), 1329–1360. MR 2005k:11214
- [Bhargava 2005] M. Bhargava, "The density of discriminants of quartic rings and fields", *Ann. of Math. (2)* **162**:2 (2005), 1031–1063. MR 2006m:11163 Zbl 1159.11045

- [Casnati 1998] G. Casnati, “Covers of algebraic varieties. III. The discriminant of a cover of degree 4 and the trigonal construction”, *Trans. Amer. Math. Soc.* **350**:4 (1998), 1359–1378. MR 98i:14021
- [Casnati and Ekedahl 1996] G. Casnati and T. Ekedahl, “Covers of algebraic varieties. I. A general structure theorem, covers of degree 3, 4 and Enriques surfaces”, *J. Algebraic Geom.* **5**:3 (1996), 439–460. MR 97c:14014
- [Davenport and Heilbronn 1971] H. Davenport and H. Heilbronn, “On the density of discriminants of cubic fields. II”, *Proc. Roy. Soc. London Ser. A* **322**:1551 (1971), 405–420. MR 58 #10816 Zbl 0212.08101
- [Deligne 2000] P. Deligne, letter to W. T. Gan, B. Gross and G. Savin, November 13 2000.
- [Deligne 2004] P. Deligne, letter to M. Bhargava, March 5 2004.
- [Delone and Faddeev 1940] B. N. Delone and D. K. Faddeev, Теория иррациональностей третьей степени, *Trudy Mat. Inst. Steklov* **11**, 1940. Translated as *The theory of irrationalities of the third degree*, *Trans. Math. Monographs* **10**, Amer. Math. Soc., Providence, 1964. Original at <http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=tm&paperid=900>. MR 2,349d Zbl 0061.09001
- [EGA III.2 1963] A. Grothendieck, “Éléments de géométrie algébrique, III: Étude cohomologique des faisceaux cohérents, II”, *Inst. Hautes Études Sci. Publ. Math.* **17** (1963), 137–223. MR 29 #1210 Zbl 0122.16102
- [Eisenbud 2005] D. Eisenbud, *The geometry of syzygies: a second course in commutative algebra and algebraic geometry*, *Graduate Texts in Mathematics* **229**, Springer, New York, 2005. MR 2005h:13021 Zbl 1066.14001
- [Gan et al. 2002] W. T. Gan, B. Gross, and G. Savin, “Fourier coefficients of modular forms on  $G_2$ ”, *Duke Math. J.* **115**:1 (2002), 105–169. MR 2004a:11036 Zbl 1165.11315
- [Hahn and Miranda 1999] D. W. Hahn and R. Miranda, “Quadruple covers of algebraic varieties”, *J. Algebraic Geom.* **8**:1 (1999), 1–30. MR 99k:14028 Zbl 0982.14008
- [Hartshorne 1966] R. Hartshorne, *Residues and duality: lecture notes of a seminar on the work of A. Grothendieck*, *Lecture Notes in Math.* **20**, Springer, Berlin, 1966. MR 36 #5145
- [Miranda 1985] R. Miranda, “Triple covers in algebraic geometry”, *Amer. J. Math.* **107**:5 (1985), 1123–1158. MR 86k:14008 Zbl 0611.14011
- [Poonen 2008] B. Poonen, “The moduli space of commutative algebras of finite rank”, *J. Eur. Math. Soc. (JEMS)* **10**:3 (2008), 817–836. MR 2009d:14009 Zbl 1151.14011
- [Voight 2010] J. Voight, “Rings of low rank with a standard involution”, preprint, 2010. to appear in *Ill. J. Math.* arXiv 1003.3512
- [Weibel 1994] C. A. Weibel, *An introduction to homological algebra*, *Cambridge Studies in Adv. Math.* **38**, Cambridge University Press, 1994. MR 95f:18001 Zbl 0797.18001
- [Wood 2011a] M. M. Wood, “Gauss composition over an arbitrary base”, *Adv. Math.* **226**:2 (2011), 1756–1771. MR 2012a:11047 Zbl 05835547
- [Wood 2011b] M. M. Wood, “Rings and ideals parameterized by binary  $n$ -ic forms”, *J. Lond. Math. Soc. (2)* **83**:1 (2011), 208–231. MR 2763952 Zbl 1228.11053

Communicated by Hendrik W. Lenstra

Received 2010-06-29

Revised 2010-09-28

Accepted 2010-10-27

mmwood@math.wisc.edu

*Department of Mathematics, University of Wisconsin–Madison,  
480 Lincoln Drive, Madison, WI 53705, United States*

*American Institute of Mathematics, 360 Portage Ave,  
Palo Alto, CA 94306, United States*



# Coleman maps and the $p$ -adic regulator

Antonio Lei, David Loeffler and Sarah Livia Zerbes

We study the Coleman maps for a crystalline representation  $V$  with non-negative Hodge–Tate weights via Perrin-Riou’s  $p$ -adic “regulator” or “expanded logarithm” map  $\mathcal{L}_V$ . Denote by  $\mathcal{H}(\Gamma)$  the algebra of  $\mathbb{Q}_p$ -valued distributions on  $\Gamma = \text{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$ . Our first result determines the  $\mathcal{H}(\Gamma)$ -elementary divisors of the quotient of  $\mathbb{D}_{\text{cris}}(V) \otimes (\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0}$  by the  $\mathcal{H}(\Gamma)$ -submodule generated by  $(\varphi^* \mathbb{N}(V))^{\psi=0}$ , where  $\mathbb{N}(V)$  is the Wach module of  $V$ . By comparing the determinant of this map with that of  $\mathcal{L}_V$  (which can be computed via Perrin-Riou’s explicit reciprocity law), we obtain a precise description of the images of the Coleman maps. In the case when  $V$  arises from a modular form, we get some stronger results about the integral Coleman maps, and we can remove many technical assumptions that were required in our previous work in order to reformulate Kato’s main conjecture in terms of cotorsion Selmer groups and bounded  $p$ -adic  $L$ -functions.

1. Introduction	1095
2. Refinements of crystalline representations and $\mathcal{H}(\Gamma)$ -structure	1107
3. The construction of Coleman maps	1116
4. Images of the Coleman maps	1117
5. The Coleman maps for modular forms	1125
Acknowledgements	1129
References	1129

## 1. Introduction

**1A. Background.** Let  $p$  be an odd prime, and write  $\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})$ . Define the Galois groups  $\Gamma = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$  and  $\Gamma_1 = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}(\mu_p))$ . Note that  $\Gamma \cong \Delta \times \Gamma_1$ , where  $\Delta$  is cyclic of order  $p-1$  and  $\Gamma_1 \cong \mathbb{Z}_p$ . For  $H \in \{\Gamma, \Gamma_1\}$ , denote by  $\Lambda(H)$  the Iwasawa algebra of  $H$ , and  $\Lambda_{\mathbb{Q}_p}(H) = \Lambda(H) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ .

The authors’ research is supported by the following grants: ARC grant DP1092496 (Lei); EPSRC postdoctoral fellowship EP/F04304X/1 (Loeffler); EPSRC postdoctoral fellowship EP/F043007/1 (Zerbes).

*MSC2010:* primary 11R23; secondary 11F80, 11S25.

*Keywords:*  $p$ -adic regulator, Wach module, Selmer groups of modular forms.

Let  $V$  be a crystalline representation of  $\mathcal{G}_{\mathbb{Q}_p}$  of dimension  $d$  with non-negative Hodge–Tate weights. (We adopt the convention that the cyclotomic character has Hodge–Tate weight 1, so this condition is equivalent to  $\text{Fil}^1 \mathbb{D}_{\text{cris}}(V) = 0$ .) We define

$$H_{\text{Iw}}^1(\mathbb{Q}_p, V) := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n H^1(\mathbb{Q}(\mu_{p^n}), T),$$

where  $T$  is a  $\mathcal{G}_{\mathbb{Q}_p}$ -stable  $\mathbb{Z}_p$ -lattice in  $V$ . This is a  $\Lambda_{\mathbb{Q}_p}(\Gamma)$ -module independent of the choice of  $T$ . In [Lei et al. 2010], we construct  $\Lambda(\Gamma)$ -homomorphisms (called the Coleman maps)

$$\underline{\text{Col}}_i : H_{\text{Iw}}^1(\mathbb{Q}_p, V) \longrightarrow \Lambda_{\mathbb{Q}_p}(\Gamma)$$

for  $i = 1, \dots, d$ , depending on a choice of basis of the Wach module  $\mathbb{N}(V)$ . In the case when  $V = V_f(k - 1)$ , where  $f = \sum a_n q^n$  is a modular eigenform of weight  $k \geq 2$  and level coprime to  $p$  (we assume that  $a_n \in \mathbb{Q}$  for the time being in order to simplify notation) and  $V_f$  is the 2-dimensional  $p$ -adic representation associated to  $f$  by Deligne, these maps have two important applications. Firstly, we can define two  $p$ -adic  $L$ -functions  $L_{p,1}, L_{p,2} \in \Lambda_{\mathbb{Q}_p}(\Gamma)$  on applying the Coleman maps to the localisation of the Kato zeta element as constructed in [Kato 2004]. In the supersingular case, i.e., when  $p \mid a_p$ , this enables us to obtain a decomposition of the  $p$ -adic  $L$ -functions defined in [Amice and Vélú 1975], which are not elements of  $\Lambda_{\mathbb{Q}_p}(\Gamma)$  but of the distribution algebra  $\mathcal{H}(\Gamma)$ . More precisely, we show that there exists a  $2 \times 2$  matrix  $\mathcal{M} \in M(2, \mathcal{H}(\Gamma_1))$  depending only on  $k$  and  $a_p$  such that

$$\begin{pmatrix} L_{p,\alpha} \\ L_{p,\beta} \end{pmatrix} = \mathcal{M} \begin{pmatrix} L_{p,1} \\ L_{p,2} \end{pmatrix}.$$

This generalises the results of [Pollack 2003] (when  $a_p = 0$ ) and [Sprung 2009] (when  $f$  corresponds to an elliptic curve over  $\mathbb{Q}$  and  $p = 3$ ). Secondly, by modifying the local conditions at  $p$  in the definition of the  $p$ -Selmer group using the kernels of the maps  $\underline{\text{Col}}_i$ , we define two new Selmer groups  $\text{Sel}_p^i(f/\mathbb{Q}_\infty)$ . These are both  $\Lambda(\Gamma)$ -cotorsion, which is not true of the usual Selmer group in the supersingular case.

Fixing a character  $\eta$  of  $\Delta$  and restricting to the  $\eta$ -isotypical component, we get maps

$$\underline{\text{Col}}_i^\eta : H_{\text{Iw}}^1(\mathbb{Q}_p, V)^\eta \rightarrow \Lambda_{\mathbb{Q}_p}(\Gamma_1).$$

Via the Poitou–Tate exact sequence, we can reformulate Kato’s main conjecture (after tensoring with  $\mathbb{Q}_p$ ) as follows:

**Conjecture 1.1.** *For  $i = 1, 2$ , and each character  $\eta$  of  $\Delta$ ,*

$$\text{Char}_{\Lambda_{\mathbb{Q}_p}(\Gamma_1)}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \text{Sel}_p^i(f/\mathbb{Q}_\infty)^{\eta, \vee}) = \text{Char}_{\Lambda_{\mathbb{Q}_p}(\Gamma_1)}(\text{Im}(\underline{\text{Col}}_i^\eta)/(L_{p,i}^\eta)),$$

where  $M^\vee$  denotes the Pontryagin dual of a  $\Lambda(\Gamma_1)$ -module  $M$  and  $\text{Char}_{\Lambda_{\mathbb{Q}_p}(\Gamma_1)} M$  denotes the  $\Lambda_{\mathbb{Q}_p}(\Gamma_1)$ -characteristic ideal of  $M$ .

When  $v_p(a_p)$  is sufficiently large, we make use of the basis of  $\mathbb{N}(V)$  constructed in [Berger et al. 2004] to show that the first Coleman map is surjective under some additional technical conditions. Therefore, we can rewrite Conjecture 1.1 as follows (see [Lei et al. 2010, Corollary 6.6]):

**Theorem 1.2.** *Under certain technical conditions, the case  $i = 1$  in Conjecture 1.1 is equivalent to the assertion that  $\text{Char}_{\Lambda_{\mathbb{Q}_p}(\Gamma_1)}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \text{Sel}_p^1(f/\mathbb{Q}_\infty)^{\eta, \vee})$  is generated by  $L_{p,1}^\eta$ .*

(In fact we can show that this equivalence holds integrally, i.e., without tensoring with  $\mathbb{Q}_p$ .)

**1B. Main results.** In this paper, we extend the above results in several ways. Let  $V$  be a crystalline representation of  $\mathcal{G}_{\mathbb{Q}_p}$  of dimension  $d$  with non-negative Hodge–Tate weights. We make the following assumption:

**Assumption 1.3.** *The representation  $V$  admits at least one non-critical refinement, after a suitable extension of coefficients.*

See Section 1C5 below for the definition of a non-critical refinement. For now, let it suffice to say that this assumption holds for all 2-dimensional representations, and conjecturally for all representations “arising from geometry”.

We identify  $\Lambda(\Gamma_1)$  with the power series ring  $\mathbb{Z}_p[[X]]$ , where  $X = \gamma - 1$  for a topological generator  $\gamma$  of  $\Gamma_1$ . Denote by  $\chi : \mathcal{G}_{\mathbb{Q}_p} \rightarrow \mathbb{Z}_p^\times$  the cyclotomic character.

Firstly, we study the structure of  $\mathbb{N}_{\text{rig}}(V) := \mathbb{N}(V) \otimes_{\mathbb{B}_{\mathbb{Q}_p}^+} \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  as a  $\Gamma$ -module. If  $\varphi^* \mathbb{N}_{\text{rig}}(V)$  denotes the  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -span of  $\varphi(\mathbb{N}_{\text{rig}}(V))$ , then  $(\varphi^* \mathbb{N}_{\text{rig}}(V))^{\psi=0}$  is contained in  $(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0} \otimes_{\mathbb{Q}_p} \mathbb{D}_{\text{cris}}(V)$ , and both are free  $\mathcal{H}(\Gamma)$ -modules of rank equal to  $d = \dim_{\mathbb{Q}_p} V$ . We determine the elementary divisors of the quotient of these modules:

**Theorem A** (Theorem 2.10). *The  $\mathcal{H}(\Gamma)$ -elementary divisors of the quotient*

$$\mathbb{D}_{\text{cris}}(V) \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma) / (\varphi^* \mathbb{N}_{\text{rig}}(V))^{\psi=0}$$

are  $\mathfrak{n}_{r_1}, \dots, \mathfrak{n}_{r_d}$ , where  $r_1, \dots, r_d$  are the Hodge–Tate weights of  $V$  and

$$\mathfrak{n}_k = \frac{\log(1 + X)}{X} \cdots \frac{\log(\chi(\gamma)^{1-k}(1 + X))}{X - \chi(\gamma)^{k-1} + 1}.$$

This can be seen as a  $\mathcal{H}(\Gamma)$ -module analogue of [Berger 2004, Proposition III.2.1], which states that the  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -elementary divisors of the quotient

$$(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \otimes_{\mathbb{Q}_p} \mathbb{D}_{\text{cris}}(V)) / \mathbb{N}_{\text{rig}}(V)$$

are  $(\frac{t}{\pi})^{r_1}, \dots, (\frac{t}{\pi})^{r_d}$ . It is striking to note that for any  $k \geq 0$ , the Mellin transform of  $\mathfrak{n}_k$  agrees with  $(1 + \pi)\varphi(\frac{t}{\pi})^k$  up to a unit in  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  (see Proposition 1.6).

The second aim of this paper is to use Theorem A to determine the image of the map

$$1 - \varphi : \mathbb{N}_{\text{rig}}(V)^{\psi=1} \rightarrow (\varphi^* \mathbb{N}_{\text{rig}}(V))^{\psi=0}.$$

To do this, we make use of the following commutative diagram of  $\mathcal{H}(\Gamma)$ -modules:

$$\begin{array}{ccc} \mathbb{N}(V)^{\psi=1} & \xrightarrow{\cong} & H_{\text{Iw}}^1(V) \\ \downarrow 1-\varphi & \searrow h_{\text{Iw}, V}^1 & \downarrow \mathcal{L}_V \\ (\varphi^* \mathbb{N}_{\text{rig}}(V))^{\psi=0} & & \mathbb{D}_{\text{cris}}(V) \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma) \\ \downarrow & \searrow \text{1} \otimes \mathfrak{M}^{-1} & \\ \mathbb{D}_{\text{cris}}(V) \otimes_{\mathbb{Q}_p} (\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0} & \xrightarrow{\text{1} \otimes \mathfrak{M}^{-1}} & \mathbb{D}_{\text{cris}}(V) \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma). \end{array}$$

Here the map  $\mathcal{L}_V$  is Perrin-Riou’s “regulator” or “expanded logarithm” map (see [Perrin-Riou 1995]), which is a dual version of the more familiar exponential maps  $\Omega_{V, h}$  appearing in [Perrin-Riou 1994]; and

$$\mathfrak{M} : \mathcal{H}(\Gamma) \xrightarrow{\cong} (\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0}$$

denotes the Mellin transform. The commutativity of the diagram is a theorem of Berger [2003, Theorem II.13]. Colmez’s proof of the “ $\delta_V$ -conjecture” (see [Colmez 1998, Theorem IX.4.4]), which is part of Perrin-Riou’s explicit reciprocity law, gives a formula for the determinant of the matrix of  $\mathcal{L}_V$  (up to units). We can compare this with the determinant of the bottom left-hand map, which follows from Theorem A, to deduce that  $1 - \varphi : \mathbb{N}_{\text{rig}}(V)^{\psi=1} \rightarrow (\varphi^* \mathbb{N}_{\text{rig}}(V))^{\psi=0}$  is surjective up to a small error term:

**Theorem B** (Corollary 4.13). *Suppose that no eigenvalue of  $\varphi$  on  $\mathbb{D}_{\text{cris}}(V)$  lies in  $p^{\mathbb{Z}}$ . Then for each character  $\eta$  of  $\Delta$ , there is a short exact sequence of  $\mathcal{H}(\Gamma_1)$ -modules*

$$0 \longrightarrow \mathbb{N}(V)^{\psi=1, \eta} \xrightarrow{1-\varphi} (\varphi^* \mathbb{N}(V))^{\psi=0, \eta} \xrightarrow{A_\eta} \bigoplus_{i=0}^{r_d-1} (\mathbb{D}_{\text{cris}}(V) / V_{i, \eta})(\chi^i \chi_0^{-i} \eta) \longrightarrow 0.$$

Here  $V_{i, \eta}$  is a subspace of  $\mathbb{D}_{\text{cris}}(V)$  of the same dimension as  $\text{Fil}^{-i} \mathbb{D}_{\text{cris}}(V)$ , and the map  $A_\eta$  is the composition of the inclusion of  $(\varphi^* \mathbb{N}_{\text{rig}}(V))^{\psi=0}$  in  $\mathbb{D}_{\text{cris}}(V) \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma)$  with the map  $\bigoplus_i (\text{id} \otimes A_{\eta, i})$ , where  $A_{\eta, i}$  is the natural reduction map  $\mathcal{H}(\Gamma) \rightarrow \mathbb{Q}_p(\chi^i \chi_0^{-i} \eta)$  obtained by quotienting out by the ideal  $(X + 1 - \chi(\gamma)^i) \cdot e_\eta$ .

Using this we can describe the images of the Coleman maps (for any choice of basis of  $\mathbb{N}(V)$ ):

**Theorem C** (Corollary 4.15). *Let  $\eta$  be any character of  $\Delta$ . Then for all  $1 \leq i \leq d$ ,*

$$\text{Im}(\underline{\text{Col}}_i^\eta) = \prod_{j \in I_i^\eta} (X - \chi(\gamma)^j + 1) \Lambda_{\mathbb{Q}_p}(\Gamma_1)$$

for some  $I_i^\eta \subset \{0, \dots, r_d - 1\}$ .

As a corollary of the proof, we also obtain a formula for the elementary divisors of the matrix of the map  $\mathcal{L}_V$ , which can be seen as a refinement of the statement of the  $\delta(V)$ -conjecture. For  $i \in \mathbb{Z}$ , define

$$\ell_i = \frac{\log(1 + X)}{\log_p(\chi(\gamma))} - i.$$

**Theorem D** (Theorem 4.16). *The elementary divisors of the  $\mathcal{H}(\Gamma)$ -module quotient*

$$\frac{\mathcal{H}(\Gamma) \otimes_{\mathbb{Q}_p} \mathbb{D}_{\text{cris}}(V)}{\mathcal{H}(\Gamma) \otimes_{\Lambda_{\mathbb{Q}_p}(\Gamma)} \text{Im}(\mathcal{L}_V)}$$

are  $[\lambda_{r_1}; \lambda_{r_2}; \dots; \lambda_{r_d}]$ , where  $\lambda_k = \ell_0 \ell_1 \dots \ell_{k-1}$ .

Suppose now that  $V = V_f(k - 1)$ , where  $f = \sum a_n e^{2\pi i n z}$  is a modular form of weight  $k \geq 2$  and level prime to  $p$ , and  $V_f$  is the 2-dimensional  $p$ -adic representation associated to  $f$  by Deligne. (Thus the Hodge–Tate weights of  $V_f$  are 0 and  $1 - k$ , and those of  $V$  are 0 and  $k - 1$ .) As we show in Section 1C5, Assumption 1.3 is automatically satisfied in this case, since  $V$  is 2-dimensional. In this case, we can refine the results above to study the integral structure of the Coleman maps. Let  $T_f$  be a  $\mathcal{G}_{\mathbb{Q}_p}$ -stable lattice in  $V_f$ , and let us assume that the  $\mathbb{B}_{\mathbb{Q}_p}^+$ -basis of  $\mathbb{N}(V_f)$  used to define the Coleman maps is in fact an  $\mathbb{A}_{\mathbb{Q}_p}^+$ -basis of  $\mathbb{N}(T_f)$ .

**Theorem E** (Theorem 5.10). *For  $i = 1, 2$  and for each character  $\eta$  of  $\Delta$ , the image of  $H_{\text{Iw}}^1(\mathbb{Q}_p, T_f)^\eta$  under  $\underline{\text{Col}}_i^\eta$  is a submodule of finite index of the module*

$$\left( \prod_{j \in I_i^\eta} (X - \chi(\gamma)^j + 1) \right) \Lambda(\Gamma_1)$$

for some subset  $I_i^\eta \subset \{0, \dots, k - 2\}$ . Moreover, for each  $\eta$  the sets  $I_1^\eta$  and  $I_2^\eta$  are disjoint.

This theorem generalises [Kurihara and Pollack 2007, Proposition 1.2], which determines the images of  $(\underline{\text{Col}}_1^\Delta, \underline{\text{Col}}_2^\Delta)$  for elliptic curves with  $a_p = 0$ . As a consequence of Theorem E, we can rewrite Conjecture 1.1 as below, without making any technical assumptions.

**Theorem F.** For  $i = 1, 2$ , Conjecture 1.1 is equivalent to the assertion that for each  $\eta$  the characteristic ideal  $\text{Char}_{\Lambda_{\mathbb{Q}_p}(\Gamma_1)}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \text{Sel}_p^i(f/\mathbb{Q}_\infty)^{\eta, \vee})$  is generated by  $L_{p,i}^\eta / \prod_{j \in I_i^\eta} (X - \chi(\gamma)^j + 1)$  where  $I_i^\eta$  is as given by Theorem E.

Finally, we explain in Section 5C how it is possible to choose a basis in such a way that  $I_1^\eta = I_2^\eta = \emptyset$ , i.e., the modules  $\Lambda(\Gamma_1)/\text{Im}(\text{Col}_i^\eta)$  are pseudo-null for both  $i = 1$  and  $2$ .

**Remark 1.4.** The local results in this paper (Theorems A, B, C and D) hold with representations of  $\mathcal{G}_{\mathbb{Q}_p}$  replaced by representations of  $\mathcal{G}_F$  for an arbitrary finite unramified extension  $F/\mathbb{Q}_p$ , with essentially the same proofs. We have chosen to work over  $\mathbb{Q}_p$  for the sake of simplicity, since this is all that is needed for applications to modular forms.

