Algebra & Number Theory

Volume 4
2010
No. 5

mathematical sciences publishers

Algebra & Number Theory

www.jant.org

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

The subscription price for 2010 is US $140/year for the electronic version, and $200/year (+$30 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™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://www.mathscipub.org

A NON-PROFIT CORPORATION

Typeset in LaTeX

ALGEBRA AND NUMBER THEORY 4:5(2010)

On the Spiegelungssatz for the 4-rank

Étienne Fouvry and Jürgen Klüners

Let d be a nonsquare positive integer. We give the value of the natural probability that the narrow ideal class groups of the quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-d})$ have the same 4-ranks.

1. Introduction

Conventions and notations. Throughout this work, the letter D is reserved for the number 1 or a fundamental discriminant, that is, the discriminant of a linear or quadratic extension of $\mathbb{Q}$. Let $K = \mathbb{Q}(\sqrt{D})$. On the set of nonzero fractional ideals of the ring of integers of K we say that two fractional ideals $\mathfrak{I}$ and $\mathfrak{J}$ are *equivalent in the narrow sense*, if there is an element $a \in K$, such that $\mathfrak{I} = (a)\mathfrak{J}$ and a has positive norm. By the multiplication of the ideal classes, we obtain the *(narrow) class group of* K, that we denote by C_D. This is a finite abelian group.

We extend this definition of C_D in the following way: if d is a nonsquare integer, not necessarily a fundamental discriminant, we also denote by C_d the class group of the quadratic field $\mathbb{Q}(\sqrt{d})$. When d is a nonzero perfect square, we define $\mathrm{C}_d = \mathrm{C}_1$ to be the trivial group.

We reserve the letter p for prime numbers. For positive integers n we denote by $\omega(n)$ the number of distinct prime divisors of n.

If A is a finite multiplicative abelian group and p is a prime number, the *p-rank* is, by definition, $\mathrm{rk}_p(A) := \dim_{\mathbb{F}_p}(A/A^p)$. More generally, if k is an integer ≥ 1, we define the *p^k-rank* of A by $\mathrm{rk}_{p^k}(A) := \dim_{\mathbb{F}_p}(A^{p^{k-1}}/A^{p^k})$.

Scholz's Theorem. The original *Spiegelungssatz* concerned the 3-rank of C_D and was proved by Scholz [1932] in the form of the double inequality

$$\mathrm{rk}_3(\mathrm{C}_d) \leq \mathrm{rk}_3(\mathrm{C}_{-3d}) \leq \mathrm{rk}_3(\mathrm{C}_d) + 1 \tag{1}$$

for any nonsquare $d \geq 1$. With the convention above, it is straightforward to extend (1) to any $d \geq 1$, since the group C_{-3} is trivial.

Hence, when $d \geq 1$ is given, the integer $\mathrm{rk}_3(\mathrm{C}_{-3d})$ can only take two values: $\mathrm{rk}_3(\mathrm{C}_d)$ or $\mathrm{rk}_3(\mathrm{C}_d) + 1$. Each of these possibilities is well described in algebraic

MSC2000: primary 11R29; secondary 11R11.
Keywords: quadratic fields, class groups, reflection principle.

terms. But the natural question is to know the frequency of each of these events. Dutarte [1984], further pushing the probabilistic model leading to the heuristics of Cohen–Lenstra [1984], proposed a value of the second frequency, namely:

Conjecture 1.1 [Dutarte 1984, Formula 3, p. 8] . *For every integer $r \geq 0$ we have*

$$\lim_{X\to+\infty} \frac{\sharp\big\{D : 0 \leq D \leq X,\ \mathrm{rk}_3(\mathrm{C}_D) = r,\ \mathrm{rk}_3(\mathrm{C}_{-3D}) = r+1\big\}}{\sharp\big\{D : 0 \leq D \leq X,\ \mathrm{rk}_3(\mathrm{C}_D) = r\big\}} = 3^{-(r+1)}. \tag{2}$$

This conjectural equality can be seen as a conditional probability under the following convention: Let $\mathscr{A}$ be a subset of the set $\mathscr{D}^+$ of positive fundamental discriminants D. We define the probability of the event $D \in \mathscr{A}$ as being equal to the following limit, if it exists:

$$\mathrm{Prob}^+(\mathscr{A}) := \lim_{X\to+\infty} \Big(\sum_{\substack{0<D\leq X\\ D\in\mathscr{A}}} 1 \Big/ \sum_{0<D\leq X} 1 \Big). \tag{3}$$

In an analogous way we define Prob^- to be the natural density within the set $\mathscr{D}^-$ of negative fundamental discriminants.

We now formulate in this notation certain statements of the Cohen–Lenstra heuristics [1984, C5 and C9, pp. 56–57], extended by Gerth to $p = 2$:

Conjecture 1.2. *Let p be prime and $r \geq 0$, and for all $k \in \mathbb{N} \cup \{\infty\}$ and $t > 1$ define*

$$\eta_k(t) := \prod_{j=1}^{k} \big(1 - t^{-j}\big). \tag{4}$$

Then:

(i) $\mathrm{Prob}^-(\{D \in \mathscr{D}^- : \mathrm{rk}_p(\mathrm{C}_D^2) = r\}) = a_p^-(r) := p^{-r^2}\eta_\infty(p)\eta_r(p)^{-2}$.

(ii) $\mathrm{Prob}^+(\{D \in \mathscr{D}^+ : \mathrm{rk}_p(\mathrm{C}_D^2) = r\}) = a_p^+(r) := p^{-r^2-r}\eta_\infty(p)\eta_r(p)^{-1}\eta_{r+1}(p)^{-1}$.

With these definitions, Conjecture 1.1 is just a statement concerning the existence and value of a conditional probability. In other words, Dutarte believes that for any $r \geq 0$ we have the equality

$$\mathrm{Prob}^+\big(\mathrm{rk}_3(\mathrm{C}_{-3D}) = r+1 \text{ and } \mathrm{rk}_3(\mathrm{C}_D) = r \,\big|\, \mathrm{rk}_3(\mathrm{C}_D) = r\big) = 3^{-r-1}. \tag{5}$$

Conjectures 1.1 and 1.2 imply, for every $r \geq 0$, the equalities

$$\mathrm{Prob}^+\big(\mathrm{rk}_3(\mathrm{C}_{-3D}) - 1 = \mathrm{rk}_3(\mathrm{C}_D) = r\big) = 3^{-(r+1)}a_3^+(r), \tag{6}$$

$$\mathrm{Prob}^+\big(\mathrm{rk}_3(\mathrm{C}_{-3D}) = \mathrm{rk}_3(\mathrm{C}_D) = r\big) = \big(1 - 3^{-(r+1)}\big)\, a_3^+(r). \tag{7}$$

Let $\mathscr{D}^+(X)$ be the cardinality of the set $\mathscr{D}^+ \cap [1, X]$, and let R be a fixed parameter. Then summing (6) and (7) for all $0 \leq r \leq R$, we get the two lower bounds

$$\sharp\{D \in \mathcal{D}^+ : D \le X,\ \mathrm{rk}_3(\mathrm{C}_{-3D}) = \mathrm{rk}_3(\mathrm{C}_D) + 1\} \ \ge\ \Big(\sum_{r=0}^{R} 3^{-(r+1)} a_3^+(r) - o_R(1)\Big)\mathcal{D}^+(X),$$

$$\sharp\{D \in \mathcal{D}^+ : D \le X,\ \mathrm{rk}_3(\mathrm{C}_{-3D}) = \mathrm{rk}_3(\mathrm{C}_D)\} \ \ge\ \Big(\sum_{r=0}^{R} (1 - 3^{-(r+1)}) a_3^+(r) - o_R(1)\Big)\mathcal{D}^+(X),$$

where $X \to \infty$. However, since the two sets appearing on the left side of these two inequalities form a partition of $\mathcal{D}^+ \cap [1, X]$, we obtain the double inequality

$$\begin{aligned}\sum_{r=0}^{R} 3^{-(r+1)} a_3^+(r) - o_R(1) \le \frac{\sharp\{D \in \mathcal{D}^+ : D \le X,\ \mathrm{rk}_3(\mathrm{C}_{-3D}) = \mathrm{rk}_3(\mathrm{C}_D) + 1\}}{\mathcal{D}^+(X)} \\ \le 1 - \sum_{r=0}^{R} (1 - 3^{-(r+1)})\, a_3^+(r) + o_R(1). \qquad (8)\end{aligned}$$

The relation

$$\sum_{r=0}^{\infty} a_p^+(r) = 1 \qquad (9)$$

implies the equality

$$\sum_{r=0}^{\infty} 3^{-(r+1)} a_3^+(r) = 1 - \sum_{r=0}^{\infty} (1 - 3^{-(r+1)}) a_3^+(r). \qquad (10)$$

Hence, letting $R \to \infty$ in (8), we obtain the equality

$$\begin{aligned}\mathrm{Prob}^+\big(\mathrm{rk}_3(\mathrm{C}_{-3D}) = \mathrm{rk}_3(\mathrm{C}_D) + 1\big) &= \lim_{R\to\infty} \sum_{r=0}^{R} 3^{-(r+1)} a_3^+(r) \\ &= \eta_\infty(3) \sum_{r=0}^{\infty} 3^{-(r+1)^2}\, \eta_r^{-2}(3)\, (1 - 3^{-(r+1)})^{-1} \qquad (11) \\ &= 0.29765117\ldots.\end{aligned}$$

But this equality is conjectural for the moment. It has been tested on a computer by Dutarte [1984, §4.2]. We ran similar experiments and the constants are close, but not too close. We remark that similar problems occur in experiments when we check proved results for the 4-rank in this way, or when one wishes to test one of the Cohen–Lenstra heuristics. For example, similar problems for experiments occur in [Heath-Brown 1994, p. 336] and in [Stevenhagen 1993]. Usually the problem is that the second expected main term in the asymptotic expansion is close to the main term (see [Roberts 2001] for the case $p = 3$).

As far as we know, the only result concerning the conjectural value (11) is due to Belabas [1999, Theorem 2.1; 2004], who proved the equality

$$\frac{\displaystyle\sum_{\substack{0<D\le X \\ \mathrm{rk}_3(\mathrm{C}_{-3D}) = \mathrm{rk}_3(\mathrm{C}_D)+1}} 3^{\mathrm{rk}_3(\mathrm{C}_D)}}{\displaystyle\sum_{0<D\le X} 3^{\mathrm{rk}_3(\mathrm{C}_D)}} = \tfrac{1}{4} + O\big(\exp(-\tfrac{1}{5}(\log X \log\log X)^{1/2})\big) \qquad (12)$$

as X tends to $+\infty$. This equality can be seen as a weighted version of (11). These weights are chosen in order to easily apply the seminal work of Davenport and Heilbronn [1971] concerning the average behavior of the 3-part of C_D.

1.1. ***The Damey–Payan Theorem and Gerth's contribution.*** Damey and Payan [1970, Theorems II.9 and II.10] have proved a similar phenomenon for the 4-rank:

Theorem 1.3 (Spiegelungssatz for the 4-rank). *For every $d \geq 1$ we have*

$$\mathrm{rk}_4(\mathrm{C}_d) \leq \mathrm{rk}_4(\mathrm{C}_{-d}) \leq \mathrm{rk}_4(\mathrm{C}_d) + 1. \tag{13}$$

Note the equality $\mathbb{Q}(\sqrt{-d}\,) = \mathbb{Q}(\sqrt{-4d}\,)$. We shall say that the fields $\mathbb{Q}(\sqrt{d}\,)$ and $\mathbb{Q}(\sqrt{-d}\,)$ are *reflected*. Note that $\mathbb{Q}$ is reflected to $\mathbb{Q}(\sqrt{-1}\,)$ by definition.

As for the 3-rank, the natural question is to evaluate the frequency of each of the events "$\mathrm{rk}_4(\mathrm{C}_{-d}) = \mathrm{rk}_4(\mathrm{C}_d)$" and "$\mathrm{rk}_4(\mathrm{C}_{-d}) = \mathrm{rk}_4(\mathrm{C}_d) + 1$". The only paper concerning this question is [Gerth 2001]. To present its results we introduce several notations. For $x \geq 1$ and integers $r, t \geq 0$ we introduce the two sets

$$A_{t;x} := \big\{m \in [1, x] : m \text{ squarefree and exactly } t \text{ primes ramify in } \mathbb{Q}(\sqrt{-m}\,)/\mathbb{Q}\big\}$$

and

$$A^{=}_{t,r;x} := \big\{m : m \in A_{t,x},\ \mathrm{rk}_4(\mathrm{C}_{-m}) = \mathrm{rk}_4(\mathrm{C}_m) = r\big\}.$$

Theorem 1.4 [Gerth 2001, p. 2551]. *For every integer $r \geq 0$ we have*

$$\lim_{t\to\infty} \lim_{x\to\infty} \frac{\sharp\, A^{=}_{t,r;x}}{\sharp\, A_{t;x}} = 2^{-r}\, 2^{-r^2}\, \eta_\infty(2)\eta_r(2)^{-2} = 2^{-r} a_2^-(r). \tag{14}$$

In this statement, Gerth has chosen to list all imaginary quadratic fields in the form $\mathbb{Q}(\sqrt{-m}\,)$ with m squarefree. Gerth could have adopted the other point of view of writing these imaginary fields in the form $\mathbb{Q}(\sqrt{D}\,)$ with D as a negative fundamental discriminant. This is the point of view that we prefer to adopt in this paper. Also remember that $D = -m$ or $D = -4m$ according to the cases $m \equiv 3 \bmod 4$ or $m \equiv 1$ or $2 \bmod 4$, and that exactly $\omega(|D|)$ primes ramify in $\mathbb{Q}(\sqrt{D}\,)$.

More precisely, here is the variant of Theorem 1.4 that we have in mind and that could have been equally proved by Gerth in [2001]:

Theorem 1.5. *For every integer $r \geq 0$ we have*

$$\lim_{t\to\infty} \lim_{X\to\infty} \frac{\sharp\big\{D\,;\ 0 < -D \leq X,\ \omega(|D|) = t,\ \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) = r\big\}}{\sharp\big\{D : 0 < -D \leq X,\ \omega(|D|) = t\big\}} = 2^{-r}\, a_2^-(r).$$

Theorems 1.4 and 1.5 deserve several remarks. By mixing Theorem 1.5 with the central result of [Gerth 1984, Formula 1.5], we get:

Corollary 1.6 [Gerth 2001, p. 2551]. *For every integer $r \geq 0$ we have*

$$\lim_{t\to\infty} \lim_{X\to\infty} \frac{\sharp\{D;\ 0 < -D \leq X,\ \omega(|D|) = t,\ \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) = r\}}{\sharp\{D : 0 < -D \leq X,\ \omega(|D|) = t,\ \mathrm{rk}_4(\mathrm{C}_D) = r\}} = 2^{-r}.$$

This corollary, roughly speaking, asserts that for an imaginary quadratic field with 4-rank equal to r, the probability (in the special sense introduced by Gerth) that its reflected field has the same 4-rank is equal to 2^{-r}.

Secondly, if we sum the equality contained in Theorem 1.5 for all $r \geq 0$ and appeal to the same trick already used in the proof of the equality (11), we obtain:

Corollary 1.7 [Gerth 2001, Theorem 1].

$$\lim_{t\to\infty} \lim_{X\to\infty} \frac{\sharp\{D : 0 < -D \leq X,\ \omega(-D) = t,\ \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D})\}}{\sharp\{D : 0 < -D \leq X,\ \omega(|D|) = t\}} = \sum_{r=0}^{\infty} 2^{-r}\, a_2^-(r) = 0.610321\ldots\,.$$

The third remark is that Gerth could have equally stated Theorem 1.4 by first considering the value r of $\mathrm{rk}_4(\mathrm{C}_m)$ instead of $\mathrm{rk}_4(\mathrm{C}_{-m})$. Then the value of the second part of the equalities contained in Theorems 1.4, 1.5 and Corollary 1.6 would have been modified. Of course, the numerical constant appearing in Corollary 1.7 would have been unchanged.

The purpose of this paper is to prove the statements of Theorem 1.5 and Corollaries 1.6 and 1.7, but in the context of the more natural probability space, as defined in (3). This is far from being a simple transposition of the original proofs of Gerth, since he writes [2001, p. 2547]: "However, computing these limits appears to be very difficult." We will make an explicit comparison at the bottom of the next page. The limits given in the results above by Gerth are those that will appear in Theorem 1.8 below.

Statement of the results. The next theorem states the main result for the following natural densities, where Prob is defined in (3):

Theorem 1.8. *For every integer $r \geq 0$,*

$$\mathrm{Prob}^-(\{D \in \mathcal{D}^- : \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) = r\}) = a_2^-(r)\, 2^{-r}, \tag{15}$$

$$\mathrm{Prob}^-(\{D \in \mathcal{D}^- : \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) + 1 = r\}) = a_2^-(r)\,(1 - 2^{-r}), \tag{16}$$

$$\mathrm{Prob}^+(\{D \in \mathcal{D}^+ : \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) = r\}) = a_2^+(r)\,(1 - 2^{-(r+1)}), \tag{17}$$

$$\mathrm{Prob}^+(\{D \in \mathcal{D}^+ : \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) - 1 = r\}) = a_2^+(r)\, 2^{-(r+1)}. \tag{18}$$

The given densities are the same, if we further restrict to the negative (*positive*) *fundamental D congruent to* 1 mod 4, 0 mod 8, *or* 4 mod 8.

These results can be easily stated in conditional probabilities:

Corollary 1.9. *For $D < 0$ we get the conditional probabilities*

$$\mathrm{Prob}^-(\{\mathrm{rk}_4(\mathrm{C}_{-D}) = s \mid \mathrm{rk}_4(\mathrm{C}_D) = r\}) = \begin{cases} 2^{-r} & \text{if } r = s, \\ (1 - 2^{-r}) & \text{if } s + 1 = r, \\ 0 & \text{otherwise.} \end{cases}$$

For $D > 0$ we get the conditional probabilities

$$\mathrm{Prob}^+(\{\mathrm{rk}_4(\mathrm{C}_{-D}) = s \mid \mathrm{rk}_4(\mathrm{C}_D) = r\}) = \begin{cases} (1 - 2^{-(r+1)}) & \text{if } r = s, \\ 2^{-(r+1)} & \text{if } s - 1 = r, \\ 0 & \text{otherwise.} \end{cases}$$

This follows as an obvious byproduct of Theorem 1.8 as soon as one applies the central result of [Fouvry and Klüners 2007], which is recalled as Theorem 2.3 below. We remark that the values of these conditional probabilities, in the case of positive D, coincide with the values suggested by Dutarte (Conjecture 1.1), with the natural replacement of 2 by 3.

In Section 3 we also prove:

Corollary 1.10. *We have the equalities*

$$\mathrm{Prob}^-(\{D \in \mathcal{D}^- : \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D})\}) = \sum_{r=0}^{\infty} 2^{-r}\, a_2^-(r), \tag{19}$$

$$\mathrm{Prob}^-(\{D \in \mathcal{D}^- : \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) + 1\}) = \sum_{r=0}^{\infty} (1 - 2^{-r})\, a_2^-(r), \tag{20}$$

$$\mathrm{Prob}^+(\{D \in \mathcal{D}^+ : \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D})\}) = \sum_{r=0}^{\infty} (1 - 2^{-(r+1)})\, a_2^+(r), \tag{21}$$

$$\mathrm{Prob}^+(\{D \in \mathcal{D}^+ : \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) - 1\}) = \sum_{r=0}^{\infty} 2^{-(r+1)}\, a_2^+(r). \tag{22}$$

The given densities are the same, if we further restrict to the negative (*positive*) *fundamental D congruent to* 1 mod 4, 0 mod 8, *or* 4 mod 8.

It is important to remark that the values appearing on the right sides of Equations (15) and (19) coincide with the values appearing in Theorem 1.5 and Corollary 1.7, but the probabilistic models are not the same at all. However, these coincidences confirm an intuition of Gerth [2001, p. 2547]: "Although the limits we compute are not guaranteed to equal the limits above, our results do provide some insight into this question."

Comparison of our result with Gerth's approach. It is useful to compare Gerth's approach [2001] to ours, and the same comments apply to [Fouvry and Klüners 2007] when compared with [Gerth 1984]. To summarize the situation, let $\mathcal{Y}$ be a set of positive integers. We consider two ways of measuring the density of $\mathcal{Y}$:

- the natural one, defined by

$$\mathrm{dens}_{\mathrm{nat}}(\mathcal{Y}) := \lim_{X\to\infty} \frac{\#\{m \le X : m \in \mathcal{Y}\}}{\#\{m \le X\}},$$

- the density introduced by Gerth and defined by

$$\mathrm{dens}_{\mathrm{Gerth}}(\mathcal{Y}) := \lim_{t\to\infty} \lim_{X\to\infty} \frac{\#\{m \le X : m \in \mathcal{Y},\ \omega(m) = t\}}{\#\{m \le X : \omega(m) = t\}}.$$

These densities may not exist. There is no reason, generally speaking, that there exists a link between the existence of these two densities or between their values, as can be seen in the next two examples. First, let

$$\mathcal{Y} := \{m \ge 1 : \omega(m) \ge \tfrac{1}{2}\log\log(m+1)\}.$$

In this case, both densities exist and we have the equality

$$\mathrm{dens}_{\mathrm{nat}}(\mathcal{Y}) = 1.$$

This is a consequence of the well known fact that the function $m \mapsto \log\log(m+1)$ is a normal order of the additive function $m \mapsto \omega(m)$. For this notion, see for instance [Tenenbaum 2008, Chapter III.3]. We also have the trivial equality

$$\mathrm{dens}_{\mathrm{Gerth}}(\mathcal{Y}) = 0.$$

The second example consists in now defining $\mathcal{Y}$ as

$$\mathcal{Y} := \{m \ge 1 : \omega(m) \equiv 0 \bmod 2\}.$$

By the prime number theorem, we know that $\mathrm{dens}_{\mathrm{nat}}(\mathcal{Y}) = \frac{1}{2}$ and we trivially see that $\mathrm{dens}_{\mathrm{Gerth}}(\mathcal{Y})$ does not exist.

However, a link could be established between these two densities if the situation is such that one can ensure some uniformity in the double limit $\lim_{t\to\infty}\lim_{X\to\infty}$.

Gerth [1984; 2001] builds his proofs on the theory of Rédei matrices with dimension t, and it seems quite difficult to introduce the required uniformity in such an approach. In [Fouvry and Klüners 2007] we draw a new way of attacking these questions by replacing the theory of Rédei matrices by the study of oscillations of Jacobi symbols, without any restriction on the number of prime factors in the numerator and denominator. Note also that our proofs can be adapted to recover Gerth's results.

2. General results on the 4-rank

We have already seen that our problem is deeply connected to the Cohen–Lenstra heuristics, which were extended by Gerth to the case $p = 2$. In this section we collect the statements needed for our proofs.

As usual for quadratic fields, we need to distinguish between positive and negative D, corresponding to totally real and totally imaginary quadratic fields. For each case we also need to consider the behavior at 2, that is, if $D \equiv a \bmod q$ for the cases

$$(a, q) \in \big\{(1, 4),\ (0, 8),\ (4, 8)\big\}. \tag{23}$$

Therefore we introduce six counting functions:

$$\mathscr{D}^{\pm}(X, a, q) := \sum_{\substack{0<\pm D\le X\\ D\equiv a \bmod q}} 1. \tag{24}$$

These are the cardinalities of positive (negative) fundamental discriminants (including 1) up to X, which are congruent to a mod q. These cardinalities are well known since we have

$$\mathscr{D}^{-}(X, 1, 4),\ 4\cdot\mathscr{D}^{-}(X, 0, 8),\ 4\cdot\mathscr{D}^{-}(X, 4, 8) = \frac{2}{\pi^2}X + O(\sqrt{X}), \tag{25}$$

$$\mathscr{D}^{+}(X, 1, 4),\ 4\cdot\mathscr{D}^{+}(X, 0, 8),\ 4\cdot\mathscr{D}^{+}(X, 4, 8) = \frac{2}{\pi^2}X + O(\sqrt{X}), \tag{26}$$

uniformly for $X \ge 2$. The equalities (25) and (26) are just variations of the classical formula

$$\sum_{n\le X} \mu^2(n) = \frac{6}{\pi^2}X + O(\sqrt{X}),$$

which counts the number of squarefree numbers up to X, where $\mu(n)$ is the Möbius function.

In [Fouvry and Klüners 2007, Theorem 3] we proved that Conjecture 1.2 is true for $p = 2$ and all $r \ge 0$. For our main result we need the stronger result that the densities above are the same when we restrict the fundamental discriminants to the cases $D \equiv a \bmod q$ for $(a, q) \in \{(1, 4),\ (0, 8),\ (4, 8)\}$. We could easily have stated this extension in that paper, but unfortunately we did not. We explain briefly how to get the stronger result. In [Fouvry and Klüners 2007] we introduced the following sums, which are moments of order k of the arithmetic function $2^{\mathrm{rk}_4(\mathrm{C}_D)}$:

$$S^{\pm}(X, k, a, q) := \sum_{\substack{0<\pm D\le X\\ D\equiv a \bmod q}} 2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}, \tag{27}$$

where $X \ge 2$ is a real number, $k \ge 0$ is an integer, and (a, q) is one of $(1, 4)$, $(0, 8)$, and $(4, 8)$. Then we proved in Theorems 6–11 of the same reference the following results, where $\mathcal{N}(k, 2)$ denotes the number of $\mathbb{F}_2$-vector subspaces of $\mathbb{F}_2^k$.

Theorem 2.1. *Let* $(a, q) \in \{(1, 4),\ (0, 8),\ (4, 8)\}$. *For every positive integer* k *and every positive* ε *we have, uniformly for* $X \ge 2$,

$$S^{-}(X, k, a, q) \;=\; \mathcal{N}(k, 2)\,\mathscr{D}^{-}(X, a, q) \;+\; O_{\varepsilon,k}\big(X(\log X)^{-2^{-k}+\varepsilon}\big)$$

and

$$S^+(X,k,a,q)=\frac{1}{2^k}(\mathcal{N}(k+1,2)-\mathcal{N}(k,2))\,\mathcal{D}^+(X,a,q)+O_{\varepsilon,k}(X(\log X)^{-2^{-k}+\varepsilon}).$$

Using the same proof as in [Fouvry and Klüners 2007, Proposition 1] and applying it to Theorem 2.1, we get the following result for our six families.

Theorem 2.2. *Let* $(a,q)\in\{(1,4),\ (0,8),\ (4,8)\}$. *For every positive integer* k,

$$\lim_{X\to\infty}\frac{\displaystyle\sum_{\substack{0<-D\le X\\ D\equiv a \bmod q}}\prod_{0\le i<k}(2^{\mathrm{rk}_4(\mathrm{C}_D)}-2^i)}{\mathcal{D}^-(X,a,q)}=1,\quad \lim_{X\to\infty}\frac{\displaystyle\sum_{\substack{0<D\le X\\ D\equiv a \bmod q}}\prod_{0\le i<k}(2^{\mathrm{rk}_4(\mathrm{C}_D)}-2^i)}{\mathcal{D}^+(X,a,q)}=2^{-k}.$$

We remark that this theorem is a positive answer to [Cohen and Lenstra 1984, C6 and C10, p. 56f] for the case $p=2$. We can use the same approach for our six subfamilies as in the proofs of [Fouvry and Klüners 2006, Theorems 1 and 2]. Altogether, we get the following result, which extends [Fouvry and Klüners 2007, Theorem 3] to the six families.

Theorem 2.3. *Let* (a,q) *satisfy* (23). *For every* $r\ge 0$ *we have*

$$\lim_{X\to\infty}\frac{\sharp\left\{D:0<-D\le X,\ D\equiv a \bmod q,\ \mathrm{rk}_4(\mathrm{C}_D)=r\right\}}{\mathcal{D}^-(X,a,q)}=a_2^-(r),$$

$$\lim_{X\to\infty}\frac{\sharp\left\{D:0<D\le X,\ D\equiv a \bmod q,\ \mathrm{rk}_4(\mathrm{C}_D)=r\right\}}{\mathcal{D}^+(X,a,q)}=a_2^+(r).$$

3. Proofs of our main results

We start with some formulas between the densities occurring in the Cohen–Lenstra heuristics. In this paper we are using them only for $p=2$ and $p=3$, but it is easy to give them for every prime p.

Lemma 3.1. *Let* p *be prime and* $a_p^\pm(r)$ *be defined as in Conjecture 1.2. Then*

(i) $a_p^+(r)=\dfrac{p}{p^{r+1}-1}\,a_p^-(r)$ *for all* $r\ge 0$,

(ii) $a_p^-(r+1)=\dfrac{p}{(p^{r+1}-1)^2}\,a_p^-(r)$ *for all* $r\ge 1$.

Proof.

(i) $a_p^+(r)=p^{-r}\left(1-\dfrac{1}{p^{r+1}}\right)^{-1}a_p^-(r)=\dfrac{p}{p^{r+1}-1}\,a_p^-(r)$,

(ii) $a_p^-(r)=p^{-2r-1}\left(1-\dfrac{1}{p^{r+1}}\right)^{-2}a_p^-(r)=\dfrac{p}{(p^{r+1}-1)^2}\,a_p^-(r)$. □

Now we define the quantities which, for $p=2$ and $p=3$, appear quite naturally in the reflection principle.

Definition 3.2. For $r, s \geq 0$ we recursively define

(i) $c_p(0,0) := a_p^-(0), c_p(0,1) := a_p^+(0) - c(0,0) = a_p^+(0) - a_p^-(0)$;

(ii) $c_p(r,r) := a_p^-(r) - c_p(r-1,r)$ and $c_p(r,r+1) := a^+(r) - c_p(r,r) = a^+(r) - a_p^-(r) + c(r-1,r)$ for all $r \geq 1$;

(iii) $c(r,s) = 0$ in all other cases, that is, when $s - r \notin \{0,1\}$.

We have the two easy identities

$$a_p^-(r) = c_p(r-1,r) + c_p(r,r) \quad \text{for } r \geq 1,$$
$$a_p^+(r) = c_p(r,r) + c_p(r,r+1) \quad \text{for } r \geq 0.$$

Lemma 3.3. *Let p be a prime.*

(i) *For all $r \geq 0$ we have $c_p(r,r)/a_p^-(r) = p^{-r}$.*

(ii) *For all $r \geq 1$ we have $c_p(r-1,r)/a_p^-(r) = 1 - p^{-r}$.*

(iii) *For all $r \geq 0$ we have $c_p(r,r)/a_p^+(r) = 1 - p^{-(r+1)}$.*

(iv) *For all $r \geq 0$ we have $c_p(r,r+1)/a_p^+(r) = p^{-(r+1)}$.*

Proof. We prove (i) by induction, the case $r = 0$ being trivial. Now

$$\frac{c_p(r+1,r+1)}{a_p^-(r+1)} = \frac{a_p^-(r+1) - c_p(r,r+1)}{a_p^-(r+1)} = 1 - \frac{a_p^+(r) - c_p(r,r)}{a_p^-(r+1)}.$$

Using Lemma 3.1 twice we reduce this expression to

$$1 - \frac{p/(p^{r+1}-1)\, a_p^-(r) - c_p(r,r)}{a_p^-(r)\, p/(p^{r+1}-1)^2} = 1 - (p^{r+1}-1) + \frac{1}{p^r}\frac{(p^{r+1}-1)^2}{p},$$

the equality being checked by induction. But this equals $p^{-(r+1)}$, which proves (i).

Part (ii) follows easily from (i) and $c_p(r-1,r) + c_p(r,r) = a_p^-(r)$.

By part (i) and by Lemma 3.1 we have

$$\frac{c_p(r,r)}{a_p^+(r)} = \frac{c_p(r,r)}{a_p^-(r)\, p/(p^{r+1}-1)} = p^{-r}\frac{p^{r+1}-1}{p} = 1 - p^{-(r+1)},$$

which proves part (iii).

The last part follows from (iii) and $a_p^+(r) = c(r,r) + c(r,r+1)$. □

The main step. Now we are able to prove the main result, which gives the natural density of the set of negative D, such that the 4-rank of C_D and C_{-D} have prescribed values. To state this result, for integers a, q, nonnegative integers r, s, and $X \geq 1$, we introduce

$$B^{\pm}(X,a,q,r,s) := \sharp\big\{D : 0 < \pm D \leq X,\ D \equiv a \bmod q,\ \mathrm{rk}_4(\mathrm{C}_{-D}) = r,\ \mathrm{rk}_4(\mathrm{C}_D) = s\big\}.$$

Theorem 3.4. *Let* $(a, q) \in \{(1, 4), (0, 8), (4, 8)\}$. *For every* r *and* $s \geq 0$ *we have*

$$\lim_{X\to\infty} \frac{B^-(X, a, q, r, s)}{\mathscr{D}^-(X, a, q)} = c_2(r, s).$$

Proof. We shall fix the case $(a, q) = (1, 4)$ and give indications for the other two cases. A direct application of Theorems 1.3 and 2.3 leads to the following asymptotic behaviors for $X \to \infty$:

$$B^-(X, 1, 4, 0, 0) \sim a_2^-(0)\mathscr{D}^-(X, 1, 4), \tag{28}$$

$$B^-(X, 1, 4, s, s) + B^-(X, 1, 4, s-1, s) \sim a_2^-(s)\mathscr{D}^-(X, 1, 4) \quad \text{if } s \geq 1. \tag{29}$$

Note that when $D < 0$ is congruent to 1 mod 4, the reflected field $\mathbb{Q}(\sqrt{-D})$ has discriminant $-4D$; hence the reflection creates a one-to-one correspondence between negative discriminants congruent to 1 mod 4 and not less than $-X$, on the one hand, and positive discriminants congruent to 4 mod 8 and not exceeding $\leq 4X$, on the other. We use this bijection in the form of the equalities

$$\mathscr{D}^-(X, 1, 4) = \mathscr{D}^+(4X, 4, 8), \quad B^-(X, 1, 4, r, s) = B^+(4X, 4, 8, s, r), \tag{30}$$

which are true for any integers r and s. Using Theorems 1.3 and 2.3 once more we have

$$B^+(4X, 4, 8, s, s) + B^+(4X, 4, 8, s+1, s) \sim a_2^+(s)\mathscr{D}^+(4X, 4, 8) \tag{31}$$

as $X \to \infty$ for any $s \geq 0$. We reinterpret this relation by appealing to (30), obtaining

$$B^-(X, 1, 4, s, s) + B^-(X, 1, 4, s, s, +1) \sim a_2^+(s)\mathscr{D}^-(X, 1, 4). \tag{32}$$

Let $b^-(X, r, s) := B^-(X, 1, 4, r, s)/\mathscr{D}^-(X, 1, 4)$. The relations (28), (29) and (32) are written as

$$\begin{aligned} b^-(X, 0, 0) &\sim a_2^-(0), \\ b^-(X, s, s) + b^-(X, s-1, s) &\sim a_2^-(s) \quad \text{for } s \geq 1, \\ b^-(X, s, s) + b^-(X, s, s+1) &\sim a_2^+(s) \quad \text{for } s \geq 0, \end{aligned} \tag{33}$$

as $X \to \infty$. (Recall that $b^-(X, r, s) = 0$ when $s - r \notin \{0, 1\}$.) An easy induction applied to the asymptotics (33) proves that each $b^-(X, r, s)$ has a limit as $X \to \infty$, which is denoted by $b^-(r, s)$. We then get from (33) the following equalities among these limits:

$$\begin{aligned} b^-(0, 0) &\sim a_2^-(0), \\ b^-(s, s) + b^-(s-1, s) &\sim a_2^-(s) \quad \text{for } s \geq 1, \\ b^-(s, s) + b^-(s, s+1) &\sim a_2^+(s) \quad \text{for } s \geq 0. \end{aligned} \tag{34}$$

We exactly recognize the identities satisfied by the coefficients $c_2(r, s)$ for all r and s. By an easy induction, we deduce that $b^-(r, s) = c_2(r, s)$. This completes

the proof of Theorem 1.8 when $(a, q) = (1, 4)$. It remains to give some hints on the other cases.

- When $(a, q) = (4, 8)$, the reflection creates a bijection between the set of negative discriminants $\geq -X$ and congruent to 4 mod 8 with the set of positive discriminants (including 1) $\leq X/4$ and congruent to 1 mod 4.
- When $(a, q) = (0, 8)$, the reflection creates a bijection between the set of negative discriminants $\geq -X$ and congruent to 0 mod 8 with the set of positive discriminants $\leq X$ and congruent to 0 mod 8.

With these remarks, the counting process is the same. □

Proof of Theorem 1.8. By Theorem 3.4 we see that (15) and (16) are obvious when we use the first two formulas of Lemma 3.3 for $p = 2$ in the three cases of $D \equiv 1 \bmod 4$, $D \equiv 4 \bmod 8$ and $D \equiv 0 \bmod 8$. For the equalities (17) and (18), we shall restrict ourselves to the case $D \equiv 1 \bmod 4$ since the other cases are similar. So we are concerned with the limit of the ratio

$$\frac{\sharp\{D : 0 < D \leq X,\ \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) = r,\ D \equiv 1 \bmod 4\}}{\mathscr{D}^+(X, 1, 4)}.$$

By the reflection map, this ratio is equal to

$$\frac{\sharp\{D : 0 < -D \leq 4X,\ \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{C}_{-D}) = r,\ D \equiv 4 \bmod 8\}}{\mathscr{D}^+(4X, 4, 8)}.$$

By Theorem 3.4 as $X \to \infty$, this ratio tends to

$$c_2(r, r) = a_2^+(r)(1 - 2^{-(r+1)}),$$

by Lemma 3.3(iii). □

Proof of Corollary 1.10. Heuristically, we want to sum up the results of Theorem 1.8. But this is an infinite summation of all the probabilities corresponding to $0 \leq r < \infty$. Following the technique used in the proof of (11), we can perform this infinite series. Hence we can pass from each of the four equalities of Theorem 1.8 to each of the four equalities of Corollary 1.10. □

The case p = 3. Analyzing the proof of Theorem 1.8, we see that everything works for $p = 3$ as soon as we have a suitable proven version of Conjecture 1.2. For $p = 2$ we used Theorem 2.3, which gives the corresponding densities for the cases $D \equiv a \bmod q$ and (a, q) as in (23). It is important for our argument in the proof of Theorem 3.4 that the reflection from $\mathbb{Q}(\sqrt{d})$ to $\mathbb{Q}(\sqrt{-d})$ is order-preserving and is a permutation of the set consisting of the three congruence classes defined in (23).

The latter is true for $p = 3$ when we restrict to the cases $D \equiv 0 \bmod 3$ and $D \equiv 1, 2 \bmod 3$. Indeed, if $D > 0$ is a fundamental discriminant, then $-3D$ is

a fundamental discriminant, when $D \not\equiv 0 \bmod 3$. In case that $D \equiv 0 \bmod 3$, the reflected field has discriminant $-D/3$. Since $-3 \equiv 1 \bmod 4$, we have no problems with ramification at 2 in this case.

Here also we recognize a permutation of the set consisting of the two subsets $\{D \equiv 0 \bmod 3\}$ and $\{D \not\equiv 0 \bmod 3\}$. Denote by

$$\mathscr{A}_0^{\pm} := \{D \in \mathscr{D}^{\pm} : D \equiv 0 \bmod 3\}, \quad \mathscr{A}_{\not\equiv 0}^{\pm} := \{D \in \mathscr{D}^{\pm} : D \not\equiv 0 \bmod 3\}$$

four different sets. The proof of the following theorem is now obvious using the remarks above.

Theorem 3.5. *Assume that the following four equations are true, where* $* \in \{+, -\}$ *and* b *can be* 0 *or* $\neq 0$:

$$\lim_{X\to\infty} \frac{\sharp\left\{D \in \mathscr{A}_b^* : 0 < |D| \le X,\ \mathrm{rk}_3(\mathrm{C}_D) = r\right\}}{\sharp\{D \in \mathscr{A}_b^* : 0 < |D| \le X\}} = a_3^*(r).$$

Then the corresponding result of Theorem 1.8 is true. Especially, Conjecture 1.1 is true.

The four statements assumed in the hypotheses of Theorem 3.5 are only extensions of some Cohen–Lenstra heuristics (see Conjecture 1.2 above, with $p = 3$) to congruence classes modulo 3.

A weighted version. We already said in (12) that in [Belabas 1999; 2004] a weaker result for $p = 3$ is proved. Here the density is considered with some weight, which makes it possible to deduce this result by knowing only the following averages for $p = 3$:

$$\lim_{X\to\infty} \frac{\sum\limits_{0<D\le X} p^{\mathrm{rk}_p(\mathrm{C}_D^2)}}{\sum\limits_{0<D\le X} 1} = 1 + 1/p, \quad \lim_{X\to\infty} \frac{\sum\limits_{0<-D\le X} p^{\mathrm{rk}_p(\mathrm{C}_D^2)}}{\sum\limits_{0<-D\le X} 1} = 2.$$

Knowing these averages (and some proven error term) for all discriminants divisible by 3 and not divisible by 3, respectively, for $p = 3$, Equation (12) can be deduced.

We mention this type of result for two reasons. First, it can be proven for $p = 3$ and second we get rational constants for this weighted density. On the other hand, this weighted density is not the one we want. As in Theorem 1.8 we have four different points of view to express this result. It is clear that in [Belabas 1999; 2004] all of these four viewpoints could have been proved. For $p = 2$, that is, the reflection principle for 4-ranks, we can easily prove similar statements. Let us

define (if they exist) the following weighted densities for $p \in \{2, 3\}$, $a \in \{0, 1\}$:

$$d_{3,a,\pm} := \lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<\pm D\le X \\ \mathrm{rk}_3(C^2_{-3D})=\mathrm{rk}_3(C^2_D)\mp a}} 3^{\mathrm{rk}_3(C^2_D)}}{\displaystyle\sum_{0<\pm D\le X} 3^{\mathrm{rk}_3(C^2_D)}}, \tag{35}$$

$$d_{2,a,\pm} := \lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<\pm D\le X \\ \mathrm{rk}_2(C^2_{-D})=\mathrm{rk}_2(C^2_D)\mp a}} 2^{\mathrm{rk}_2(C^2_D)}}{\displaystyle\sum_{0<\pm D\le X} 2^{\mathrm{rk}_2(C^2_D)}}. \tag{36}$$

Theorem 3.6. *Let $p = 2$ or 3. Then the weighted densities exist and are given by*

$$d_{p,1,+} = \frac{1}{p+1}, \quad d_{p,0,+} = \frac{p}{p+1}, \quad d_{p,1,-} = \frac{1}{2}, \quad d_{p,0,-} = \frac{1}{2}.$$

Proof. Let us start with $d_{2,0,-}$. We multiply (15) in Theorem 1.8 by 2^r and, using the same arguments as in the proof of Corollary 1.10, we perform the summation:

$$\sum_{r=0}^{\infty} a_2^-(r)2^{-r}2^r = \sum_{r=0}^{\infty} a_2^-(r) = 1.$$

We know that the denominator of (36) has average 2 by Theorem 2.1, and therefore we get $\frac{1}{2}$ as the weighted density. The result $d_{2,1,-} = 1 - \frac{1}{2} = \frac{1}{2}$ is now obvious.

Now we look at $d_{2,1,+}$ and we are led to the sum

$$\sum_{r=0}^{\infty} a_2^+(r)2^{-(r+1)}2^r = \frac{1}{2}\sum_{r=0}^{\infty} a_2^+(r) = \frac{1}{2}.$$

The denominator has average $\frac{3}{2}$ by Theorem 2.1 and we get $\frac{1}{2}\big/\frac{3}{2} = \frac{1}{3}$ as the weighted density.