In [Loeffler and Zerbes 2012], these methods are applied to the study of the “critical-slope”  $L$ -function attached to an ordinary modular form (corresponding to the non-unit Frobenius eigenvalue).

**1C. Setup and notation.**

**1C1. Fontaine rings.** We review the definitions of the Fontaine rings we use in this paper. Details can be found in [Berger 2004] or [Lei et al. 2010].

Throughout this paper,  $p$  is an odd prime. If  $K$  is a number field or a local field of characteristic 0, then  $G_K$  denotes its absolute Galois group and  $\mathbb{O}_K$  the ring of integers of  $K$ . We write  $\Gamma$  for the Galois group  $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ , which we identify with  $\mathbb{Z}_p^\times$  via the cyclotomic character  $\chi$ . Then  $\Gamma \cong \Delta \times \Gamma_1$ , where  $\Delta$  is of order  $p - 1$  and  $\Gamma_1 \cong \mathbb{Z}_p$ . We fix a topological generator  $\gamma$  of  $\Gamma_1$ .

We write  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  for the ring of power series  $f(\pi) \in \mathbb{Q}_p[[\pi]]$  such that  $f(X)$  converges everywhere on the open unit  $p$ -adic disc. Equip  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  with actions of  $\Gamma$  and a Frobenius operator  $\varphi$  by  $g \cdot \pi = (\pi + 1)^{\chi(g)} - 1$  and  $\varphi(\pi) = (\pi + 1)^p - 1$ . We can then define a left inverse  $\psi$  of  $\varphi$  satisfying

$$\varphi \circ \psi(f(\pi)) = \frac{1}{p} \sum_{\zeta^{p-1}} f(\zeta(1 + \pi) - 1).$$

Inside  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ , we have subrings  $\mathbb{A}_{\mathbb{Q}_p}^+ = \mathbb{Z}_p[[\pi]]$  and  $\mathbb{B}_{\mathbb{Q}_p}^+ = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{A}_{\mathbb{Q}_p}^+$ . Moreover, the actions of  $\varphi$ ,  $\psi$  and  $\Gamma$  preserve these subrings. Finally, we write  $t = \log(1 + \pi) \in \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  and  $q = \varphi(\pi)/\pi \in \mathbb{A}_{\mathbb{Q}_p}^+$ . A formal power series calculation shows that  $g(t) = \chi(g)t$  for  $g \in \Gamma$  and  $\varphi(t) = pt$ .

**1C2. Iwasawa algebras and power series.** Given a finite extension  $K$  of  $\mathbb{Q}_p$ , denote by  $\Lambda_{\mathbb{O}_K}(\Gamma)$  (respectively  $\Lambda_{\mathbb{O}_K}(\Gamma_1)$ ) the Iwasawa algebra  $\mathbb{Z}_p[[\Gamma]] \otimes_{\mathbb{Z}_p} \mathbb{O}_K$  (respectively  $\mathbb{Z}_p[[\Gamma_1]] \otimes_{\mathbb{Z}_p} \mathbb{O}_K$ ) over  $\mathbb{O}_K$ . We further write  $\Lambda_K(\Gamma) = \mathbb{Q} \otimes \Lambda_{\mathbb{O}_K}(\Gamma)$  and  $\Lambda_K(\Gamma_1) = \mathbb{Q} \otimes \Lambda_{\mathbb{O}_K}(\Gamma_1)$ . If  $M$  is a finitely generated torsion  $\Lambda_{\mathbb{O}_K}(\Gamma_1)$ -module, we write  $\text{Char}_{\Lambda_{\mathbb{O}_K}(\Gamma_1)}(M)$  for its characteristic ideal.

Let  $\mathcal{H}(\Gamma)$  be the space of distributions on  $\Gamma$  (the continuous dual of the space of locally analytic functions on  $\Gamma$ ), with the ring structure defined by convolution. We may identify this with the space of formal power series

$$\{f \in \mathbb{Q}_p[[\Delta]][[X]] : f \text{ converges everywhere on the open unit } p\text{-adic disc}\},$$

where  $X$  corresponds to  $\gamma - 1$ . We may identify  $\Lambda_{\mathbb{Q}_p}(\Gamma)$  with the subring of  $\mathcal{H}(\Gamma)$  consisting of power series with bounded coefficients.

The action of  $\Gamma$  on  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  gives an isomorphism of  $\mathcal{H}(\Gamma)$  with  $(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0}$ , the Mellin transform

$$\begin{aligned} \mathfrak{M} : \mathcal{H}(\Gamma) &\rightarrow (\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0} \\ f(\gamma - 1) &\mapsto f(\gamma - 1) \cdot (\pi + 1). \end{aligned}$$

In particular,  $\Lambda_{\mathbb{Z}_p}(\Gamma)$  corresponds to  $(\mathbb{A}_{\mathbb{Q}_p}^+)^{\psi=0}$  under  $\mathfrak{M}$ . Similarly, we define  $\mathcal{H}(\Gamma_1)$  as the subring of  $\mathcal{H}(\Gamma)$  defined by power series over  $\mathbb{Q}_p$ , rather than  $\mathbb{Q}_p[[\Delta]]$ . Then,  $\mathcal{H}(\Gamma_1)$  corresponds to  $(1 + \pi)\varphi(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)$  under  $\mathfrak{M}$ , and  $\Lambda_{\mathbb{Z}_p}(\Gamma_1)$  to  $(1 + \pi)\varphi(\mathbb{A}_{\mathbb{Q}_p}^+)$ . (See [Perrin-Riou 2001, B.2.8] for more details.)

If  $d$  is an integer and  $S$  is a  $\Lambda_K(\Gamma_1)$ -submodule of  $K \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma_1)^{\oplus d}$  which is free of rank  $d$ , we write  $\det(S)$  for the determinant of any basis of  $S$ , which is well-defined up to multiplication by a unit of  $\Lambda_K(\Gamma_1)$ . If  $F$  is a homomorphism of  $\Lambda_K(\Gamma_1)$ -modules whose image is a free rank  $d$   $\Lambda_K(\Gamma_1)$ -submodule of  $K \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma_1)^{\oplus d}$ , we write  $\det(F)$  for  $\det(\text{Im}(F))$ .

For an integer  $i$ , define

$$\left. \begin{aligned} \ell_i &= \frac{\log(1 + X)}{\log_p(\chi(\gamma))} - i \\ \delta_i &= \frac{\ell_i}{X + 1 - \chi(\gamma)^i} \end{aligned} \right\} \in \mathcal{H}(\Gamma_1).$$

Note that  $\ell_i$  is independent of the choice of generator  $\gamma$  (hence the choice of normalising factor), but  $\delta_i$  is not.

**Remark 1.5.** Note that for any positive integer  $k$ , we have

$$\mathfrak{n}_k = a_k \delta_{k-1} \dots \delta_0,$$

where  $a_k = \log(\chi(\gamma))^k \in \mathbb{Z}_p$  is nonzero.

The following result slightly refines [Berger 2003, Lemma II.2].

**Proposition 1.6.** *For any  $k \geq 0$ , we have*

$$\begin{aligned} \mathfrak{M}(\ell_{k-1} \dots \ell_0 \mathfrak{H}(\Gamma)) &= (t^k \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0} \\ \mathfrak{M}(\delta_{k-1} \dots \delta_0 \mathfrak{H}(\Gamma)) &= \left( \left( \frac{t}{\varphi(\pi)} \right)^k \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \right)^{\psi=0}. \end{aligned}$$

*Proof.* One checks easily that  $\ell_i$  acts on  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  as the differential operator

$$(1 + \pi)t \frac{d}{d\pi} - i,$$

and hence

$$\ell_j(t^j f) = t^{j+1} (1 + \pi) \frac{df}{d\pi}.$$

Since  $(1 + \pi) \frac{d}{d\pi}$  is an isomorphism on  $(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0}$  (it is the map on distributions dual to the map  $f(x) \mapsto xf(x)$  on functions), it follows that each  $\ell_j$  maps  $(t^j \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0}$  bijectively onto  $(t^{j+1} \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0}$ .

To prove a similar statement for the  $\delta_i$ , we note that

$$(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ / \varphi(\pi) \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0}$$

is isomorphic to  $\mathbb{Q}_p[\Delta]$  as a  $\Gamma$ -module. Since  $t$  is a uniformiser of the ideal  $\varphi(\pi)$ , we have

$$(\varphi(\pi)^j \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ / \varphi(\pi)^{j+1} \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0} = (t^j \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ / t^j \varphi(\pi) \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0} \cong \mathbb{Q}_p[\Delta](j)$$

as a  $\Gamma$ -module. Hence its annihilator is  $X + 1 - \chi(\gamma)^j$ . These factors are mutually coprime and coprime to  $\delta_0 \dots \delta_{k-1}$ , and the product is  $\ell_0 \dots \ell_{k-1}$ , so the result follows.  $\square$

**1C3. Isotypical components.** Let  $\eta : \Delta \rightarrow \mathbb{Z}_p^\times$  be a character. We write  $e_\eta = (p - 1)^{-1} \sum_{\sigma \in \Delta} \eta^{-1}(\sigma) \sigma$ . If  $M$  is a  $\Lambda_E(\Gamma)$ -module, its  $\eta$ -isotypical component is given by  $M^\eta = e_\eta M$ . When  $\eta = 1$ , we write  $M^\Delta$  in place of  $M^\eta$ .

We identify  $\Lambda_E(\Gamma_1)$  with the power series in  $X = \gamma - 1$  with bounded coefficients in  $E$ . Given

$$F = \sum_{\sigma \in \Delta, n \geq 0} a_{\sigma, n} \sigma (\gamma - 1)^n \in \Lambda(\Gamma),$$

we write  $F^\eta = e_\eta F$  for its image in  $\Lambda_E(\Gamma)^\eta$ . In particular,

$$F^\eta = e_\eta \sum_{n \geq 0} \left( \sum_{\sigma \in \Delta} a_{\sigma, n} \eta(\sigma) \right) (\gamma - 1)^n \in e_\eta \Lambda_E(\Gamma_1).$$

Therefore, we can identify  $F^\eta$  with a power series in  $X = \gamma - 1$ . Under this identification, the value  $F^\eta|_{X=\chi(\gamma)^j - 1}$  is given by  $\chi^j \chi_0^{-j} \eta(F)$  where  $\chi_0 = \chi|_\Delta$  for all  $j \in \mathbb{Z}$ .



**1C4. Crystalline representations.** Let  $E$  and  $F$  be finite extensions of  $\mathbb{Q}_p$ . Let  $V$  be a crystalline  $E$ -linear representation of  $G_{\mathbb{Q}_p}$ . We denote the Dieudonné module of  $V$  by  $\mathbb{D}_{\text{cris}}(V)$ . If  $j \in \mathbb{Z}$ ,  $\text{Fil}^j \mathbb{D}_{\text{cris}}(V)$  denotes the  $j$ th step in the de Rham filtration of  $\mathbb{D}_{\text{cris}}(V)$ . We say  $V$  is *positive* if  $\mathbb{D}_{\text{cris}}(V) = \text{Fil}^0 \mathbb{D}_{\text{cris}}(V)$  (following the standard, but unfortunate, convention that positive representations are precisely those with non-positive Hodge–Tate weights).

The  $(\varphi, \Gamma)$ -module of  $V$  is denoted by  $\mathbb{D}(V)$ . As shown by Fontaine (unpublished; for a reference see [Cherbonnier and Colmez 1999, Section II]), we have a canonical isomorphism of  $\Lambda_E(\Gamma)$ -modules

$$h_{\text{Iw}, V}^1 : \mathbb{D}(V)^{\psi=1} \rightarrow H_{\text{Iw}}^1(\mathbb{Q}_p, V).$$

We write  $\exp_{F, V} : F \otimes \mathbb{D}_{\text{cris}}(V) \rightarrow H^1(F, V)$  for the Bloch–Kato exponential over  $F$ .

For an integer  $j$ ,  $V(j)$  denotes the  $j$ th Tate twist of  $V$ , i.e.,  $V(j) = V \otimes E e_j$  where  $G_{\mathbb{Q}_p}$  acts on  $e_j$  via  $\chi^j$ . We have

$$\mathbb{D}_{\text{cris}}(V(j)) = t^{-j} \mathbb{D}_{\text{cris}}(V) \otimes e_j.$$

For any  $v \in \mathbb{D}_{\text{cris}}(V)$ ,  $v_j = t^{-j} v \otimes e_j$  denotes its image in  $\mathbb{D}_{\text{cris}}(V(j))$ .

If  $h \geq 1$  is an integer such that  $\text{Fil}^{-h} \mathbb{D}_{\text{cris}}(V) = \mathbb{D}_{\text{cris}}(V)$ , we write  $\Omega_{V, h}$  for the Perrin-Riou exponential as defined in [Perrin-Riou 1994].

Let  $T$  be an  $\mathbb{O}_E$ -lattice in  $V$  which is stable under  $G_{\mathbb{Q}_p}$ . We denote the Wach module of  $V$  (respectively  $T$ ) by  $\mathbb{N}(V)$  (respectively  $\mathbb{N}(T)$ ), a free module of rank  $d$  over  $\mathbb{B}_{\mathbb{Q}_p}^+$  (respectively  $\mathbb{A}_{\mathbb{Q}_p}^+$ ). Recall that  $\Gamma$  acts on both of these objects, and there is a map  $\varphi : \mathbb{N}(T)[\pi^{-1}] \rightarrow \mathbb{N}(T)[\varphi(\pi)^{-1}]$ , preserving  $\mathbb{N}(T)$  if  $T$  is positive (and similarly for  $V$ ).

For any  $j \in \mathbb{Z}$  we can identify  $\mathbb{N}(T(j))$  with  $\pi^{-j} \mathbb{N}(T) \otimes e_j$ , where  $e_j$  is as above. Given an  $R$ -module  $M$  with an action of  $\varphi$  and a submodule  $N$ ,  $\varphi^* N$  denotes the  $R$ -submodule of  $M$  generated by  $\varphi(N)$ , e.g.,  $\varphi^* \mathbb{N}(T)$  denotes the  $\mathbb{A}_{\mathbb{Q}_p}^+$ -submodule of  $\mathbb{N}(T)[\pi^{-1}]$  generated by  $\varphi(\mathbb{N}(T))$ . Finally, we write

$$\mathbb{N}_{\text{rig}}(V) = \mathbb{N}(V) \otimes_{\mathbb{B}_{\mathbb{Q}_p}^+} \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+.$$

The following lemma is implicit in the calculations of [Lei et al. 2010, §3], but for the convenience of the reader we give a separate proof:

**Lemma 1.7.** *If the Hodge–Tate weights of  $V$  are  $\geq 0$ , then we have*

$$\mathbb{N}(T) \subseteq \varphi^* \mathbb{N}(T)$$

and similarly for  $\mathbb{N}(V)$ .

*Proof.* It suffices to prove the result for  $T$ . Suppose that the Hodge–Tate weights of  $V$  are in  $[0, m]$ . Then  $\mathbb{N}(T) = \pi^{-m} \mathbb{N}(T(-m))$ . Since  $T(-m)$  is positive,  $\varphi$

preserves  $\mathbb{N}(T(-m))$  and  $\mathbb{N}(T(-m))/\varphi^*\mathbb{N}(T(-m))$  is killed by  $q^m$  [Berger 2004, proof of Theorem III.3.1]. Equivalently, we have

$$q^m \cdot \pi^m \mathbb{N}(T) \subseteq \varphi^*(\pi^m \mathbb{N}(T)) = \varphi(\pi)^m \varphi^* \mathbb{N}(T).$$

Since  $q = \varphi(\pi)/\pi$ , the result follows. □

**1C5. Refinements of crystalline representations.** Let  $V$  be an  $E$ -linear crystalline representation of  $G_{\mathbb{Q}_p}$  of dimension  $d$ , and let  $s_1 \leq \dots \leq s_d$  be the jumps in the filtration of  $\mathbb{D}_{\text{cris}}(V)$ , so the Hodge–Tate weights are  $-s_i$ . If  $Y$  is an  $E$ -linear subspace of  $\mathbb{D}_{\text{cris}}(V)$  of dimension  $e \leq d$ , we say  $Y$  is *in general position* (with respect to the Hodge filtration) if the intersections  $\text{Fil}^j Y = Y \cap \text{Fil}^j \mathbb{D}_{\text{cris}}(V)$  have the smallest possible dimension; that is,

$$\dim \text{Fil}^j Y = \begin{cases} \dim \text{Fil}^j \mathbb{D}_{\text{cris}}(V) - d + e & \text{if } \dim \text{Fil}^j V \geq d - e, \\ 0 & \text{otherwise.} \end{cases}$$

This is equivalent to the requirement that the jumps of the filtration  $\text{Fil}^j Y$  are  $s_1, \dots, s_e$ .

As in [Bellaïche and Chenevier 2009, §2.4.1], we define a *refinement* of  $V$  to be a family  $\underline{Y} = (Y_i)_{i=1}^d$  of  $E$ -linear subspaces of  $\mathbb{D}_{\text{cris}}(V)$  stable under  $\varphi$ , with  $0 \subsetneq Y_1 \subsetneq \dots \subsetneq Y_d = \mathbb{D}_{\text{cris}}(V)$ , so  $\dim_E Y_i = i$ . It is clear that refinements exist if and only if the eigenvalues of  $\varphi$  on  $\mathbb{D}_{\text{cris}}(V)$  lie in  $E$ .

We say that the refinement is *non-critical* if each of the subspaces  $Y_i$  is in general position, or equivalently if  $Y_i \cap \text{Fil}^{s_i+1} \mathbb{D}_{\text{cris}}(V) = 0$  for all  $i$ .

(If the Hodge–Tate weights of  $V$  are distinct, as Bellaïche and Chenevier assume, then this is equivalent to the assertion that  $\mathbb{D}_{\text{cris}}(V) = Y_i \oplus \text{Fil}^{s_i+1} \mathbb{D}_{\text{cris}}(V)$  for each  $i$ , which coincides with Definition 2.4.5 of [op. cit.]).

**Proposition 1.8.** *If the eigenvalues of Frobenius on  $\mathbb{D}_{\text{cris}}(V)$  lie in  $E$ , and either  $d = 2$  or  $\varphi$  acts semisimply on  $\mathbb{D}_{\text{cris}}(V)$ , then there exists a non-critical refinement of  $V$ .*

*Proof.* As noted in [Bellaïche and Chenevier 2009, Remark 2.4.6(iii)], the case where  $\varphi$  acts semisimply is obvious: any basis of eigenvectors of  $\mathbb{D}_{\text{cris}}(V)$  defines  $d!$  refinements, one for each ordering of the basis vectors, and it is easy to see that we can choose an ordering such that the resulting refinement is non-critical. Hence let us assume that  $V$  is 2-dimensional and  $\varphi$  acts non-semisimply on  $\mathbb{D}_{\text{cris}}(V)$ . Thus  $\mathbb{D}_{\text{cris}}(V)$  has a basis  $(e_1, e_2)$  such that  $\varphi(e_1) = \alpha e_1$  and  $\varphi(e_2) = e_1 + \alpha(e_2)$ , for some  $\alpha \in E^\times$ . By twisting, we may assume that the jumps in the Hodge filtration are 0 and  $s$  with  $s \geq 0$ . Let  $N$  be the valuation of  $\alpha$ ; the Newton and Hodge numbers of  $\mathbb{D}_{\text{cris}}(V)$  are  $t_H = s$  and  $t_N = 2N$ , so we have  $s = 2N$  by weak admissibility.

The unique possible refinement is given by  $Y_1 = Ee_1$ , and this is non-critical unless  $s > 0$  and  $\text{Fil}^1 \mathbb{D}_{\text{cris}}(V) = Y_1$ . If this is the case, then the Newton and Hodge

numbers of  $Y_1$  are respectively  $t_H(Y_1) = s$  and  $t_N(Y_1) = N$ , and since  $s = 2N > N$  this contradicts the weak admissibility of  $\mathbb{D}_{\text{cris}}(V)$ .  $\square$

**Remark 1.9.** (1) It is shown in [Milne 1994] that the Tate conjecture implies the semisimplicity of  $\varphi$  on the crystalline cohomology groups of any smooth projective variety over  $\mathbb{F}_p$  (or, more generally, on the crystalline realisation of any motive over  $\mathbb{F}_p$ ); so the hypotheses of the proposition conjecturally hold for all crystalline representations “arising from geometry”.

(2) For representations of dimension  $\geq 3$  with non-semisimple Frobenius there may be no non-critical refinements, as the following counterexample shows. Let  $D = \mathbb{Q}_p^3$  with its standard basis  $e_1, e_2, e_3$ , and let  $\varphi : D \rightarrow D$  be given by the matrix

$$\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix},$$

where  $\alpha \in \mathbb{Z}_p$  has valuation 1. We define a filtration on  $D$  with jumps  $\{0, 1, 2\}$  by  $\text{Fil}^0(D) = D$ ,  $\text{Fil}^1 D = \mathbb{Q}_p e_1 + \mathbb{Q}_p e_3$ ,  $\text{Fil}^2 D = \mathbb{Q}_p e_3$ ,  $\text{Fil}^3 D = 0$ . Then the only  $\varphi$ -stable submodules are  $Y_0 = 0$ ,  $Y_1 = \mathbb{Q}_p e_1$ , and  $Y_2 = \mathbb{Q}_p e_1 + \mathbb{Q}_p e_2$  and  $Y_3 = D$ . The Hodge and Newton numbers are given by

$i$	$t_H(Y_i)$	$t_N(Y_i)$
1	1	1
2	1	2
3	3	3

so  $D$  is a weakly admissible filtered  $\varphi$ -module; and the unique refinement of  $D$  is  $(Y_i)_{i=0,\dots,3}$ , but  $Y_1$  is not in general position.

**1C6. Modular forms.** Let  $f(z) = \sum a_n e^{2\pi i n z}$  be a normalised new eigenform of weight  $k \geq 2$ , level  $N$  and nebentypus  $\varepsilon$ . Write  $F_f = \mathbb{Q}(a_n : n \geq 1)$  for its coefficient field. Let

$$\tilde{f}(z) = \sum \bar{a}_n e^{2\pi i n z}$$

be the dual form to  $f$ , which also has coefficients in  $F_f$ . We assume that  $p \nmid N$  and  $a_p$  is not a  $p$ -adic unit, so  $f$  is supersingular at  $p$ .

**Remark 1.10.** We make this assumption in order to save ourselves from doing the same calculations twice in Section 5; they easily generalise to the ordinary case.

We fix a prime of  $F_f$  above  $p$ . We denote the completion of  $F_f$  at this prime by  $E$  and fix a uniformiser  $\varpi_E$ . We write  $V_f$  for the 2-dimensional  $E$ -linear representation of  $G_{\mathbb{Q}}$  associated to  $f$  from [Deligne 1971]. We fix an  $\mathbb{O}_E$ -lattice  $T_f$

stable under  $G_{\mathbb{Q}}$ , which determines a lattice  $T_{\bar{f}}$  of  $V_{\bar{f}}$ . When restricted to  $G_{\mathbb{Q}_p}$ ,  $V_f$  is crystalline and its de Rham filtration is given by

$$\dim_E \text{Fil}^i \mathbb{D}_{\text{cris}}(V_f) = \begin{cases} 2 & \text{if } i \leq 0, \\ 1 & \text{if } 1 \leq i \leq k-1, \\ 0 & \text{if } i \geq k. \end{cases}$$

The action of  $\varphi$  on  $\mathbb{D}_{\text{cris}}(V_f)$  satisfies  $\varphi^2 - a_p\varphi + \varepsilon(p)p^{k-1} = 0$ . Let us choose a “good basis”  $v_1, v_2$  of  $\mathbb{D}_{\text{cris}}(V_f)$  as in [Lei et al. 2010, §3.3]; that is,  $v_1$  spans  $\text{Fil}^1 \mathbb{D}_{\text{cris}}(V_f)$  and  $v_2 = p^{1-k}\varphi(v_1)$ . We also choose a basis  $\bar{v}_1, \bar{v}_2$  of  $\mathbb{D}_{\text{cris}}(V_{\bar{f}})$  in the same way. The isomorphism  $V_{\bar{f}} = V_f^*(1-k)$  gives a pairing  $\mathbb{D}_{\text{cris}}(V_f) \times \mathbb{D}_{\text{cris}}(V_{\bar{f}}) \rightarrow \mathbb{D}_{\text{cris}}(E(1-k)) = E \cdot t^{k-1}e_{1-k} \cong E$ . As noted in [Lei et al. 2010, §3.4], we have  $[v_1, \bar{v}_1] = [v_2, \bar{v}_2] = 0$  and  $[v_2, \bar{v}_1] = -[v_1, \bar{v}_2]$ , and (by scaling) we may assume without loss of generality that  $[v_1, \bar{v}_2] = 1$ .

Unless otherwise stated, we always assume that the eigenvalues of  $\varphi$  on  $\mathbb{D}_{\text{cris}}(V_f)$  are not integral powers of  $p$  and the nebentypus of  $f$  is trivial. Our assumption on the eigenvalues of  $\varphi$  allows us to define the Perrin-Riou pairing

$$\mathcal{L}_i = \mathcal{L}_{1, (1+\pi) \otimes v_{i,1}} : H_{\text{Iw}}^1(\mathbb{Q}_p, V_{\bar{f}}(k-1)) \rightarrow \mathcal{H}(\Gamma)$$

for  $i = 1, 2$  where we have identified  $V_f(1)^*(1)$  with  $V_{\bar{f}}(k-1)$  (see [Lei 2011, Section 3.2] or [Lei et al. 2010, Section 3.3] for details).

**1C7. Adequate rings and elementary divisors.** Let  $R$  be a commutative integral domain with identity, such that the following conditions hold:

- All finitely generated ideals in  $R$  are principal (i.e.,  $R$  is a Bézout domain).
- $R$  is *adequate*; i.e., for any  $a, b \in R$  with  $a \neq 0$ , we may write  $a = a_1a_2$ , where  $(a_1, b) = (1)$  and  $(d, b) \neq (1)$  for every non-unit divisor  $d$  of  $a_2$ .

Then  $R$  is an elementary divisor ring. That is, let  $M \subseteq N$  be finitely generated  $R$ -modules such that  $N \cong R^d$ . Then there exists a  $R$ -basis  $n_1, \dots, n_d$  of  $N$  and  $r_1, \dots, r_d \in R$  (unique up to units of  $R$ ) such that  $r_1 \mid \dots \mid r_d$  and  $r_1n_1, \dots, r_dn_e$ , where  $e$  is the largest integer such that  $r_e \neq 0$ , form a  $R$ -basis of  $M$ . In particular, we have  $\det(M) = r_1 \dots r_d$ . In this case, we write  $[N : M] = [N : M]_R = [r_1; \dots; r_d]$ . When  $d = 1$ , we simply write  $[N : M] = r_1$ .

If  $Q$  is an arbitrary finitely presented  $R$ -module, then we may write  $Q$  as a quotient  $N/M$  where  $N$  is a free module of finite rank and  $M$  is a finitely generated submodule of  $N$ , so the elementary divisors  $[N : M]_R$  are defined. It is easy to check that these are independent of the choice of presentation of  $Q$ , and we define these to be the elementary divisors of  $Q$ .

As explained in [Berger 2002, §4.2],  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  is an adequate Bézout domain and hence an elementary divisor ring. The same is true of  $E \otimes_{\mathbb{Q}_p} \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  for any finite

extension  $E$  of  $\mathbb{Q}_p$ , and of  $\mathcal{H}(\Gamma_1)$  (which is isomorphic to  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  as an abstract ring).

We will need the following lemma; see [Lang 2002, Lemma III.7.6].

**Lemma 1.11.** *Let  $R$  be an adequate Bézout domain,  $M$  a finitely presented  $R$ -module, and  $N$  a submodule of  $M$ . Suppose that there is some  $a \in R$  such that  $N \cong R/a$  and  $aM = 0$ . Then  $M \cong N \oplus M/N$ .*

*Proof.* Let  $q_1, \dots, q_r$  be a set of generators for  $M/N$ , with annihilators  $a_i$ , giving an isomorphism  $M/N \cong \bigoplus_{i=1}^r R/a_i$ . Since  $aM = 0$ , each  $a_i$  divides  $a$ . Let  $p_i$  be an arbitrary lift of  $q_i$ ; then  $a_i p_i \in N$ , so  $a_i p_i = b_i p_0$  where  $p_0$  is a generator of  $N$  and  $b_i \in R/aR$ . Since  $aM = 0$ , we have  $0 = (a/a_i)a_i p_i = (a/a_i)b_i p_0$ .

Then we must have  $(a/a_i)b_i \in aR$ , so  $ab_i \in aa_i R$ . Since  $R$  is an integral domain, we must have  $a_i \mid b_i$ , and we may write  $b_i = a_i c_i$ . Thus  $p'_i = p_i - c_i p_0$  is a lift of  $p_i$  such that  $a_i p'_i = a_i p_i - a_i c_i p_0 = a_i p_i - b_i p_0 = 0$ . It follows that the subgroup generated by the  $p'_i$  maps bijectively to  $M/N$ , giving the required splitting.  $\square$

A straightforward induction gives the following generalisation:

**Corollary 1.12.** *If  $M$  is an  $R$ -module with a filtration by submodules  $0 = M_0 \subseteq M_1 \subseteq \dots \subseteq M_d = M$ , and there are elements  $a_1, \dots, a_d \in R$  such that for each  $i = 1, \dots, d$  we have  $M_i/M_{i-1} \cong R/a_i$  and  $a_i M \subseteq M_{i-1}$ , then  $M \cong \bigoplus_{i=1}^d R/a_i$ .*

The ring  $\mathcal{H}(\Gamma)$  is not a domain; but it is equal to the direct sum of its subrings  $e_\eta \mathcal{H}(\Gamma)$ , where  $e_\eta$  is the idempotent in  $\mathbb{Q}_p[\Delta]$  corresponding to the character  $\eta : \Delta \rightarrow \mathbb{Q}_p^\times$  as above. Each of these subrings is isomorphic to  $\mathcal{H}(\Gamma_1)$ , and hence admits a theory of elementary divisors. If  $M$  is a submodule of  $\mathcal{H}(\Gamma)^{\oplus d}$ , we define the  $i$ th elementary divisor of  $M$  to be  $\sum_\eta e_\eta a_i^\eta$ , where  $a_i^\eta$  is the  $i$ th elementary divisor of the submodule  $M^\eta = e_\eta M \subseteq e_\eta \mathcal{H}(\Gamma)$  considered as a  $\mathcal{H}(\Gamma_1)$ -module. In practice we shall only apply this in situations where  $M$  has the form  $\mathbb{Q}_p[\Gamma] \otimes_{\mathbb{Q}_p} M'$  for an  $\mathcal{H}(\Gamma_1)$ -module  $M'$ , in which case the isotypical components  $M^\eta$  all have the same elementary divisors.

## 2. Refinements of crystalline representations and $\mathcal{H}(\Gamma)$ -structure

In this section, we will prove Theorem A. We will do this by working with a certain filtration of the module  $\mathbb{N}_{\text{rig}}(V)$ , which is a  $(\varphi, \Gamma)$ -module over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ ; the steps in this filtration are  $(\varphi, \Gamma)$ -modules over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ , but they are not necessarily of the form  $\mathbb{N}_{\text{rig}}(W)$  for any representation  $W$ , so we begin by systematically developing a theory of such modules. Our approach is very much influenced by the description of the theory of  $(\varphi, \Gamma)$ -modules over the Robba ring  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^\dagger$  given in [Bellaïche and Chenevier 2009, §2.2].

**2A. Some properties of  $(\varphi, \Gamma)$ -modules over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ .** We define a  $(\varphi, \Gamma)$ -module over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  to be a free  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -module  $\mathcal{N}$  of finite rank, endowed with semilinear commuting actions of  $\varphi$  and  $\Gamma$ , such that the quotient  $\mathcal{N}/\varphi^*(\mathcal{N})$  is annihilated by some power of  $q$  (where  $q = \varphi(\pi)/\pi$  as above). We define

$$\mathbb{D}_{\text{cris}}(\mathcal{N}) = \mathcal{N}^\Gamma.$$

We equip  $\mathbb{D}_{\text{cris}}(\mathcal{N})$  with the filtration defined by

$$\text{Fil}^i \mathbb{D}_{\text{cris}}(\mathcal{N}) = \{v \in \mathbb{D}_{\text{cris}}(\mathcal{N}) : \varphi(v) \in q^i \mathcal{N}\}.$$

Let  $K_n = \mathbb{Q}_p(\mu_{p^n})$  and  $K_\infty = \bigcup_n K_n$ . We define

$$\mathbb{D}_{\text{dR}}^{(n)}(\mathcal{N}) = (K_\infty \otimes_{K_n} K_n[[t]] \otimes_{\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+} \mathcal{N})^\Gamma,$$

where the tensor product is via the embedding  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \hookrightarrow K_n[[t]]$  arising from the fact that

$$K_n \cong \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ / \varphi^{n-1}(q)$$

and  $t$  is a uniformiser of the prime ideal  $\varphi^{n-1}(q)$ . We endow  $K_n[[t]]$  with the obvious semilinear action of  $\Gamma$ , for which this homomorphism is  $\Gamma$ -equivariant, and the  $t$ -adic filtration. Then  $\mathbb{D}_{\text{dR}}^{(n)}(\mathcal{N})$  is a filtered  $\mathbb{Q}_p$ -vector space, of dimension  $\leq d$  where  $d$  is the  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -rank of  $\mathcal{N}$  (since  $K_\infty((t))^\Gamma = \mathbb{Q}_p$  [Bellaïche and Chenevier 2009, §2.2.7]); the operator  $\varphi$  gives an isomorphism of filtered  $\mathbb{Q}_p$ -vector spaces

$$\mathbb{D}_{\text{dR}}^{(n)}(\mathcal{N}) \xrightarrow{\cong} \mathbb{D}_{\text{dR}}^{(n+1)}(\mathcal{N})$$

for each  $n$ , and an embedding of filtered  $\mathbb{Q}_p$ -vector spaces

$$\mathbb{D}_{\text{cris}}(\mathcal{N}) \hookrightarrow \mathbb{D}_{\text{dR}}^{(1)}(\mathcal{N}).$$

We say that  $\mathcal{N}$  is *crystalline* if  $\dim_{\mathbb{Q}_p} \mathbb{D}_{\text{cris}}(\mathcal{N}) = d$ , and we say it is *de Rham* if  $\dim_{\mathbb{Q}_p} \mathbb{D}_{\text{dR}}^{(n)}(\mathcal{N}) = d$  (for some, and hence all,  $n \geq 1$ ). If  $\mathcal{N}$  is de Rham, we define the *Hodge–Tate weights* of  $\mathcal{N}$  to be the integers  $r$  such that  $\text{Fil}^{-r} \mathbb{D}_{\text{dR}}^{(n)}(\mathcal{N}) \neq \text{Fil}^{1-r} \mathbb{D}_{\text{dR}}^{(n)}(\mathcal{N})$  (with multiplicities given by the size of the jump in dimension). Note that these are necessarily  $\leq 0$ , which is unfortunate but necessary for compatibility with the usual definition in the case of Galois representations.

Finally, we define  $\mathbb{D}_{\text{Sen}}^{(n)}(\mathcal{N}) = K_\infty \otimes_{K_n} \mathcal{N} / \varphi^{n-1}(q)\mathcal{N}$ . This is a  $K_\infty$ -vector space of dimension  $d$ , with a semilinear action of  $\Gamma$ . As above, the  $\varphi$  operator gives isomorphisms  $\mathbb{D}_{\text{Sen}}^{(n)}(\mathcal{N}) \rightarrow \mathbb{D}_{\text{Sen}}^{(n+1)}(\mathcal{N})$ , of  $K_\infty$ -vector spaces with semilinear  $\Gamma$ -action. (So both  $\mathbb{D}_{\text{Sen}}(\mathcal{N})$  and  $\mathbb{D}_{\text{dR}}(\mathcal{N})$  are independent of  $n$  as abstract objects; we retain the  $n$  in the notation when we are interested in the relation between these spaces and the original module  $\mathcal{N}$ .)

**Proposition 2.1.** *Let  $j \geq 0$ , and suppose  $\mathcal{N}$  is de Rham. Then there is an isomorphism of  $\mathbb{Q}_p$ -vector spaces*

$$\mathrm{Fil}^j \mathbb{D}_{\mathrm{dR}}(\mathcal{N}) / \mathrm{Fil}^{j+1} \mathbb{D}_{\mathrm{dR}}(\mathcal{N}) \xrightarrow{\cong} \mathbb{D}_{\mathrm{Sen}}(\mathcal{N})^{\Gamma=\chi^{-j}}.$$

*Proof.* Let us fix an  $n \geq 1$  and let  $\theta$  be the reduction map  $K_n[[t]] \rightarrow K_n$ . Then  $\theta$  induces a map

$$\mathbb{D}_{\mathrm{dR}}^{(n)}(\mathcal{N}) \rightarrow \mathbb{D}_{\mathrm{Sen}}^{(n)}(\mathcal{N})^{\Gamma}$$

with kernel  $\mathrm{Fil}^1 \mathbb{D}_{\mathrm{dR}}(\mathcal{N})$  and whose image is a  $\mathbb{Q}_p$ -linear subspace  $S_0 \subseteq \mathbb{D}_{\mathrm{Sen}}(\mathcal{N})^{\Gamma}$ . Similarly, we find that  $\theta \circ t^{-j}$  gives an injection

$$\mathrm{Fil}^j \mathbb{D}_{\mathrm{dR}}(\mathcal{N}) / \mathrm{Fil}^{j+1} \mathbb{D}_{\mathrm{dR}}(\mathcal{N}) \rightarrow \mathbb{D}_{\mathrm{Sen}}(\mathcal{N})^{\Gamma=\chi^{-j}},$$

whose image is a  $\mathbb{Q}_p$ -linear subspace  $S_j$ .

Since  $\bigoplus_{j=0}^{\infty} S_j$  has dimension  $d$ , it suffices to show that

$$\dim_{\mathbb{Q}_p} \bigoplus_{j=0}^{\infty} \mathbb{D}_{\mathrm{Sen}}(\mathcal{N})^{\Gamma=\chi^{-j}} \leq d.$$

This follows from the fact that it is a subspace of  $(K_{\infty}((t)) \otimes_{K_{\infty}} \mathbb{D}_{\mathrm{Sen}}(\mathcal{N}))^{\Gamma}$ , and (as remarked above)  $K_{\infty}((t))$  is a field, with  $K_{\infty}((t))^{\Gamma} = \mathbb{Q}_p$ .  $\square$

**Corollary 2.2.** *If  $\mathcal{N}$  is crystalline, then the map*

$$\mathbb{D}_{\mathrm{cris}}(\mathcal{N}) = \mathcal{N}^{\Gamma} \xrightarrow{\varphi^n} (\mathcal{N} / \varphi^{n-1}(q)^r \mathcal{N})^{\Gamma}$$

*is surjective for all  $r \geq 1$  and  $n \geq 1$ , with kernel  $\mathrm{Fil}^r \mathbb{D}_{\mathrm{cris}}(\mathcal{N})$ .*

*Proof.* Let us define  $\mathcal{N}^{(n)} = K_{\infty} \otimes_{K_n} K_n[[t]] \otimes_{\mathbb{B}_{\mathrm{rig}, \mathbb{Q}_p}^+} \mathcal{N}$ , so  $(\mathcal{N}^{(n)})^{\Gamma} = \mathbb{D}_{\mathrm{dR}}(\mathcal{N})$ . By hypothesis the map  $\varphi^n : \mathbb{D}_{\mathrm{cris}}(\mathcal{N}) \rightarrow \mathbb{D}_{\mathrm{dR}}^{(n)}(\mathcal{N})$  is an isomorphism of filtered vector spaces, and the filtration on  $\mathbb{D}_{\mathrm{dR}}(\mathcal{N})$  is defined by the  $t$ -adic filtration of  $\mathcal{N}^{(n)}$ , so it suffices to show that reduction modulo  $t^r$  gives a surjection

$$(\mathcal{N}^{(n)})^{\Gamma} \rightarrow (\mathcal{N}^{(n)} / t^r \mathcal{N}^{(n)})^{\Gamma}.$$

We show that for each  $j$ , the map  $(t^j \mathcal{N}^{(n)})^{\Gamma} \rightarrow (t^j \mathcal{N}^{(n)} / t^{j+1} \mathcal{N}^{(n)})^{\Gamma}$  is surjective. Multiplication by  $t^{-j}$  gives an isomorphism

$$(t^j \mathcal{N}^{(n)} / t^{j+1} \mathcal{N}^{(n)})^{\Gamma} \rightarrow (\mathcal{N}^{(n)} / t \mathcal{N}^{(n)})^{\Gamma=\chi^{-j}};$$

but  $\mathcal{N}^{(n)} / t \mathcal{N}^{(n)} = \mathbb{D}_{\mathrm{Sen}}^{(n)}(\mathcal{N})$ , and by the preceding proposition we know that  $\theta \circ t^{-j}$  gives an isomorphism from  $\mathrm{Fil}^j \mathbb{D}_{\mathrm{dR}}(\mathcal{N}) / \mathrm{Fil}^{j+1} \mathbb{D}_{\mathrm{dR}}(\mathcal{N})$  to  $\mathbb{D}_{\mathrm{Sen}}^{(n)}(\mathcal{N})^{\Gamma=\chi^{-j}}$ . So the map  $(\mathcal{N}^{(n)})^{\Gamma} \rightarrow (\mathcal{N}^{(n)} / t^r \mathcal{N}^{(n)})^{\Gamma}$  is a morphism of filtered vector spaces for which the associated map of graded modules is surjective. Since the domain and codomain

are finite-dimensional and their filtrations are separated, the original map is itself surjective.  $\square$

Let us write  $\mathcal{M} = \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \otimes_{\mathbb{Q}_p} \mathbb{D}_{\text{cris}}(\mathcal{N}) \subseteq \mathcal{N}$ .

**Proposition 2.3.** *If  $\mathcal{N}$  is crystalline and  $\Gamma$  acts trivially on  $\mathcal{N}/\pi\mathcal{N}$ , then the elementary divisors of  $\mathcal{N}/\mathcal{M}$  are*

$$\left(\frac{t}{\pi}\right)^{s_1}, \dots, \left(\frac{t}{\pi}\right)^{s_d},$$

where  $-s_1 \geq \dots \geq -s_d$  are the Hodge–Tate weights of  $\mathcal{N}$ .

*Proof.* This follows exactly as in [Berger 2004, Proposition III.2.1].  $\square$

**2B. Quotients of  $(\varphi, \Gamma)$ -modules.** We now let  $\mathcal{N}$  be a  $(\varphi, \Gamma)$ -module over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ , as above. We assume that  $\mathcal{N}$  is crystalline and  $\Gamma$  acts trivially on  $\mathcal{N}/\pi\mathcal{N}$ , and investigate the properties of a certain class of  $(\varphi, \Gamma)$ -modules obtained as quotients of  $\mathcal{N}$ . We continue to write  $\mathcal{M} = \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \otimes_{\mathbb{Q}_p} \mathbb{D}_{\text{cris}}(\mathcal{N}) \subseteq \mathcal{N}$ .

Let  $Y$  be a  $\varphi$ -stable  $E$ -linear subspace of  $\mathbb{D}_{\text{cris}}(\mathcal{N})$ . We set

$$\mathfrak{Y} = \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \otimes_{\mathbb{Q}_p} Y \subseteq \mathcal{M}.$$

and

$$\mathfrak{X} = \mathcal{N} \cap \mathfrak{Y} \left[ \left(\frac{t}{\pi}\right)^{-1} \right] = \left\{ x \in \mathcal{N} : \left(\frac{t}{\pi}\right)^m x \in \mathfrak{Y} \text{ for some } m \right\} \subseteq \mathcal{N}.$$

**Proposition 2.4.** *The spaces  $Y, \mathfrak{Y}, \mathfrak{X}$  have the following properties:*

- (a)  $\mathfrak{X}$  is a  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -submodule of  $\mathcal{N}$  stable under  $\varphi$  and  $\Gamma$ ;
- (b)  $\mathfrak{X} = \{x \in \mathcal{N} : ax \in \mathfrak{Y} \text{ for some nonzero } a \in \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+\}$  (the saturation of  $\mathfrak{Y}$ );
- (c)  $\mathfrak{X}$  is free of rank  $\dim_{\mathbb{Q}_p} Y$  as an  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -module;
- (d)  $Y = \mathfrak{X} \cap \mathbb{D}_{\text{cris}}(\mathcal{N})$  and  $\mathfrak{Y} = \mathfrak{X} \cap \mathcal{M}$ ;
- (e)  $\mathfrak{X}$  and  $\mathfrak{W} = \mathcal{N}/\mathfrak{X}$  are  $(\varphi, \Gamma)$ -modules over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ .

*Proof.* Part (a) is immediate from the definition.

For (b), suppose  $x \in \mathcal{N}$  and there is some nonzero  $a \in \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  such that  $ax \in \mathfrak{Y}$ . By Proposition 2.3, we can find  $m$  such that  $\left(\frac{t}{\pi}\right)^m x \in \mathcal{M}$ , and  $a \left(\frac{t}{\pi}\right)^m x \in \mathfrak{Y}$ . Since  $\mathfrak{Y}$  is clearly saturated in  $\mathcal{M}$ , we deduce that  $\left(\frac{t}{\pi}\right)^m x \in \mathfrak{Y}$ , and hence  $x \in \mathfrak{X}$  as required.

For part (c), we note that  $\mathfrak{X}$  is a closed submodule of  $\mathcal{N}$ , since it is the intersection of the closed submodules  $\left(\frac{t}{\pi}\right)^{-N} \mathfrak{Y}$  and  $\mathcal{N}$  of  $\left(\frac{t}{\pi}\right)^{-N} \mathcal{N}$ , for any sufficiently large  $N$ . (It suffices to take  $N$  larger than  $s_d$ , where  $-s_d$  is the lowest Hodge–Tate weight of  $\mathcal{N}$ .) Hence  $\mathfrak{X}$  is also a free module, of finite rank. As  $\mathfrak{X} \left[ \left(\frac{t}{\pi}\right)^{-1} \right]$  is clearly free of rank  $\dim_{\mathbb{Q}_p} Y$  as a  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \left[ \left(\frac{t}{\pi}\right)^{-1} \right]$ -module, the rank of  $\mathfrak{X}$  over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  must also be equal to  $\dim_{\mathbb{Q}_p} Y$ .

For part (d), it is clear that  $\mathfrak{Y} \subseteq \mathfrak{X} \cap \mathcal{M}$ ; and this inclusion is an equality, since  $\mathcal{M}/\mathfrak{Y}$  is torsion-free and  $\mathfrak{X}/\mathfrak{Y}$  is torsion. Since  $\mathfrak{Y} \cap \mathbb{D}_{\text{cris}}(\mathcal{N}) = Y$ , the statement follows.