The result for $p = 3$ is proven in [Belabas 1999; 2004] for $d_{3,1,+}$. Then $d_{3,0,+} = 1 - d_{3,1,+}$ and the other two densities can be proved analogously. □

4. Some remarks

In an earlier version of this paper we gave a much more complicated proof of Theorem 1.8. We defined for (a, q) in (23):

$$S^-_{\mathrm{mix}}(X, k, a, q) := \sum_{\substack{0<-D\le X \\ D\equiv a \bmod q}} 2^{k\,\mathrm{rk}_4(C_D)} \cdot 2^{\mathrm{rk}_4(C_{-D})}. \tag{37}$$

We then proved the following theorem using techniques similar to those of [Fouvry and Klüners 2007]:

Theorem 4.1. *Let* (a, q) *satisfy* (23). *For any integer* $k \geq 0$ *and for any* $\varepsilon > 0$ *we have the equality*

$$S^{-}_{\mathrm{mix}}(X, k, a, q) = \frac{\mathcal{N}(k+1, 2) + \mathcal{N}(k, 2)}{2} \cdot \mathcal{D}^{-}(X, a, q) + O_{k,\varepsilon}\big(X(\log X)^{-2^{-k}+\varepsilon}\big),$$

uniformly for $X \geq 2$.

Then it was possible to deduce Theorem 1.8 from this theorem and the main result in [Fouvry and Klüners 2007].

Our new proof is simply a corollary of Theorem 2.3, which is a slight extension of [Fouvry and Klüners 2007, Theorem 3]. Unfortunately, we did not know about this possibility when we wrote that paper. We already mentioned the results of Gerth [1984; 2001], which prove these things by considering the number of prime factors. In the second of those papers Gerth also starts by reproving all the things in a similar way as he did in the first. It is possible to use the same procedure to derive the results in [Gerth 2001] from the earlier paper [1984], provided that it has been generalized to each of the congruence classes appearing in (23).

Dutarte [1984] checked the compatibility of different principles leading to the Cohen–Lenstra heuristics and to the probabilities occurring in the reflection principle. Theorem 3.5 shows that the corresponding probabilities in the reflection principle can be deduced when we know that Cohen–Lenstra heuristics are true for $p = 3$ in congruence classes modulo 3. This was not seen in [Dutarte 1984]. Nevertheless, he produces heuristics for the other direction.

References

[Belabas 1999] K. Belabas, "On the mean 3-rank of quadratic fields", *Compositio Math.* **118**:1 (1999), 1–9. MR 2000g:11102 Zbl 0929.11046

[Belabas 2004] K. Belabas, "Corrigendum: On the mean 3-rank of quadratic fields", *Compos. Math.* **140**:5 (2004), 1221. MR 2005b:11176

[Cohen and Lenstra 1984] H. Cohen and H. W. Lenstra, Jr., "Heuristics on class groups of number fields", pp. 33–62 in *Number theory* (Noordwijkerhout, 1983), edited by H. Jager, Lecture Notes in Math. **1068**, Springer, Berlin, 1984. MR 85j:11144 Zbl 0558.12002

[Damey and Payan 1970] P. Damey and J.-J. Payan, "Existence et construction des extensions Galoisiennes et non-abéliennes de degré 8 d'un corps de caractéristique différente de 2", *J. Reine Angew. Math.* **244** (1970), 37–54. MR 43 #6186 Zbl 0206.34401

[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

[Dutarte 1984] P. Dutarte, "Compatibilité avec le Spiegelungssatz de probabilités conjecturales sur le p-rang du groupe des classes", in *Théorie des nombres* 1983/1984 (Exposé 4), Université de Franche-Comté, Besançon, 1984. MR 86m:11103

[Fouvry and Klüners 2006] É. Fouvry and J. Klüners, "Cohen–Lenstra heuristics of quadratic number fields", pp. 40–55 in *Algorithmic number theory* (Berlin, 2006), edited by F. Hess et al., Lecture Notes in Comput. Sci. **4076**, Springer, Berlin, 2006. MR 2008f:11125

[Fouvry and Klüners 2007] É. Fouvry and J. Klüners, "On the 4-rank of class groups of quadratic number fields", *Invent. Math.* **167**:3 (2007), 455–513. MR 2007k:11187

[Gerth 1984] F. Gerth, III, "The 4-class ranks of quadratic fields", *Invent. Math.* **77**:3 (1984), 489–515. MR 85j:11137 Zbl 0533.12004

[Gerth 2001] F. Gerth, III, "Comparison of 4-class ranks of certain quadratic fields", *Proc. Amer. Math. Soc.* **129**:9 (2001), 2547–2552. MR 2002c:11149 Zbl 1012.11097

[Heath-Brown 1994] D. R. Heath-Brown, "The size of Selmer groups for the congruent number problem, II", *Invent. Math.* **118**:1 (1994), 331–370. MR 95h:11064 Zbl 0815.11032

[Roberts 2001] D. P. Roberts, "Density of cubic field discriminants", *Math. Comp.* **70**:236 (2001), 1699–1705. MR 2002e:11142 Zbl 0985.11068

[Scholz 1932] A. Scholz, "Über die Beziehung der Klassenzahlen quadratischer Körper zueinander", *J. für Reine Angew. Math.* **166** (1932), 201–203. Zbl 0004.05104 JFM 58.0181.05

[Stevenhagen 1993] P. Stevenhagen, "The number of real quadratic fields having units of negative norm", *Experiment. Math.* **2**:2 (1993), 121–136. MR 94k:11120 Zbl 0792.11041

[Tenenbaum 2008] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 3rd ed., Belin, Paris, 2008.

Communicated by Bjorn Poonen
Received 2008-10-02 Revised 2009-11-30 Accepted 2010-01-19

Etienne.Fouvry@math.u-psud.fr *Université de Paris-Sud, Laboratoire de Mathématiques, 91405 Orsay Cedex, France*

CNRS, 91405 Orsay Cedex, France

klueners@math.uni-paderborn.de *Universität Paderborn, Institut für Mathematik, Warburger Straße 100, 33098 Paderborn, Germany*

ALGEBRA AND NUMBER THEORY 4:5(2010)

The Manin constant of elliptic curves over function fields

Ambrus Pál

We study the p-adic valuation of the values of normalised Hecke eigenforms attached to nonisotrivial elliptic curves defined over function fields of transcendence degree one over finite fields of characteristic p. We derive upper bounds on the smallest attained valuation in terms of the minimal discriminant under a certain assumption on the function field, and provide examples to show that our estimates are optimal. As an application of our results, we prove the analogue of the degree conjecture unconditionally for strong Weil curves with squarefree conductor defined over function fields satisfying the assumption mentioned above.

1. Introduction

Notation 1.1. Let F denote the function field of $\mathscr{C}$, where the latter is a geometrically connected smooth projective curve defined over the finite field $\mathbb{F}_q$ of characteristic p. Let $\mathbb{A}$ denote the ring of adèles of F, and let GL_2 denote the group scheme of invertible two-by-two matrices. Let E be a nonisotrivial elliptic curve defined over F. Then we may associate a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ to E as follows. Let $E_{\bar{F}}$ denote the base change of E to the separable closure $\bar{F}$ of F. For every prime l different from p, one may attach to the étale cohomology group $H^1(E_{\bar{F}}, \mathbb{Q}_l(1))$, considered as a representation of the absolute Galois group of F, an irreducible cuspidal automorphic representation ρ_E with trivial central character via the Langlands correspondence. As the notation indicates, this representation is independent of the choice of l.

Let V_E denote the irreducible constituent of the space of cuspidal automorphic forms on $\mathrm{GL}_2(\mathbb{A})$ that realises the representation ρ_E. Then there is a distinguished element ψ_E of V_E that we will call the normalised Hecke eigenform attached to E. It is characterised by the fact that it is invariant under the action of the Hecke congruence group of level $\mathfrak{n}$, where $\mathfrak{n}$ denotes the conductor of the elliptic curve E,

MSC2000: primary 11G05; secondary 11G40, 14F30.
Keywords: elliptic curves, Hecke eigenforms, degree conjecture.
The author was partially supported by the EPSRC grant P19164.

and its leading Fourier coefficient is 1. (For an explanation of these concepts as well as an explicit description of the Hecke eigenform, see Section 2.) By a classical theorem of Harder, the automorphic form ψ_E takes only finitely many values. On the other hand, it is easy to see that it takes only rational values. Hence there is a unique positive rational number $c(E)$ such that the subgroup of $\mathbb{Q}$ generated by the values of ψ_E is equal to $c(E)\mathbb{Z}$.

Proposition 1.2. *There is a natural number $m(E)$ such that $c(E) = p^{-m(E)}$.*

It is natural to guess that $m(E)$, which we will call the Manin constant of E, is always zero. Although this hypothesis is frequently made (sometimes implicitly) in the literature (see for example [Papikian 2005; 2007; Rück and Tipp 2000]), it is actually false. One of the aims of this paper is to exhibit many cases when $m(E)$ is not zero. Because the Manin constant could be nonzero, many formulas in the literature have to be corrected to include this nontrivial factor. Hence the latter is a very interesting isogeny invariant of the elliptic curve, and therefore it is desirable to compute it, or at least to give upper bounds, in terms of more well-known invariants. This is the other major aim of this paper. (This problem has been already studied in [Tan 1993]; see Remark 7.9). We will also discuss the implication of our results in connection with one of the formulas mentioned above.

We now formulate the main results of this paper. For every E as above, let Δ_E denote the discriminant of a relatively minimal elliptic surface $\mathscr{E} \to \mathscr{C}$ whose generic fibre is E. Then Δ_E is an effective divisor on the curve $\mathscr{C}$. Moreover, let g denote the genus of $\mathscr{C}$, and let d be the positive integer such that $q = p^d$. We will show:

Theorem 1.3. *Assume that p does not divide the order of $\mathrm{Pic}_0(\mathscr{C})(\mathbb{F}_q)$. Then*

$$m(E) \leq d\left(\tfrac{1}{12}\deg(\Delta_E) + g - 1\right),$$

and the two sides of the inequality above are equal when the elliptic surface $\mathscr{E}$ is ordinary in dimension 2.

The condition on $\mathrm{Pic}_0(\mathscr{C})(\mathbb{F}_q)$ in the theorem above is satisfied, for example, when $\mathscr{C}$ is a rational curve or a supersingular elliptic curve. Moreover, the moduli space of smooth projective connected curves of genus g with p-rank zero is a variety of dimension $2g-3$ over $\overline{\mathbb{F}}_p$ when $g \geq 2$ and p is odd [Faber and van der Geer 2004, Theorem 2.3 and Proposition 2.7]. Hence there are plenty of curves satisfying this condition. It is natural to expect that most elliptic surfaces are ordinary in dimension 2 (for a precise formulation of this conjecture, see Remark 6.12). In particular, our estimate in Theorem 1.3 should be the best possible (at least if we want to make one in terms of the discriminant). We can verify the ordinariness condition in many cases. The following result is just a sample of what can be proven with our methods.

Theorem 1.4. *Let p be a prime number and let n be a positive integer such that $n \mid p-1$ and $6 \mid n$. Let E be the elliptic curve defined over the rational function field $F = \mathbb{F}_p(T)$ by the Weierstrass equation*

$$y^2 + xy = x^3 - T^n.$$

Then E is not isotrivial and

$$m(E) = \tfrac{1}{6}n - 1 = \tfrac{1}{12}\deg(\Delta_E) - 1.$$

The basic strategy of the proof of Theorem 1.3 is to relate the Manin constant to the p-adic valuation of coefficients of L-functions of E. The key tools in estimating the latter are a mild equivariant extension of Katz's conjecture relating the Newton and Hodge polygons and a theorem of Chinburg computing the refined equivariant Euler characteristic of the de Rham complex of varieties equipped with tame group actions in terms of ϵ-constants. The proof of Theorem 1.4 is closely related. In fact, the reason why it is particularly convenient to work with those elliptic curves that appear in the theorem is that Ulmer [2002] computed their Hasse–Weil L-functions rather explicitly.

In the rest of the introduction we describe the application of Theorem 1.3 in this paper, which was the main motivation for our investigations. Fix a closed point ∞ of $\mathscr{C}$ and assume that E has split multiplicative reduction at ∞. Then $\mathfrak{n} = \mathfrak{m}\infty$ for an effective divisor $\mathfrak{m}$ on $\mathscr{C}$; here and throughout we write the addition of divisors multiplicatively. Let A denote the ring of rational functions on $\mathscr{C}$ regular away from ∞, and let $X_0(\mathfrak{m})$ denote the unique smooth projective curve over F that contains the affine Drinfeld modular curve $Y_0(\mathfrak{m})$ parametrising Drinfeld A-modules of rank two of generic characteristic with Hecke level $\mathfrak{m}$-structure as a dense open subscheme. Then there is a nontrivial map $\pi : X_0(\mathfrak{m}) \to E$ of curves defined over F. We say that E is a strong Weil curve if the modular parametrisation π above can be chosen so that the kernel of the map induced by π via Albanese functoriality is smooth and connected in the Jacobian of $X_0(\mathfrak{m})$. In this case we say that π is optimal. Up to isomorphism, there is exactly one strong Weil curve in the isogeny class of E. With the help of Theorem 1.3 and the Pesenti–Szpiro inequality, we will show:

Theorem 1.5. *Assume that p does not divide the order of* $\mathrm{Pic}_0(\mathscr{C})(\mathbb{F}_q)$. *Also suppose that π is optimal and $\mathfrak{m}$ is square-free. Then*

$$\deg(\pi) < q^{18g+4\deg(\infty)+1} \cdot q^{2\deg(\mathfrak{m})} \cdot \deg(\mathfrak{m})^3.$$

The result above is an analogue of Frey's celebrated degree conjecture, formulated originally for strong Weil curves over $\mathbb{Q}$. Our result completes [Papikian 2007], where a conjecture is made that implies that the Manin constant is zero (at

least when F is the rational function field and ∞ is the point at infinity), and where under this assumption an inequality significantly stronger than that in Theorem 1.5 was derived. As we saw, this hypothesis does not hold in general. In fact it is quite reasonable to expect that $m(E)$ be $d(\frac{1}{12}\deg(\Delta_E) + g - 1)$ when E is minimal in its isogeny class (see Section 7 for the definition). This is reflected by the fact that the contribution of our estimate of the term $c(E)^{-2}$ to our bound on the degree of the modular parametrisation is significant — it is of size $O(q^{\deg(\mathfrak{m})})$.

Contents. In Section 2 we give an explicit description of the Hecke eigenform and prove Proposition 1.2. In Section 3 we carefully work out in detail the analogue of the theory of modular symbols for function fields, something that is missing from the current literature. In Section 4, we use these results to derive lower and upper bounds on the Manin constant in terms of the p-adic valuation of coefficients of L-functions of E twisted with tamely ramified abelian characters. In Section 5, our aim is to relate the Galois module structure of the second coherent cohomology of the structure sheaf of elliptic surfaces equipped with a group action respecting the elliptic fibration to ϵ-constants of Galois representations of the function field of the base in a special case. We prove a mild equivariant extension of Katz's conjecture relating the Newton and Hodge polygons, and with its aid we derive Theorem 1.3 from our previous results in Section 6. In Section 7 we show that the isogeny class of E contains an elliptic curve whose j-invariant is not a p-th power, and we then use this result and the Pesenti–Szpiro inequality to deduce a bound on $m(E)$ in terms of the degree of the conductor of E in Theorem 1.3. In Section 8 we first review [Ulmer 2002], and then use it and a classical result of Stickelberger on p-adic valuations of Gauss sums to prove Theorem 1.4. We show that the usual characterisation of strong Weil curves and optimal modular parametrisations holds in the function field setting as well in Section 9. In Section 10 we first show that a certain homomorphism defined in [Gekeler and Reversat 1996] has finite cokernel of exponent dividing $q^{\deg(\infty)} - 1$. Then we combine this result with the bound in Section 7 and the work of Papikian to show Theorem 1.5.

2. The normalised Hecke eigenform

Notation 2.1. Let $\mathbb{O}$ denote the maximal compact subring of the ring $\mathbb{A}$ of adèles of F. Let $|\mathscr{C}|$ denote the set of closed points of $\mathscr{C}$. For every adèle $a \in \mathbb{A}$ and $x \in |\mathscr{C}|$, let a_x denote the x-th component of a. Let μ, μ^* be Haar measures on the locally compact abelian topological groups $\mathbb{A}$ and $\mathbb{A}^*$. Also assume that $\mu(\mathbb{O})$ and $\mu^*(\mathbb{O}^*)$ are both equal to 1. Since these measures are left-invariant with respect to the discrete subgroups F^* and F by definition, each induces a measure, on $F^*\backslash\mathbb{A}^*$ and $F\backslash\mathbb{A}$, respectively, both denoted by the same letter by abuse of notation. For every divisor $\mathfrak{m}$ on $\mathscr{C}$, let $\mathfrak{m}\mathbb{O}$, $\mathbb{K}_0(\mathfrak{m})$ denote the sub-$\mathbb{O}$-module of $\mathbb{A}$ generated by

those idèles whose divisor is $\mathfrak{m}$, and the Hecke congruence subgroup of $\mathrm{GL}_2(\mathbb{A})$ of level $\mathfrak{m}$:

$$\mathbb{K}_0(\mathfrak{m}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{O}) \,|\, c \in \mathfrak{m}\mathbb{O} \right\}.$$

Let $\tau : F\backslash\mathbb{A} \to \mathbb{C}^*$ be a nontrivial continuous additive character. The composition of the quotient map $\mathbb{A} \to F\backslash\mathbb{A}$ and τ will be denoted by the same symbol by the usual abuse of notation. Let $\mathfrak{D}$ denote the $\mathbb{O}$-module $\mathfrak{D} = \{x \in \mathbb{A} \,|\, \tau(x\mathbb{O}) = 1\}$, and let $\mathfrak{d}$ be a divisor on $\mathscr{C}$ such that $\mathfrak{D} = \mathfrak{d}\mathbb{O}$. Let $\mathfrak{n}$ be the conductor of E. The latter is an effective divisor on $\mathscr{C}$. We may assume that the divisor $\mathfrak{d}$ is relatively prime to $\mathfrak{n}$ by changing τ, if necessary. Let B denote the group scheme of invertible upper triangular two-by-two matrices. Let P denote the group scheme of invertible upper triangular two-by-two matrices with 1 on the lower right corner. Finally let Z denote the centre of the group scheme GL_2.

Definition 2.2. For every idèle $u \in \mathbb{A}^*$, let (u) denote the corresponding divisor on $\mathscr{C}$. Often we will denote (u) simply by u by slight abuse of notation, when this does not cause confusion. We will call two divisors $\mathfrak{m}$ and $\mathfrak{n}$ on $\mathscr{C}$ relatively prime if their support is disjoint. Let $\mathrm{Div}(\mathscr{C})$ denote the group of divisors on $\mathscr{C}$. We will call a function $f : \mathrm{Div}(\mathscr{C}) \to \mathbb{C}$ multiplicative if it vanishes on noneffective divisors, if $f(1) = 1$, and if for every pair of relatively prime divisors $\mathfrak{n}$ and $\mathfrak{m}$ we have $f(\mathfrak{nm}) = f(\mathfrak{n})f(\mathfrak{m})$. Let E be a nonisotrivial elliptic curve defined over $\mathscr{C}$ of conductor $\mathfrak{n}$. For every divisor $\mathfrak{r}$ on $\mathscr{C}$, let $\deg(\mathfrak{r})$ denote the degree of $\mathfrak{r}$. For every $x \in |\mathscr{C}|$, let $L_x(E, t)$ denote the local factor of the Hasse–Weil L-function of E at x. It can be written as

$$L_x(E, t) = \sum_{n=0}^{\infty} a(x^n)(tq)^{n \deg(x)} \in \mathbb{Z}[\![t]\!]$$

for some $a(x^n) \in \mathbb{Z}[\frac{1}{p}]$. Let a denote the unique multiplicative function into the multiplicative semigroup of $\mathbb{Q}$ such that $a(x^n)$ is the same as above for each natural number n and each $x \in |\mathscr{C}|$. A continuous function $\psi_E : \mathrm{GL}_2(\mathbb{A}) \to \mathbb{Q}$ is called a normalised Hecke eigenform attached to E is if it satisfies the following properties:

- It is automorphic: $\psi_E(\gamma h) = \psi_E(h)$ for all $\gamma \in \mathrm{GL}_2(F)$.
- It has trivial central character: $\psi_E(hz) = \psi_E(h)$ for all $z \in Z(\mathbb{A})$.
- It is right $\mathbb{K}_0(\mathfrak{n})$-invariant: $\psi_E(hk) = \psi_E(h)$ for all $k \in \mathbb{K}_0(\mathfrak{n})$.
- It is cuspidal:

$$\int_{F\backslash\mathbb{A}} \psi_E\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} h\right) d\mu(x) = 0 \text{ for all } h \in \mathrm{GL}_2(\mathbb{A}).$$

- Its Fourier coefficients are a:

$$a(\mathfrak{m}\mathfrak{d}) = \mu(F\backslash\mathbb{A})^{-1}\int_{F\backslash\mathbb{A}} \psi_E\Big(\begin{pmatrix}\overline{\mathfrak{m}} & x\\ 0 & 1\end{pmatrix}\Big)\tau(-x)d\mu(x) \text{ for all } \mathfrak{m}\in \mathrm{Div}(\mathcal{C}),$$

  where $\overline{\mathfrak{m}}\in\mathbb{A}^*$ and $(\overline{\mathfrak{m}}) = \mathfrak{m}$.

Note that the last two conditions make sense because of the first; we may (and will) consider ψ_E as a function on $\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})$ as well.

Proposition 2.3. *There is a unique normalised Hecke eigenform attached to E.*

This claim is certainly very well known, and the only fact that needs an additional argument is that ψ_E takes only rational values. Since we will shortly prove a stronger claim, we omit the proof. By a classical theorem of Harder [1974], the normalised Hecke eigenform ψ_E is supported on a finite set as a function on the double coset $\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})/\mathbb{K}_0(\mathfrak{n})Z(\mathbb{A})$. Let $L(E)\subseteq\mathbb{Q}$ denote the $\mathbb{Z}$-module generated by the values of ψ_E. Then there is a unique positive rational number $c(E)\in\mathbb{Q}$ such that $L(E) = c(E)\mathbb{Z}$.

Proposition 2.4. *There is a nonnegative natural number $m(E)$ such that $c(E) = p^{-m(E)}$.*

As mentioned in the introduction, we call $m(E)$ the Manin constant of the elliptic curve E.

Proof. First we show that $L(E)\subseteq\mathbb{Z}[\frac{1}{p}]$. By the approximation theorem, we have $\mathrm{GL}_2(\mathbb{A}) = \mathrm{GL}_2(F)P(\mathbb{A})Z(\mathbb{A})\mathbb{K}_0(\mathfrak{n})$. Therefore it will suffice to prove that $\psi_E(h)\in\mathbb{Z}[\frac{1}{p}]$ for every element h of $P(\mathbb{A})$. By the definition of Fourier coefficients,

$$\psi_E\Big(\begin{pmatrix}y & x\\ 0 & 1\end{pmatrix}\Big) = \sum_{\eta\in F^*} a(\eta y\mathfrak{d}^{-1})\tau(\eta x) = \sum_{\eta\in S} a(\eta y\mathfrak{d}^{-1})\Big(\sum_{\epsilon\in\mathbb{F}_q^*}\tau(\eta\epsilon x)\Big)$$

for all $y\in\mathbb{A}^*$, $x\in\mathbb{A}$, where S is a set of representatives of the quotient $\mathbb{F}_q^*\backslash F^*$, since ψ_E is cuspidal. The character sums on the right side are all equal to -1 or $q-1$. Moreover, the sum above is finite. As $a(\mathfrak{m})\in\mathbb{Z}[\frac{1}{p}]$ for every effective divisor $\mathfrak{m}$, the claim is now clear. Now we only need to show that $-1\in L(E)$ in order to prove the proposition. Let $\overline{\mathfrak{d}}\in\mathbb{A}^*$ be such that $(\overline{\mathfrak{d}}) = \mathfrak{d}$. Then by the Fourier expansion,

$$\psi_E\Big(\begin{pmatrix}\overline{\mathfrak{d}} & x\\ 0 & 1\end{pmatrix}\Big) = \sum_{\eta\in F^*} a(\eta)\tau(\eta x) = \sum_{\epsilon\in\mathbb{F}_q^*} a(\epsilon)\tau(\epsilon x) = \sum_{\epsilon\in\mathbb{F}_q^*}\tau(\epsilon x),$$

because $F^*\cap\mathcal{O} = \mathbb{F}_q^*$ and $a(1) = 1$ by definition. The character sum on the right side is equal to -1 if $x\notin\mathfrak{D}$. □

3. Epsilon constants and toric integrals

Notation 3.1. For the rest of the paper, fix a prime number l different from p. By the axiom of choice we may pick an isomorphism $\iota : \overline{\mathbb{Q}}_l \to \mathbb{C}$. We will identify $\overline{\mathbb{Q}}_l$ with $\mathbb{C}$ via ι in all that follows. Let E_l be a finite extension of $\mathbb{Q}_l$ and let $\rho : \mathrm{Gal}(\overline{F} \,|\, F) \to \mathrm{GL}_{E_l}(W)$ be an l-adic representation on a finite dimensional vector space W over E_l. Moreover, let $L(\rho, t) \in E_l[\![t]\!]$ denote the Grothendieck L-function associated to ρ as defined in [Deligne 1973, 9.1]. By a classical theorem of Grothendieck [Deligne 1973, §10], the series $L(\rho, t)$ is a rational function in the variable t and also satisfies the functional equation

$$L(\rho, t) = \epsilon(\rho) t^{\alpha(\rho)} L(\rho^\vee, q^{-1} t^{-1}),$$

where $\alpha(\rho) \in \mathbb{Z}$, $\epsilon(\rho) \in E_l^*$ and $\rho^\vee$ are the degree of the conductor of ρ (in the sense of [Laumon 1987, page 179]), the ϵ-constant of ρ, and the dual l-adic representation on $\mathrm{Hom}(W, E_l)$, respectively.

Notation 3.2. Let K be a local field, let dx be a Haar measure on K, and let ψ be a nontrivial additive character on K. For every continuous homomorphism $\alpha : K^* \to \mathbb{C}^*$, let $\epsilon(K, \alpha, \psi, dx)$ denote the local ϵ-factor attached to the triple (α, ψ, dx) as defined in [Deligne 1973, 3.3]. Let $W(\overline{K} \,|\, K) < \mathrm{Gal}(\overline{K} \,|\, K)$ denote the Weil group of K (as defined in [Deligne 1973, 2.2.4]). Local class field theory furnishes an isomorphism $j : K^* \to W(\overline{K} \,|\, K)^{ab}$. We normalise this isomorphism so that for every uniformiser $\pi \in K^*$, the image of $j(\pi)$ with respect to the map $W(\overline{K} \,|\, K) \to \mathbb{Z}$ introduced in [Deligne 1973, 2.2.4] is the geometric Frobenius (similarly to [Deligne 1973, 2.3]). For every homomorphism $\alpha : \mathrm{Gal}(\overline{K} \,|\, K) \to \mathbb{C}^*$, let the same symbol α denote the composition of j, considered here as an imbedding $j : K^* \to \mathrm{Gal}(\overline{K} \,|\, K)^{ab}$, with the map $\mathrm{Gal}(\overline{K} \,|\, K)^{ab} \to \mathbb{C}^*$ induced by the character α by slight abuse of notation.

Notation 3.3. For every $x \in |\mathcal{C}|$, let F_x and $\mathbb{O}_x$ denote the completion of F at x and the valuation ring of F_x, respectively. For every $x \in |\mathcal{C}|$, let μ_x and μ_x^* be the unique Haar measures on the locally compact abelian topological groups F_x and F_x^*, respectively, so that $\mu(\mathbb{O}_x)$ and $\mu^*(\mathbb{O}_x^*)$ are both equal to 1. Moreover, for every $x \in |\mathcal{C}|$ let $\tau_x : F_x \to \mathbb{C}^*$ be the unique continuous additive character such that $\tau(a) = \prod_{x \in |\mathcal{C}|} \tau_x(a_x)$ for every $a \in \mathbb{A}$. For every homomorphism $\alpha : \mathrm{Gal}(\overline{F} \,|\, F) \to \mathbb{C}^*$ and for every $x \in |\mathcal{C}|$, let $\alpha_x : \mathrm{Gal}(\overline{F}_x \,|\, F) \to \mathbb{C}^*$ denote the restriction of α onto the decomposition group at x.

Theorem 3.4. *For every continuous homomorphism $\alpha : \mathrm{Gal}(\overline{K} \,|\, K) \to \mathbb{C}^*$ with finite image,*

$$\epsilon(\alpha) = q^{1-g} \prod_{x \in |\mathcal{C}|} \epsilon(F_x, \alpha_x, \tau_x, \mu_x).$$

Proof. This is just a special case of [Laumon 1987, théorème 3.2.1.1]. □

Definition 3.5. For every divisor $\mathfrak{m}$ on $\mathscr{C}$, let $\underline{\mathfrak{m}}$ denote the support of $\mathfrak{m}$. Let $c \in \mathbb{A}^*$ be an idèle so that $\mathfrak{c} = (c)$ is an effective divisor on $\mathscr{C}$. For every such c, let $\hat{c} \in \mathbb{A}$ be the unique adèle such that $\hat{c}_x = c_x^{-1}$ for every $x \in \underline{\mathfrak{c}}$, and $\hat{c}_x = 0$ otherwise. Let $\alpha : F\backslash\mathbb{A}^* \to \mathbb{C}^*$ be a continuous character with finite image whose conductor $\mathfrak{c}'$ divides $\mathfrak{c}$. For every $z \in \mathbb{C}$, let $I(\psi_E, \mathfrak{c}, \alpha, z)$ denote the integral

$$I(\psi_E, \mathfrak{c}, \alpha, z) = \int_{F^*\backslash\mathbb{A}^*} \psi_E\left(\begin{pmatrix} y & y\hat{c} \\ 0 & 1 \end{pmatrix}\right)\alpha(y)z^{\deg(y)}d\mu^*(y) \in \mathbb{C}.$$

Lemma 3.6. *The integral $I(\psi_E, \mathfrak{c}, \alpha, z)$ is well-defined and independent of the choice of c, as the notation indicates.*

Proof. By [Tan 1993, Lemma 2], the integrand of $I(\psi_E, \mathfrak{c}, \alpha, z)$ is compactly supported. Hence $I(\psi_E, \mathfrak{c}, \alpha, z)$ is well-defined. Choose another idèle $c' \in \mathbb{A}^*$ such that $(c') = \mathfrak{c}$. Then there is an $u \in \mathbb{O}^*$ such that $c' = uc$ and therefore $\hat{c}\,' = u\hat{c}$. Now the claim follows from the $\mathrm{GL}_2(\mathbb{O})$-invariance of ψ_E. □

Notation 3.7. Let $W(\bar{F}\,|\,F) < \mathrm{Gal}(\bar{F}\,|\,F)$ denote the Weil group of F (as defined in [Deligne 1973, 2.4]). Global class field theory furnishes an isomorphism

$$\mathbf{j} : F^*\backslash\mathbb{A}^* \to W(\bar{F}\,|\,F)^{ab}$$

that is compatible with the isomorphism between F_x^* and $W(\bar{F}_x\,|\,F_x)^{ab}$ introduced in Notation 3.2 for every $x \in |\mathscr{C}|$ (in the sense of [Deligne 1973, 2.4]). For every homomorphism $\alpha : \mathrm{Gal}(\bar{F}\,|\,F) \to \mathbb{C}^*$, let the same symbol α denote the composition of $\mathbf{j}$, considered here as an imbedding $\mathbf{j} : F^*\backslash\mathbb{A}^* \to \mathrm{Gal}(\bar{F}\,|\,F)^{ab}$, with the map $\mathrm{Gal}(\bar{F}\,|\,F)^{ab} \to \mathbb{C}^*$ induced by the character α. Moreover, let α also denote the composition of the quotient map $\mathbb{A}^* \to F^*\backslash\mathbb{A}^*$ and the map $\alpha : F^*\backslash\mathbb{A}^* \to \mathbb{C}^*$ introduced above by the usual abuse of notation.

Notation 3.8. For every divisor $\mathfrak{m}$ on $\mathscr{C}$ relatively prime to $\mathfrak{c}$, and for every $\overline{\mathfrak{m}} \in \mathbb{A}^*$ such that $(\overline{\mathfrak{m}}) = \mathfrak{m}$, the complex number $\alpha(\overline{\mathfrak{m}})$ is independent of the choice of $\overline{\mathfrak{m}}$. We let $\alpha(\mathfrak{m})$ denote this common value. Let σ_E denote the natural l-adic representation of $\mathrm{Gal}(\bar{F}\,|\,F)$ on the cohomology group $H^1(E_{\bar{F}}, \mathbb{Q}_l)$. By definition, $L(E, t) = L(\sigma_E, t)$. The twisted L-function $L(\sigma_E \otimes \alpha, t)$ is actually a polynomial in the variable t, and therefore it can be evaluated at any complex number $t = z$. Finally, let $G(E, \alpha, \mathfrak{c}, t) \in \mathbb{C}[t]$ denote the polynomial

$$G(E, \alpha, \mathfrak{c}, t) = \prod_{x \in \underline{\mathfrak{c}} - \underline{\mathfrak{c}}'} \left(-1 + a(x)\alpha(x)(qt)^{\deg(x)} - \alpha(x)^2 t^{2\deg(x)}\right).$$

Proposition 3.9. *Assume that* $\mathfrak{c}$ *is square-free and relatively prime to* $\mathfrak{dn}$. *Then*

$$I(\psi_E, \mathfrak{c}, \alpha, z) = \alpha(\mathfrak{d}^2\mathfrak{c}')\epsilon(\alpha^{-1})\prod_{x\in\underline{\mathfrak{c}}}(q^{\deg(x)}-1)^{-1}\Big(\frac{z^2}{q}\Big)^{g-1}G(E,\alpha,\mathfrak{c},z)L(\sigma_E\otimes\alpha, zq^{-1}).$$

Proof. According to the Fourier expansion of ψ_E, we have

$$\psi_E\Big(\begin{pmatrix} y & y\hat{c} \\ 0 & 1\end{pmatrix}\Big) = \sum_{\eta\in F^*} a(\eta y\mathfrak{d}^{-1})\tau(\eta y\hat{c})$$

for every $y\in\mathbb{A}^*$, and the sum on the right is finite. If we interchange this summation and the integration, we get

$$I(\psi_E, \mathfrak{c}, \alpha, q^{-s}) = \int_{\mathbb{A}^*} a(y\mathfrak{d}^{-1})\tau(y\hat{c})\alpha(y)q^{-s\deg(y)}d\mu^*(y) \tag{1}$$

for every $s\in\mathbb{C}$. This computation is justified by Lebesgue's convergence theorem if the second integral is absolutely convergent. This is so if $\operatorname{Re} s > \frac{1}{2}$, as the function $y\mapsto a(y\mathfrak{d}^{-1})$ has support on $\mathfrak{d}^{-1}\mathbb{O}$ and

$$|a(y\mathfrak{d}^{-1})\tau(y\hat{c})| = |a(y\mathfrak{d}^{-1})| \le 2q^{-1/2\deg(y\mathfrak{d}^{-1})}$$

by the Weil conjectures.

Let $\mathbb{A}_{\mathfrak{c}}$ and $\mathbb{O}_{\mathfrak{c}}$ denote the restricted direct products $\prod'_{x\notin\underline{\mathfrak{c}}}F_x$ and $\prod'_{x\notin\underline{\mathfrak{c}}}\mathbb{O}_x$, respectively. Then $\mathbb{A}_{\mathfrak{c}}$ is a locally compact topological ring and $\mathbb{O}_{\mathfrak{c}}$ is its maximal compact subring. Let $\nu^*_{\mathfrak{c}}$ be a Haar measure on $\mathbb{A}^*_{\mathfrak{c}}$ such that $\nu^*_{\mathfrak{c}}(\mathbb{O}^*_{\mathfrak{c}})$ is equal to 1. Let $|\cdot|_x$ be the absolute value on F_x normalised so that $\mu_x(t\mathbb{O}) = |t|_x$ for every $y\in F_x$. Using Fubini's theorem, the integral (1) can be rewritten as

$$\int_{\mathbb{A}^*_{\mathfrak{c}}} a(y\mathfrak{d}^{-1})\alpha(y)q^{-s\deg(y)}d\nu^*_{\mathfrak{c}}(y)\cdot\prod_{x\in\underline{\mathfrak{c}}}\int_{F_x^*}a(t)\tau_x(tc_x^{-1})\alpha_x(t)|t|_x^s d\mu_x^*(t). \tag{2}$$

The integrand of the first integral of (2) is invariant under multiplication by $\mathbb{O}^*_{\mathfrak{c}}$. Therefore it is equal to

$$\sum_{\substack{\mathfrak{m}\in\mathrm{Div}(\mathscr{C})\\ \underline{\mathfrak{m}}\cap\underline{\mathfrak{c}}=\varnothing}} a(\mathfrak{m})\alpha(\mathfrak{m}\mathfrak{d})q^{-s\deg(\mathfrak{m}\mathfrak{d})} = \alpha(\mathfrak{d})q^{-s\deg(\mathfrak{d})}\cdot\prod_{x\notin\underline{\mathfrak{c}}}L_x(\sigma_E\otimes\alpha, q^{-(s+1)}). \tag{3}$$

For every $x\in\underline{\mathfrak{c}}$, the corresponding term in the product (2) can be rewritten as

$$\int_{F_x^*}a(t)\tau_x(tc_x^{-1})\alpha_x(t)|t|_x^s d\mu_x^*(t) = \sum_{n=0}^{\infty}a(x^n)\alpha_x(c_x)^n|c_x|_x^{ns}\int_{\mathbb{O}_x^*}\tau_x(tc_x^{n-1})\alpha_x(t)d\mu_x^*(t), \tag{4}$$

because $c_x \in F_x^*$ is a uniformiser, and $a(x^n) = 0$ if $n < 0$. Suppose now that x divides the conductor of α. Then the restriction of α_x onto $\mathbb{O}_x^*$ is a nontrivial character, and therefore

$$\int_{\mathbb{O}_x^*} \tau_x(tc_x^{n-1})\alpha_x(t)d\mu_x^*(t) = \begin{cases} \dfrac{\alpha_x(c_x)}{q^{\deg(x)}-1}\epsilon(F_x, \alpha_x^{-1}, \tau_x, \mu_x) & \text{if } n = 0, \\ 0 & \text{otherwise,} \end{cases} \tag{5}$$

by [Deligne 1973, (3.4.3.2)] and the fact that the additive character τ_x restricted to $\mathbb{O}_x$ is trivial. Hence

$$\int_{F_x^*} a(t)\tau_x(tc_x^{-1})\alpha_x(t)|t|_x^s d\mu_x^*(t) = \frac{\alpha_x(c_x)}{q^{\deg(x)}-1}\epsilon(F_x, \alpha_x^{-1}, \tau_x, \mu_x) \tag{6}$$

in this case. Otherwise, the restriction of α_x onto $\mathbb{O}_v^*$ is the trivial character, and therefore the left side of (4) is equal to

$$\frac{-1}{q^{\deg(x)}-1} + \sum_{n=1}^{\infty} a(x^n)\alpha_x(c_x)^n|c_x|_x^{ns} = L_x(\sigma_E \otimes \alpha, q^{-(s+1)}) - \frac{q^{\deg(x)}}{q^{\deg(x)}-1}. \tag{7}$$

Because both σ_E and α are unramified at x, we have

$$L_x(\sigma_E \otimes \alpha, q^{-(s+1)}) = \left(1 - a(x)\alpha(x)q^{-s\deg(x)} + \alpha(x)^2 q^{-(2s+1)\deg(x)}\right)^{-1}. \tag{8}$$

Hence, in this case,

$$\begin{aligned} \int_{F_x^*} a(t)\tau_x(tc_x^{-1})\alpha_x(t)|t|_x^s d\mu_x^*(t) \\ = \frac{1}{q^{\deg(x)}-1}\left(-1 + a(x)\alpha(x)q^{(1-s)\deg(x)} - \alpha(x)^2 q^{-2s\deg(x)}\right) \\ \cdot L_x(\sigma_E \otimes \alpha, q^{-(s+1)}). \end{aligned} \tag{9}$$

By Theorem 3.4, we have

$$\epsilon(\alpha^{-1}) = q^{1-g}\alpha^{-1}(\mathfrak{d})q^{\deg(\mathfrak{d})}\prod_{x \in \underline{\mathfrak{c}}'} \epsilon(F_x, \alpha_x^{-1}, \tau_x, \mu_x), \tag{10}$$

because according to [Deligne 1973, (3.4.3.1)], we have

$$\epsilon(F_x, \alpha_x^{-1}, \tau_x, \mu_x) = \alpha_x^{-1}(\mathfrak{d}_x)q^{\deg(\mathfrak{d}_x)}$$

if α_x is unramified, since we assumed that $\mu_x(\mathbb{O}_x) = 1$ and $\mathfrak{c}$ and $\mathfrak{d}$ are relatively prime. Combining (3), (6), (9), and (10), we get

$$\begin{aligned} I(\psi_E, \mathfrak{c}, \alpha, q^{-s}) = \alpha(\mathfrak{d}^2\mathfrak{c}')\epsilon(\alpha^{-1})q^{g-1-(s+1)\deg(\mathfrak{d})}\prod_{x \in \underline{\mathfrak{c}}}(q^{\deg(x)}-1)^{-1} \\ \cdot G(E, \alpha, \mathfrak{c}, q^{-s})L(\sigma_E \otimes \alpha, q^{-(s+1)}), \end{aligned} \tag{11}$$

if we also use that $L_x(\sigma_E \otimes \alpha, q^{-(s+1)}) = 1$ when $x \in \underline{\mathfrak{c}}'$. Because $\deg(\mathfrak{d}) = 2g-2$, the claim now follows for every complex number q^{-s} such that $\operatorname{Re} s > \frac{1}{2}$. But both sides of the equation in the proposition above are polynomials in z; hence the claim must hold for every complex number as well. □

4. Lower and upper bounds

Notation 4.1. For every field K, let $\overline{K}$ denote a separable closure of K. Let $v_q : \overline{\mathbb{Q}}_p^* \to \mathbb{Q}$ denote the p-adic valuation normalised such that $v_q(q) = 1$. Every polynomial $P(t) \in \overline{\mathbb{Q}}_p[t]$ can be written in the form

$$P(t) = at^k \prod_{i=1}^{n-k} (1 - \lambda_i t), \quad a \in \overline{\mathbb{Q}}_p^*, \quad \lambda_i \in \overline{\mathbb{Q}}_p,$$

where the λ_i are the reciprocal roots of $P(t)$. Let $l_q(P(t)) \in \mathbb{Q}$ denote the nonnegative number

$$l_q(P(t)) = \sum_{v_q(\lambda_i) \le 1} (1 - v_q(\lambda_i)).$$

Let μ_∞, $\mu_{\infty,p} \subset \overline{\mathbb{Q}}_p^*$ denote the subgroup of roots of unity and of roots of unity whose order is prime to p, respectively.

Lemma 4.2. *With the same notation as above*,

$$\min_{\epsilon \in \mu_\infty} (v_q(P(\epsilon q^{-1}))) = v_q(a) - k - l_q(P(t)).$$

Moreover, the minimum is attained at all but finitely many $\epsilon \in \mu_{\infty,p}$.