For the final statement (e), since  $\mathcal{X}$  and  $\mathcal{W} = \mathcal{N}/\mathcal{X}$  are both free  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -modules with semilinear actions of  $\varphi$  and  $\Gamma$ , it suffices to check that the modules  $\mathcal{X}/\varphi^*\mathcal{X}$  and  ${}^{\circ}\mathcal{W}/\varphi^*{}^{\circ}\mathcal{W}$  are annihilated by a power of  $q$ . Since  $\mathcal{X}$  is saturated in  $\mathcal{N}$ , and  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  is an elementary divisor ring, we can find a  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -basis  $n_1, \dots, n_d$  of  $\mathcal{N}$  such that  $n_1, \dots, n_r$  is a basis of  $\mathcal{X}$  and the images of  $n_{r+1}, \dots, n_d$  are a basis of  ${}^{\circ}\mathcal{W}$ , where  $r = \dim_{\mathbb{Q}_p} Y$ . Since  $\mathcal{X}$  is  $\varphi$ -stable, the matrix of  $\varphi$  in this basis is of the form  $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ . Hence we have  $\det(\varphi^*\mathcal{N}) = \det(A)\det(C)$ . As  $\mathcal{N}/\varphi^*\mathcal{N}$  is annihilated by a power of  $q$ ,  $\det(\varphi^*\mathcal{N})$  is a power of  $q$ , and thus the same is true of  $\det(A)$  and  $\det(C)$ . Since  $A$  and  $C$  are the matrices of  $\varphi$  on  $\mathcal{X}$  and  ${}^{\circ}\mathcal{W}$  in the bases described above, the modules  $\mathcal{X}/\varphi^*\mathcal{X}$  and  ${}^{\circ}\mathcal{W}/\varphi^*{}^{\circ}\mathcal{W}$  are also annihilated by a power of  $q$ , as required.  $\square$

Let  $W = \mathbb{D}_{\text{cris}}(\mathcal{N})/Y$ , and (as above) let  ${}^{\circ}\mathcal{W} = \mathcal{N}/\mathcal{X}$ . The natural map  $W \hookrightarrow \mathbb{D}_{\text{cris}}({}^{\circ}\mathcal{W})$  is injective, by part (d) of the preceding proposition; hence it is also surjective, for reasons of dimension. Thus  ${}^{\circ}\mathcal{W}$  is a crystalline  $(\varphi, \Gamma)$ -module and  $\mathbb{D}_{\text{cris}}({}^{\circ}\mathcal{W}) = W$ .

**Proposition 2.5.** *The quotient filtration  $\text{Fil}^\bullet W$  induced on  $W$  by the filtration of  $\mathbb{D}_{\text{cris}}(\mathcal{N})$  agrees with the filtration  $\underline{\text{Fil}}$  given by*

$$\underline{\text{Fil}}^r W = \{w \in W : \varphi(w) \in q^r {}^{\circ}\mathcal{W}\}.$$

*Proof.* It is clear from the definition that  $\text{Fil}^r W \subseteq \underline{\text{Fil}}^r W$ .

Conversely, let  $y \in \mathbb{D}_{\text{cris}}(\mathcal{N})$  such that  $[y] \in \underline{\text{Fil}}^r W$ , so we can write  $\varphi(y) = q^r y' + z$  for some  $y' \in \mathcal{N}$  and  $z \in \mathcal{X}$ . Then

$$z \bmod q^r \mathcal{X} \in (\mathcal{X}/q^r \mathcal{X})^\Gamma.$$

Applying Corollary 2.2 to  $\mathcal{X}$ , we find that  $z$  is congruent modulo  $q^r$  to an element of  $\mathcal{X}^\Gamma = Y$ .  $\square$

The final result we will need about these quotients is the following slightly fiddly lemma. Let us suppose that the jumps in the filtration of  $\mathbb{D}_{\text{cris}}(\mathcal{N})$ , with multiplicity, are  $s_1 \leq s_2 \leq \dots \leq s_d$  (i.e., the Hodge–Tate weights of  $\mathcal{N}$  are  $-s_i$ ). We say that the  $\varphi$ -stable subspace  $Y$  is *in general position* (with respect to the Hodge filtration of  $\mathbb{D}_{\text{cris}}(\mathcal{N})$ ) if the jumps in the filtration  $\text{Fil}^\bullet Y$  are  $s_1, \dots, s_j$ , where  $j = \dim_{\mathbb{Q}_p} Y$ .

**Lemma 2.6.** *If  $Y$  is in general position, then for any  $m \geq s_d$ , we have*

$$\left(\frac{t}{\pi}\right)^{m-s_{(j+1)}} \mathcal{M} \subseteq \left(\frac{t}{\pi}\right)^m \mathcal{N} + \mathfrak{y}.$$

*Proof.* As remarked above, the quotient module  ${}^{\circ}\mathcal{W} = \mathcal{N}/\mathcal{X}$  is a crystalline  $(\varphi, \Gamma)$ -module over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  of rank  $d - j$ , with  $\Gamma$  acting trivially modulo  $\pi$ . By Proposition 2.5, the Hodge–Tate weights of  ${}^{\circ}\mathcal{W}$  are exactly  $\{-s_{(j+1)}, \dots, -s_d\}$ ; hence its  $\Gamma$ -invariants lie in  $\left(\frac{t}{\pi}\right)^{s_{(j+1)}} {}^{\circ}\mathcal{W}$ . This is equivalent to  $\mathcal{M} \subseteq \left(\frac{t}{\pi}\right)^{s_{(j+1)}} \mathcal{N} + \mathcal{X}$ . Multiplying

by  $(\frac{t}{\pi})^{m-s(j+1)}$ , we see that

$$\left(\frac{t}{\pi}\right)^{m-s(j+1)} \mathcal{M} \subseteq \left(\frac{t}{\pi}\right)^m \mathcal{N} + \left(\frac{t}{\pi}\right)^{m-s(j+1)} \mathcal{X}.$$

Since both  $(\frac{t}{\pi})^{m-s(j+1)} \mathcal{M}$  and  $(\frac{t}{\pi})^m \mathcal{N}$  are manifestly contained in  $\mathcal{M}$ , we may replace the last term with its intersection with  $\mathcal{M}$ , which is clearly contained in  $\mathcal{X} \cap \mathcal{M} = \mathcal{Y}$ . □

**2C. Application to crystalline representations.** Let  $V$  be a  $d$ -dimensional crystalline representation of  $G_{\mathbb{Q}_p}$  with Hodge–Tate weights  $\{-s_1, \dots, -s_d\}$ , where  $0 \leq s_1 \leq \dots \leq s_d$  (so  $V$  is positive in the sense of Section 1C4 above). As above, we define  $\mathbb{N}_{\text{rig}}(V) = \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \otimes_{\mathbb{B}_{\mathbb{Q}_p}^+} \mathbb{N}(V)$ , where  $\mathbb{N}(V)$  is the Wach module of  $V$  as constructed in [Berger 2004]. Then  $\mathbb{N}_{\text{rig}}(V)$  is a crystalline  $(\varphi, \Gamma)$ -module over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  with  $\Gamma$  acting trivially modulo  $\pi$ , and  $\mathbb{D}_{\text{cris}}(V)$  is isomorphic (as a filtered  $\varphi$ -module over  $\mathbb{Q}_p$ ) to  $\mathbb{D}_{\text{cris}}(\mathbb{N}_{\text{rig}}(V))$  as defined in the previous section [Berger 2004, Theorems II.2.2 and III.4.4].

If  $V$  is in fact an  $E$ -linear representation, for  $E$  some finite extension of  $\mathbb{Q}_p$ , then  $\mathbb{N}_{\text{rig}}(V)$  is naturally an  $E \otimes_{\mathbb{Q}_p} \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -module, and  $\mathbb{D}_{\text{cris}}(V)$  is a filtered  $E$ -vector space. If we choose an  $E$ -linear  $\varphi$ -stable subspace, then all of the above constructions commute with the additional  $E$ -linear structure.

We shall suppose that  $V$  admits a non-critical refinement, and fix a choice of such a refinement  $\underline{Y}$ . Applying the above theory to each of the subspaces  $Y_i$ , we obtain  $E \otimes_{\mathbb{Q}_p} \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -submodules  $\mathcal{Y}_i = \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \otimes_{\mathbb{Q}_p} Y_i \subseteq \mathcal{M}$  and  $\mathcal{X}_i = \mathcal{Y}_i^{\text{sat}}$  of  $\mathbb{N}_{\text{rig}}(V)$ .

Let us consider the representation  $V(m)$ , for some  $m \geq s_d$ . This has non-negative Hodge–Tate weights  $\{m - s_i\}_{i=1, \dots, d}$ . If  $e_m$  denotes a basis of  $\mathbb{Q}_p(m)$ , then we have

$$\begin{aligned} \mathbb{D}_{\text{cris}}(V(m)) &= \{t^{-m}x \otimes e_m : x \in \mathbb{D}_{\text{cris}}(V)\}, \\ \mathbb{N}_{\text{rig}}(V(m)) &= \{\pi^{-m}y \otimes e_m : y \in \mathbb{N}_{\text{rig}}(V)\}. \end{aligned}$$

We define  $\mathcal{A}_i = \{\pi^{-m}y \otimes e_m : y \in \mathcal{X}_i\}$  and  $\mathcal{B}_i = \{t^{-m}x \otimes e_m : x \in \mathcal{Y}_i\}$ .

**Proposition 2.7.** *For each  $i = 1, \dots, d$ ,*

- (a)  $(\frac{t}{\pi})^{m-s_i} \mathcal{B}_i \supseteq \mathcal{A}_i \supseteq (\frac{t}{\pi})^{m-s_1} \mathcal{B}_i$ ;
- (b)  $\mathcal{B}_i$  is the saturation of  $\mathcal{A}_i$  in  $\mathcal{B}_d = \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \otimes \mathbb{D}_{\text{cris}}(V(m))$ ;
- (c) The inclusion  $\mathcal{A}_d \hookrightarrow \mathcal{B}_d$  identifies  $\mathcal{A}_d/\mathcal{A}_{i-1}$  with a submodule of  $\mathcal{B}_d/\mathcal{B}_{i-1}$  and the quotient is annihilated by  $(\frac{t}{\pi})^{m-s_i}$ .

*Proof.* The chain of inclusions in (a) is equivalent to  $(\frac{t}{\pi})^{s_1} \mathcal{X}_i \supseteq \mathcal{Y}_i \supseteq (\frac{t}{\pi})^{s_i} \mathcal{X}_i$ , and this is a consequence of Proposition 2.3 since the Hodge–Tate weights of  $\mathcal{X}_i$  are  $\{-s_1, \dots, -s_i\}$ . Moreover,  $\mathcal{B}_i$  is manifestly saturated in  $\mathcal{B}_d$  (being the base extension of a subspace of  $\mathbb{D}_{\text{cris}}(V(m))$ ), and together with (a), this proves (b). For

part (c), we note that  $\mathcal{A}_d \cap \mathcal{B}_{i-1} = \mathcal{A}_{i-1}$ , so the given map is well-defined and injective; to show that the annihilator is as claimed, we must check that

$$\left(\frac{t}{\pi}\right)^{m-s_i} \mathcal{B}_d \subseteq \mathcal{B}_{i-1} + \mathcal{A}_d,$$

which is equivalent to Lemma 2.6. □

We now pass from the “additive” to the “multiplicative” situation. Let us define  $\tilde{\mathcal{A}}_i = \bigoplus_{s=1}^{p-1} (1+\pi)^s \varphi(\mathcal{A}_i)$ , and similarly for  $\tilde{\mathcal{B}}_i$ . Note that these are  $\Gamma$ -stable, since  $\Gamma$  and  $\varphi$  commute. Moreover, the action of  $\Gamma$  on  $\tilde{\mathcal{B}}_d$  clearly extends to an action of the ring  $\mathcal{H}(\Gamma)$ , which is continuous with respect to the Fréchet topologies of  $\mathcal{H}(\Gamma)$  and  $\tilde{\mathcal{B}}_d$ . As the submodules  $\tilde{\mathcal{B}}_i$  and  $\tilde{\mathcal{A}}_i$  are all clearly closed and  $\Gamma$ -invariant, they also inherit a Fréchet topology and a continuous action of  $\mathcal{H}(\Gamma)$ .

**Remark 2.8.** Note that we can define an operator  $\psi : \mathcal{B}_d \rightarrow \mathcal{B}_d$  which is  $\varphi^{-1}$  on  $\mathbb{D}_{\text{cris}}(V)$  and is  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -semilinear (for the usual definition of  $\psi$  acting on  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ ). Then  $\tilde{\mathcal{A}}_i = (\varphi^* \mathcal{A}_i)^{\psi=0}$ , where  $\varphi^* \mathcal{A}_i$  is the  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -submodule of  $\mathcal{B}_i$  generated by  $\varphi(\mathcal{A}_i)$ . Clearly we have  $\varphi^*(\mathcal{B}_i) = \mathcal{B}_i$  for all  $i$ , and  $\tilde{\mathcal{B}}_i = (\varphi^* \mathcal{B}_i)^{\psi=0} = \mathcal{B}_i^{\psi=0}$ .

**Lemma 2.9.** *For each  $i = 1, \dots, d$ , these spaces have the following properties:*

- (a)  $\tilde{\mathcal{A}}_i \subseteq \tilde{\mathcal{B}}_i$ .
- (b)  $\tilde{\mathcal{A}}_d \cap \tilde{\mathcal{B}}_i = \tilde{\mathcal{A}}_i$ .
- (c) *The quotient  $\tilde{\mathcal{B}}_d / (\tilde{\mathcal{B}}_{i-1} + \tilde{\mathcal{A}}_d)$  is annihilated by  $\mathfrak{n}_{m-s_i}$ .*
- (d) *The quotient  $\tilde{\mathcal{B}}_i / (\tilde{\mathcal{B}}_{i-1} + \tilde{\mathcal{A}}_i)$  is cyclic as a  $\mathcal{H}(\Gamma)$ -module; it is generated by  $(1+\pi)\varphi(v_i)$ , and its annihilator is  $\mathfrak{n}_{m-s_i}$ .*

*Proof.* Parts (a) and (b) are clear from the corresponding statements for the spaces  $\mathcal{A}_i$  and  $\mathcal{B}_i$ . For part (c), we note that  $\mathcal{B}_d / \mathcal{B}_{i-1}$  is isomorphic as a  $(\varphi, \Gamma)$ -module over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  to the tensor product

$$\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \otimes_{\mathbb{Q}_p} (Y_d / Y_{i-1})$$

with  $\Gamma$  acting trivially on the latter factor and the  $\varphi$ -action multiplied by  $p^{-m}$ . By Proposition 1.6, we have

$$\mathfrak{n}_k \cdot (\mathcal{B}_d / \mathcal{B}_{i-1})^{\psi=0} = \left( \left( \frac{t}{\varphi(\pi)} \right)^k \mathcal{B}_d / \mathcal{B}_{i-1} \right)^{\psi=0}. \tag{*}$$

Since  $\mathcal{B}_d / (\mathcal{B}_{i-1} + \mathcal{A}_d)$  is annihilated by  $\left(\frac{t}{\pi}\right)^{m-s_i}$ , we deduce that  $\mathcal{B}_d / (\mathcal{B}_{i-1} + \varphi^* \mathcal{A}_d)$  is annihilated by

$$\left( \frac{t}{\varphi(\pi)} \right)^{m-s_i}.$$

Hence, by (\*),  $\tilde{\mathcal{B}}_d / (\tilde{\mathcal{B}}_{i-1} + \tilde{\mathcal{A}}_d)$  is annihilated by the ideal  $\mathfrak{n}_{m-s_i}$  of  $\mathcal{H}(\Gamma_1)$ .

Similarly,  $\mathcal{B}_i/(\mathcal{B}_{i-1} + \mathcal{A}_i)$  has the single elementary divisor

$$\left(\frac{t}{\pi}\right)^{m-s_i}$$

(by applying Proposition 2.3 to  $\mathcal{X}_i/\mathcal{X}_{i-1}$ , which is a  $(\varphi, \Gamma)$ -module over  $\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$  by Proposition 2.4(e)). Hence we deduce that  $\mathfrak{n}_{m-s_i}$  is the exact annihilator of the corresponding  $\mathcal{H}(\Gamma)$ -module  $\tilde{\mathcal{B}}_i/(\tilde{\mathcal{B}}_{i-1} + \tilde{\mathcal{A}}_i)$ .  $\square$

We are now in a position to complete the proof of Theorem A.

**Theorem 2.10** (Theorem A). *Let  $W$  be any  $E$ -linear crystalline representation of  $G_{\mathbb{Q}_p}$  with non-negative Hodge–Tate weights  $r_1 \leq \dots \leq r_d$ . Suppose that there exists a finite extension  $F$  of  $E$  such that  $V \otimes_E F$  admits a non-critical refinement. Then the  $E \otimes \mathcal{H}(\Gamma)$ -elementary divisors of the quotient*

$$(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0} \otimes \mathbb{D}_{\text{cris}}(W)/(\varphi^* \mathbb{N}_{\text{rig}}(W))^{\psi=0}$$

are  $[\mathfrak{n}_{r_1}; \dots; \mathfrak{n}_{r_d}]$ .

*Proof.* Let us choose an  $m$  such that  $V = W(-m)$  is positive. Then the Hodge–Tate weights of  $V$  are  $-s_1 \geq \dots \geq -s_d$ , where  $s_i = m - r_{d+1-i} \geq 0$ . Suppose first that  $V$  admits a non-critical refinement. Choosing such a refinement, we may argue as above to deduce that the  $E \otimes \mathcal{H}(\Gamma)$ -module

$$M = (\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0} \otimes \mathbb{D}_{\text{cris}}(W)/(\varphi^* \mathbb{N}_{\text{rig}}(W))^{\psi=0} = \mathcal{B}_d/\mathcal{A}_d$$

has a filtration by  $E \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma)$ -modules  $M_i = \mathcal{B}_i/\mathcal{A}_i$  where  $M_i/M_{i-1}$  is cyclic with annihilator  $\mathfrak{n}_{m-s_i}$ , and  $\mathfrak{n}_{m-s_i}$  annihilates  $M/M_{i-1}$ . So for each character  $\eta$  of  $\Delta$ , the module  $M^\eta$  is an  $\mathcal{H}(\Gamma_1)$ -module of the type covered by Corollary 1.12. This gives the result in this special case.

If  $V$  only admits a non-critical refinement after extending scalars to an extension  $F/E$ , then we may consider the representation  $V \otimes_E F$  and apply the above argument to this representation. It is clear that if  $M$  is any  $E \otimes \mathcal{H}(\Gamma)$ -module, then the elementary divisors of  $F \otimes_E M$  as a  $F \otimes \mathcal{H}(\Gamma)$ -module are the base extensions of the elementary divisors of  $M$ ; by uniqueness, this gives the proposition.  $\square$

We now briefly explain how  $\varphi^* \mathbb{N}_{\text{rig}}(V)$  is related to the Wach module  $\mathbb{N}(V)$  considered in our earlier work. Note that  $\mathcal{H}(\Gamma)$  and  $\varphi(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)$  are both Fréchet–Stein algebras in the sense of [Schneider and Teitelbaum 2003] (by Theorem 5.1 of that reference); hence any finite-rank free module over either one of these algebras has a canonical topology, and a submodule of such a module is finitely generated if and only if it is closed in this topology (Corollary 3.4(ii) of [op. cit.]). Moreover,  $(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0} = \bigoplus_{i=1}^{p-1} (1 + \pi)^i \varphi(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)$  is a free module over  $\varphi(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)$  of rank  $p - 1$ .

**Proposition 2.11.** *There is an isomorphism*

$$(\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0} \cong \mathcal{H}(\Gamma) \otimes_{\Lambda_{\mathbb{Q}_p}(\Gamma)} (\varphi^*\mathbb{N}(V))^{\psi=0}.$$

*Proof.* We first note that  $(\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0} = \bigoplus_{i=1}^{p-1} (1 + \pi)^i \varphi(\mathbb{N}_{\text{rig}}(V))$  is a finitely generated  $\varphi(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)$ -submodule of  $\mathbb{D}_{\text{cris}}(V) \otimes_{\mathbb{Q}_p} (\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0}$ . Hence it is closed in the canonical Fréchet topology of the latter space. It is also  $\Gamma$ -stable. Since the Mellin transform is a topological isomorphism between  $(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0}$  and  $\mathcal{H}(\Gamma)$ , we see that  $(\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0}$  is a closed  $\Gamma$ -stable subspace of a finite-rank free  $\mathcal{H}(\Gamma)$ -module; hence the action of  $\Gamma$  extends to a (continuous) action of  $\mathcal{H}(\Gamma)$ . So there is a natural embedding of  $\mathcal{H}(\Gamma) \otimes_{\Lambda_{\mathbb{Q}_p}(\Gamma)} (\varphi^*\mathbb{N}(V))^{\psi=0}$  into  $(\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0}$ .

The image of this embedding is a  $\mathcal{H}(\Gamma)$ -submodule, which is finitely generated, since  $(\varphi^*\mathbb{N}(V))^{\psi=0}$  is finitely generated as a  $\Lambda_E$ -module [Lei et al. 2010, Theorem 3.5]. So it is closed. On the other hand, the image contains  $(\varphi^*\mathbb{N}(V))^{\psi=0}$ . Since we evidently have

$$(\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0} = \bigoplus_{i=1}^{p-1} (1 + \pi)^i \varphi(\mathbb{N}_{\text{rig}}(V))$$

and  $\varphi(\mathbb{N}_{\text{rig}}(V)) = \varphi(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+) \otimes_{\varphi(\mathbb{B}_{\mathbb{Q}_p}^+)} \varphi(\mathbb{N}(V))$ , it follows that

$$\begin{aligned} (\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0} &= \varphi(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+) \otimes_{\varphi(\mathbb{B}_{\mathbb{Q}_p}^+)} \left( \bigoplus_{i=1}^{p-1} (1 + \pi)^i \varphi(\mathbb{N}(V)) \right) \\ &= \varphi(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+) \otimes_{\varphi(\mathbb{B}_{\mathbb{Q}_p}^+)} (\varphi^*\mathbb{N}(V))^{\psi=0}. \end{aligned}$$

Since  $\varphi(\mathbb{B}_{\mathbb{Q}_p}^+)$  is dense in  $\varphi(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)$ , it follows now that  $(\varphi^*\mathbb{N}(V))^{\psi=0}$  is dense in  $(\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0}$ . Thus the image of  $\mathcal{H}(\Gamma) \otimes_{\Lambda_{\mathbb{Q}_p}(\Gamma)} (\varphi^*\mathbb{N}(V))^{\psi=0}$  in  $(\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0}$  is both dense and closed; hence it is everything.  $\square$

We recall the following result from our previous work:

**Theorem 2.12** ([Lei et al. 2010, Lemma 3.15]).  *$(\varphi^*\mathbb{N}(V))^{\psi=0}$  is a free  $\Lambda_E(\Gamma)$ -module of rank  $d$ . More specifically, for any basis  $v_1, \dots, v_d$  of  $\mathbb{D}_{\text{cris}}(V)$ , there exists a  $E \otimes \mathbb{B}_{\mathbb{Q}_p}^+$ -basis  $n_1, \dots, n_d$  of  $\mathbb{N}(V)$  such that  $n_i = v_i \bmod \pi$  and  $(1 + \pi)\varphi(n_1), \dots, (1 + \pi)\varphi(n_d)$  form a  $\Lambda_E(\Gamma)$ -basis of  $(\varphi^*\mathbb{N}(V))^{\psi=0}$ .*

Combining this with Proposition 2.11, the following corollary is immediate:

**Corollary 2.13.**  *$(\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0}$  is a free  $E \otimes \mathcal{H}(\Gamma)$ -module of rank  $d$ . More specifically, for any basis  $v_1, \dots, v_d$  of  $\mathbb{D}_{\text{cris}}(V)$ , there exists a  $E \otimes \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -basis  $n_1, \dots, n_d$  of  $\mathbb{N}_{\text{rig}}(V)$  such that  $n_i = v_i \bmod \pi$  and  $(1 + \pi)\varphi(n_1), \dots, (1 + \pi)\varphi(n_d)$  form a  $E \otimes \mathcal{H}(\Gamma)$ -basis of  $(\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0}$ .*

**Remark 2.14.** We conjecture that for any  $E \otimes \mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+$ -basis  $m_1, \dots, m_d$  of  $\mathbb{N}_{\text{rig}}(V)$ , the vectors  $(1 + \pi)\varphi(m_i)$  are a  $E \otimes \mathcal{H}(\Gamma)$ -basis of  $(\varphi^*\mathbb{N}_{\text{rig}}(V))^{\psi=0}$ , and similarly for  $\mathbb{N}(V)$ ; but we do not know a proof of this statement.

### 3. The construction of Coleman maps

**3A. Coleman maps and the Perrin-Riou  $p$ -adic regulator.** Let  $E$  be a finite extension of  $\mathbb{Q}_p$ . Let  $V$  be a  $d$ -dimensional  $E$ -linear representation of  $G_{\mathbb{Q}_p}$  with non-negative Hodge–Tate weights  $r_1 \leq r_2 \leq \dots \leq r_d$ . We assume that  $V$  has no quotient isomorphic to the trivial representation. Let  $T$  be a  $\mathcal{G}_{\mathbb{Q}_p}$ -stable  $\mathbb{O}_E$ -lattice in  $V$ . Under these assumptions, there is a canonical isomorphism of  $\Lambda_{\mathbb{O}_E}(\Gamma)$ -modules

$$h_{1w}^1 : \mathbb{N}(T)^{\psi=1} \xrightarrow{\cong} H_{1w}^1(\mathbb{Q}_p, T).$$

by [Berger 2003, Theorem A.3]. Moreover, since the Hodge–Tate weights of  $V$  are non-negative, we have  $\mathbb{N}(T) \subseteq \varphi^*\mathbb{N}(T)$  by Lemma 1.7. Hence there is a well-defined map  $1 - \varphi : \mathbb{N}(T) \rightarrow \varphi^*\mathbb{N}(T)$ , which maps  $\mathbb{N}(T)^{\psi=1}$  to  $(\varphi^*\mathbb{N}(T))^{\psi=0}$ .

As we recalled above, [Lei et al. 2010, Theorem 3.5] (due to Laurent Berger) shows that for some basis  $n_1, \dots, n_d$  of  $\mathbb{N}(T)$  as an  $\mathbb{O}_E \otimes \mathbb{A}_{\mathbb{Q}_p}^+$ -module, the vectors  $(1 + \pi)\varphi(n_1), \dots, (1 + \pi)\varphi(n_d)$  form a basis of  $(\varphi^*\mathbb{N}(T))^{\psi=0}$  as a  $\Lambda_{\mathbb{O}_E}(\Gamma)$ -module. This basis gives an isomorphism

$$\mathfrak{J} : (\varphi^*\mathbb{N}(T))^{\psi=0} \xrightarrow{\cong} \Lambda_{\mathbb{O}_E}(\Gamma)^{\oplus d}$$

(the *Iwasawa transform*), and we define the Coleman map

$$\text{Col} = (\text{Col}_i)_{i=1}^d : \mathbb{N}(T)^{\psi=1} \rightarrow \Lambda_{\mathbb{O}_E}(\Gamma)^{\oplus d}$$

as the composition  $\mathfrak{J} \circ (1 - \varphi)$ .

**Remark 3.1.** This direct definition of the Coleman map is equivalent to that given in our earlier work, but applies to any representation with non-negative Hodge–Tate weights, rather than starting with a positive representation and twisting by the sum of its Hodge–Tate weights as in [Lei et al. 2010].

Let  $v_1, \dots, v_d$  be a basis of  $\mathbb{D}_{\text{cris}}(V)$ , so  $(1 + \pi) \otimes v_1, \dots, (1 + \pi) \otimes v_d$  are a basis of  $(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+)^{\psi=0} \otimes \mathbb{D}_{\text{cris}}(V)$  as an  $\mathcal{H}(\Gamma)$ -module; and let  $n_1, \dots, n_d$  be a basis of  $\mathbb{N}(V)$  lifting  $v_1, \dots, v_d$  as in Theorem 2.12. Then there exists a unique  $d \times d$  matrix  $\underline{M}$  with entries in  $\mathcal{H}(\Gamma)$  such that

$$\begin{pmatrix} (1 + \pi)\varphi(n_1) \\ \vdots \\ (1 + \pi)\varphi(n_d) \end{pmatrix} = \underline{M} \cdot \begin{pmatrix} (1 + \pi) \otimes v_1 \\ \vdots \\ (1 + \pi) \otimes v_d \end{pmatrix}. \tag{1}$$

In fact  $\underline{M}$  is defined over  $\mathcal{H}(\Gamma_1)$ , since the  $n_i$  lie in  $(1 + \pi)\varphi(\mathbb{N}(V)) \subseteq (1 + \pi)\varphi(\mathbb{B}_{\text{rig}, \mathbb{Q}_p}^+ \otimes \mathbb{D}_{\text{cris}}(V))$ . By Theorem 2.10, we know that the elementary divisors of  $\underline{M}$  are  $\mathfrak{n}_{r_1}, \dots, \mathfrak{n}_{r_d}$ .

**Corollary 3.2.** *Up to a unit,  $\det(\underline{M})$  is equal to  $\prod_{i=1}^d \mathfrak{n}_{r_i}$ .*

We can write the Coleman map  $\underline{\text{Col}}$  in terms of  $\underline{M}$  as follows:

**Lemma 3.3.** *For  $x \in \mathbb{N}(T)^{\psi=1}$ , we have*

$$(1 - \varphi)(x) = \underline{\text{Col}}(x) \cdot \underline{M} \cdot \begin{pmatrix} (1 + \pi) \otimes v_1 \\ \vdots \\ (1 + \pi) \otimes v_d \end{pmatrix}.$$

*Proof.* We have by definition

$$(1 - \varphi)x = \underline{\text{Col}}(x) \cdot \begin{pmatrix} (1 + \pi)\varphi(n_1) \\ \vdots \\ (1 + \pi)\varphi(n_d) \end{pmatrix}.$$

Therefore, we are done on combining this with (1). □

**Definition 3.4.** The Perrin-Riou  $p$ -adic regulator  $\mathcal{L}_V$  for  $V$  is defined to be the  $\Lambda_E(\Gamma)$ -homomorphism

$$(\mathfrak{M}^{-1} \otimes 1) \circ (1 - \varphi) \circ (h_{\text{Iw}, V}^1)^{-1} : H_{\text{Iw}}^1(\mathbb{Q}_p, V) \longrightarrow \mathcal{H}(\Gamma) \otimes \mathbb{D}_{\text{cris}}(V).$$

Using the isomorphism  $h_{\text{Iw}, V}^1 : \mathbb{N}(V)^{\psi=1} \rightarrow H_{\text{Iw}}^1(\mathbb{Q}_p, V)$ , we can thus rewrite Lemma 3.3 as

$$\mathcal{L}_V(z) = (\underline{\text{Col}} \circ (h_{\text{Iw}, V}^1)^{-1})(z) \cdot \underline{M} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix}. \tag{2}$$

### 4. Images of the Coleman maps

Let  $\eta$  be a character on  $\Delta$ . In this section, we study the image of  $\underline{\text{Col}}^\eta(\mathbb{N}(V)^{\psi=1})$  as a subset of  $\Lambda_E(\Gamma_1)^{\oplus d}$  for a crystalline representation  $V$  of dimension  $d$  with non-negative Hodge–Tate weights. We then consider the projection of this image, giving a description of  $\text{Im}(\underline{\text{Col}}_i^\eta)$  for  $i = 1, \dots, d$ .

**4A. Preliminary results on  $\Lambda_E(\Gamma_1)$ -modules.** Recall that we identify  $\Lambda_E(\Gamma_1)$  with the power series ring  $E \otimes \mathbb{C}_E[[X]]$  by identifying  $\gamma - 1$  with  $X$ . Therefore, if  $F \in \Lambda_E(\Gamma_1)$  and  $x$  is an element of the maximal ideal of  $E$ ,  $F|_{X=x} \in E$ .

**Lemma 4.1.** *Let  $V$  be an  $E$ -subspace of  $E^d$  with codimension  $n$ . For a fixed element  $x$  of the maximal ideal of  $E$ , we define the  $\Lambda_E(\Gamma_1)$ -module*

$$S = \{(F_1, \dots, F_d) \in \Lambda_E(\Gamma_1)^{\oplus d} : (F_1(x), \dots, F_d(x)) \in V\}.$$

*Then,  $S$  is free of rank  $d$  over  $\Lambda_E(\Gamma_1)$  and  $\det(S) = (X - x)^n$ .*

*Proof.* Let  $v_1, \dots, v_d$  be a basis of  $E$  such that  $\sum_{i=1}^d e_i v_i \in V$  if and only if  $e_i = 0$  for all  $i > d - n$ . On multiplying elementary matrices in  $\mathrm{GL}_d(E)$  if necessary, we may assume that  $S$  is of the form

$$\begin{aligned} S &= \{(F_1, \dots, F_d) \in \Lambda_E(\Gamma_1)^{\oplus d} : F_{d-n+1}(x) = \dots = F_d(x) = 0\} \\ &= \Lambda_E(\Gamma_1)^{\oplus(d-n)} \oplus ((X - x)\Lambda_E(\Gamma_1))^{\oplus n}, \end{aligned}$$

so we are done. □

**Proposition 4.2.** *Let  $I = \{x_0, \dots, x_m\}$  be a subset of the maximal ideal of  $E$ . For each  $i = 0, \dots, m$ , let  $V_i$  be an  $E$ -subspace of  $E^{\oplus d}$  with codimension  $n_i$ . Define*

$$S = \{(F_1, \dots, F_d) \in \Lambda_E(\Gamma_1)^{\oplus d} : (F_1(x_i), \dots, F_d(x_i)) \in V_i, i = 0, \dots, m\},$$

*then  $S$  is free of rank  $d$  over  $\Lambda_E(\Gamma_1)$ , and  $\det(S) = \prod_{i=0}^m (X - x_i)^{n_i}$ .*

*Proof.* We prove the result by induction on  $m$ . The case  $m = 0$  is just Lemma 4.1.

Assume that  $m > 0$  and let

$$S' = \{(F_1, \dots, F_d) \in \Lambda_E(\Gamma_1)^{\oplus d} : (F_1(x_i), \dots, F_d(x_i)) \in V_i, i = 0, \dots, m - 1\}.$$

By induction,  $S'$  is free of rank  $d$  over  $\Lambda_E(\Gamma_1)$  and  $\det(S') = \prod_{i=0}^{m-1} (X - x_i)^{n_i}$ . Let  $F^{(i)} = (F_1^{(i)}, \dots, F_d^{(i)})$ ,  $i = 1, \dots, d$ , be a  $\Lambda_E(\Gamma_1)$ -basis of  $S'$ . Write  $\mathcal{F}_m$  for the  $d \times d$  matrix with entries  $F_j^{(i)}(x_m)$ . As  $X - x_m$  does not divide  $\det(F_j^{(i)})$ , we have  $\mathcal{F}_m \in \mathrm{GL}_d(E)$ . Define

$$S'' = \{(G_1, \dots, G_d) \in \Lambda_E(\Gamma_1)^{\oplus d} : (G_1(x_m), \dots, G_d(x_m)) \in V_m \mathcal{F}_m^{-1}\}.$$

By Lemma 4.1,  $S''$  is free of rank  $d$  over  $\Lambda_E(\Gamma_1)$  and  $\det(S'') = (X - x_m)^{n_m}$ . Say,  $(G_1^{(k)}, \dots, G_d^{(k)})$ ,  $k = 1, \dots, d$ , is a basis.

For  $(G_1, \dots, G_d) \in \Lambda_E(\Gamma_1)^{\oplus d}$ , we have  $\sum_{i=1}^d G_i F^{(i)} \in S' \subset S$  by definition. It is easy to check that  $\sum_{i=1}^d G_i F^{(i)} \in S$  if and only if  $(G_1, \dots, G_d) \in S''$ . Therefore, a basis for  $S$  is given by the row vectors of  $(G_i^{(k)})(F_j^{(i)})$  and  $\det(S) = \det(S') \det(S'')$ . Hence, we are done. □

**Lemma 4.3.** *If  $S$  is a  $\Lambda_E(\Gamma_1)$ -module as in the statement of Proposition 4.2, then the image of a projection from  $S$  into  $\Lambda_E(\Gamma_1)$  is of the form  $\prod_{i \in J} (X - x_i)\Lambda_E(\Gamma_1)$  where  $J$  is some subset of  $\{0, \dots, m\}$ .*



*Proof.* We consider the first projection  $\text{pr}_1 : (F_1, \dots, F_d) \mapsto F_1$ . Let

$$J = \{i \in [0, m] : (e_1, \dots, e_d) \in V_i \Rightarrow e_1 = 0\}.$$

It is clear that  $\text{Im}(\text{pr}_1) \subset \prod_{i \in J} (X - x_i) \Lambda_E(\Gamma_1)$ . It remains to show that

$$\prod_{i \in J} (X - x_i) \in \text{Im}(\text{pr}_1).$$

By definition, for each  $i \notin J$ , there exist  $e_k^{(i)} \in E, k = 2, \dots, d$ , such that

$$\left( \prod_{j \in J} (x_i - x_j), e_2^{(i)}, \dots, e_d^{(i)} \right) \in V_i.$$

Similarly, take any  $(0, e_2^{(i)}, \dots, e_d^{(i)}) \in V_i$  for  $i \in J$ . There exist polynomials  $F_k$  over  $E$  such that  $F_k(x_i) = e_j^{(i)}$  for  $k = 2, \dots, d$  and  $i = 0, \dots, m$ . It is then clear that

$$\left( \prod_{i \in J} (X - x_i), F_2, \dots, F_d \right) \in S.$$

Hence we are done. □

**4B. On the image of the Perrin-Riou  $p$ -adic regulator.** with Hodge–Tate weights  $-r_d \leq -r_{d-1} \leq \dots \leq -r_1 \leq 0$ . As in Section 3A, fix bases  $n_1, \dots, n_d$  and  $v_1, \dots, v_d$  of  $\mathbb{N}(\mathcal{T})$  and  $\mathbb{D}_{\text{cris}}(V)$ , respectively, such that  $v_i = n_i \pmod{\pi}$ . For the rest of this paper, we make the following assumption.

$\mathcal{G}_{\mathbb{Q}_p}$  with non-negative Hodge–Tate weights  $m - r_1 \geq \dots \geq m - r_d \geq 0$ . Moreover, our assumption on the eigenvalues of  $\varphi$  implies that  $V$  has no quotient isomorphic to  $E$ .

Let  $V$  be a  $d$ -dimensional  $E$ -linear crystalline representation of  $\mathcal{G}_{\mathbb{Q}_p}$  with non-negative Hodge–Tate weights  $r_1 \leq \dots \leq r_d$ .

**Definition 4.4.** For an integer  $i \geq 0$ , we write

$$n_i = \dim_E \text{Fil}^{-i} \mathbb{D}_{\text{cris}}(V) = \#\{j : r_j \leq i\}.$$

We make the following assumption:

**Assumption 4.5.** *The eigenvalues of  $\varphi$  on  $\mathbb{D}_{\text{cris}}(V)$  are not integer powers of  $p$ .*

Recall from [Perrin-Riou 1994] that we have the exponential map

$$\Omega_{V,r_d} : (\mathbb{B}_{\text{rig},\mathbb{Q}_p}^+)^{\psi=0} \otimes \mathbb{D}_{\text{cris}}(V) \rightarrow \mathcal{H}(\Gamma) \otimes H_{\text{Iw}}^1(\mathbb{Q}_p, V).$$

The Perrin-Riou  $p$ -adic regulator is related to  $\Omega_{V,r_d}$  via the following equation.

**Theorem 4.6.** *As maps on  $H_{\text{Iw}}^1(\mathbb{Q}_p, V)$ , we have*

$$\mathcal{L}_V = (\mathfrak{M}^{-1} \otimes 1) \left( \prod_{i=0}^{r_d-1} \ell_i \right) (\Omega_{V,r_d})^{-1}.$$

*Proof.* By definition, this is the same as saying

$$(1 - \varphi) \circ (h_{\text{Iw},V}^1)^{-1} = \left( \prod_{i=0}^{r_d-1} \ell_i \right) (\Omega_{V,r_d})^{-1},$$

which is just a rewrite of [Berger 2003, Theorem II.13]. □

**Corollary 4.7.** *We have*

$$\det(\mathcal{L}_V) = \prod_{i=0}^{r_d-1} (\ell_i)^{d-n_i}.$$

*Proof.* The  $\delta(V)$ -conjecture (see [Perrin-Riou 1994, Conjecture 3.4.7]) predicts that

$$\det(\Omega_{V,r_d}) = \prod_{i \leq r_d-1} (\ell_i)^{n_i}.$$

As pointed out in Proposition 3.6.7 of the same work, this conjecture is a consequence of Perrin-Riou’s explicit reciprocity law, labeled “Conjecture (Réc)” in [op. cit.], and proved in [Colmez 1998, théorème IX.4.5]. Therefore, Theorem 4.6 implies that

$$\det(\mathcal{L}_V) = \left( \prod_{i=0}^{r_d-1} (\ell_i)^d \right) \left( \prod_{i \leq r_d-1} (\ell_i)^{-n_i} \right),$$

which finishes the proof, since  $n_i = 0$  for  $i < 0$ . □

Let  $z \in H_{\text{Iw}}^1(\mathbb{Q}_p, V)$ . Then  $\mathcal{L}_V(z) \in \mathcal{H}(\Gamma) \otimes_{\mathbb{Q}_p} \mathbb{D}_{\text{cris}}(V)$ , so we can apply to  $\mathcal{L}_V(z)$  any character on  $\Gamma$  to obtain an element in  $\mathbb{D}_{\text{cris}}(V)$ . The following proposition studies elements obtained in this way when we choose characters of a specific kind. Recall that we denote by  $\chi$  the cyclotomic character, and by  $\chi_0$  the restriction of  $\chi$  to  $\Delta$ .

**Proposition 4.8.** *Let  $z \in H_{\text{Iw}}^1(\mathbb{Q}_p, V)$ . Then for any integer  $0 \leq i \leq r_d - 1$  and any Dirichlet character  $\delta$  of conductor  $p^n > 1$ , we have*

$$(1 - \varphi)^{-1} (1 - p^{-1}\varphi^{-1}) \chi^i(\mathcal{L}_V(z) \otimes t^i e_{-i}) \in \text{Fil}^0 \mathbb{D}_{\text{cris}}(V(-i)); \tag{3}$$

and

$$\varphi^{-n} (\chi^i \delta(\mathcal{L}_V(z) \otimes t^i e_{-i})) \in \mathbb{Q}_{p,n} \otimes \text{Fil}^0 \mathbb{D}_{\text{cris}}(V(-i)). \tag{4}$$

*Proof.* We write  $[ \ , \ ]$  for the pairing

$$\mathbb{D}_{\text{cris}}(V(-i)) \times \mathbb{D}_{\text{cris}}(V^*(1+i)) \longrightarrow \mathbb{D}_{\text{cris}}(E(1)) = E \cdot t^{-1}e_1.$$

The orthogonal complement of  $\text{Fil}^0 \mathbb{D}_{\text{cris}}(V(-i))$  under  $[ \ , \ ]$  is  $\text{Fil}^0(V^*(1+i))$ . Let  $x \in \text{Fil}^0 \mathbb{D}_{\text{cris}}(V^*(1+i))$  and  $x' = (1-\varphi)(1-p^{-1}\varphi^{-1})^{-1}x$ , and write  $x'_{-i}$  for  $x' \otimes t^i e_{-i}$ . Then

$$\begin{aligned} [(1-\varphi)^{-1}(1-p^{-1}\varphi^{-1})\chi^i(\mathcal{L}_V(z) \otimes t^i e_{-i}), x] &= [\chi^i(\mathcal{L}_V(z) \otimes t^i e_{-i}), x'] \\ &= \chi^i[\mathcal{L}_V(z), x'_{-i}], \end{aligned}$$

where the first equality follows from the observation that  $1-\varphi$  and  $1-p^{-1}\varphi^{-1}$  are adjoint to each other under the pairing  $[ \ , \ ]$ .

We extend  $[ \ , \ ]$  to a pairing on

$$\mathcal{H}(\Gamma) \otimes_{\mathbb{Q}_p} \mathbb{D}_{\text{cris}}(V) \times \mathcal{H}(\Gamma) \otimes_{\mathbb{Q}_p} \mathbb{D}_{\text{cris}}(V^*(1)) \longrightarrow E \otimes_{\mathbb{Q}_p} \mathcal{H}(\Gamma)$$

in the natural way. By Perrin-Riou’s explicit reciprocity law (see previous proof) and Theorem 4.6, we have

$$[\mathcal{L}_V(z), x'_{-i}] = (-1)^{r_d-1} \left\langle \left( \prod_{j=0}^{r_d-1} \ell_j \right) z, \Omega_{V^*(1), 1-r_d}((1+\pi) \otimes x'_{-i}) \right\rangle \quad (5)$$

where  $\langle \ , \ \rangle$  denotes the pairing

$$(\mathcal{H}(\Gamma) \otimes H_{\text{Tw}}^1(\mathbb{Q}_p, V)) \times (\mathcal{H}(\Gamma) \otimes H_{\text{Tw}}^1(\mathbb{Q}_p, V^*(1))) \longrightarrow E \otimes \mathcal{H}(\Gamma)$$

as defined in [Perrin-Riou 1994, § 3.6]. By [Perrin-Riou 1994, Lemme 3.6.1(i)], the right-hand side of (5) in fact equals

$$\left\langle z, \left( \prod_{j=0}^{r_d-1} \ell_{-j} \right) \Omega_{V^*(1), 1-r_d}((1+\pi) \otimes x'_{-i}) \right\rangle = \langle z, \Omega_{V^*(1), 1}((1+\pi) \otimes x'_{-i}) \rangle. \quad (6)$$

By an abuse of notation, we let  $\text{Tw}$  denote the twist map on the  $H_{\text{Tw}}^1$ ’s as well as the map on  $\mathcal{H}(\Gamma)$  that sends any  $g \in \Gamma$  to  $\chi(g)g$ . We have

$$\langle \text{Tw}^{-i}(x), \text{Tw}^i(y) \rangle = \text{Tw}^i \langle x, y \rangle$$

for any  $x$  and  $y$  by [Perrin-Riou 1994, Lemme 3.6.1(ii)]. Therefore, by combining (5) and (6),  $\chi^i[\mathcal{L}_V(z), x'_{-i}]$  is equal to the projection of

$$\langle \text{Tw}^{-i}(z), \text{Tw}^i(\Omega_{V^*(1), 1}((1+\pi) \otimes x'_{-i})) \rangle$$

into  $E$ . The projection of  $\text{Tw}^i(\Omega_{V^*(1), 1}((1+\pi) \otimes x'_{-i}))$  into  $H^1(\mathbb{Q}_p, V^*(1+i))$  at the origin is equal to a scalar multiple of

$$\exp_{\mathbb{Q}_p, V^*(1+i)}((1-p^{-1}\varphi^{-1})(1-\varphi)^{-1}(x'))$$

(see for example [Lei et al. 2010, Proposition 3.19]). But

$$(1 - p^{-1}\varphi^{-1})(1 - \varphi)^{-1}(x') = x \in \text{Fil}^0 \mathbb{D}_{\text{cris}}(V^*(1+i))$$

by definition. Therefore, as  $\exp_{\mathbb{Q}_p, V^*(1+i)}$  vanishes on  $\text{Fil}^0 \mathbb{D}_{\text{cris}}(V^*(1+i))$  by construction, it follows that

$$\exp_{\mathbb{Q}_p, V^*(1+i)} \left( (1 - \varphi)^{-1}(1 - p^{-1}\varphi^{-1})(x') \right) = 0$$

and hence that

$$\left[ (1 - \varphi)^{-1} (1 - p^{-1}\varphi^{-1}) \chi^i (\mathcal{L}_V(z) \otimes t^i e_{-i}), x \right] = \chi^i [\mathcal{L}_V(z), x'_{-i}] = 0.$$

This implies (3), and (4) can be proved similarly. □

For any character  $\eta$  of  $\Delta$  and an integer  $0 \leq i \leq r_d - 1$ , define

$$V_{i,\eta} = \begin{cases} (1 - p^i\varphi)(1 - p^{-1-i}\varphi^{-1})^{-1} \text{Fil}^{-i} \mathbb{D}_{\text{cris}}(V) & \text{if } \chi_0^i = \eta, \\ \varphi(\text{Fil}^{-i} \mathbb{D}_{\text{cris}}(V)) & \text{otherwise.} \end{cases}$$

Note that  $V_{i,\eta}$  is a subspace of  $\mathbb{D}_{\text{cris}}(V)$  of the same dimension as  $\text{Fil}^{-i} \mathbb{D}_{\text{cris}}(V)$ .