Proof. For a fixed $i = 1, 2, \ldots, k$ and for every $\epsilon \in \mu_\infty$, we have

$$v_q(1 - \lambda_i \epsilon q^{-1}) = -1 + v_q(\lambda_i - \epsilon^{-1} q) \ge \min\{0, v_q(\lambda_i) - 1\},$$

so for all but finitely many $\epsilon \in \mu_{\infty,p}$, we have

$$v_q(1 - \lambda_i \epsilon q^{-1}) = \min\{0, v_q(\lambda_i) - 1\}.$$

Therefore, for all but finitely many $\epsilon \in \mu_{\infty,p}$,

$$v_q(P(\epsilon q^{-1})) = \min_{\zeta \in \mu_\infty} (v_q(P(\zeta q^{-1}))) = v_q(a) - k + \sum_{i=1}^{\deg(P)} \min\{0, v_q(\lambda_i) - 1\}. \quad \square$$

Let $\mathfrak{c}$ be a square-free effective divisor on $\mathscr{C}$ that is relatively prime to $\mathfrak{d}\mathfrak{n}$. Let $\alpha : F \backslash \mathbb{A}^* \to \mathbb{C}^*$ be a continuous character with finite image whose conductor $\mathfrak{c}'$ divides $\mathfrak{c}$.

Lemma 4.3. *The minimum of* $v_q(G(E, \alpha, \mathfrak{c}, \epsilon))$ *for* ϵ *ranging over* μ_∞ *is zero, and it is attained at all but finitely many* $\epsilon \in \mu_{\infty,p}$.

Proof. For every $x \in \underline{\mathfrak{c}} - \underline{\mathfrak{c}}'$, we have $q^{\deg(x)}a(x) \in \mathbb{Z}$. Hence, for every $\epsilon \in \mu_\infty$ and x as above, we have

$$v_q(-1 + a(x)\alpha(x)q^{\deg(x)}\epsilon^{\deg(x)} - \alpha(x)^2\epsilon^{2\deg(x)}) \geq 0,$$

and for all but finitely many $\epsilon \in \mu_{\infty,p}$, the left side is equal to 0. The claim follows by taking the product over all $x \in \underline{\mathfrak{c}} - \underline{\mathfrak{c}}'$. □

Lemma 4.4. *For every $y \in \mathbb{A}^*$ and $x \in \mathbb{A}$, there are $\eta \in F$, $u \in \mathbb{O}$ and $c \in \mathbb{A}^*$ such that (c) is a square-free effective divisor that is relatively prime to $\mathfrak{n}$ and*

$$x + u + y^{-1}\eta = \hat{c}.$$

Proof. Let $z \in \mathbb{A}^*$ be the unique idèle such that for every $v \in |\mathscr{C}|$ we have $z_v = x_v^{-1}$ if $x_v \notin \mathbb{O}_v$, and $z_v = 1$ otherwise. Then $\mathfrak{z} = (z)$ is an effective divisor. Let $\mathfrak{y}$ denote the divisor of y^{-1} and let $\mathfrak{b}$ be a square-free effective divisor whose degree is at least $2g - 1 - \deg(\mathfrak{y})$ and which is relatively prime to $\mathfrak{n}\mathfrak{z}$. Let Z denote the closed scheme of $\mathscr{C}$ whose sheaf of ideals is $\mathbb{O}_{\mathscr{C}}(\mathfrak{z})^\vee \subseteq \mathbb{O}_{\mathscr{C}}$, where for every vector bundle $\mathscr{F}$ on $\mathscr{C}$ we let $\mathscr{F}^\vee$ denote the dual of $\mathscr{F}$. We have an exact sequence

$$H^0(\mathscr{C}, \mathbb{O}_{\mathscr{C}}(\mathfrak{y}\mathfrak{b})) \longrightarrow H^0(\mathscr{C}, \mathbb{O}_{\mathscr{C}}(\mathfrak{z}\mathfrak{y}\mathfrak{b})) \xrightarrow{i_Z} H^0(Z, \mathbb{O}_{\mathscr{C}}(\mathfrak{z}\mathfrak{y}\mathfrak{b})|_Z),$$

where the first map is induced by the inclusion $\mathbb{O}_{\mathscr{C}}(\mathfrak{y}\mathfrak{b}) \subset \mathbb{O}_{\mathscr{C}}(\mathfrak{z}\mathfrak{y}\mathfrak{b})$, and the second map i_Z is the restriction map. By the Riemann–Roch theorem for curves,

$$\dim_{\mathbb{F}_q} H^0(\mathscr{C}, \mathscr{F}) = 2 - 2g + \deg(\mathscr{F})$$

for every line bundle $\mathscr{F}$ on $\mathscr{C}$ whose degree is at least $2g - 1$. Comparing the dimensions of $H^0(\mathscr{C}, \mathbb{O}_{\mathscr{C}}(\mathfrak{y}\mathfrak{b}))$ and $H^0(\mathscr{C}, \mathbb{O}_{\mathscr{C}}(\mathfrak{z}\mathfrak{y}\mathfrak{b}))$, we get that the image of i_Z has dimension $\deg(\mathfrak{z})$ over $\mathbb{F}_q$. But the dimension of $H^0(Z, \mathbb{O}_{\mathscr{C}}(\mathfrak{z}\mathfrak{y}\mathfrak{b})|_Z)$ is the same, and hence i_Z is surjective.

Let $b \in \mathbb{A}^*$ be an idèle such that $(b) = \mathfrak{b}$ and $b_v = 1$ for every $v \notin \underline{\mathfrak{b}}$. Recall that for every idèle $t \in \mathbb{A}^*$ we have: $H^0(\mathscr{C}, \mathbb{O}_{\mathscr{C}}(t)) = F \cap t^{-1}\mathbb{O}$. Moreover, for every such t we have $H^0(Z, \mathbb{O}_{\mathscr{C}}(t\mathfrak{z})|_Z) = (tz)^{-1}\mathbb{O}/t^{-1}\mathbb{O}$. Under these identifications, i_Z is the composition of the inclusion $F \cap (zb)^{-1}y\mathbb{O} \to (zb)^{-1}y\mathbb{O}$ and the reduction map $(zb)^{-1}y\mathbb{O} \to (zb)^{-1}y\mathbb{O}/b^{-1}y\mathbb{O}$. Therefore, there is an $\eta \in F$ such that for every $v \in |\mathscr{C}|$, we have $(zby^{-1}\eta)_v \in -1 + z_v\mathbb{O}_v$ if $v \in \underline{\mathfrak{z}}$, and $(zy^{-1}b\eta)_v = (y^{-1}b\eta)_v \in \mathbb{O}_v$ otherwise. Because $\mathfrak{b}$ is relatively prime to $\mathfrak{z}$, we get that $(y^{-1}\eta)_v \in -x_v + \mathbb{O}_v$ if $v \in \underline{\mathfrak{z}}$. Let $c \in \mathbb{A}^*$ be the unique idèle such that $c_v = (y\eta^{-1})_v$ if $v \notin \underline{\mathfrak{z}}$ and $(y^{-1}\eta)_v \notin \mathbb{O}_v$, and $c_v = 1$ otherwise. Thus (c) divides $\mathfrak{b}$, so it is a square-free effective divisor relatively prime to $\mathfrak{n}$. Let $u = -x - y^{-1}\eta + \hat{c}$. By the above, $u \in \mathbb{O}$, so this choice of η, c and u satisfies the requirements of the claim. □

Let $\mathbb{X}(\mathfrak{n})$ denote the set of tamely ramified continuous characters $F\backslash\mathbb{A}^* \to \mathbb{C}^*$ with finite image whose conductor is relatively prime to $\mathfrak{n}$.

Proposition 4.5.

$$m(E) \geq d \cdot \sup_{\alpha \in \mathbb{X}(\mathfrak{n})} \big(l_q(L(\sigma_E \otimes \alpha, t)) + g - 1 - v_q(\epsilon(\alpha^{-1})) \big).$$

When p does not divide the order of $\mathrm{Pic}_0(\mathscr{C})(\mathbb{F}_q)$, *the two sides are equal.*

Proof. Fix an isomorphism $\overline{\mathbb{Q}}_p \cong \mathbb{C}$ and let $\alpha \in \mathbb{X}(\mathfrak{n})$ have conductor $\mathfrak{c}$. Without loss of generality, we may assume that $\mathfrak{c}$ is relatively prime to $\mathfrak{d}$ by changing τ, if necessary. According to Proposition 3.9,

$$I(\psi_E, \mathfrak{c}, \alpha, z) = \alpha(\mathfrak{d}^2\mathfrak{c}')\epsilon(\alpha^{-1}) \prod_{x \in \underline{\mathfrak{c}}} (q^{\deg(x)} - 1)^{-1} (z^2/q)^{g-1} L(\sigma_E \otimes \alpha, zq^{-1}). \quad (12)$$

Let $\mathbb{O}_{\mathfrak{c}} < \mathbb{A}^*$ denote the subgroup $\mathbb{O}^*$ if $\mathfrak{c} = 1$, and $1 + \mathfrak{c}\mathbb{O}$ otherwise. The integrand of the integral on the left side of (12) is constant on the cosets of the subgroup $\mathcal{U}_{\mathfrak{c}} < F^*\backslash\mathbb{A}^*$, where $\mathcal{U}_{\mathfrak{c}} = (\mathbb{F}_q^* \cap \mathbb{O}_c)\backslash\mathbb{O}_c$. Because $\mathfrak{c}$ is square-free, p does not divide $|\mathbb{O}^*/\mathbb{O}_{\mathfrak{c}}|$. Hence $\mu^*(\mathcal{U}_{\mathfrak{c}})$ is a rational number whose denominator is not divisible by p. Therefore $I(\psi_E, \mathfrak{c}, \alpha, \epsilon) \in p^{-m(E)}\mathbb{Z}_p[\epsilon]$ for every $\epsilon \in \mu_\infty$. In particular, $v_q(I(\psi_E, \mathfrak{c}, \alpha, \epsilon))$ is at least $-m(E)/d$. Note that for every $\alpha \in \mathbb{X}(\mathfrak{n})$,

$$L(\sigma_E \otimes \alpha, t) \in 1 + t\overline{\mathbb{Q}}_p[t],$$

and hence by Lemma 4.2 there is an $\epsilon \in \mu_\infty$ such that $v_q(L(\sigma_E \otimes \alpha, \epsilon q^{-1})) = -l_q(L(\sigma_E \otimes \alpha, t))$. Hence the first part of the claim above is true.

Assume now that p does not divide the order of $\mathrm{Pic}_0(\mathscr{C})(\mathbb{F}_q)$, and let $h(E)$ denote the right side of the inequality in Proposition 4.5. As we already noted in the proof of Proposition 2.4, in order to show the second half of the claim, we only need to show that $p^{h(E)}\psi_E(g) \in \mathbb{Z}$ for every element $g = \left(\begin{smallmatrix} y & yx \\ 0 & 1 \end{smallmatrix}\right) \in P(\mathbb{A})$. By Lemma 4.4, there are $\eta \in F$, $u \in \mathbb{O}$ and $c \in \mathbb{A}^*$ such that (c) is a square-free effective divisor that is relatively prime to $\mathfrak{n}$ and $x + u + y^{-1}\eta = \hat{c}$. Because

$$\begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} y & yx \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} y & y(x + u + y^{-1}\eta) \\ 0 & 1 \end{pmatrix}$$

and ψ_E is invariant on the left with respect to $P(F)$ and on the right with respect to $P(\mathbb{O})$, we may assume that $x = \hat{c}$.

Let $\mathfrak{c}$ be (c) and let H denote the quotient group $\mathbb{A}^*/F^*\mathbb{O}_{\mathfrak{c}}$, where we continue to use the notation above. Then H can be decomposed as a direct product $G \times \mathbb{Z}$, where G is a finite subgroup. By class field theory, $|G| = |\mathrm{Pic}_0(\mathscr{C})| \cdot |\mathbb{O}^*/(\mathbb{O}_{\mathfrak{c}}\mathbb{F}_q^*)|$. As noted above, p does not divide $|\mathbb{O}^*/\mathbb{O}_{\mathfrak{c}}|$, and hence does not divide the order of G by our assumption. Let $(\,\cdot\,)_H : \mathbb{A}^* \to H$ be the quotient map and let $[\,\cdot\,] : H \to G$ denote the projection onto the factor G. Note that for every $y \in \mathbb{A}^*$, the value

$$\psi_E\left(\begin{pmatrix} y & y\hat{c} \\ 0 & 1 \end{pmatrix}\right) t^{\deg(y)} \in \mathbb{Q}[G][t, t^{-1}]$$

only depends on $(y)_H$. Let $f : H \to \mathbb{Q}[t, t^{-1}]$ be the corresponding function, and define $I = \sum_{\substack{g\in G \\ n\in\mathbb{Z}}} c_{g,n} g t^n \in \mathbb{Q}[G][t, t^{-1}]$ by the formula

$$I = \sum_{g\in G} \Big(\sum_{\substack{h\in H \\ [h]=g}} f(h) \Big) g.$$

The function I is well-defined because for every $g \in G$, the set of those $h \in H$ such that $[h] = g$ and $f(y) \neq 0$ is finite. Also the set $\{c_{g,n} | g \in G, n \in \mathbb{Z}\}$ and the image of the function $\mathbb{A}^* \to \mathbb{Q}$ given by the rule $y \mapsto \psi_E\big(\left(\begin{smallmatrix} y & y\hat{c} \\ 0 & 1 \end{smallmatrix}\right)\big)$ are equal, and hence it will suffice to show that $p^{h(E)} I \in \mathbb{Z}[G][t, t^{-1}]$. For every group homomorphism $\alpha : G \to \overline{\mathbb{Q}}_p^*$, by slight abuse of notation, let the same symbol α denote the unique ring homomorphism $\mathbb{Q}[G][t, t^{-1}] \to \overline{\mathbb{Q}}_p[t, t^{-1}]$, whose restriction onto G is α and $\alpha(t) = t$. Because p does not divide $|G|$, it will suffice to show that $v_q(a) \leq -h(E)/d$ for every coefficient a of $\alpha(I)$ for every α as above. Let the symbol α denote also the composition $\alpha \circ [\,\cdot\,] \circ (\,\cdot\,)_H : \mathbb{A}^* \to \overline{\mathbb{Q}}_p^*$. Choose the character τ so that $\mathfrak{d}$ is relatively prime to $\mathfrak{c}$. Then $\alpha(I)$ is the polynomial

$$\alpha(I) = \alpha(\mathfrak{d}^2\mathfrak{c}')\epsilon(\alpha^{-1}) \prod_{x\in\underline{\mathfrak{c}}} (q^{\deg(x)} - 1)^{-1} \Big(\frac{t^2}{q}\Big)^{g-1} G(E, \alpha, \mathfrak{c}, t) L(\sigma_E \otimes \alpha, tq^{-1})$$

by Proposition 3.9. Since for every polynomial $P(t) = \sum_{k=0}^{N} b_k t^k \in \overline{\mathbb{Q}}_p$ we have

$$\min_{\epsilon\in\mu_\infty} (v_q(P(\epsilon))) = \min_{0\leq k\leq N} (v_q(b_k)),$$

the claim now follows from Lemmas 4.2 and 4.3. □

5. Galois module structure of the coherent cohomology of elliptic surfaces

Definition 5.1. In this section, G will be a finite group. Let A be a noetherian ring and let Y be a scheme that is separated and of finite type over $\mathrm{Spec}(A)$. By an $A[G]$-module on Y, we mean a sheaf of $A[G]$-modules on Y. These form the objects of a category whose morphisms are maps respecting the $A[G]$-module structure. Suppose now that $\mathcal{F}$ is an $A[G]$-module on Y that is also an $\mathcal{O}_Y$-module in such a way that the actions of $\mathcal{O}_Y$ and G commute and the $A[G]$-module structure of $\mathcal{F}$ respects the structure morphism $Y \to \mathrm{Spec}(A)$. If $\mathcal{F}$ is also a quasicoherent or coherent $\mathcal{O}_Y$-module, then we will call $\mathcal{F}$ a quasicoherent or coherent $\mathcal{O}_Y[G]$-module, respectively. As noted in [Chinburg 1994, p. 447], there are enough injectives in the category of $A[G]$-modules on Y, and hence the global section functor Γ has a derived functor into the localisation of the category of complexes of $A[G]$-complexes bounded from below with respect to the multiplicative system of quasiisomorphisms which will be denoted by $R\Gamma^+$.

Definition 5.2. An $A[G]$-module M is cohomologically trivial if the Tate cohomology group $\widehat{H}^i(H, M)$ vanishes for all subgroups H of G and for all integers i. Let $CT(A[G])$ denote the Grothendieck group of all finitely generated $A[G]$-modules that are cohomologically trivial. For every cohomologically trivial $A[G]$-module M, let $[M]$ denote its class in $CT(A[G])$). Suppose that $\mathcal{F}$ is a quasicoherent $\mathcal{O}_Y$-module such that each stalk of $\mathcal{F}$ is a cohomologically trivial $A[G]$-module. Then by [Chinburg 1994, Theorem 1.1], the complex $R\Gamma^+(\mathcal{F})$ is isomorphic in the derived category of $A[G]$-modules to a bounded complex M^* of finitely generated cohomologically trivial $A[G]$-modules. Moreover, the Euler characteristic $\sum(-1)^i[M^i]$ in $CT(A[G])$ only depends on $\mathcal{F}$ and will be denoted by $\chi(\mathcal{F})$.

Definition 5.3. Let X be a normal scheme that is of finite type over $\mathrm{Spec}(A)$. Assume that the finite group G acts on X on the left. Let $\mathcal{F}$ be a coherent sheaf on X. A G-linearisation on $\mathcal{F}$ is a collection $\Psi = \{\psi_g\}_{g\in G}$ of isomorphisms $\psi_g : g_*(\mathcal{F}) \to \mathcal{F}$ for every $g \in G$ such that

- $\psi_1 = \mathrm{Id}_{\mathcal{F}}$ and
- for every $g, h \in G$ we have $\psi_{hg} = \psi_h \circ h_*(\psi_g)$,

where $h_*(\psi_g) : (hg)_*(\mathcal{F}) = h_*(g_*(\mathcal{F})) \to h_*(\mathcal{F})$ is the direct image of the map $\psi_g : g_*(\mathcal{F}) \to \mathcal{F}$ under the action of h. We define a G-sheaf over X to be a sheaf on X equipped with a G-linearisation. A coherent G-sheaf is a coherent sheaf on X equipped with a G-linearisation Ψ such that $\psi_g : g_*(\mathcal{F}) \to \mathcal{F}$ is $\mathcal{O}_X$-linear for every $g \in G$.

Definition 5.4. Let $f : X \to Y$ be a tame G-cover as defined in [Chinburg 1994, Definition 2.2], and let $\mathcal{F}$ be a coherent G-sheaf on X. The G-linearisation on $\mathcal{F}$ induces an $\mathcal{O}_Y$-linear action of G on the direct image sheaf $f_*(\mathcal{F})$ that makes the latter a coherent $\mathcal{O}_Y[G]$-module. By [Chinburg 1994, Theorem 2.7], each stalk of the $\mathcal{O}_Y[G]$-sheaf $f_*(\mathcal{F})$ is a cohomologically trivial $A[G]$-module. Hence the Euler characteristic $\chi(f_*(\mathcal{F})) \in CT(A[G])$ introduced in Definition 5.2 is well-defined, and will be denoted by $\chi(G, \mathcal{F})$.

Now suppose that A is a field and that its characteristic does not divide the order of G. Then every finitely generated $A[G]$-module is cohomologically trivial. Also assume that Y is proper over $\mathrm{Spec}(A)$, and let $\mathcal{F}$ be again a coherent G-sheaf on X. Then for every $n \in \mathbb{N}$, the cohomology group $H^n(X, \mathcal{F})$ is a cohomologically trivial, finitely generated $A[G]$-module with respect to the natural $A[G]$-action.

Lemma 5.5. $\chi(G, \mathcal{F}) = \sum_{n\in\mathbb{N}} (-1)^n [H^n(X, \mathcal{F})] \in CT(A[G])$.

Proof. Because finite maps are affine, the higher derived sheaves $R^i f_*(\mathcal{F})$ are vanishing. Hence $H^n(X, \mathcal{F}) = H^n(Y, f_*(\mathcal{F}))$ as $A[G]$-modules. Now the claim follows from [Chinburg 1994, Proposition 1.5]. □

Suppose now that $f : X \to Y$ as above is a map of smooth, projective curves over $\mathrm{Spec}(A)$. Let $\mathscr{L}$ be a line bundle on Y. The line bundle $f^*(\mathscr{L})$ on X is naturally equipped with the structure of a coherent G-sheaf.

Lemma 5.6. *Keeping the same notation and assumptions, we have in* $CT(A[G])$

$$\chi(G, f^*(\mathscr{L})) = \chi(G, \mathbb{O}_X) + \deg(\mathscr{L})[A[G]].$$

Proof. Of course we are going to show the claim with the usual dévissage argument. By the Riemann–Roch theorem, there is a divisor D on Y whose support is disjoint from the ramification divisor of the cover f and $\mathscr{L} = O_Y(D)$. First assume that D is effective. When $\deg(D) = 0$ the claim is obvious. Otherwise $D = D' + \mathfrak{p}$, where D' is an effective divisor with $\deg(D') < \deg(D)$ and $\mathfrak{p}$ is a closed point on Y. There is a short exact sequence

$$0 \to f^*(\mathbb{O}_Y(D')) \to f^*(\mathbb{O}_Y(D)) \to f^*(A\mathfrak{p}) \to 0,$$

where $A\mathfrak{p}$ denotes the skyscraper sheaf on Y with support $\mathfrak{p}$. Because $\mathfrak{p}$ is not in the ramification locus of f, we have $H^0(f_* f^*(A\mathfrak{p}), Y) \cong A[G]^{\deg(\mathfrak{p})}$ as $A[G]$-modules. Moreover, all higher cohomology groups of the skyscraper sheaf $f_* f^*(A\mathfrak{p})$ vanish. Hence by the additivity of the Euler characteristic we get

$$\chi(G, f^*(\mathbb{O}_Y(D))) = \chi(G, f^*(\mathbb{O}_Y(D'))) + \deg(\mathfrak{p})[A[G]].$$

Now the claim follows by induction on $\deg(D)$. Consider next the general case and write $D = D_1 - D_2$, where D_1 and D_2 are divisors on X whose supports are disjoint. We are going to prove the claim by induction on $\deg(D_2)$. We already proved the claim when $\deg(D_2) = 0$. Otherwise $D_2 = D_2' + \mathfrak{p}$, where D_2' is an effective divisor with $\deg(D_2') < \deg(D_2)$ and $\mathfrak{p}$ is a closed point on Y. By repeating the same argument that we used above, we get

$$\chi(G, f^*(\mathbb{O}_Y(D))) = \chi(G, f^*(\mathbb{O}_Y(D_1 - D_2'))) - \deg(\mathfrak{p})[A[G]]. \qquad \square$$

Definition 5.7. Assume now that $A = \mathbf{k}$ is a perfect field of characteristic p, and let W denote the ring of Witt vectors of $\mathbf{k}$ of infinite length. Moreover, let K denote the field of fractions of W. Let M be a finitely generated cohomologically trivial $\mathbf{k}[G]$-module. Then M is a projective $\mathbf{k}[G]$-module by [Chinburg 1994, Proposition 4.1(a)]. Hence M is isomorphic to P/pP for some finitely generated projective W-module P. The character of the $\overline{K}[G]$-module $\overline{K} \otimes_W P$ can be written in the form $\sum m_\alpha \alpha$, where the sum is over the set $R(G)$ of irreducible $\overline{K}$-valued characters of G. The integer m_α is independent of the choice of P. Let $\Delta(M) : R(G) \to \mathbb{Z}$ be the function defined by the formula $\Delta(M)(\alpha) = m_\alpha$. This map extends uniquely to a homomorphism from $CT(A[G])$ to the group of $\mathbb{Z}$-valued functions on $R(G)$ which will be denoted by Δ as well.

Suppose that A is a finite extension of the field B. Then the restriction of operators from $A[G]$ to $B[G]$ induces a homomorphism $\mathrm{Res}_{A\to B} : CT(A[G]) \to CT(B[G]))$. Assume now that A is the finite field $\mathbb{F}_q$. Then every $\alpha \in R(G)$ can be considered as a representation of the absolute Galois group of the function field of X. In particular the ϵ-constant $\epsilon(\alpha) \in \overline{\mathbb{Q}}_p$ is defined.

Theorem 5.8. $\Delta(\mathrm{Res}_{\mathbb{F}_q\to\mathbb{F}_p}(\chi(G,\mathbb{O}_X)))(\alpha) = -dv_q(\epsilon(\alpha^{-1}))$ *for all* $\alpha \in R(G)$.

Proof. This is a special case of [Chinburg 1994, Theorem 5.2]. □

Notation 5.9. Suppose now that $Y = \mathscr{C}$, and let $\mathscr{E}$ and Δ_E be the same as in the introduction. Assume that the ramification divisor of the cover $f : X \to Y$ has support disjoint from the conductor of E. Let $g' : \mathscr{E}' \to X$ be the base change of the elliptic fibration $g : \mathscr{E} \to Y$ with respect to the map f. Note that the X-scheme $\mathscr{E}'$ is a relatively minimal regular model of the base change of E to the function field of X. Moreover, $\mathscr{E}'$ is equipped with a unique action of G fixing the zero section such that g' is equivariant with respect to this action and the one on X.

Theorem 5.10. *The* $\mathbb{F}_q[G]$*-module* $H^2(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})$ *is cohomologically trivial and*

$$\Delta(\mathrm{Res}_{\mathbb{F}_q\to\mathbb{F}_p}([H^2(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})]))(\alpha) = \tfrac{1}{12}d\deg(\Delta_E) + dv_q(\epsilon(\alpha^{-1})) \quad \textit{for all } \alpha \in R(G).$$

Proof. By Lemma 5.5, we have

$$\chi(G, \mathbb{O}_{\mathscr{E}'}) = [H^0(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})] - [H^1(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})] + [H^2(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})]. \tag{13}$$

By [Goldfeld and Szpiro 1995, Lemma 4], the map $(g')^* : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(\mathscr{E}')$ induced by Picard functoriality is an isomorphism. Because this map is equivariant with respect to the induced G-actions on $\mathrm{Pic}^0(X)$ and $\mathrm{Pic}^0(\mathscr{E}')$, we get that $H^1(\mathscr{E}', \mathbb{O}_{\mathscr{E}'}) = H^1(X, \mathbb{O}_X)$ as $\mathbb{F}_q[G]$-modules, since these modules are isomorphic to the tangent spaces at the zero of the abelian varieties $\mathrm{Pic}^0(\mathscr{E}')$ and $\mathrm{Pic}^0(X)$, respectively. Obviously $H^0(\mathscr{E}', \mathbb{O}_{\mathscr{E}'}) = H^0(X, \mathbb{O}_X)$ as $\mathbb{F}_q[G]$-modules, and hence from (13) and Lemma 5.5 we get

$$[H^2(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})] = \chi(G, \mathbb{O}_{\mathscr{E}'}) - \chi(G, \mathbb{O}_X). \tag{14}$$

Let $\Omega^1_{\mathscr{E}/Y}$ and $\Omega^1_{\mathscr{E}'/X}$ denote the sheaf of relative Kähler differentials of the Y-scheme $\mathscr{E}$ and that of the X-scheme $\mathscr{E}'$. Let $\omega_{\mathscr{E}/Y}$ and $\omega_{\mathscr{E}'/X}$ denote the pull-backs of $\Omega^1_{\mathscr{E}/Y}$ and $\Omega^1_{\mathscr{E}'/X}$ with respect to the zero section. These sheaves are line bundles on Y and X, respectively. Moreover, by Grothendieck's duality we have $\mathbb{R}^1 g'_*(\mathbb{O}_{\mathscr{E}'}) = \omega^{\otimes -1}_{\mathscr{E}'/X}$. In particular, $\chi(G, R^1 g'_*(\mathbb{O}_{\mathscr{E}'})) = -\chi(G, \omega_{\mathscr{E}'/X})$. Therefore, because all boundary maps in the spectral sequence $H^p(Y, R^q g'_*(\mathbb{O}_{\mathscr{E}'})) \Rightarrow H^{p+q}(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})$ are $\mathbb{F}_q[G]$-linear, we get from Lemma 5.5 that

$$\chi(G, \mathbb{O}_{\mathscr{E}'}) = \chi(G, \mathbb{O}_X) - \chi(G, R^1 g'_*(\mathbb{O}_{\mathscr{E}'})) = \chi(G, \mathbb{O}_X) - \chi(G, \omega^{\otimes -1}_{\mathscr{E}'/X}). \tag{15}$$

Combining (14) and (15), we get that

$$[H^2(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})] = -\chi(G, \omega_{\mathscr{E}'/X}^{\otimes -1}). \tag{16}$$

By definition, Δ_E is the zero divisor of a nonzero section of $\omega_{\mathscr{E}/Y}^{\otimes 12}$. Therefore $\deg(\Delta_E) = 12\deg(\omega_{\mathscr{E}/Y})$. Moreover $\omega_{\mathscr{E}'/X} = f^*(\omega_{\mathscr{E}/Y})$. Hence we see from (16) and Lemma 5.6 that

$$[H^2(\mathscr{E}, \mathbb{O}_{\mathscr{E}})] = \tfrac{1}{12}\deg(\Delta_E)[\mathbb{F}_q[G]] - \chi(G, \mathbb{O}_X).$$

The claim now follows from Theorem 5.8. □

6. Slope estimates

Definition 6.1. Let $\sigma : W \to W$ denote the absolute Frobenius automorphism. Let $W(\!(V)\!)$ denote the W-algebra of formal Laurent series $\sum_{i \geq n} a_i V^i$, where $a_i \in W$ and $n \in \mathbb{Z}$ are arbitrary, with the usual addition and with multiplication defined by

$$\Big(\sum_{i \geq n} a_i V^i\Big) \cdot \Big(\sum_{j \geq m} b_j V^j\Big) = \sum_{k \geq n+m} \Big(\sum_{i+j=k} a_i \sigma^{-i}(b_j)\Big) V^k.$$

Moreover, let $W[V]$ and $W[\![V]\!]$ denote the subring of $W(\!(V)\!)$ consisting of polynomials and formal power series in the variable V, respectively. Let M be a module over the ring $W[V]$. Then the kernel and the cokernel of the multiplication by $V : M \to M$ are W-modules, and we define

$$\chi(M) = \mathrm{length}_W(\mathrm{Ker}(V)) - \mathrm{length}_W(\mathrm{Coker}(V)),$$

provided both numbers on the right are finite. Let $W[V, F]$ denote the ring generated by the variable V over W subject to the relations $VF = FV = p$, $Fc = \sigma(c)F$ and $Vc = \sigma^{-1}(c)V$, for every $c \in W$. For every module M over the Dieudonné ring $W[F, V]$ that is free and finitely generated as a W-module, the tensor product $M \otimes_W K$ is an F-isocrystal over W with respect to multiplication by $F \otimes_W \mathrm{id}_K$. For every F-isocrystal M over W, let $l(M)$ denote $\sum m_i(1 - \lambda_i)$, where the λ_i are the slopes of M and m_i is the multiplicity of λ_i.

Lemma 6.2. (i) *If $0 \to M' \to M \to M \to 0$ is a short exact sequence of $W[V]$-modules, then $\chi(M)$ is defined if $\chi(M')$ and $\chi(M'')$ are defined and*

$$\chi(M) = \chi(M') + \chi(M'').$$

(ii) *If M is a module over the ring $W[F, V]$ that is free and finitely generated as a W-module, then $\chi(M) = -l(M \otimes_W K)$.*

(iii) *If M is a finitely generated torsion $W[\![V]\!]$-module, then*

$$\chi(M) = -\mathrm{length}_{W(\!(V)\!)} M \otimes_{W[\![V]\!]} W(\!(V)\!).$$

Proof. This is [Milne 1975, Lemma 7.2]. □

Definition 6.3. Let G be a finite abelian group whose order is not divisible by p, and assume that $\mathbf{k}$ is algebraically closed. Then every $\alpha \in R(G)$ takes values in W, so the element $\pi_\alpha = \sum_{g\in G} \alpha(g)^{-1} g \in W[G]$ is well-defined. For every $W[G]$-module M, let M^α denote the sub-$W[G]$-module $\pi_\alpha M$. Finally, for every F-isocrystal M over W and real numbers $a \le b$, let $M_{[a,b)}$ denote the maximal subquotient of M with slopes in the interval $[a, b)$.

Let X be a smooth projective variety defined over $\mathbf{k}$, and assume that G acts on X. Let $H^m(X/W)$ denote the m-th crystalline cohomology group of W. Then $W[G]$ acts on $H^m(X/W)$ and $H^m(X, \mathbb{O}_X)$ by functoriality for every m.

Proposition 6.4. $l(H^r(X/W)^\alpha \otimes_W K_{[0,1)}) \le \dim_{\mathbf{k}}(H^r(X, \mathbb{O}_X)^\alpha)$, *for every* $r \in \mathbb{N}$ *and* $\alpha \in R(G)$.

Proof. Let $H^r(X, W)$ denote the r-th Witt vector cohomology group of the variety X. This is a $W[V]$-module and there is a long exact sequence

$$\cdots \to H^{r-1}(X, \mathbb{O}_X) \to H^r(X, W) \xrightarrow{V} H^r(X, W) \to H^r(X, \mathbb{O}_X) \to \cdots$$

The group G acts on all cohomology groups in this sequence, and the maps are equivariant with respect to this action, so there is a long exact sequence

$$\cdots \to H^{r-1}(X, \mathbb{O}_X)^\alpha \to H^r(X, W)^\alpha \xrightarrow{V} H^r(X, W)^\alpha \to H^r(X, \mathbb{O}_X)^\alpha \to \cdots$$

Because X is projective, the vector spaces $H^r(X, \mathbb{O}_X)^\alpha$ have finite dimension. Therefore $\chi(H^r(X, W)^\alpha)$ is well-defined and

$$\chi(H^r(X, W)^\alpha) \ge -\dim_{\mathbf{k}}(H^r(X, \mathbb{O}_X)^\alpha). \tag{17}$$

Write

$$H^r(X, W)^\alpha_t = \mathrm{Ker}(H^r(X, W)^\alpha \to H^r(X, W)^\alpha \otimes_W K).$$

Then $H^r(X, W)^\alpha_t$ is a torsion $W[\![V]\!]$-module, and there is a short exact sequence of $W[V]$-modules

$$0 \to H^r(X, W)^\alpha_t \to H^r(X, W)^\alpha \to H^r(X, W)^\alpha_{ct} \to 0$$

such that $H^r(X, W)^\alpha_{ct}$ is a module over the Dieudonné ring $W[F, V]$ that is free and finitely generated as a W-module. Therefore by of Lemma 6.2(i), we have

$$\chi(H^r(X, W)^\alpha) = \chi(H^r(X, W)^\alpha_t) + \chi(H^r(X, W)^\alpha_{ct}). \tag{18}$$

Because the slope spectral sequence degenerates modulo torsion [Illusie 1979, théorème 3.2], there is an isomorphism between the F-isocrystals $H^r(X, W) \otimes_W K$ and $H^r(X/W) \otimes K_{[0,1)}$. Since this isomorphism is equivariant with respect to the

action of G, the F-isocrystals $H^r(X, W)^\alpha \otimes_W K$ and $H^r(X/W)^\alpha \otimes_W K_{[0,1)}$ are also isomorphic. Hence

$$\chi(H^r(X, W)^\alpha_{ct}) = -l(H^r(X, W)^\alpha_{ct} \otimes_W K) = -l(H^r(X/W)^\alpha \otimes_W K_{[0,1)}) \quad (19)$$

by Lemma 6.2(ii). According to (iii), the number $\chi(H^r(X, W)^\alpha_t)$ is not positive. Hence (17), (18), and (19) imply that

$$-l(H^r(X/W)^\alpha \otimes_W K_{[0,1)}) \geq -\dim_{\mathbf{k}}(H^r(X, \mathcal{O}_X)^\alpha). \qquad \square$$

Notation 6.5. Assume now that $\mathbf{k}$ is the algebraic closure of $\mathbb{F}_q$, and for every $\mathrm{Spec}(\mathbb{F}_q)$-scheme S, let $\overline{S}$ denote its base change to $\mathrm{Spec}(\mathbf{k})$. Moreover let $F : \overline{S} \to \overline{S}$ denote the Frobenius relative to $\mathbb{F}_q$ for every such S. Assume now that X is a smooth projective variety defined over $\mathbf{k}$ equipped with an action of G. Recall that we've chosen a prime $l \neq p$. Now fix an isomorphism $\nu : \overline{\mathbb{Q}}_l \to \overline{\mathbb{Q}}_p$. Since the group G acts on the étale cohomology group $H^m(\overline{X}, \overline{\mathbb{Q}}_l)$, we may consider the latter as a $\mathbb{W}[G]$-module if we identify $\overline{\mathbb{Q}}_l$ and $\overline{\mathbb{Q}}_p$ via ν. Then the map $F^* : H^m(\overline{X}, \overline{\mathbb{Q}}_l) \to H^m(\overline{X}, \overline{\mathbb{Q}}_l)$ induced by the Frobenius morphism F commutes with the action of G, so $H^m(\overline{X}, \overline{\mathbb{Q}}_l)^\alpha$ is an F^*-invariant subspace.

Lemma 6.6. $l_q(\det(1 - F^*t \,|\, H^m(\overline{X}, \overline{\mathbb{Q}}_l)^\alpha)) = l(H^m(\overline{X}/W)^\alpha \otimes_W K_{[0,1)})$.

Proof. For every $g \in G$, let the same symbol denote the base change $\overline{X} \to \overline{X}$ to $\mathrm{Spec}(\mathbf{k})$ of the automorphism $X \to X$ furnished by the given action of G on X. For every positive integer n, the composition

$$g \circ F^{[n]} = g \circ \underbrace{F \circ \cdots \circ F}_{n \text{ times}}$$

induces the zero map on tangent spaces, and hence the Lefschetz trace formula applied to $g \circ F^{[n]}$ both in the l-adic and the crystalline cohomology theories implies

$$\sum_{m=0}^{2\dim(\overline{X})} (-1)^m \mathrm{Tr}(1 - g^*(F^*)^n \,|\, H^m(\overline{X}, \overline{\mathbb{Q}}_l)) = \sum_{m=0}^{2\dim(\overline{X})} (-1)^m \mathrm{Tr}(1 - g^*(F^*)^n \,|\, H^m(\overline{X}/W) \otimes_W K). \quad (20)$$

Let $l_m(\alpha, t)$ and $c_m(\alpha, t)$ denote the polynomials

$$\det(1 - F^*t \,|\, H^m(\overline{X}, \overline{\mathbb{Q}}_l)^\alpha) \quad \text{and} \quad \det(1 - F^*t \,|\, H^m(\overline{X}/W) \otimes_W K^\alpha).$$

By the orthogonality of characters, (20) implies that

$$\prod_{m=0}^{2\dim(\overline{X})} l_m(\alpha, t)^{(-1)^m} = \prod_{m=0}^{2\dim(\overline{X})} c_m(\alpha, t)^{(-1)^m}. \quad (21)$$

By Deligne's purity theorem and [Katz and Messing 1974, Theorem 1], the reciprocal roots of the polynomials $l_m(\alpha, t)$ and $c_m(\alpha, t)$ are Weil numbers with squared complex norm q^m. Hence there are no cancellations in the alternating products in (21). Therefore $l_m(\alpha, t) = c_m(\alpha, t)$ for every m. Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the eigenvalues of F^* considered as a linear transformation of $H^m(\overline{X}/W) \otimes_W K^\alpha$. The claim now follows from the fact that $v_q(\lambda_1), v_q(\lambda_2), \ldots, v_q(\lambda_k)$ are the slopes of the F-isocrystal $H^m(\overline{X}/W) \otimes_W K^\alpha$. □

Notation 6.7. Let us consider now the same situation as in the introduction. Fix a tamely ramified character $\alpha \in \mathbb{X}(\mathfrak{n})$ and let $\pi : X \to \mathscr{C}$ be the Galois cover corresponding to the extension $F' | F$, where F' is the subfield of $\bar{F}$ fixed by the kernel of α. Let G denote the Galois group of the cover π and let $g' : \mathscr{E}' \to X$ denote the base change of $g : \mathscr{E} \to \mathscr{C}$ with respect to the map f as in Notation 5.9. We will also keep on using the notation introduced in Notation 6.5.

Lemma 6.8. $l_q(L(\sigma_E \otimes \alpha, t)) = l(H^2(\overline{\mathscr{E}}'/W)^\alpha \otimes_W K_{[0,1)})$.