**Corollary 4.9.** *If  $\eta$  is a character on  $\Delta$ , then*

$$\{ \chi^i \chi_0^{-i} \eta(e_\eta \mathcal{L}_V(z)) : z \in H_{\text{Iw}}^1(\mathbb{Q}_p, V) \} \subset V_{i,\eta}.$$

*Proof.* Note that  $\text{Fil}^{-i} \mathbb{D}_{\text{cris}}(V) = \text{Fil}^0 \mathbb{D}_{\text{cris}}(V(-i)) \otimes t^{-i} e_i$ . Therefore, if  $\chi_0^i = \eta$ , the result follows from (3) and the fact that  $\varphi(t^i e_{-i}) = p^i t^i e_{-i}$ . Assume otherwise. Since  $\chi^i \chi_0^{-i} \eta|_\Delta = \eta$ , we have  $\chi^i \chi_0^{-i} \eta(e_\eta \mathcal{L}_V(z)) = \chi^i \chi_0^{-i} \eta(\mathcal{L}_V(z))$ . Hence, (4) implies that

$$\varphi^{-1} \left( \chi^i \chi_0^{-i} \eta(e_\eta \mathcal{L}_V(z) \otimes t^i e_{-i}) \right) \in \mathbb{Q}_p(\mu_p) \otimes \text{Fil}^0 \mathbb{D}_{\text{cris}}(V(-i)).$$

But

$$\chi^i \chi_0^{-i} \eta(e_\eta \mathcal{L}_V(z) \otimes t^i e_{-i}) = \mathcal{L}_V(z)^\eta|_{X=\chi(\gamma)^{i-1}} \otimes t^i e_{-i}$$

in fact lies inside  $\mathbb{D}_{\text{cris}}(V(-i))$ . Hence,

$$\varphi^{-1} \left( \chi^i \chi_0^{-i} \eta(e_\eta \mathcal{L}_V(z) \otimes t^i e_{-i}) \right) \in \text{Fil}^0 \mathbb{D}_{\text{cris}}(V(-i)) = \text{Fil}^{-i} \mathbb{D}_{\text{cris}}(V) \otimes t^i e_{-i}$$

and we are done on applying  $\varphi$  to both sides. □

**Corollary 4.10.** *If  $\eta$  is a character on  $\Delta$ , then*

$$\{ \mathcal{L}_V(z)^\eta|_{X=\chi(\gamma)^{i-1}} : z \in H_{\text{Iw}}^1(\mathbb{Q}_p, V) \} \subset V_{i,\eta}.$$

*Proof.* This is immediate from Corollary 4.9, since

$$\mathcal{L}_V(z)^\eta|_{X=\chi(\gamma)^{i-1}} = \chi^i \chi_0^{-i} \eta(e_\eta \mathcal{L}_V(z)). \quad \square$$

**4C. Images of the Coleman maps.** We now fix a character  $\eta : \Delta \rightarrow \mathbb{Z}_p^\times$ . Let  $v_1, \dots, v_d$  be a basis of  $\mathbb{D}_{\text{cris}}(V)$  and  $n_1, \dots, n_d$  a basis of  $\mathbb{N}(V)$  lifting  $v_1, \dots, v_d$  as in Theorem 2.12. We consider the image of the Coleman map defined with respect to this basis as in Section 3.

**Proposition 4.11.** *The image of the map*

$$\underline{\text{Col}}^\eta : \mathbb{N}(V)^{\psi=1} \longrightarrow \Lambda_E(\Gamma_1)^{\oplus d}$$

lies inside a  $\Lambda_E(\Gamma_1)$ -submodule  $S$  as described in the statement of Proposition 4.2 with

$$I = \{x_i = \chi(\gamma)^i - 1 : 0 \leq i \leq r_d - 1\} \quad \text{and} \quad V_i = V_{i,\eta},$$

which is an  $E$ -vector space of the same (co-)dimension as  $\text{Fil}^{-i} \mathbb{D}_{\text{cris}}(V)$ .

*Proof.* Recall from (2) that

$$\mathcal{L}_V = (\underline{\text{Col}} \circ h_{\text{Iw},V}^1) \underline{M} \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix}$$

where  $\underline{M}$  is as defined in (1). Note that  $\underline{M}^\eta = \underline{M}$  for any character  $\eta$  of  $\Delta$ , since  $\underline{M}$  is defined over  $\mathcal{H}(\Gamma_1)$ . Moreover, Corollary 3.2 implies that  $X - \chi(\gamma)^i + 1$  does not divide  $\det(\underline{M})$ , so  $\underline{M}|_{X=\chi(\gamma)^i-1} \in \text{GL}_d(E)$ . Therefore, we are done by Corollary 4.10. □

**Theorem 4.12.** *Equality holds in Proposition 4.11.*

*Proof.* Write  $S$  for the basis matrix of the  $\Lambda_E(\Gamma_1)$ -submodule of  $\Lambda_E(\Gamma_1)^{\oplus d}$  described in the statement of Proposition 4.11. Then, Proposition 4.2 says that

$$\det(S) = \prod_{i=0}^{r_d-1} (X - \chi(\gamma)^i + 1)^{d-n_i}.$$

But

$$\det(\underline{M}) = \prod_{j=1}^d \left( \prod_{i=0}^{r_j-1} \frac{\ell_i}{X - \chi(\gamma)^i + 1} \right) = \prod_{i=0}^{r_d-1} \left( \frac{\ell_i}{X - \chi(\gamma)^i + 1} \right)^{d-n_i},$$

since  $n_i = \#\{j : r_j \leq i\}$ , as noted above. Hence, Corollary 4.7 implies that

$$\det(\mathcal{L}_V) = \det(\underline{M}) \det(S)$$

and we are done. □

We can summarize the above results via the following short exact sequence:

**Corollary 4.13.** *Suppose that no eigenvalue of  $\varphi$  on  $\mathbb{D}_{\text{cris}}(V)$  lies in  $p^{\mathbb{Z}}$ . Then for each character  $\eta$  of  $\Delta$ , there is a short exact sequence of  $\mathcal{H}(\Gamma_1)$ -modules*

$$0 \longrightarrow \mathbb{N}(V)^{\psi=1,\eta} \xrightarrow{1-\varphi} (\varphi^*\mathbb{N}(V))^{\psi=0,\eta} \xrightarrow{A_\eta} \bigoplus_{i=0}^{r_d-1} (\mathbb{D}_{\text{cris}}(V)/V_{i,\eta})(\chi^i \chi_0^{-i} \eta) \longrightarrow 0.$$

Here the map  $A_\eta$  equals  $\bigoplus_i (1 \otimes A_{\eta,i})$ , where  $A_{\eta,i}$  is the natural reduction map  $\mathcal{H}(\Gamma) \rightarrow \mathbb{Q}_p(\chi^i \chi_0^{-i} \eta)$  obtained by quotienting out by the ideal  $(X + 1 - \chi(\gamma)^i) \cdot e_\eta$ .

**Remark 4.14.** The short exact sequence in Corollary 4.13 can be seen as an analogue of Perrin-Riou’s exact sequence (see [Perrin-Riou 1994, §2.2])

$$\begin{aligned} 0 \longrightarrow \bigoplus_{i=0}^{r_d} t^i \mathbb{D}_{\text{cris}}(V)^{\varphi=p^{-i}} &\longrightarrow (\mathbb{B}_{\text{rig},\mathbb{Q}_p}^+ \otimes \mathbb{D}_{\text{cris}}(V))^{\psi=1} \\ &\xrightarrow{\varphi-1} (\mathbb{B}_{\text{rig},\mathbb{Q}_p}^+)^{\psi=0} \otimes \mathbb{D}_{\text{cris}}(V) \longrightarrow \bigoplus_{i=0}^{r_d} \left( \frac{\mathbb{D}_{\text{cris}}(V)}{1 - p^i \varphi} \right) (i) \longrightarrow 0. \end{aligned}$$

In particular, the injectivity of the first map in our sequence follows from Perrin-Riou’s sequence, whose first term vanishes in view of our assumption on  $V$ .

We can now prove Theorem C.

**Corollary 4.15.** *For  $i = 1, \dots, d$ , we have*

$$\text{Im}(\text{Col}_i^\eta) = \prod_{j \in I_i^\eta} (X - \chi(\gamma)^j + 1) \Lambda_E(\Gamma_1)$$

for some  $I_i^\eta \subset \{0, \dots, r_d - 1\}$ .

*Proof.* This follows immediately from Lemma 4.3. □

We can also use this argument to determine the elementary divisors of the cokernel of the map  $\mathcal{L}_V$ , refining the result of Corollary 4.7.

**Theorem 4.16.** *The elementary divisors of the  $\mathcal{H}(\Gamma)$ -module quotient*

$$\frac{\mathcal{H}(\Gamma) \otimes_{\mathbb{Q}_p} \mathbb{D}_{\text{cris}}(V)}{\mathcal{H}(\Gamma) \otimes_{\Lambda_{\mathbb{Q}_p}(\Gamma)} \text{Im}(\mathcal{L}_V)}$$

are  $[\lambda_{r_1}; \dots; \lambda_{r_d}]$ , where  $\lambda_k = \ell_0 \ell_1 \dots \ell_{k-1}$ .

*Proof.* We know that the matrix of  $\mathcal{L}_V$  is equal to  $M \cdot S$ , where  $M$  and  $S$  have elementary divisors that are coprime. Hence the elementary divisors of the product matrix are the products of the elementary divisors, which gives the above formula. □

### 5. The Coleman maps for modular forms

In this section, we fix a modular form  $f$  as in Section 1C6. We pick bases  $n_1, n_2$  of  $\mathbb{N}(T_{\bar{f}})$  and  $\bar{v}_1, \bar{v}_2$  of  $\mathbb{D}_{\text{cris}}(V_{\bar{f}})$  as in [Lei et al. 2010, Section 3.3]. Let  $V = V_{\bar{f}}(k-1)$ , which has Hodge–Tate weights 0 and  $k-1$ . We consider the Coleman maps  $\underline{\text{Col}}_1^\eta$  and  $\underline{\text{Col}}_2^\eta$  defined on  $\mathbb{N}(V)^{\psi=1}$  where  $\eta$  is a fixed character on  $\Delta$ . As a special case for Theorem 4.12 and Corollary 4.15, we have the following result.

**Proposition 5.1.** *There exist 1-dimensional  $E$ -subspaces  $V_i$  of  $E^2$  for  $0 \leq i < k-1$  such that*

$$\text{Im}(\underline{\text{Col}}^\eta) = \{(F, G) \in \Lambda_E(\Gamma_1) : (F(\chi^i(\gamma) - 1), G(\chi^i(\gamma) - 1)) \in V_i\}.$$

Moreover, for  $l = 1, 2$ , we have

$$\text{Im}(\underline{\text{Col}}_l^\eta) = \prod_{j \in I_l^\eta} (X - \chi^j(\gamma) + 1) \Lambda_E(\Gamma_1)$$

for some  $I_l^\eta \subset \{0, \dots, k-2\}$  with  $I_1^\eta$  and  $I_2^\eta$  disjoint.

*Proof.* For  $0 \leq j \leq k-2$ ,  $\text{Fil}^{-j} \mathbb{D}_{\text{cris}}(V)$  is of dimension 1 over  $E$ . Hence the first part of the proposition by Theorem 4.12. The second part of the proposition follows by putting

$$I_1^\eta = \{i : V_i = 0 \oplus E\} \quad \text{and} \quad I_2^\eta = \{i : V_i = E \oplus 0\}. \quad \square$$

**Remark 5.2.** Note that the second part of the proposition is a slightly stronger version of Corollary 4.15.

**Corollary 5.3.** *In particular, there exist nonzero elements  $r_i \in E$  for  $i \in I_3^\eta := \{0, \dots, k-2\} \setminus (I_1^\eta \cup I_2^\eta)$  such that*

$$\text{Im}(\underline{\text{Col}}^\eta) = \left\{ (F, G) \in \Lambda_E(\Gamma_1) \left| \begin{array}{l} F(u^i - 1) = 0 \text{ if } i \in I_1^\eta \\ G(u^i - 1) = 0 \text{ if } i \in I_2^\eta \\ F(u^i - 1) = r_i G(u^i - 1) \text{ if } i \in I_3^\eta \end{array} \right. \right\}$$

where  $u = \chi(\gamma)$ .

The aim of this section is to study the set above in more detail.

**5A. Some explicit linear relations.** Recall from [Lei et al. 2010, proof of Proposition 3.22] that the maps  $\mathcal{L}_1$  and  $\mathcal{L}_2$  as defined in Section 1C6 satisfy

$$\mathcal{L}_V(z) = -\mathcal{L}_2(z)\bar{v}_{1,k-1} + \mathcal{L}_1(z)\bar{v}_{2,k-1}$$

for any  $z \in H_{\text{Iw}}^1(\mathbb{Q}_p, V)$ . Therefore, Corollary 4.9 says that  $\mathcal{L}_1(z)$  and  $\mathcal{L}_2(z)$  satisfy some linear relations when evaluated at  $\chi^j \delta$  for  $0 \leq j \leq k-2$  and  $\delta$  some character on  $\Delta$ . We now make these relations explicit. First we recall that we have:

**Lemma 5.4.** *Let  $j, n \geq 0$  be integers and  $i \in \{1, 2\}$ . For  $z \in H_{\text{Iw}}^1(\mathbb{Q}_p, V)$ , we write  $z_{-j,n}$  for the image of  $z$  under*

$$H_{\text{Iw}}^1(\mathbb{Q}_p, V) \rightarrow H_{\text{Iw}}^1(\mathbb{Q}_p, V(-j)) \rightarrow H^1(\mathbb{Q}_{p,n}, V(-j)) \tag{7}$$

where the first map is the twist map  $(-1)^j \text{Tw}_j$  and the second map is the projection. Then, we have

$$\chi^j(\mathcal{L}_i(z)) = j![(1 - \varphi)^{-1}(1 - p^{-1}\varphi^{-1})v_{i,j+1}, \exp_{\mathbb{Q}_{p,1},V(j)}^*(z_{-j,0})]. \tag{8}$$

If  $\delta$  is a character of  $G_n$  which does not factor through  $G_{n-1}$  with  $n \geq 1$ , then

$$\chi^j \delta(\mathcal{L}_i(z)) = \frac{j!}{\tau(\delta^{-1})} \sum_{\sigma \in G_n} \delta^{-1}(\sigma) [\varphi^{-n}(v_{i,j+1}), \exp_{\mathbb{Q}_{p,1},V(j)}^*(z_{-j,n}^\sigma)] \tag{9}$$

where  $\tau$  denotes the Gauss sum.

*Proof.* See, for example, [Lei 2011, Lemma 3.5 and (4)]. □

**Lemma 5.5.** *If  $0 \leq j \leq k - 2$  and  $\delta$  is a nontrivial character on  $\Delta$ , then*

$$\chi^j \delta(\mathcal{L}_2(z)) = 0.$$

*Proof.* On putting  $n = 1$  in (9), we have

$$\chi^j \delta(\mathcal{L}_2(z)) = \frac{j!}{\tau(\delta^{-1})} \sum_{\sigma \in \Delta} \delta^{-1}(\sigma) [\varphi^{-1}(v_{2,j+1}), \exp_{\mathbb{Q}_{p,1},V(j)}^*(z_{-j,1}^\sigma)].$$

But  $v_2 = p^{1-k}\varphi(v_1)$ , so

$$\varphi^{-1}(v_{2,j+1}) \in E \cdot v_{1,j+1} = \text{Fil}^0 \mathbb{D}_{\text{cris}}(V_f(j+1)).$$

Therefore, we have

$$[\varphi^{-1}(v_{2,j+1}), \exp_{\mathbb{Q}_{p,1},V(j)}^*(z^\sigma)] = 0$$

for all  $\sigma \in \Delta$  and we are done. □

**Lemma 5.6.** *If  $\varphi^2 + a\varphi + b = 0$ , then*

$$(1 - \varphi)^{-1}(1 - p^{-1}\varphi^{-1}) = \frac{(1 + a + pb)\varphi + a(1 + a + pb) + b(p - 1)}{pb(1 + a + b)}.$$

*Proof.* We can write  $\varphi^2 + a\varphi + b = 0$ ,  $\varphi^2 - 1 + a(\varphi - 1) = -1 - a - b$ , and  $(1 - \varphi)(\varphi + 1 + a) = 1 + a + b$ . Therefore,

$$(1 - \varphi)^{-1} = \frac{\varphi + 1 + a}{1 + a + b}.$$

Similarly, we have

$$\varphi^{-1} = -\frac{\varphi + a}{b}.$$

The result then follows from explicit calculation. □



**Corollary 5.7.** *For  $0 \leq j \leq k - 2$ , we have*

$$(-a_p + p^{j+1} + p^{k-1-j})\chi^j(\mathcal{L}_2(z)) = (p - 1)\chi^j(\mathcal{L}_1(z)).$$

*Proof.* On  $\mathbb{D}_{\text{cris}}(V_{\bar{f}}(k - 1 - j))$ ,  $\varphi$  satisfies

$$\varphi^2 - a_p p^{-k+1+j} \varphi + p^{-k+1+2j} = 0,$$

as we assume  $\varepsilon(p) = 1$ . Let

$$\begin{aligned} u &= 1 - a_p p^{-k+1+j} + p^{-k+2+2j}, \\ u' &= -a_p p^{-k+1+j} u + p^{-k+1+2j} (p - 1). \end{aligned}$$

Then, Proposition 4.8 and Lemma 5.6 imply that

$$(u\varphi + u')\chi^j(-\mathcal{L}_2(z)\bar{v}_{1,k-1-j} + \mathcal{L}_1(z)\bar{v}_{2,k-1-j})$$

lies in  $\text{Fil}^0 \mathbb{D}_{\text{cris}}(V_{\bar{f}}(k - 1 - j)) = E v_{1,k-1-j}$ . On writing this expression as a linear combination of  $v_{1,k-1-j}$  and  $v_{2,k-1-j}$ , the coefficient of the latter turns out to be

$$-p^j u \chi^j(\mathcal{L}_2(z)) + (u' + a_p p^{-k+1+j} u) \chi^r(\mathcal{L}_1(z)),$$

which must be zero, hence the result. □

**Remark 5.8.** The coefficient  $-a_p + p^{j+1} + p^{k-1-j}$  is nonzero by the Weil bound.

Recall from [Lei et al. 2010, (32)] that we have

$$(-\mathcal{L}_2 \ \mathcal{L}_1) = (\underline{\text{Col}} \circ h_{\text{Iw},V}^1) \underline{M}.$$

By [Lei et al. 2010, proof of Proposition 3.28 and Theorem 5.4], we have

$$\underline{M}|_{X=0} = A_\varphi^T = \begin{pmatrix} 0 & p^{k-1} \\ -1 & a_p \end{pmatrix}.$$

Therefore, the relations for  $j = 0$  are given by

$$\begin{aligned} (-a_p + 1 + p^{k-2}) \underline{\text{Col}}_2(x)^\Delta|_{X=0} &= p^{k-2} (p - 1) \underline{\text{Col}}_1(x)^\Delta|_{X=0} && \text{if } \eta = 1, \\ \underline{\text{Col}}_2(x)^\eta|_{X=0} &= 0 && \text{if } \eta \neq 1. \end{aligned}$$

In particular, for the case  $k = 2$ , we have the following analogue of [Kurihara and Pollack 2007, Proposition 1.2].

**Proposition 5.9.** *If  $k = 2$ , the trivial isotypical component of the Coleman maps give a short exact sequence*

$$0 \longrightarrow H_{\text{Iw}}^1(\mathbb{Q}_p, V) \xrightarrow{\text{Col}^\Delta} \Lambda_E(\Gamma_1) \oplus \Lambda_E(\Gamma_1) \xrightarrow{\rho} \mathbb{Q}_p \longrightarrow 0,$$

where  $\rho$  is defined by

$$\rho(g(X), h(X)) = (2 - a_p)g(0) - (p - 1)h(0).$$

**5B. Integral structure of the images.** We now describe the integral structure of  $\text{Im}(\underline{\text{Col}}_i)^\eta$ . Under the notation of Corollary 5.3, we define

$$X_i^\eta = \prod_{j \in I_i^\eta} (X - \chi(\gamma)^j + 1).$$

Then, we have:

**Theorem 5.10.** *For  $i = 1, 2$ , let  $X_i^\eta$  be as defined above. Then*

$$\underline{\text{Col}}_i(\mathbb{D}(T_{\bar{f}}(k-1))^{\psi=1})^\eta \subset X_i^\eta \Lambda_{\mathbb{O}_E}(\Gamma_1).$$

Moreover,  $X_i^\eta \Lambda_{\mathbb{O}_E}(\Gamma_1) / \underline{\text{Col}}_i(\mathbb{D}(T_{\bar{f}}(k-1))^{\psi=1})^\eta$  is pseudo-null.

*Proof.* Let

$$X_k = \prod_{j=0}^{k-2} (X - \chi(\gamma)^j + 1).$$

Note that the proof of Proposition 4.11 in [Lei et al. 2010] is true integrally. We therefore have

$$(\varphi^{k-1}(\pi)\varphi^*\mathbb{N}(T_{\bar{f}}(k-1)))^{\psi=0} \subset (1-\varphi)\mathbb{N}(T_{\bar{f}}(k-1))^{\psi=1}.$$

This implies that  $X_k \in \text{Im}(\underline{\text{Col}}_i)$  for  $i = 1, 2$ . Hence, we have the following inclusions:

$$X_k \Lambda_{\mathbb{O}_E}(\Gamma_1) \subset \underline{\text{Col}}_i(\mathbb{D}(T_{\bar{f}}(k-1))^{\psi=1})^\eta \subset X_i^\eta \Lambda_{\mathbb{O}_E}(\Gamma_1)$$

for  $i = 1, 2$ . Since  $X_k$  is not divisible by  $\varpi_E$ , the quotient

$$X_i^\eta \Lambda_{\mathbb{O}_E}(\Gamma_1) / X_k \Lambda_{\mathbb{O}_E}(\Gamma_1)$$

is a free  $\mathbb{O}_E$ -module of finite rank. Moreover, for a coset representative,  $x$  say, it follows from Corollary 4.15 that there exists an integer  $n$  such that

$$\varpi_E^n x \in \underline{\text{Col}}_i(\mathbb{D}(T_{\bar{f}}(k-1))^{\psi=1})^\eta.$$

Therefore,  $\underline{\text{Col}}_i(\mathbb{D}(T_{\bar{f}}(k-1))^{\psi=1})^\eta$  is of finite index in  $X_i^\eta \Lambda_{\mathbb{O}_E}(\Gamma_1)$ . □

**5C. Surjectivity via a change of basis.** Unfortunately, we do not have an explicit description of the sets  $I_i^\eta$  given by Corollary 5.3. However, this can be resolved by choosing a different basis:

**Proposition 5.11.** *Let  $S$  be a subset of  $\Lambda_E(\Gamma_1)^{\oplus 2}$  as defined in Corollary 5.3. Then, there exists  $A \in \text{GL}(2, \mathbb{O}_E)$  such that  $SA = S'$  for some  $S'$  which is of the form*

$$\{(F, G) \in \Lambda_E(\Gamma_1)^{\oplus 2} : F(u^i - 1) = r'_i G(u^i - 1), 0 \leq i \leq k-2\}$$

for some nonzero elements  $r'_i \in E$ .

*Proof.* Let  $e_1, e_2 \in \mathbb{O}_E$  be nonzero elements such that  $e_1 e_2 \neq 1$ , then

$$\begin{pmatrix} 1 & e_2 \\ e_1 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{O}_E).$$

Let  $(F, G) \in \Lambda_E(\Gamma_1)^{\oplus 2}$ , we write  $(F' \ G') = (F \ G) A = (F + e_1 G \ G + e_2 F)$ . We have

$$F(u^i - 1) = 0 \iff F'(u^i - 1) = e_1 G'(u^i - 1);$$

$$G(u^i - 1) = 0 \iff G'(u^i - 1) = e_2 F'(u^i - 1);$$

$$F(u^i - 1) = r_i G(u^i - 1) \iff (e_2 r_i + 1) F'(u^i - 1) = (e_1 + r_i) G'(u^i - 1).$$

Therefore, we are done on choosing  $e_2 \neq -r_i^{-1}$  and  $e_1 \neq -r_i$  for all  $i \in I_3^\eta$ .  $\square$

**Remark 5.12.** In the construction of the Coleman maps, replacing  $\begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$  by  $A \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$ , where  $A \in \mathrm{GL}(2, \mathbb{O}_E)$ , is equivalent to replacing  $\underline{M}$  by  $\underline{A}\underline{M}$ .

Therefore, on multiplying  $\underline{M}$  by an appropriate matrix in  $\mathrm{GL}(2, \mathbb{O}_E)$  on the left, we can make both Coleman maps surjective (though we cannot assume  $\underline{M}|_{X=0} = A_\varphi^T$  any more). By Proposition 5.11, we deduce

**Theorem 5.13.** *There exists a basis of  $\mathbb{N}(T_{\bar{f}})$  such that the corresponding Coleman maps have the following properties:*

$$\Lambda_{\mathbb{O}_E}(\Gamma_1) / \underline{\mathrm{Col}}_i(\mathbb{D}(T_{\bar{f}}(k-1))^{\psi=1})^\eta$$

is pseudo-null for  $i = 1, 2$ .

### Acknowledgements

We are very grateful to Bernadette Perrin-Riou for giving us some unpublished notes about her  $p$ -adic regulator; and to the anonymous referee, for numerous helpful comments and corrections.

### References

- [Amice and Vélú 1975] Y. Amice and J. Vélú, “Distributions  $p$ -adiques associées aux séries de Hecke”, pp. 119–131 in *Journées Arithmétiques de Bordeaux* (Bordeaux, 1974), Astérisque **24-25**, Soc. Math. France, Paris, 1975. MR 51 #12709 Zbl 0332.14010
- [Bellaïche and Chenevier 2009] J. Bellaïche and G. Chenevier, *Families of Galois representations and Selmer groups*, Astérisque **324**, 2009. MR 2011m:11105 Zbl 1192.11035
- [Berger 2002] L. Berger, “Représentations  $p$ -adiques et équations différentielles”, *Invent. Math.* **148**:2 (2002), 219–284. MR 2004a:14022 Zbl 1113.14016
- [Berger 2003] L. Berger, “Bloch and Kato’s exponential map: three explicit formulas”, pp. 99–129 in *Kazuya Kato’s fiftieth birthday*, edited by S. Bloch et al., Documenta Mathematica, Bielefeld, 2003. Collection appeared as an unnumbered extra volume of *Doc. Math.* (2003). MR 2005f:11268 Zbl 1064.11077

- [Berger 2004] L. Berger, “Limites de représentations cristallines”, *Compos. Math.* **140**:6 (2004), 1473–1498. MR 2098398 (2006c:11138) Zbl 1071.11067
- [Berger et al. 2004] L. Berger, H. Li, and H. J. Zhu, “Construction of some families of 2-dimensional crystalline representations”, *Math. Ann.* **329**:2 (2004), 365–377. MR 2005k:11104 Zbl 1085.11028
- [Cherbonnier and Colmez 1999] F. Cherbonnier and P. Colmez, “Théorie d’Iwasawa des représentations  $p$ -adiques d’un corps local”, *J. Amer. Math. Soc.* **12**:1 (1999), 241–268. MR 99g:11141 Zbl 0933.11056
- [Colmez 1998] P. Colmez, “Théorie d’Iwasawa des représentations de de Rham d’un corps local”, *Ann. of Math. (2)* **148**:2 (1998), 485–571. MR 2000f:11077 Zbl 0928.11045
- [Deligne 1971] P. Deligne, “Formes modulaires et représentations  $\ell$ -adiques”, pp. 139–172 (exposé 355) in *Séminaire Bourbaki, 1968/69*, Lecture Notes in Mathematics **179**, Springer, Berlin, 1971. Zbl 0206.49901
- [Kato 2004] K. Kato, “ $p$ -adic Hodge theory and values of zeta functions of modular forms”, pp. 117–290 in *Cohomologies  $p$ -adiques et applications arithmétiques, III*, edited by P. Berthelot et al., Astérisque **295**, Société Mathématique de France, Paris, 2004. MR 2006b:11051 Zbl 1142.11336
- [Kurihara and Pollack 2007] M. Kurihara and R. Pollack, “Two  $p$ -adic  $L$ -functions and rational points on elliptic curves with supersingular reduction”, pp. 300–332 in  *$L$ -functions and Galois representations* (Durham, 2004), edited by D. Burns et al., London Math. Soc. Lecture Note Ser. **320**, Cambridge Univ. Press, 2007. MR 2009g:11069 Zbl 1148.11029
- [Lang 2002] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics **211**, Springer, New York, 2002. MR 2003e:00003 Zbl 0984.00001
- [Lei 2011] A. Lei, “Iwasawa theory for modular forms at supersingular primes”, *Compos. Math.* **147**:3 (2011), 803–838. MR 2012e:11186 Zbl 1234.11148
- [Lei et al. 2010] A. Lei, D. Loeffler, and S. L. Zerbes, “Wach modules and Iwasawa theory for modular forms”, *Asian J. Math.* **14**:4 (2010), 475–528. MR 2774276 Zbl 05878707
- [Loeffler and Zerbes 2012] D. Loeffler and S. L. Zerbes, “Wach modules and critical slope  $p$ -adic  $L$ -functions”, *J. Reine Angew. Math.* (2012).
- [Milne 1994] J. S. Milne, “Motives over finite fields”, pp. 401–459 in *Motives* (Seattle, 1991), edited by U. Jannsen et al., Proc. Sympos. Pure Math. **55**, Amer. Math. Soc., Providence, RI, 1994. MR 95g:11053 Zbl 0811.14018
- [Perrin-Riou 1994] B. Perrin-Riou, “Théorie d’Iwasawa des représentations  $p$ -adiques sur un corps local”, *Invent. Math.* **115**:1 (1994), 81–161. MR 95c:11082 Zbl 0838.11071
- [Perrin-Riou 1995] B. Perrin-Riou, *Fonctions  $L$   $p$ -adiques des représentations  $p$ -adiques*, Astérisque **229**, Soc. Mat. de France, Paris, 1995. MR 96e:11062 Zbl 0845.11040
- [Perrin-Riou 2001] B. Perrin-Riou, *Théorie d’Iwasawa des représentations  $p$ -adiques semi-stables*, Mém. Soc. Math. Fr. (N.S.) **84**, Soc. Mat. de France, Paris, 2001. MR 2003c:11144 Zbl 1031.11064
- [Pollack 2003] R. Pollack, “On the  $p$ -adic  $L$ -function of a modular form at a supersingular prime”, *Duke Math. J.* **118**:3 (2003), 523–558. MR 2004e:11050 Zbl 1074.11061
- [Schneider and Teitelbaum 2003] P. Schneider and J. Teitelbaum, “Algebras of  $p$ -adic distributions and admissible representations”, *Invent. Math.* **153**:1 (2003), 145–196. MR 2004g:22015 Zbl 1028.11070
- [Sprung 2009] F. I. Sprung, “Iwasawa theory for elliptic curves at supersingular primes: beyond the case  $a_p = 0$ ”, preprint, 2009. arXiv 0903.3419v1

Communicated by Karl Rubin

Received 2010-11-26

Revised 2011-02-23

Accepted 2011-03-25

- antonio.lei@mcgill.ca *School of Mathematical Sciences, Monash University,  
VIC 3800, Australia*
- Current address:* *Department of Mathematics and Statistics, Burnside Hall,  
McGill University, 805 Rue Sherbrooke Ouest, Montréal, QC,  
H3A 0B9, Canada*
- d.a.loeffler@warwick.ac.uk *Mathematics Institute, Zeeman Building,  
University of Warwick, Coventry, CV4 7AL, United Kingdom*
- s.zerbes@exeter.ac.uk *Mathematics Research Institute, Harrison Building,  
University of Exeter, Exeter, EX4 4QF, United Kingdom*



# Conjecture de Shafarevitch effective pour les revêtements cycliques

Robin de Jong et Gaël Rémond

On donne une borne supérieure explicite en fonction de  $K$ ,  $S$ ,  $g$  pour la hauteur de Faltings de la jacobienne d'une courbe  $C$  de genre  $g$ , définie sur un corps de nombres  $K$  et ayant bonne réduction en dehors d'un ensemble fini  $S$  de places de  $K$ , pourvu que  $C$  puisse s'écrire comme un revêtement cyclique de degré premier de la droite projective. La preuve repose sur le fait que les birapports des points de branchement du revêtement sont des  $S$ -unités, donc de hauteur bornée, et donnent un modèle plan de  $C$ .

We give an explicit upper bound in terms of  $K$ ,  $S$ ,  $g$  for the Faltings height of the jacobian of a curve  $C$  of genus  $g$ , defined over a number field  $K$  and with good reduction outside a finite set  $S$  of places of  $K$  under the condition that  $C$  can be written as a cyclic cover of prime order of the projective line. The proof rests on the fact that the cross ratios of the branch points of the cover are  $S$ -units, thus of bounded height, and give a plane model of  $C$ .

## 1. Introduction

Dans cet article, nous démontrons une version effective de la conjecture de Shafarevitch pour les courbes qui sont revêtements cycliques de degré premier de  $\mathbb{P}^1$ . Rappelons que Faltings [1983] a établi en toute généralité la version qualitative de cette conjecture (formulée comme une question dans son allocution au congrès international de Stockholm en 1962, voir [Shafarevitch 1963]).

**Théorème 1.1.** *Soient  $K$  un corps de nombres,  $S$  un ensemble fini de places finies de  $K$  et  $g \geq 2$  un entier. Alors l'ensemble des classes d'isomorphie de courbes projectives lisses  $C$  de genre  $g$  sur  $K$  ayant bonne réduction en dehors de  $S$  est fini.*

---

Le premier auteur est financé par une subvention VENI de l'Organisation Néerlandaise pour la Recherche Scientifique (NWO).

MSC2010 : 11G30.

Mots-clefs : conjecture de Shafarevitch, courbe, revêtement, hauteur, réduction, birapport, Shafarevich conjecture, curve, cover, height, reduction, cross ratio.

La conclusion vaut également dans le cas  $g = 1$  lorsque l'on suppose que  $C$  admet un point rationnel sur  $K$ , autrement dit pour les courbes elliptiques. L'énoncé est aussi vrai pour  $g = 0$  comme l'avait déjà observé Shafarevitch.

Une manière naturelle de quantifier cet énoncé consiste à borner la hauteur d'une telle courbe. Pour cela, plusieurs notions de hauteur peuvent être employées ; ici, pour faire un choix intrinsèque, nous utilisons la hauteur de Faltings stable de la jacobienne de notre courbe, notée  $h_{\text{Falt}}(C)$ .

En guise de motivation, nous mentionnons encore qu'une majoration de  $h_{\text{Falt}}(C)$  dans le théorème 1.1 sans restriction sur  $C$  entraînerait une version effective de la conjecture de Mordell (voir [Rémond 1999]). Toutefois la majoration explicite que nous donnons ci-dessous dans le cas très particulier des revêtements cycliques de degré premier n'a pas de conséquences directes dans cette direction (il faudrait connaître une courbe pour laquelle la construction de Kodaira–Parshin fournit une famille de courbes qui soient toutes de tels revêtements ; mais ceci signifierait que l'on peut tracer une courbe complète dans l'espace des modules des courbes d'un genre donné qui soit entièrement contenue dans le lieu des courbes de ce type ; or le dit lieu se trouve être affine, voir théorème 6.1 de [González Díez 1991], donc c'est impossible).

Pour énoncer notre résultat principal, nous devons quantifier la donnée de  $K$  et  $S$ . Si nous mesurons classiquement  $K$  par son degré  $D = [K : \mathbb{Q}]$  et son discriminant absolu  $\Delta = |\Delta_{K/\mathbb{Q}}|$ , nous introduisons pour  $S$  les quantités

$$\Omega = \sum_{p \in S} \log N_{K/\mathbb{Q}}(p) + D \log 4 \quad \text{et} \quad \Delta_S = \Delta e^{\Omega^2}.$$

Le terme  $D \log 4$  interviendra pour tenir compte des places infinies ; en revanche la définition de  $\Delta_S$  est purement *ad hoc* (par exemple la quantité  $\Delta e^{\Omega}$  serait peut-être plus naturelle). Nous fixons une clôture algébrique  $\bar{K}$  de  $K$ .

**Théorème 1.2.** *Soient  $K$  un corps de nombres,  $S$  un ensemble fini de places finies de  $K$  et  $g$  un entier. Soit  $C$  une courbe projective lisse de genre  $g$  sur  $K$  ayant bonne réduction en dehors de  $S$ . On suppose qu'il existe un  $K$ -morphisme  $\pi : C \rightarrow \mathbb{P}^1$  dont l'extension à  $\bar{K}$  est un revêtement cyclique de degré premier. Alors*

$$h_{\text{Falt}}(C) \leq 2^{2229g} \Delta_S^{2^{15}g^5}.$$

Pour  $g \geq 2$ , avec les propriétés de hauteur de  $h_{\text{Falt}}$ , nous obtenons la finitude de l'ensemble des courbes en question, indépendamment des résultats de Faltings. Notre énoncé contient aussi le cas des courbes elliptiques et des courbes hyper-elliptiques ayant un point rationnel (revêtements de degré 2 de  $\mathbb{P}^1$ ) ; dans ce cas, l'énoncé de finitude était connu de Shafarevitch lui-même et de Parshin (voir [Oort



1974] et les références). Notre démarche s’inspire de cette approche telle que formulée par Oort.

La démonstration repose sur le principe suivant. On considère les points de branchement  $P_1, \dots, P_r$  de  $\pi$  sur  $\bar{K}$ . Ils forment une famille de points de  $\mathbb{P}^1(\bar{K})$  stable sous l’action de  $\text{Gal}(\bar{K}/K)$ . On leur associe ensuite leurs birapports, soit  $6\binom{r}{4}$  éléments de  $\bar{K}^\times \setminus \{1\}$  sur lesquels agissent les involutions  $x \mapsto 1 - x$  et  $x \mapsto x^{-1}$  ainsi que le groupe  $\text{Gal}(\bar{K}/K)$ . Pour un tel birapport  $b$ , on note  $L = K(b)$  et  $S'$  l’ensemble fini des places de  $L$  formé des places divisant une place de  $S$  et de celles divisant  $p = \deg \pi$ . On montre alors que  $b$  est un  $S'$ -entier et que  $L/K$  n’est pas ramifiée en dehors de  $S'$ . Cet argument s’inspire directement du cas des courbes hyperelliptiques traité par Oort [1974]. Il se base principalement sur le fait que les points de ramification de  $\pi$  (dans  $C$ ) correspondent à des points de  $p$ -torsion (dans  $\text{Jac } C$ ) et que cette  $p$ -torsion s’étend en un schéma étale au-dessus de  $\text{Spec } \mathcal{O}_{S'}$  (voir partie 2).

Comme  $K(b) = K(1 - b) = K(b^{-1})$ , ce qui précède fait en réalité de  $(1 - b, b)$  un couple de  $S'$ -unités satisfaisant l’équation  $x + y = 1$ . Cette équation aux  $S'$ -unités a été largement étudiée et l’on sait grâce à la théorie des formes linéaires de logarithmes borner la hauteur des solutions. De manière précise, nous employons ici une majoration explicite due à Györy et Yu [2006]. Elle fait apparaître le régulateur de  $L$  que nous majorons à l’aide du discriminant  $\Delta_{L/\mathbb{Q}}$  (résultat de Lenstra [1992]) puis nous contrôlons celui-ci en fonction de  $\Delta$  et  $\Omega$  en utilisant le fait que  $L/K$  n’est ramifiée qu’aux places de  $S'$ . Tout ceci conduit à  $h(b) \leq \Delta_S^{(8g)^5}$  (voir partie 3).

Pour la dernière étape, nous travaillons uniquement sur  $\bar{K}$ . Nous pouvons alors opérer un automorphisme de  $\mathbb{P}^1$  de sorte que  $0, 1$  et  $\infty$  soient des points de branchement de  $\pi$ . Les  $r - 3$  autres se retrouvent alors être parmi les birapports que nous avons étudiés et dont nous avons borné la hauteur. Maintenant, comme le corps de fonctions de  $C_{\bar{K}}$  est une extension de Kummer de  $\bar{K}(X)$ , nous voyons que notre courbe admet un modèle plan (singulier) d’équation affine  $Y^p = \prod_{i=1}^{r-1} (X - b_i)^{a_i}$  où  $1 \leq a_i \leq p - 1$  et les  $b_i$  sont les abscisses des points de branchement différents de  $\infty$ . Comme  $h(b_i) \leq \Delta_S^{(8g)^5}$ , on majore immédiatement la hauteur (naïve) de cette équation. Les résultats de [Rémond 2010] permettent alors de contrôler un plongement de  $C$  dans  $\mathbb{P}_{\bar{K}}^3$  puis la hauteur thêta de  $\text{Jac } C$ . Finalement, une comparaison due à Bost et David (voir [Pazuki 2012]) fait le lien avec la hauteur de Faltings (voir partie 4).

## 2. Bonne réduction

Nous nous plaçons sous les hypothèses du théorème 1.2. Notons  $p = \deg \pi$  et  $\sigma : C_{\bar{K}} \rightarrow C_{\bar{K}}$  un générateur du groupe de Galois de  $\pi_{\bar{K}}$ . Si  $Q_1, \dots, Q_r$  sont les

points de ramification de  $\pi$  (dans  $C(\overline{K})$ ), nous écrivons  $P_i = \pi(Q_i)$  les points de branchement correspondants. Ils sont deux à deux distincts puisque  $\pi^{-1}(P_i)$  est un ensemble de cardinal  $< p$  sur lequel  $\sigma$  (d'ordre  $p$ ) agit transitivement donc un singleton. Ceci revient à dire que l'indice de ramification de chaque  $Q_i$  vaut  $p$  et la formule d'Hurwitz donne donc

$$2g - 2 = -2p + r(p - 1) \iff 2g = (r - 2)(p - 1).$$

Nous excluons le cas où  $g = 0$  (puisque  $\text{Jac } C = 0$  on a  $h_{\text{Falt}}(C) = 0$  et le théorème est trivial) donc la relation précédente fournit  $3 \leq r \leq 2g + 2$  et  $2 \leq p \leq 2g + 1$ .

Nous utilisons quelques faits élémentaires (et classiques) sur le birapport. Le birapport de quatre éléments distincts  $a, b, c, d$  d'un corps  $k$  s'écrit

$$\text{Bir}(a, b, c, d) = \frac{c-a}{c-b} \cdot \frac{d-b}{d-a}.$$

On l'étend immédiatement aux points distincts de  $\mathbb{P}^1(k) = k \cup \{\infty\}$  (par exemple  $\text{Bir}(\infty, b, c, d) = (d-b)/(c-b)$ ). On obtient toujours un élément de  $k \setminus \{0, 1\}$ . En particulier  $\text{Bir}(\infty, 0, 1, x) = x$  pour tout  $x \in k \setminus \{0, 1\}$ . On vérifie aussi facilement que le birapport est invariant par un automorphisme de  $\mathbb{P}^1$ . On a encore

$$\text{Bir}(a, b, d, c) = \text{Bir}(a, b, c, d)^{-1} \quad \text{et} \quad \text{Bir}(a, c, b, d) = 1 - \text{Bir}(a, b, c, d).$$

Enfin

$$\text{Bir}(a, b, c, d) = \text{Bir}(b, a, d, c) = \text{Bir}(c, d, a, b) = \text{Bir}(d, c, b, a),$$

ce qui entraîne que les 24 birapports formés en permutant  $a, b, c, d$  prennent au plus 6 valeurs.

Nous formons l'ensemble des birapports des points  $P_i$  de  $\mathbb{P}^1(\overline{K})$  :

$$\mathcal{B} = \{\text{Bir}(P_i, P_j, P_k, P_\ell) \mid 1 \leq i, j, k, \ell \leq r \text{ deux à deux distincts}\}.$$

Par ce qui précède,  $\text{Card } \mathcal{B} \leq 6 \binom{r}{4}$  et  $\mathcal{B}$  est stable par les involutions  $x \mapsto x^{-1}$  et  $x \mapsto 1 - x$ . De plus, comme  $\pi$  est défini sur  $K$ , l'ensemble  $\{P_1, \dots, P_r\}$  est stable sous l'action de  $\text{Gal}(\overline{K}/K)$  et il en va donc de même de  $\mathcal{B}$ . En particulier tout élément de  $\mathcal{B}$  est de degré au plus  $6 \binom{r}{4}$ . Bien entendu, si  $r = 3$ , l'ensemble  $\mathcal{B}$  est vide et l'on peut passer directement à la partie 4.

Pour toute extension finie  $L$  de  $K$  on note  $S_L$  l'ensemble des places de  $L$  qui divisent une place de  $S$  ou  $p$ . L'objectif de cette partie consiste à montrer l'énoncé suivant.

**Proposition 2.1.** *Pour tout  $b \in \mathcal{B}$ , l'extension  $K(b)/K$  est non ramifiée en dehors de  $S_{K(b)}$  et  $b$  est un  $S_{K(b)}$ -entier.*

Bien entendu, pour établir ceci, nous pouvons nous contenter d'exhiber une extension  $K'$  de  $K$  non ramifiée en dehors de  $S_{K'}$ , contenant  $b$  comme  $S_{K'}$ -entier.

C'est ce que nous faisons en choisissant pour  $K'$  la plus petite extension de  $K$  sur laquelle tous les points  $Q_i$  sont rationnels. Vu la définition, nous avons bien  $\mathcal{B} \subset K'$ . Fixons ensuite une place finie  $v' \notin S_{K'}$  de  $K'$ ; notons  $\mathbb{O}_{v'}$  son anneau de valuation,  $v = v'|_K$  et  $\mathbb{O}_v = \mathbb{O}_{v'} \cap K$ . Pour conclure, il nous suffit de montrer sous ces hypothèses que  $\mathbb{O}_{v'}/\mathbb{O}_v$  n'est pas ramifiée et  $\mathcal{B} \subset \mathbb{O}_{v'}$ . Ces deux propriétés vont résulter de l'étude de différents modèles sur  $\mathbb{O}_v$  et  $\mathbb{O}_{v'}$  que nous introduisons maintenant.

Tout d'abord, puisque  $v \notin S$ , la courbe  $C \rightarrow \text{Spec } K$  s'étend en un morphisme projectif lisse  $\mathcal{C} \rightarrow \text{Spec } \mathbb{O}_v$ . De plus le lieu de ramification de  $\pi$  est un sous- $K$ -schéma  $Y$  de  $C$  et nous considérons son adhérence  $\mathcal{Y} \subset \mathcal{C}$  (sous-schémas fermés réduits). Nous notons ensuite  $C', Y', \mathcal{C}', \mathcal{Y}'$  l'extension de ces objets à  $K'$  ou  $\mathbb{O}_{v'}$ . Par définition de  $K'$ , le schéma  $Y' \simeq \text{Spec } (K')'$  est l'union des points rationnels  $Q_1, \dots, Q_r$ . Écrivons encore  $J'$  la jacobienne de  $C'$  et  $\mathcal{J}'$  son modèle de Néron sur  $\mathbb{O}_{v'}$ . Nous plongeons  $C'$  dans  $J'$  à l'aide du point rationnel  $Q_1$  (application  $Q \mapsto (Q) - (Q_1)$ ) et ce morphisme  $C' \rightarrow J'$  s'étend de manière unique en  $\mathcal{C}' \rightarrow \mathcal{J}'$  par la propriété de Néron.

Nous pouvons alors énoncer le lemme-clef de cette partie (comparer avec les arguments de Oort [1974], lemmes 2.1 et 2.2, dans le cas hyperelliptique).