Proof. For every morphism $m : R \to S$ of $\mathrm{Spec}(\mathbb{F}_q)$-schemes, let $\overline{m} : \overline{R} \to \overline{S}$ denote the base change to $\mathrm{Spec}(\mathbf{k})$. The Leray spectral sequence $H^p(\overline{X}, R^q\overline{g}'_*(\overline{\mathbb{Q}}_l(1))) \Rightarrow H^{p+q}(\overline{\mathscr{E}}', \overline{\mathbb{Q}}_l(1))$ furnishes an injection $\zeta : H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l(1))) \to H^2(\overline{\mathscr{E}}', \overline{\mathbb{Q}}_l(1))$, and the image of this map is the orthogonal complement of the $\overline{\mathbb{Q}}_l$-linear subspace V spanned by the Chern classes of the zero section and the fibres of the elliptic fibration $\overline{\mathscr{E}}' \to \overline{\mathscr{C}}$, considered here as divisors on the surface $\overline{\mathscr{E}}'$, with respect to the cup product pairing. The cohomology group $H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l(1)))$ is naturally equipped with a G-action because the map $\overline{g}'$ is equivariant with respect to the action of G on $\overline{\mathscr{E}}'$ and $\overline{X}$, respectively. Moreover ζ is G-linear. Hence we have an isomorphism

$$H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l))^\alpha \oplus V^\alpha(-1) \cong H^2(\overline{\mathscr{E}}', \overline{\mathbb{Q}}_l)^\alpha. \tag{22}$$

Note that the cohomology group $H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l))$ is equipped with the action of a Frobenius operator F^* that commutes with the action of G, and that the isomorphism in (22) respects the action of the operator F^* on both sides. Moreover, for every eigenvalue λ of F^* on $V(-1)$, we have $v_q(\lambda) = 1$, and hence

$$l_q(\det(1 - F^*t \,|\, H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l))^\alpha)) = l_q(\det(1 - F^*t \,|\, H^2(\overline{\mathscr{E}}', \overline{\mathbb{Q}}_l)^\alpha)).$$

We may consider α a lisse l-adic sheaf on $\mathrm{Spec}(F)$. By slight abuse of notation, let α also denote the pull-back onto $\overline{\mathscr{C}}$ of the direct image of this sheaf α with respect to the open immersion $\mathrm{Spec}(F) \to \mathscr{C}$. Because the Galois representation $H^1(E_{\overline{F}}, \overline{\mathbb{Q}}_l)$ is absolutely irreducible and self-dual, we have

$$H^0(\overline{\mathscr{C}}, R^1\overline{g}_*(\overline{\mathbb{Q}}_l) \otimes \alpha) = H^2(\overline{\mathscr{C}}, R^1\overline{g}_*(\overline{\mathbb{Q}}_l) \otimes \alpha) = 0.$$

Moreover, $H^1(\overline{\mathscr{C}}, R^1\overline{g}_*(\overline{\mathbb{Q}}_l)\otimes\alpha) = H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l))^\alpha$ by the degeneration of the Hochschild–Serre spectral sequence. Hence by the Grothendieck–Verdier trace formula,

$$l_q(L(\sigma_E\otimes\alpha,t)) = l_q(\det(1-F^*t|H^1(\overline{X}, R^1\overline{g}'_*(\overline{\mathbb{Q}}_l))^\alpha) \\ = l_q(\det(1-F^*t|H^2(\overline{\mathscr{E}}', \overline{\mathbb{Q}}_l)^\alpha)).$$

The claim now follows from Lemma 6.6. □

Theorem 6.9. *Assume that p does not divide the order of* $\mathrm{Pic}_0(\mathscr{C})(\mathbb{F}_q)$. *Then*

$$m(E) \le d(\tfrac{1}{12}\deg(\Delta_E) + g - 1).$$

Proof. Let $\alpha \in \mathbb{X}(\mathfrak{n})$ be arbitrary, and let $C(\alpha)$ denote the set of all characters $\beta : \mathrm{Gal}(F'|F) \to \overline{\mathbb{Q}}_p^*$ that are conjugate to α under the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$ on $\overline{\mathbb{Q}}_p$. For every $\beta \in C(\alpha)$, we have

$$l_q(L(\sigma_E\otimes\beta,t)) \le \dim_{\mathbf{k}}(H^2(\overline{\mathscr{E}}', \mathbb{O}_{\overline{\mathscr{E}}'})^\beta) = \dim_{\mathbf{k}}(H^2(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})\otimes_{\mathbb{F}_q}\mathbf{k}^\beta) \qquad (23)$$

by Proposition 6.4 and Lemma 6.8. By [Chinburg 1994, Remark 4.5],

$$\Delta(\mathrm{Res}_{\mathbb{F}_q\to\mathbb{F}_p}([H^2(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})])(\alpha) = \frac{d}{|C(\alpha)|}\sum_{\beta\in C(\alpha)}\dim_{\mathbf{k}}(H^2(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})\otimes_{\mathbb{F}_q}\mathbf{k}^\beta). \quad (24)$$

Because the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$ on $\overline{\mathbb{Q}}_p$ leaves the valuation v_q invariant, we have

$$l_q(L(\sigma_E\otimes\beta,t)) = l_q(L(\sigma_E\otimes\alpha,t))$$

for every $\beta \in C(\alpha)$. Hence (23), (24) and Theorem 5.10 imply that

$$\begin{aligned} l_q(L(\sigma_E\otimes\alpha,t)) &= \frac{1}{|C(\alpha)|}\sum_{\beta\in C(\alpha)} l_q(L(\sigma_E\otimes\beta,t)) \\ &\le \frac{1}{|C(\alpha)|}\sum_{\beta\in C(\alpha)}\dim_{\mathbf{k}}(H^2(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})\otimes_{\mathbb{F}_q}\mathbf{k}^\beta) \\ &= \frac{1}{d}\cdot\Delta(\mathrm{Res}_{\mathbb{F}_q\to\mathbb{F}_p}([H^2(\mathscr{E}', \mathbb{O}_{\mathscr{E}'})])(\alpha) \\ &= \tfrac{1}{12}\deg(\Delta_E) + v_q(\epsilon(\alpha^{-1})). \end{aligned}$$

The claim now follows from Proposition 4.5. □

Definition 6.10. Following [Mazur 1972], we will call a smooth projective variety V defined over a perfect field of characteristic p ordinary in dimension n if the n-dimensional Newton and Hodge polygons of V agree.

Theorem 6.11. *Assume that the elliptic surface $\mathscr{E}$ is ordinary in dimension* 2. *Then*

$$m(E) \ge d(\tfrac{1}{12}\deg(\Delta_E) + g - 1).$$

Proof. By Deligne's purity theorem, we have $\epsilon(1) = \pm q^{g-1}$, where 1 denotes the trivial representation. Hence in the special case when G is the trivial group, that is, the cover f is the identity map of $\mathscr{C}$ onto itself, Theorem 5.10 says that

$$\dim_{\mathbb{F}_q} H^2(\mathscr{E}, \mathbb{O}_{\mathscr{E}}) = \tfrac{1}{12}\deg(\Delta_E) + g - 1.$$

Because $\mathscr{E}$ is ordinary in dimension 2, we have

$$l_q(L(E,t)) = l_q(\det(1 - F^*t \mid H^2(\overline{\mathscr{E}}, \mathbb{Q}_l))) = \dim_{\mathbb{F}_q} H^2(\mathscr{E}, \mathbb{O}_{\mathscr{E}})$$

by definition. The claim now follows from Proposition 4.5. □

Remark 6.12. It is known that a smooth projective variety V is ordinary if V is a generic curve of genus g [Faber and van der Geer 2004; Miller 1972], a generic abelian variety of dimension d equipped with a polarisation of degree r [Mumford 1969; Norman and Oort 1980], or a generic complete intersection of multidegree $(a_1, a_2, \ldots, a_n)$ [Illusie 1990]. It is natural to expect that the same holds for elliptic surfaces with a section. More precisely, one might conjecture the following. Assume that $p > 3$, let $N \geq 2$ be a positive integer, let $g \in \mathbb{N}$ and let $\mathscr{M}_{g,N,p}$ denote the coarse moduli representing the functor that associates to every scheme T over $\mathrm{Spec}(\mathbb{F}_p)$ the set of isomorphism classes of smooth families of elliptic surfaces over a smooth curve of genus g over T with discriminant of degree $12N$ in all geometric fibres over T, constructed in [Seiler 1987]. Then I expect that for every p, g and N there is a nonempty open subscheme $\mathscr{U}$ of $\mathscr{M}_{g,N,p}$ such that for every geometric point of $\mathscr{U}$, the corresponding elliptic surface is ordinary. Of course it is enough to show that there is a geometric point of $\mathscr{M}_{g,N,p}$ such that the corresponding elliptic surface is ordinary in dimension two.

7. An upper bound in terms of the conductor

Notation 7.1. For every elliptic curve E defined over a field K of characteristic p, let $E^{(p)}$ denote pull-back of E with respect to the Frobenius map $K \to K$ (given by $x \mapsto x^p$). We will call $E^{(p)}$ the Frobenius twist of E. The elliptic curve $E^{(p)}$ is in fact defined over the subfield K^p of p-th powers. The absolute Frobenius $\mathbf{F}: E \to E^{(p)}$ is an isogeny defined over the field K. Finally, for every cohomology class $c \in H^1(K, \mathrm{Aut}(E))$, let E_c denote twist of E by c.

Definition 7.2. Let K be as above and let E be an elliptic curve defined over K such that $j(E) \neq 0, 1728$. Because $j(E^{(p)}) = j(E)^p$, we have $j(E^{(p)}) \neq 0, 1728$. Hence by [Silverman 1986, Proposition 1.2(c)], the groups $\mathrm{Aut}(E)$ and $\mathrm{Aut}(E^{(p)})$ are both equal to multiplication by ± 1. Therefore there is a unique isomorphism $f : \mathrm{Aut}(E) \to \mathrm{Aut}(E^{(p)})$ such that $\mathbf{F} \circ \phi = f(\phi) \circ \mathbf{F}$ for every $\phi \in \mathrm{Aut}(E)$. Let $f_*: H^1(K, \mathrm{Aut}(E)) \to H^1(K, \mathrm{Aut}(E^{(p)}))$ denote the isomorphism induced by the identification f.

The next two results will be useful, and they seem not to be recorded in the literature.

Lemma 7.3. *Assume that $j(E) \neq 0, 1728$. Then the elliptic curves $(E_c)^{(p)}$ and $(E^{(p)})_{f_*(c)}$ are isomorphic over K for every $c \in H^1(K, \mathrm{Aut}(E))$.*

Proof. For every scheme X over $\mathrm{Spec}(K)$, let $\overline{X}$ denote $X \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\overline{K})$. For every $\gamma \in \mathrm{Gal}(\overline{K}|K)$ and X as above, let the symbol γ also denote the unique endomorphism of $\overline{X}$ that makes the following diagram commutative:

$$\begin{array}{ccc} \overline{X} & \xrightarrow{\gamma} & \overline{X} \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\overline{K}) & \xrightarrow{\gamma} & \mathrm{Spec}(\overline{K}) \end{array}$$

Fix an isomorphism $\phi : \overline{E} \to \overline{E_c}$ over $\overline{K}$. Then for every $\gamma \in \mathrm{Gal}(\overline{K}|K)$, the pull-back of the diagram

$$\overline{E} \xrightarrow{\phi} \overline{E_c} \xrightarrow{\gamma} \overline{E_c} \xrightarrow{\phi^{-1}} \overline{E} \xrightarrow{\gamma^{-1}} \overline{E}$$

with respect to the Frobenius map $x \mapsto x^p$ of $\mathrm{Spec}(\overline{K})$ is

$$\overline{E^{(p)}} \xrightarrow{\psi} \overline{(E_c)^{(p)}} \xrightarrow{\gamma} \overline{(E_c)^{(p)}} \xrightarrow{\psi^{-1}} \overline{E^{(p)}} \xrightarrow{\gamma^{-1}} \overline{E^{(p)}},$$

where $\psi : \overline{E^{(p)}} \to \overline{(E_c)^{(p)}}$ is the unique isomorphism such that $\mathbf{F} \circ \phi = \psi \circ \mathbf{F}$. The $\mathrm{Aut}(E)$-valued function $\gamma \mapsto \gamma^{-1} \circ \phi^{-1} \circ \gamma \circ \phi$ on $\mathrm{Gal}(\overline{F}|F)$ is a cocycle that represents c. Note that

$$\mathbf{F} \circ \gamma^{-1} \circ \phi^{-1} \circ \gamma \circ \phi = \gamma^{-1} \circ \psi^{-1} \circ \gamma \circ \psi \circ \mathbf{F}$$

for all $\gamma \in \mathrm{Gal}(\overline{F}|F)$), and therefore the function $\gamma \mapsto \gamma^{-1} \circ \psi^{-1} \circ \gamma \circ \psi$ is a cocycle that represents $f_*(c)$. The claim is now clear. □

Proposition 7.4. *Let K be a field of characteristic p, and let E be an elliptic curve defined over K. Assume that $j(E) \neq 0, 1728$ and $j(E) \in K^p$. Then E is isomorphic to the Frobenius twist of an elliptic curve E' defined over K.*

Proof. Let $\lambda \in K$ be the unique p-th root of $j(E)$. By [Silverman 1986, Proposition 1.1], there is an elliptic curve $\widetilde{E}$ defined over K such that $j(\widetilde{E}) = \lambda$. Then the Frobenius twist $\widetilde{E}^{(p)}$ of $\widetilde{E}$ is defined over K and has the same j-invariant as E. Hence by the theory of twists, there is a cohomology class $c \in H^1(K, \mathrm{Aut}(\widetilde{E}^{(p)}))$ such that E is the twist of $\widetilde{E}^{(p)}$ by c. Let E' be the twist of $\widetilde{E}$ by $f_*^{-1}(c)$. By Lemma 7.3, E is isomorphic to the Frobenius twist of E'. □

Now let K denote the function field of a smooth, projective, geometrically irreducible curve X defined over a perfect field of characteristic p.

Corollary 7.5. *Let E be a nonisotrivial elliptic curve defined over K. Then E is isogenous to an elliptic curve E' defined over K with the property $j(E') \notin K^p$.*

Proof. By assumption, $j(E)$ does not lie in the constant field of K, and hence there are a $\lambda \in K$ and natural number n such that $\lambda \notin K^p$ and $\lambda^{p^n} = j(E)$. By Proposition 7.4, there is an elliptic curve E' defined over K such that $j(E') = \lambda$ and E is the n-fold Frobenius twist of E'. In particular, E and E' are isogenous. □

For every elliptic curve E defined over K, let Δ_E denote the discriminant of a relatively minimal elliptic surface $\mathscr{E} \to X$ whose generic fibre is E. Then Δ_E is an effective divisor on the curve X. We say that a nonisotrivial elliptic curve E is minimal in its isogeny class if $\deg(\Delta_E) = \min(\deg(\Delta_{E'}))$, where E' is any elliptic curve defined over K isogenous to E. Let $\mathfrak{n}$ denote the conductor of E.

Theorem 7.6 (Pesenti–Szpiro). *Assume that E is a nonisotrivial elliptic curve that is minimal in its isogeny class. Then*

$$\deg(\Delta_E) \leq 6(\deg(\mathfrak{n}) + 2g - 2).$$

Proof. By Corollary 7.5, the claim follows at once from [Pesenti and Szpiro 2000, théorème 0.1] and the isogeny-invariance of the conductor. □

Let us return to the situation in the introduction. Because in each isogeny class of nonisotrivial elliptic curves there is an elliptic curve that is minimal, Theorem 7.6 combined with Theorem 1.3 has the following immediate corollary:

Corollary 7.7. *Assume that p does not divide the order of* $\mathrm{Pic}_0(\mathscr{C})(\mathbb{F}_q)$. *Then*

$$m(E) \leq d(\tfrac{1}{2}\deg(\mathfrak{n}) + 2g - 2).$$

Remark 7.8. Note that this inequality is significantly weaker than Theorem 1.3 because the Pesenti–Szpiro inequality fails to be an equality in general. For example, in the special case of the elliptic curve E of Theorem 1.4, a fast inspection of [Ulmer 2002, 2.2 and 2.3] reveals that its conductor $\mathfrak{n}$ is the sum of the prime divisors of the polynomial $T(1-2^4 3^3 T^n)$. Because by the assumptions of Theorem 1.4 the prime p does not divide $2^4 3^3 n$, the greatest common divisor of $1 - 2^4 3^3 T^n$ and its derivative is

$$(1 - 2^4 3^3 T^n, -n 2^4 3^3 T^{n-1}) = (1),$$

so we get that the polynomial $1-2^4 3^3 T^n$ is square-fee and therefore $\deg(\mathfrak{n}) = n+1$. Hence in this case Corollary 7.7 says that

$$m(E) \leq \tfrac{1}{2}n - \tfrac{3}{2}.$$

On the other hand, we will see in the next section that in this case Theorem 1.3 says that

$$m(E) \leq \tfrac{1}{6}n - 1$$

and the two sides above are actually equal, by Theorem 1.4.

Remark 7.9. Corollary 7.7 was already proved in the special case when $\mathscr{C} = \mathbb{P}^1_{\mathbb{F}_q}$ and $\mathfrak{n}$ is square-free by Tan [1993]. His strategy is similar to ours in reducing the result to estimates of the p-adic valuations of coefficients of twisted L-functions. For the latter he uses the Grothendieck–Ogg–Shafarevich formula and the functional equation. His methods also use facts about the structure of the set $\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A})$ specific to the rational function field, and hence it is impossible to generalise his approach in order to show Corollary 7.7 in general.

8. Elliptic curves with positive Manin constant

Definition 8.1. Fix a positive integer n that is not divisible by p. Let E_n be the elliptic curve over $F = \mathbb{F}_q(T)$ (where $q = p^d$) with plane cubic model

$$y^2 + xy = x^3 - T^n.$$

Straightforward calculation shows that $j(E)^{-1} = T^n(1 - 2^4 3^3 T^n)$. Hence E is not isotrivial. Let Δ_{E_n} denote the discriminant of a relatively minimal elliptic surface $\mathscr{E}_n \to \mathscr{C}$ whose generic fibre is E_n. The degree of Δ_{E_n} can be easily computed from [Ulmer 2002, 2.2 and 2.3]. In particular, when $p \geq 5$, it follows at once from these results and [Silverman 1994, Table 4.1] that $\deg(\Delta_{E_n}) = 12\lceil n/6 \rceil$.

Definition 8.2. Let F_n be the Fermat surface of degree n over $\mathbb{F}_q$, that is, the hypersurface in $\mathbb{P}^3_{\mathbb{F}_q}$ defined by the equation

$$x_0^n + x_1^n + x_2^n + x_3^n = 0.$$

Let μ_n denote the group of n-th roots of unity in $\overline{\mathbb{F}}_p$. Let G be the quotient of μ_n^4 modulo the diagonally embedded copy of μ_n. For every $\underline{z} = (\zeta_0, \zeta_1, \zeta_2, \zeta_3) \in \mu_n^4$, let $[\zeta_0, \zeta_1, \zeta_2, \zeta_3]$ denote the image of $\underline{z}$ under the quotient map $\mu_n^4 \to G$. Then the group scheme G acts on F_n and the action on the level of points is given by the rule

$$[\zeta_0, \zeta_1, \zeta_2, \zeta_3] \cdot [x_0 : x_1 : x_2 : x_3] = [\zeta_0 x_0 : \zeta_1 x_1 : \zeta_2 x_2 : \zeta_3 x_3].$$

Fix a primitive n-th root of unity $\zeta \in \overline{\mathbb{F}}_p$ and let $\Gamma \subset G$ be the subgroup generated by $[\zeta^2, \zeta, 1, 1]$ and $[1, \zeta, \zeta^3, 1]$. Since a subgroup-scheme Γ is defined over $\mathbb{F}_q$, the quotient surface F_n/Γ is defined over $\mathbb{F}_q$ too.

Theorem 8.3. *The surfaces $\mathscr{E}_n$ and F_n/Γ are birationally equivalent.*

Proof. The proof of this claim can be found in [Ulmer 2002, pp. 298–301]. □

Notation 8.4. Let $\mathbb{O}_p$ denote the ring of integers of $\overline{\mathbb{Q}}_p$, and let $\mathfrak{p}$ be its maximal ideal. We view all finite fields of characteristic p as subfields of $\mathbb{O}_p/\mathfrak{p}$, which is an algebraic closure of $\mathbb{F}_p$. Reduction modulo $\mathfrak{p}$ induces an isomorphism between the group of all roots of unity of order prime to p in $\mathbb{O}_p$ and the multiplicative group of $\mathbb{O}_p/\mathfrak{p}$. We let $\alpha : (\mathbb{O}_p/\mathfrak{p})^* \to \overline{\mathbb{Q}}_p^*$ denote the inverse of this isomorphism. We will use the same letter α for the restriction to any finite field $\mathbb{F}_q^*$.

Definition 8.5. Fix a nontrivial character $\psi_0 : \mathbb{F}_p \to \overline{\mathbb{Q}}_p^*$, and for each finite extension $\mathbb{F}_{p^m}$ of $\mathbb{F}_p$, let $\psi : \mathbb{F}_{p^m} \to \overline{\mathbb{Q}}_p^*$ be defined by $\psi = \psi_0 \circ \mathrm{Tr}_{\mathbb{F}_{p^m}|\mathbb{F}_p}$. If $\chi : \mathbb{F}_{p^m}^* \to \overline{\mathbb{Q}}_p^*$ is a nontrivial character, we define the corresponding Gauss sum by

$$g(\chi, \psi) = -\sum_{x \in \mathbb{F}_{p^m}^*} \chi(x)\psi(x).$$

If $\chi_1, \ldots, \chi_r$ are characters $\mathbb{F}_{p^m}^* \to \overline{\mathbb{Q}}_p^*$, not all trivial, such that the product $\chi_1 \cdots \chi_r$ is trivial, we define the Jacobi sum $J(\chi_1, \ldots, \chi_r)$ by

$$J(\chi_1, \ldots, \chi_r) = \begin{cases} \dfrac{(-1)^r}{p^m} \prod_{i=1}^r g(\chi_i, \psi), & \text{if all } \chi_i \text{ are nontrivial,} \\ 0, & \text{otherwise.} \end{cases}$$

Theorem 8.6 (Stickelberger). *For any $1 \le k \le p^m - 2$, we have*

$$v_p(g(\alpha^{-k}, \psi)) = s(k)/(p-1),$$

where if $k = k_0 + pk_1 + \cdots + p^{m-1}k_{m-1}$ is the p-adic expansion of the integer k, we define $s(k) = k_0 + k_1 + \cdots + k_{m-1}$.

Proof. This is the second claim of [Lang 1994, Theorem 9]. □

Definition 8.7. Let G be the group that we introduced in Definition 8.2. Let $\widehat{G}$ denote the group of characters G with values in $\overline{\mathbb{Q}}_p$. Using the character $\alpha : (\mathbb{O}_p/\mathfrak{p})^* \to \overline{\mathbb{Q}}_p^*$ we can identify $\widehat{G}$ with

$$\left\{ a = (a_0, a_1, a_2, a_3) \in (\mathbb{Z}/n\mathbb{Z})^4 \,\middle|\, \sum a_i = 0 \right\},$$

where the duality pairing $G \times \widehat{G} \to \overline{\mathbb{Q}}_p^*$ is

$$a(z) = \langle (a_0, a_1, a_2, a_3), [\zeta_0, \zeta_1, \zeta_2, \zeta_3] \rangle = \prod_{i=0}^{3} \alpha(\zeta_i)^{a_i}.$$

For every $a \in \widehat{G}$, let $u(a)$ denote the smallest positive integer such that $q^{u(a)}a = a$. For every nonzero $a = (a_0, a_1, a_2, a_3) \in \widehat{G}$, define the Jacobi sum $J(a)$ as follows: let $\chi_i : \mathbb{F}_{q^{u(a)}}^* \to \overline{\mathbb{Q}}_p$ be defined as $\chi_i = \alpha^{((q^{u(a)}-1)/d)a_i}$, and set $J(a) = J(\chi_0, \ldots, \chi_3)$. Note that $J(qa) = J(a)$. By convention, we set $J(0) = q$. Let

$\Gamma^\perp \subset \widehat{G}$ be the cyclic subgroup of order n generated by $(3, -6, 2, 1)$ and let

$$\widehat{G}' = \{a = (a_0, \dots, a_3) \in \widehat{G} \mid a = 0 \text{ or } a_i \neq 0 \text{ for } i = 0, \dots 3\}.$$

As in Notation 6.5, for every $\mathrm{Spec}(\mathbb{F}_q)$-scheme S let $\overline{S}$ denote again its base change to $\mathrm{Spec}(\overline{\mathbb{F}}_p)$ and let $F : \overline{S} \to \overline{S}$ denote the Frobenius relative to $\mathbb{F}_q$ for every such S. Choose a prime $l \neq p$ and fix an isomorphism $\nu : \overline{\mathbb{Q}}_l \to \overline{\mathbb{Q}}_p$. We will identify $\overline{\mathbb{Q}}_l$ with $\overline{\mathbb{Q}}_p$ via ν.