**Lemme 2.1.** *Le morphisme  $\mathcal{Y}' \rightarrow \text{Spec } \mathbb{O}_{v'}$  est étale.*

*Démonstration.* Nous avons  $\pi^*(P_i) = p(Q_i)$  en termes de diviseurs sur  $C'$  donc  $p(Q_i) \equiv p(Q_j)$  pour  $1 \leq i, j \leq r$ . Par suite  $p((Q_i) - (Q_1)) = 0$  dans  $J'$  pour  $1 \leq i \leq r$  et ceci signifie exactement que  $Y' \rightarrow C' \rightarrow J'$  se factorise à travers le sous-schéma  $J'_p$ , noyau de la multiplication par  $p$  dans  $J'$ . Comme  $Y'$  et  $J'_p$  sont discrets et réduits, l'immersion  $a: Y' \rightarrow J'_p$  est à la fois ouverte et fermée. Maintenant l'hypothèse  $v' \notin S_{K'}$  assure que le corps résiduel de  $\mathbb{O}_{v'}$  n'est pas de caractéristique  $p$  donc  $\mathcal{J}'_p$  est étale sur  $\mathbb{O}_{v'}$ . En particulier, chaque composante connexe de  $\mathcal{J}'_p$  est intègre et coïncide donc avec l'adhérence (dans  $\mathcal{J}'$ ) d'un point de  $J'_p$ . Ainsi  $a$  s'étend en une immersion ouverte et fermée  $\mathcal{Y}' \rightarrow \mathcal{J}'_p$  (si  $\mathcal{X}'$  est une composante connexe de  $\mathcal{J}'_p$ , les seuls sous-schémas fermés de  $\mathcal{X}'$  qui induisent un sous-schéma ouvert sur la fibre générique sont  $\emptyset$  et  $\mathcal{X}'$ ). Une immersion ouverte étant étale, il en va de même de  $\mathcal{Y}'$ . □

Nous pouvons d'ores et déjà déduire de ce lemme la propriété de non-ramification. En effet, il entraîne que  $\mathcal{Y}$  est étale sur  $\text{Spec } \mathbb{O}_v$  et ceci signifie exactement que, dans chacun des corps résiduels des points de  $Y$ , la place  $v$  ne se ramifie pas. Or, par définition,  $K'$  est le compositum de ces corps donc  $\mathbb{O}_{v'}/\mathbb{O}_v$  est effectivement non ramifiée.

Soit maintenant  $K''$  une extension finie de  $K'$  sur laquelle l'automorphisme  $\sigma$  fixé plus haut est défini. Soit  $v''$  une place de  $K''$  au-dessus de  $v'$ . Nous notons  $C'', J'', \mathcal{C}'', \mathcal{Y}''$  et  $\mathcal{J}''$  les extensions de  $C', J', \mathcal{C}', \mathcal{Y}'$  et  $\mathcal{J}'$  à  $K''$  ou  $\mathbb{O}_{v''}$ . Nous notons

par la même lettre l'automorphisme  $\sigma : C'' \rightarrow C''$  et son extension en un automorphisme  $J''$  puis de  $\mathcal{F}''$  (par propriété de Néron) et enfin de  $\mathcal{C}''$  (par restriction à l'adhérence de  $C''$  dans  $\mathcal{F}''$ ). Bien entendu, à chaque étape,  $\sigma$  vérifie  $\sigma^p = \text{id}$ . Notons  $G$  le groupe d'automorphismes de  $\mathcal{C}''$  engendré par  $\sigma$ .

**Lemme 2.2.** *Le quotient  $\mathcal{C}''/G$  existe et est isomorphe à  $\mathbb{P}_{\mathbb{C}_v''}^1$ .*

*Démonstration.* Pour l'existence, d'après le théorème 4.12 de [Lønsted et Kleiman 1979], il suffit de vérifier que  $G$  agit fidèlement sur la fibre spéciale de  $\mathcal{C}''$ . Si ce n'était pas le cas,  $\sigma$  induirait l'identité sur cette fibre spéciale  $\mathcal{C}''_s$  donc également sur celle de  $\mathcal{F}''$  notée  $\mathcal{F}''_s$ . Ceci est absurde car pour un schéma abélien l'application de restriction  $\text{End } \mathcal{F}'' \rightarrow \text{End } \mathcal{F}''_s$  est toujours injective (voir [Lang 1983] page 45). Notons donc  $\mathcal{P} = \mathcal{C}''/G$  ce quotient et  $\mathcal{P}_s$  sa fibre spéciale qui est une courbe lisse de genre  $g'$ . Le revêtement  $\mathcal{C}''_s \rightarrow \mathcal{P}_s$  de groupe  $G$  a au moins  $r$  points de ramification : ceux de la fibre spéciale du schéma  $\mathcal{Y}''$ . Par suite la formule d'Hurwitz (il n'y a pas de ramification sauvage) donne

$$2g - 2 = p(2g' - 2) + r'(p - 1) \iff 2pg' + (r' - r)(p - 1) = 0$$

où  $r' \geq r$  est le nombre de points de ramification. On conclut  $r' = r$  et  $g' = 0$ . Ainsi  $\mathcal{P}$  est une famille de courbes de genre 0 et elle admet une section : il suffit de considérer un point de branchement (en d'autres termes la composée d'une section de  $\mathcal{Y}''$  avec  $\mathcal{Y}'' \rightarrow \mathcal{C}'' \rightarrow \mathcal{P}$ ). La proposition 3.3 de [Lønsted et Kleiman 1979] assure alors que  $\mathcal{P} \simeq \mathbb{P}(\mathcal{E})$  pour un faisceau localement libre  $\mathcal{E}$  de rang 2 sur  $\text{Spec } \mathbb{C}_v''$ . Par primalité de  $\mathbb{C}_v''$ , ce faisceau  $\mathcal{E}$  est libre donc  $\mathcal{P} \simeq \mathbb{P}_{\mathbb{C}_v''}^1$ .  $\square$

Nous déduisons facilement  $\mathcal{B} \subset \mathbb{C}_v''$  de cet énoncé. Il fournit en effet un morphisme  $\mathcal{C}'' \rightarrow \mathbb{P}_{\mathbb{C}_v''}^1$  dont la fibre générique coïncide avec l'extension de  $\pi$  à  $K''$  modulo un automorphisme de  $\mathbb{P}_{K''}^1$ . Comme un tel automorphisme ne modifie pas l'ensemble  $\mathcal{B}$ , nous pouvons considérer que  $P_1, \dots, P_r$  sont les points de branchement de ce morphisme. Quitte à faire un automorphisme de  $\mathbb{P}_{\mathbb{C}_v''}^1$  nous supposons même  $P_1 = \infty$ . Comme les points de branchement sont toujours distincts dans la fibre spéciale (cela vient encore de ce que  $\mathcal{Y}''$  est étale et fixé par  $\sigma$ ), nous en déduisons que  $P_i = (e_i : 1)$  où  $e_i \in \mathbb{C}_v''$ ,  $i \geq 2$  (car  $P_1 = \infty = (1 : 0)$ ) puis  $e_i - e_j \in \mathbb{C}_v''^\times$  si  $2 \leq i < j$ . Alors chaque élément de  $\mathcal{B}$  s'écrit

$$\frac{e_i - e_k}{e_i - e_j} \quad \text{ou} \quad \frac{e_i - e_k}{e_i - e_j} \cdot \frac{e_\ell - e_j}{e_\ell - e_k}$$

(selon que  $P_1$  apparaît ou non) avec  $i \neq j$  et  $k \neq \ell$ . Ceci entraîne clairement  $\mathcal{B} \subset \mathbb{C}_v''$  puis  $\mathcal{B} \subset \mathbb{C}_v'' \cap K' = \mathbb{C}_v'$  et termine donc la démonstration de la proposition 2.1.

### 3. $S$ -unités, régulateurs et discriminants

L'objectif de cette partie est d'établir la majoration suivante de la hauteur des éléments de  $\mathcal{B}$ .

**Proposition 3.1.** *Pour tout  $b \in \mathcal{B}$ , on a  $h(b) \leq \Delta_S^{(8g)^5}$ .*

Nous fixons donc un élément  $b$  de  $\mathcal{B}$  et notons  $L = K(b)$  ainsi que  $S' = S_L$ . Nous désignons par  $d$ ,  $R$  et  $h$  le degré de  $L$  (sur  $\mathbb{Q}$ ), son régulateur et son nombre de classes. En vue d'appliquer le résultat de Győry et Yu [2006] nous écrivons encore  $s$  pour le cardinal de  $S' \cup \{\text{places infinies}\}$ ,  $R_{S'}$  pour le  $S'$ -régulateur de  $L$  et  $P$  pour le maximum des  $N_{L/\mathbb{Q}}(\mathfrak{p})$ ,  $\mathfrak{p} \in S'$ . Nous abrégeons aussi  $\log^* x = \max(1, \log x)$  pour  $x > 0$ .

**Lemme 3.1.** *La hauteur de  $b$  est au plus*

$$2^{15} (16sd)^{2s+4} P R_{S'} (1 + \log^* R_{S'} / \log^* P).$$

*Démonstration.* Nous appliquons la proposition 2.1 aux quatre éléments  $b$ ,  $b^{-1}$ ,  $1 - b$  et  $(1 - b)^{-1}$  de  $\mathcal{B}$ . Ce sont donc des  $S'$ -entiers et donc des  $S'$ -unités. Le couple  $(b, 1 - b)$  appartient à  $\{(x, y) \in (\mathbb{O}_{S'}^\times)^2 \mid x + y = 1\}$  donc nous pouvons lui appliquer le théorème principal de [Győry et Yu 2006] avec  $\alpha = \beta = 1$  et  $H = 4$ . Nous obtenons alors la borne de l'énoncé en majorant  $\log(2s) \leq \sqrt{2s}$  et  $\log^*(2d) \leq \sqrt{2d}$  puis  $7s + 29 \leq 8s + 27$  dans l'exposant de 2.  $\square$

Nous estimons maintenant les quantités apparaissant dans cette formule. Notons  $E$  un majorant de  $[L : K]$ . Nous choisissons  $E \geq 2$  pour simplifier les calculs (*in fine* nous majorerons  $E$  par  $6\binom{r}{4}$ ). On pose  $u = E\Omega / \log 2$ .

Nous avons facilement  $d \leq ED \leq u$  et

$$s \leq 2ED + \sum_{\mathfrak{p} \in S} E \leq 2ED + \sum_{\mathfrak{p} \in S} E \frac{\log N_{K/\mathbb{Q}}(\mathfrak{p})}{\log 2} = u$$

car il y a au plus  $ED$  places au-dessus de  $p$ ,  $ED$  au-dessus de  $\infty$  et  $E$  au-dessus de chaque place de  $S$ . De manière analogue,  $P \leq \max(p^{ED}, 2^u)$ . Pour le  $S'$ -régulateur, nous avons

$$R_{S'} \leq hR \prod_{\mathfrak{p}' \in S'} \log N_{L/\mathbb{Q}}(\mathfrak{p}') \leq hR(\log P)^s$$

où la première inégalité vient du lemme 3 de [Bugeaud et Győry 1996]. Pour majorer  $hR$ , nous employons une estimation de Lenstra [1992, théorème 6.5]. Elle entraîne

$$hR \leq |\Delta_{L/\mathbb{Q}}|^{1/2} (\log^* |\Delta_{L/\mathbb{Q}}|)^{ED-1}.$$

La forme faible  $hR \leq |\Delta_{L/\mathbb{Q}}|^{ED/2}$  permet de majorer

$$1 + \frac{\log^* R_{S'}}{\log^* P} \leq 1 + \log^*(|\Delta_{L/\mathbb{Q}}|^{ED/2}) + s \frac{\log^* \log^* P}{\log^* P} \leq 2u \log^* |\Delta_{L/\mathbb{Q}}|.$$

En rassemblant les différents termes, il vient

$$h(b) \leq 2^{16} u (4u)^{4u+8} P (\log P)^u |\Delta_{L/\mathbb{Q}}|^{1/2} (\log^* |\Delta_{L/\mathbb{Q}}|)^{ED}.$$

Nous faisons alors intervenir  $P \leq p^u$ ,  $\log P \leq pu$  et si  $x \geq 1$

$$(\log^* x)^{ED} \leq (ED)^{ED} x^{1/2}$$

(écrire  $\log y \leq \sqrt{y}$  pour  $y = x^{1/ED}$ ). Nous aboutissons à

$$h(b) \leq 2^{16} u (4u)^{4u+8} p^{2u} u^{2u} |\Delta_{L/\mathbb{Q}}|$$

puis, en tirant parti de  $u \geq 4$ , à

$$h(b) \leq (4u)^{9u} p^{2u} |\Delta_{L/\mathbb{Q}}|.$$

Pour majorer le discriminant de  $L$ , nous devons faire intervenir le fait que  $L/K$  est non ramifiée en dehors de  $S'$  (proposition 2.1). Notons pour cela  $\mathfrak{Q}$  l'ensemble des caractéristiques résiduelles des places de  $S'$ . Un résultat de Serre [1981, proposition 4', page 129] s'écrit avec les présentes notations :

$$\log |\Delta_{L/\mathbb{Q}}| \leq E \log \Delta + D(E-1) \sum_{\ell \in \mathfrak{Q}} \log \ell + (\text{Card } \mathfrak{Q}) ED \log E.$$

Ici  $\text{Card } \mathfrak{Q} \leq \sum_{\ell \in \mathfrak{Q}} \log \ell + 1 \leq \Omega + \log p$  et donc

$$\log |\Delta_{L/\mathbb{Q}}| \leq E \log \Delta + 2ED(\Omega + \log p) \log E.$$

Nous majorons ensuite (quelque peu brutalement)  $D$  par  $\Omega$  dans cette formule,  $u$  par  $3E\Omega/2$  et  $\Omega \log \Omega$  par  $\Omega^2$  pour obtenir

$$\begin{aligned} \log h(b) &\leq 14E\Omega \log 6E + 14E\Omega^2 + 3E\Omega \log p \\ &\quad + E \log \Delta + 2E\Omega^2 \log E + 2E\Omega (\log p) (\log E) \\ &\leq 63E\Omega^2 (\log^* p) (\log^* E) + E \log \Delta \\ &\leq 2^6 E (\log \Delta_S) (\log^* p) (\log^* E). \end{aligned}$$

Pour terminer la preuve de la proposition 3.1, nous vérifions (élémentairement)

$$2^6 E (\log^* p) (\log^* E) \leq (8g)^5$$

à l'aide de  $E \leq 6\binom{r}{4}$ ,  $r \leq 2g+2$  et  $p \leq 2g+1$ .

### 4. Hauteur de la courbe

Dans cette dernière partie, nous oublions entièrement le corps  $K$  pour ne travailler que sur  $\bar{K}$ . Aussi utilisons-nous les notations  $\pi : C \rightarrow \mathbb{P}^1$  pour désigner l'extension des objets précédents. Quitte à composer  $\pi$  avec un automorphisme de  $\mathbb{P}^1$ , nous supposons que  $0, 1$  et  $\infty$  font partie des  $r \geq 3$  points de branchement. Par suite, les  $r - 3$  autres appartiennent à l'ensemble  $\mathcal{B}$ . Nous notons aussi  $H \geq 1$  la borne que nous avons obtenue pour la hauteur des éléments de  $\mathcal{B}$  (voir proposition 3.1).

Le corps des fonctions de  $C$  est une extension galoisienne de  $\bar{K}(X)$  (corps des fonctions de  $\mathbb{P}^1$ ) de groupe  $\mathbb{Z}/p\mathbb{Z}$ . Comme  $\bar{K}(X)$  contient les racines  $p$ -ièmes de l'unité, il s'agit d'une extension de Kummer et donc il existe une fraction rationnelle non nulle  $F \in \bar{K}(X)$  telle que le corps des fonctions de  $C$  soit isomorphe à

$$\bar{K}(X)[Y]/(Y^p - F(X)).$$

Bien entendu, nous pouvons modifier dans cette assertion  $F$  par une puissance  $p$ -ième ce qui permet de supposer que  $F$  est un polynôme unitaire dont toutes les racines sont de multiplicité au plus  $p - 1$ . Écrivons

$$F(X) = \prod_{i=1}^t (X - b_i)^{a_i}$$

où  $b_i \in \bar{K}$  et  $1 \leq a_i \leq p - 1$ . Notre courbe  $C$  est l'unique courbe projective lisse birationnelle à la courbe affine  $C_0$  d'équation  $Y^p = F(X)$  et  $\pi$  se factorise à travers  $C_0 \rightarrow \mathbb{A}^1, (X, Y) \mapsto X$ . Ceci entraîne immédiatement que les points de branchement de  $\pi$  sont contenus dans  $\{b_1, \dots, b_t, \infty\}$ . Réciproquement chaque  $b_i$  correspond à un point de branchement car il est l'image d'un unique point de la normalisée de  $C_0$  (localement pour la topologie étale  $C_0$  est isomorphe à la courbe  $Y^p = X^{a_i}$  dont la normalisée est  $\mathbb{A}^1$ ). Par conséquent  $b_i \in \mathcal{B} \cup \{0, 1\}$  et donc  $h(b_i) \leq H$ . Ceci montre aussi  $t = r - 1$ .

Notons à présent  $G$  le polynôme  $Y^p - F(X)$  de  $\bar{K}[X, Y]$ . Nous estimons son degré

$$\deg G \leq \max(p, (r - 1)(p - 1)) \leq 2(r - 2)(p - 1) = 4g$$

et sa hauteur naïve (celle du point projectif formé par ses coefficients, voir [Rémond 2010])

$$h_\infty(G) = h_\infty(F) \leq (\deg F) \log 2 + \sum_{i=1}^{r-1} a_i h(b_i) \leq 7gH.$$

Par conséquent, le théorème 1.5 de [ibid.] affirme qu'il existe un plongement de  $C$  dans  $\mathbb{P}_{\bar{K}}^3$  de degré au plus  $8g(2g - 1)$  et de hauteur (au sens de la hauteur

projective d'un fermé de  $\mathbb{P}^3$ )

$$h(C) \leq (4g)^{(4g)^3-5} (42gH + 9(4g)^2) \leq (4g)^{(4g)^3} H - 1.$$

Nous pouvons ensuite passer à la hauteur thêta de la jacobienne de  $C$  grâce au théorème 1.3 de [Rémond 2010]. L'entier  $m$  y apparaissant est majoré par

$$4g - 2 + 16g(2g - 1) \leq 32g^2$$

de sorte que, en écrivant  $h_\theta = h_\theta^{(4)}(\text{Jac } C, \Theta_{\text{sym}})$  la hauteur thêta associée au plongement thêta donné par le diviseur  $16\Theta_{\text{sym}}$  (voir encore [ibid.]), nous avons

$$h_\theta \leq (32g^2)^{640g^2 8^g + 32g^3} H \leq 2^{3360 \cdot g^3 8^g} H$$

(en utilisant  $32g^2 \leq 2^{5g}$ ). Le résultat de [Pazuki 2012] compare  $h_\theta$  (correspondant à  $r = 4$  dans cet article) et la hauteur de Faltings stable :

$$h_{\text{Falt}}(C) \leq 2h_\theta + 2C_1 \log(2 + \max(1, h_\theta))$$

pour une constante  $C_1$  dont on vérifie facilement qu'elle satisfait  $2^{4g} \leq C_1 \leq 2^{10g}$ . En particulier, si  $h_\theta \leq \mathcal{H}$  et  $\mathcal{H} \geq C_1^2$  alors  $h_{\text{Falt}}(C) \leq 4\mathcal{H}$ . Ceci est très largement vérifié pour  $\mathcal{H} = 2^{3360 \cdot g^3 8^g} H$ . On en déduit  $h_{\text{Falt}}(C) \leq 2^{3362 \cdot g^3 8^g} H$ . Une élémentaire étude de fonction donne  $g^3 8^g \leq 823 \cdot 9^g$  et, comme  $3362 \cdot 823 \leq 2^{22}$ , cela termine la démonstration du théorème 1.2.

**Remarque.** Nous avons établi une majoration de la forme  $h_{\text{Falt}}(C) \leq c(g)H$  pour une valeur explicite de  $c(g)$ . Cette dernière ne prétend aucunement être optimale et peut très certainement être améliorée. Une méthode pourrait être de raffiner la preuve de [Rémond 2010] dans le cas d'un polynôme particulier comme  $G$ . Une autre approche consisterait à travailler plus directement avec la hauteur de Faltings, par exemple en essayant d'explicitier une base des formes différentielles globales sur notre courbe.

## Remerciements

Nous remercions chaleureusement Bjorn Poonen pour ses commentaires sur une première version de ce texte.

## Bibliographie

- [Bugeaud et Györy 1996] Y. Bugeaud et K. Györy, "Bounds for the solutions of unit equations", *Acta Arith.* **74** :1 (1996), 67–80. MR 97b :11045 Zbl 0861.11023
- [Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73** :3 (1983), 349–366. MR 85g :11026a Zbl 0588.14026
- [González Díez 1991] G. González Díez, "Loci of curves which are prime Galois coverings of  $\mathbf{P}^1$ ", *Proc. London Math. Soc.* (3) **62** :3 (1991), 469–489. MR 92c :14021 Zbl 0679.14010



- [Győry et Yu 2006] K. Győry et K. Yu, “Bounds for the solutions of  $S$ -unit equations and decomposable form equations”, *Acta Arith.* **123** :1 (2006), 9–41. MR 2007d :11032 Zbl 1163.11026
- [Lang 1983] S. Lang, *Complex multiplication*, Grundlehren Math. Wiss. **255**, Springer, New York, 1983. MR 85f :11042 Zbl 0536.14029
- [Lenstra 1992] H. W. Lenstra, Jr., “Algorithms in algebraic number theory”, *Bull. Amer. Math. Soc. (N.S.)* **26** :2 (1992), 211–244. MR 93g :11131 Zbl 0759.11046
- [Lønsted et Kleiman 1979] K. Lønsted et S. L. Kleiman, “Basics on families of hyperelliptic curves”, *Compositio Math.* **38** :1 (1979), 83–111. MR 80g :14028 Zbl 0406.14017
- [Oort 1974] F. Oort, “Hyperelliptic curves over number fields”, pp. 211–218 dans *Classification of algebraic varieties and compact complex manifolds*, édité par H. Popp, Lecture Notes in Math. **412**, Springer, Berlin, 1974. MR 50 #7154 Zbl 0299.14017
- [Pazuki 2012] F. Pazuki, “Theta height and Faltings height”, *Bull. Soc. Math. France* **140** :1 (2012), 19–49. Zbl 06032258
- [Rémond 1999] G. Rémond, “Hauteurs thêta et construction de Kodaira”, *J. Number Theory* **78** :2 (1999), 287–311. MR 2000g :11059 Zbl 0947.14016
- [Rémond 2010] G. Rémond, “Nombre de points rationnels des courbes”, *Proc. Lond. Math. Soc.* (3) **101** :3 (2010), 759–794. MR 2011k :11088 Zbl 1210.11073
- [Serre 1981] J.-P. Serre, “Quelques applications du théorème de densité de Chebotarev”, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401. MR 83k :12011 Zbl 0496.12011
- [Shafarevitch 1963] I. R. Shafarevitch, “Поля алгебраических чисел”, pp. 163–176 dans *Proc. Internat. Congr. Mathematicians* (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963. Traduction anglaise : “Algebraic number fields”, dans *Amer. Math. Soc. Transl.* **231** (1963), 25–39. MR 34 #2569 Zbl 0126.06902

Communicated by Hendrik W. Lenstra

Received 2011-01-06    Revised 2011-03-07    Accepted 2011-03-07

rdejong@math.leidenuniv.nl    *Mathematisch Instituut, Universiteit Leiden, PO Box 9512,  
2300 RA Leiden, Netherlands*

Gael.Remond@ujf-grenoble.fr    *Institut Fourier, UMR 5582, Université Grenoble I, BP 74,  
38402 Saint-Martin-d'Hères Cedex, France*



## 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 L<sup>A</sup>T<sub>E</sub>X but submissions in other varieties of T<sub>E</sub>X, 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 BibT<sub>E</sub>X 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@msp.org](mailto:graphics@msp.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 5    No. 8    2011

---

The behavior of Hecke $L$ -functions of real quadratic fields at $s = 0$ BYUNGHEUP JUN and JUNGYUN LEE	1001
The Picard group of a $K3$ surface and its reduction modulo $p$ ANDREAS-STEPHAN ELSENHANS and JÖRG JAHNEL	1027
Linear determinantal equations for all projective schemes JESSICA SIDMAN and GREGORY G. SMITH	1041
Involutions, weights and $p$ -local structure GEOFFREY R. ROBINSON	1063
Parametrizing quartic algebras over an arbitrary base MELANIE MATCHETT WOOD	1069
Coleman maps and the $p$ -adic regulator ANTONIO LEI, DAVID LOEFFLER and SARAH LIVIA ZERBES	1095
Conjecture de Shafarevitch effective pour les revêtements cycliques ROBIN DE JONG and GAËL RÉMOND	1133



1937-0652(2011)5:8;1-9