Theorem 8.8. *Let $A_1, \dots, A_k$ be the orbits of multiplication by q on $\Gamma^\perp \cap \widehat{G}'$ and choose $a_i \in A_i$. Then*

$$\det\left(1 - F^* t \,|\, H^2(\overline{F_n/\Gamma}, \overline{\mathbb{Q}}_l)\right) = \prod_{i=1}^{k} (1 - J(a_i) t^{u(a_i)}).$$

Proof. This is [Ulmer 2002, Corollary 7.7]. □

Definition 8.9. As in Notation 3.1, pick an isomorphism $\iota : \overline{\mathbb{Q}}_l \to \mathbb{C}$ and identify $\overline{\mathbb{Q}}_l$ with $\mathbb{C}$ via ι in all that follows. Let $|\cdot|_\infty$ denote the usual archimedean absolute value on $\mathbb{C}$. For every $\alpha \in \mathbb{R}$, finite dimensional $\overline{\mathbb{Q}}_l$-vector space V and $\overline{\mathbb{Q}}_l$-linear endomorphism $\Psi : V \to V$ we say that the pair (V, Ψ) has weights at most α if for every eigenvalue λ of Ψ we have $|\lambda|_\infty \leq |q|^\alpha$. Moreover we say that (V, Ψ) has slope α if for every λ as above $v_q(\lambda) = \alpha$. For every $\alpha \in \mathbb{R}$, $k \in \mathbb{N}$ and scheme X of finite type over $\mathrm{Spec}(\mathbb{F}_q)$ we say that X has weights at most α in dimension k if the pair $(H^k(\overline{X}, \overline{\mathbb{Q}}_l), F^*)$ has weights at most α. Similarly we say that X has slope α in dimension k if the pair $(H^k(\overline{X}, \overline{\mathbb{Q}}_l), F^*)$ has slope α.

Now let C be a curve over $\mathbb{F}_q$, that is, a one-dimensional (but necessarily equidimensional) variety defined over $\mathbb{F}_q$.

Lemma 8.10. *The curve C has weights at most* 1 *in dimension* 1, *and the curve C has slope* 1 *in dimension* 2.

Proof. Let U be a smooth dense open subscheme of C and let $i : U \to C$ be the inclusion map. Let S be the reduced closed subscheme of C whose underlying set is the complement of U and let $j : S \to C$ be the inclusion map. Then there is a cohomological long exact sequence

$$H^1(\overline{C}, i_!(\overline{\mathbb{Q}}_l)) \xrightarrow{\alpha} H^1(\overline{C}, \overline{\mathbb{Q}}_l) \longrightarrow H^1(\overline{C}, j_*(\overline{\mathbb{Q}}_l)) \longrightarrow$$
$$\cdots \longrightarrow H^2(\overline{C}, i_!(\overline{\mathbb{Q}}_l)) \xrightarrow{\beta} H^2(\overline{C}, \overline{\mathbb{Q}}_l) \longrightarrow H^2(\overline{C}, j_*(\overline{\mathbb{Q}}_l)).$$

Because $j_*(\mathbb{Q}_l)$ is the direct sum of skyscraper sheaves, it is acyclic. Hence the map α is surjective and the map β is an isomorphism. By the proper base change theorem, $H^1_c(\overline{U}, \overline{\mathbb{Q}}_l) = H^1(\overline{C}, i_!(\overline{\mathbb{Q}}_l))$ so the pair $(H^1(\overline{C}, i_!(\overline{\mathbb{Q}}_l)), F^*)$ has weights at most 1 by Deligne's purity theorem. Similarly, $H^2_c(\overline{U}, \overline{\mathbb{Q}}_l) = H^2(\overline{C}, i_!(\overline{\mathbb{Q}}_l))$ so

the pair $(H^2(\overline{C}, i_!(\overline{\mathbb{Q}}_l), F^*)$ has slope 1 by the duality theorem. Because the maps α and β are F^*-equivariant, the claims are now clear. □

Notation 8.11. Now let X be a surface over $\mathbb{F}_q$, that is, a two-dimensional variety defined over $\mathbb{F}_q$. Let U be a smooth dense open subscheme of X and let $i : U \to X$ be the inclusion map. Then we have a map

$$i_* : H_c^2(\overline{U}, \overline{\mathbb{Q}}_l) \longrightarrow H^2(\overline{X}, \overline{\mathbb{Q}}_l)$$

that is the composition of the isomorphism $H_c^2(\overline{U}, \overline{\mathbb{Q}}_l) = H^2(\overline{X}, i_!(\overline{\mathbb{Q}}_l))$ furnished by proper base change and the homomorphism $H^2(\overline{X}, i_!(\overline{\mathbb{Q}}_l)) \to H^2(\overline{X}, \overline{\mathbb{Q}}_l)$ induced by the inclusion $i_!(\overline{\mathbb{Q}}_l) \subseteq \overline{\mathbb{Q}}_l$.

Lemma 8.12. (i) *The pair* $(\mathrm{Ker}(i_*), F^*)$ *has weights at most* 1.

(ii) *The pair* $(\mathrm{Coker}(i_*), F^*)$ *has slope* 1.

Proof. Let C be the reduced closed subscheme whose underlying set is the complement of U and let $j : C \to X$ be the inclusion map. Then C is a curve and there is a cohomological long exact sequence

$$H^1(\overline{X}, j_*(\overline{\mathbb{Q}}_l)) \to H^2(\overline{X}, i_!(\overline{\mathbb{Q}}_l)) \to H^2(\overline{X}, \overline{\mathbb{Q}}_l) \to H^2(\overline{X}, j_*(\overline{\mathbb{Q}}_l)).$$

Because $H^1(\overline{X}, j_*(\overline{\mathbb{Q}}_l)) = H^1(\overline{C}, \overline{\mathbb{Q}}_l)$ and $H^2(\overline{X}, j_*(\overline{\mathbb{Q}}_l)) = H^2(\overline{C}, \overline{\mathbb{Q}}_l)$, the pair $(H^1(\overline{X}, j_*(\overline{\mathbb{Q}}_l)), F^*)$ has weights at most 1 and the pair $(H^2(\overline{X}, j_*(\overline{\mathbb{Q}}_l)), F^*)$ has slope 1 by Lemma 8.10. The claims are now clear. □

Proposition 8.13. *Let* X_1 *and* X_2 *be two birationally equivalent geometrically irreducible projective surfaces over* $\mathrm{Spec}(\mathbb{F}_q)$. *Assume that both* X_1 *and* X_2 *are pure of weight* 2 *in dimension* 2. *Then*

$$l_q(\det(1 - F^* t \,|\, H^2(\overline{X}_1, \overline{\mathbb{Q}}_l))) = l_q(\det(1 - F^* t \,|\, H^2(\overline{X}_2, \overline{\mathbb{Q}}_l))).$$

Proof. Let U be a smooth, two-dimensional scheme over $\mathrm{Spec}(\mathbb{F}_q)$ such that there are open immersions $i_1 : U \to X_1$ and $i_2 : U \to X_1$. Then

$$l_q(\det(1 - F^* t \,|\, \mathrm{Im}(i_{k*})) = l_q(\det(1 - F^* t \,|\, H^2(\overline{X}_k, \overline{\mathbb{Q}}_l)))$$

for $k = 1, 2$, using the notation of 8.11, by Lemma 8.12(ii). Let V denote the largest F^*-invariant $\overline{\mathbb{Q}}_l$-linear subspace of $H_c^2(\overline{U}, \overline{\mathbb{Q}}_l)$ that has weights at most 1. Because $H^2(\overline{X}_k, \overline{\mathbb{Q}}_l)$ is pure of weight 2 we have $V \subseteq \mathrm{Ker}(i_{k*})$ for $k = 1, 2$. But $V \supseteq \mathrm{Ker}(i_{k*})$ by Lemma 8.12(i). Hence

$$\det(1 - F^* t \,|\, \mathrm{Im}(i_{1*})) = \det(1 - F^* t \,|\, H_c^2(\overline{U}, \overline{\mathbb{Q}}_l)/V) = \det(1 - F^* t \,|\, \mathrm{Im}(i_{2*})),$$

so the claim is clear. □

Now assume that $q = p$.

Theorem 8.14. *Let p be a prime number and let n be a positive integer as above. Assume that $n \mid p-1$ and $6 \mid n$. Then E_n is not isotrivial and*

$$m(E_n) = \tfrac{1}{6}n - 1 = \tfrac{1}{12}\deg(\Delta_{E_n}) - 1.$$

Proof. Let $\underline{a} = (-3, 6, -2, -1) \in \widehat{G}$. By our assumption for every $k = 0, 1, \ldots, n-1$ we have $k\underline{a} \in \widehat{G}'$ if and only if $k \neq n/6, n/3, n/2, 2n/3$ or $5n/6$. Because of our assumption $n \mid p-1$ every orbit of multiplication by p on $\Gamma^{\perp} \cap \widehat{G}'$ consists of one element. Hence

$$\det(1 - F^* t \mid H^2(\overline{F_n/\Gamma}, \overline{\mathbb{Q}}_l)) = \prod_{\substack{0 \leq k \leq n-1; \\ k \neq n/6, n/3, n/2, \\ 2n/3, 5n/6}} (1 - J(k\underline{a})t) \tag{25}$$

by Theorem 8.8. Gauss sums are Weil numbers of weight 1, and hence the reciprocal roots of the polynomial in (25) are Weil numbers of weight 2. The surface $\mathscr{E}_n$ is smooth, so it is pure of weight 2 in dimension 2 by Deligne's purity theorem. Hence by Theorem 8.3 and Proposition 8.13, we have

$$l_q(L(E_n, t)) = l_q(\det(1 - F^* t \mid H^2(\overline{\mathscr{E}}_n, \overline{\mathbb{Q}}_l))) = l_q(\det(1 - F^* t \mid H^2(\overline{F_n/\Gamma}, \overline{\mathbb{Q}}_l))).$$

For every $k = 1, 2, \ldots, n/6 - 1$, we have

$$\begin{aligned} &\upsilon_p(J(k\underline{a})) = \\ &\upsilon_p\big(g(\alpha^{-3k(p-1)/n}, \psi)g(\alpha^{6k(p-1)/n-p+1}, \psi)g(\alpha^{-2k(p-1)/n}, \psi)g(\alpha^{-k(p-1)/n}, \psi)\big) - 1 \\ &\qquad = \frac{3k}{n} + 1 - \frac{6k}{n} + \frac{2k}{n} + \frac{k}{n} - 1 = 0 \end{aligned}$$

by Theorem 8.6, since every exponent of α^{-1} in the equation above is a positive integer strictly less than p. Hence by Proposition 4.5 and the above,

$$m(E_n) \geq l_q(L(E_n, t)) \geq \tfrac{1}{6}n - 1.$$

Because $6 \mid p-1$ by our assumptions, we have $p \geq 7$. Hence

$$m(E_n) \leq \tfrac{1}{12}\deg(\Delta_{E_n}) - 1 = \tfrac{1}{6}n - 1$$

by Theorem 6.9 and by our remark at the end of Definition 8.1. □

9. Strong Weil curves

Definition 9.1. Fix now a closed point ∞ of $\mathscr{C}$ and let A denote the ring of rational functions on $\mathscr{C}$ regular away from ∞ as in the introduction. For any nonzero ideal $\mathfrak{m}$ of A, an irreducible affine algebraic curve $Y_0(\mathfrak{m})$ is defined over F, the Drinfeld modular curve parametrising Drinfeld A-modules of rank 2 of generic characteristic with Hecke level $\mathfrak{m}$-structure. There is a unique nonsingular projective curve

$X_0(\mathfrak{m})$ over F that contains $Y_0(\mathfrak{m})$ as a dense open subvariety. Let $J_0(\mathfrak{m})$ denote the Jacobian of the curve $X_0(\mathfrak{m})$. The ideals of A and the effective divisors on $\mathscr{C}$ whose support does not contain ∞ are in a natural one-to-one correspondence, and we will not distinguish them in what follows. Let E be an elliptic curve defined over F that has split multiplicative reduction at ∞. Then its conductor is of the form $\mathfrak{m}\infty$, where $\mathfrak{m}$ is an ideal of A. By the function field analogue of the Taniyama–Weil conjecture, there is a nonconstant map $\pi : X_0(\mathfrak{m}) \to E$ defined over F. For any map $h : X_0(\mathfrak{m}) \to C$, where C is an elliptic curve, let $h_* : J_0(\mathfrak{m}) \to C$ and $h^* : C \to J_0(\mathfrak{m})$ denote the maps induced by the Albanese and the Picard functorialities.

Theorem 9.2. *The following are equivalent*:

(i) *The kernel of the map $\pi_* : J_0(\mathfrak{m}) \to E$ is an abelian variety.*

(ii) *The map $\pi^* : E \to J_0(\mathfrak{m})$ is a closed immersion.*

(iii) *The degree of π is minimal among all nondegenerate maps $\rho : X_0(\mathfrak{m}) \to E'$, where E' is any elliptic curve isogenous to E over F.*

Proof. This result is well known in the mathematical folklore, but it is difficult to track down a proof — the standard reference, [Mazur 1973, Lemme 3], only shows the equivalence of (i) and (iii). Our excuse for giving a full proof other than that is that we consider the more delicate case of positive characteristic. First assume that (i) holds. By the multiplicity 1 theorem for the action of the Hecke algebra on $J_0(\mathfrak{m})$, the abelian variety $\mathrm{Ker}(\pi_*)$ has no quotient isogenous to E, so for every nondegenerate map $\rho : X_0(\mathfrak{m}) \to E'$, where E' is any elliptic curve isogenous to E over F, the kernel of ρ_* must contain $\mathrm{Ker}(\pi_*)$. Hence the map ρ factors through π, and in particular its degree is at least as big as that of π. On the other hand, if (iii) holds, then $\mathrm{Ker}(\pi_*)$ contains the reduction of the connected component of its identity element as a closed subgroup-scheme. The quotient E' of $J_0(\mathfrak{m})$ by the latter is an elliptic curve isogenous to E; hence the degree of the corresponding map $\rho : X_0(\mathfrak{m}) \to E'$ is at least as big as $\deg(\pi)$. But π factors through ρ, so they must be equal. Note that the map π^* is just the dual of the morphism $\pi_* : J_0(\mathfrak{m}) \to E$ of the principally polarised abelian varieties. The equivalence of (i) and (ii), and therefore the theorem itself, now follows from the lemma below. □

Lemma 9.3. *Let $\phi : A \to B$ be a surjective homomorphism of abelian varieties and let $\phi^\vee : B^\vee \to A^\vee$ be its dual. Then the following are equivalent*:

(i) *The kernel of ϕ is an abelian variety.*

(ii) *The map $\phi^\vee$ is a closed immersion.*

Proof. This proof was explained to me by Laurent Fargues. For any S-scheme T let T also denote the sheaf represented by T on the *fppf* topology on S. Attached

to the short exact sequence

$$0 \longrightarrow \mathrm{Ker}(\phi) \longrightarrow A \xrightarrow{\phi} B \longrightarrow 0$$

of sheaves on the *fppf* topology, there is a cohomological exact sequence

$$\mathrm{Hom}(A, \mathbb{G}_m) \longrightarrow \mathrm{Hom}(\mathrm{Ker}(\phi), \mathbb{G}_m) \longrightarrow \mathrm{Ext}^1(B, \mathbb{G}_m) \xrightarrow{\phi^\vee} \mathrm{Ext}^1(A, \mathbb{G}_m).$$

By a theorem of Grothendieck, for any abelian scheme C the sheaf $\mathrm{Ext}^1(C, \mathbb{G}_m)$ is represented by the dual of C and for any morphism $\phi : A \to B$ of abelian varieties the induced map $\mathrm{Ext}^1(B, \mathbb{G}_m) \to \mathrm{Ext}^1(A, \mathbb{G}_m)$ is the dual of ϕ, as the notation above indicates. Moreover the sheaf $\mathrm{Hom}(C, \mathbb{G}_m)$ is trivial for any abelian scheme C, and hence $\phi^\vee$ is an immersion if and only if $\mathrm{Hom}(\mathrm{Ker}(\phi), \mathbb{G}_m)$ is trivial. Let $\mathrm{Ker}(\phi)_0$ denote the reduced group scheme associated to the connected component of $\mathrm{Ker}(\phi)$, considered as a closed subgroup-scheme. It is an abelian subscheme of $\mathrm{Ker}(\phi)$ such that the quotient $G = \mathrm{Ker}(\phi)/\mathrm{Ker}(\phi)_0$ is a finite, flat group scheme. By looking at the cohomological exact sequence attached to the short exact sequence

$$0 \longrightarrow \mathrm{Ker}(\phi)_0 \longrightarrow \mathrm{Ker}(\phi) \longrightarrow G \longrightarrow 0$$

of sheaves on the *fppf* topology, we get that $\mathrm{Hom}(\mathrm{Ker}(\phi), \mathbb{G}_m) = \mathrm{Hom}(G, \mathbb{G}_m)$. The sheaf $\mathrm{Hom}(G, \mathbb{G}_m)$ is represented by the Cartier dual of the group scheme G, so it is trivial if and only if G is trivial. □

Definition 9.4. If the equivalent conditions of Lemma 9.3 hold, then we say that E is a strong Weil curve and the modular parametrisation $\pi : X_0(\mathfrak{m}) \to E$ is optimal. By the proof above, it is clear that up to isomorphism E is unique in its isogeny class and there is only one strong Weil map parametrising E. On the other hand, by property (i), the quotient of $J_0(\mathfrak{m})$ by the reduced group scheme associated to the connected component of the kernel of the map $\pi_* : J_0(\mathfrak{m}) \to E$ induced by any modular parametrisation $\pi : X_0(\mathfrak{m}) \to E$ is a strong Weil curve. Hence there is a strong Weil curve in the isogeny class of every elliptic curve having split multiplicative reduction at ∞.

10. Applications to the degree conjecture

Definition 10.1. For any graph G, let $\mathscr{V}(G)$ and $\mathscr{E}(G)$ denote its set of vertices and edges, respectively. Let R be a commutative group and let G be a locally finite oriented graph. In this paper we will assume that every oriented graph G is equipped with an involution $\bar{\cdot} : \mathscr{E}(G) \to \mathscr{E}(G)$ such that for each edge $e \in \mathscr{E}(G)$, the original and terminal vertices of the edge $\bar{e} \in \mathscr{E}(G)$ are the terminal and original vertices of e, respectively. The edge $\bar{e}$ is called the edge e with reversed orientation. If for each edge $e \in \mathscr{E}(G)$ there is exactly one edge $\bar{e} \in \mathscr{E}(G)$ whose original and terminal vertices are the terminal and original vertices of e, then there is a

unique involution of this type. The Bruhat–Tits tree $\mathcal{T}$ is such a graph. A function $\phi : \mathcal{E}(G) \to R$ is called a harmonic R-valued cochain if it satisfies the following conditions:

- $\phi(e) + \phi(\bar{e}) = 0$ for all $e \in \mathcal{E}(G)$.
- If for an edge e we introduce the notation $o(e)$ and $t(e)$ for its original and terminal vertex respectively,

$$\sum_{\substack{e \in \mathcal{E}(G) \\ o(e) = v}} \phi(e) = 0 \quad \text{for all } v \in \mathcal{V}(G).$$

We denote by $H(G, R)$ the group of R-valued harmonic cochains on G.

Definition 10.2. Let $Y \subset F^2$ be an A-lattice, that is, a projective A-submodule of rank 2. Let $\Gamma(Y)$ denote the F-linear automorphisms of F^2 leaving Y invariant, and for every ideal $\mathfrak{a} \lhd A$, let $\Gamma(Y, \mathfrak{a}) \leq \Gamma(Y)$ denote the subgroup of those elements that induce the identity on the quotient A-module $Y/\mathfrak{a}Y$. We say that a subgroup Γ of $\mathrm{GL}_2(F)$ is arithmetic if there is an A-lattice Y and an ideal $\mathfrak{a}$ such that Γ is contained in $\Gamma(Y)$ and it contains $\Gamma(Y, \mathfrak{a})$. Let Γ be an arithmetic subgroup of $\mathrm{GL}_2(F)$ and let F_∞ denote the completion of F with respect to the valuation corresponding to ∞. As a subgroup of $\mathrm{GL}_2(F_\infty)$, the arithmetic group Γ acts on the Bruhat–Tits tree associated to $\mathrm{PGL}_2(F_\infty)$ on the left, which we will denote by $\mathcal{T}$. For any abelian group M, let $H_!(\mathcal{T}, M)^\Gamma$ denote the group of those Γ-invariant, M-valued harmonic cochains on $\mathcal{T}$ that has finite support as a function on the edges of the quotient graph $\Gamma\backslash\mathcal{T}$.

Definition 10.3. Next we define the first homology group $H_1(\Gamma\backslash\mathcal{T}, \mathbb{Z})$, which has several descriptions. It may be defined as the first topological homology group of the CW-complex attached to $\Gamma\backslash\mathcal{T}$ with integral coefficients. It is also canonically isomorphic to the abelianization of the quotient $\Gamma^* = \Gamma/\Gamma_f$, where Γ_f is the normal subgroup of Γ generated by the elements of finite order. We will use a third, purely combinatorial description, since it is the most convenient for our purposes. Recall that a path on an oriented graph G is a sequence of edges $e_1, e_2, \ldots, e_n \in \mathcal{E}(G)$ such that $t(e_i) = o(e_{i+1})$ for $i = 1, 2, \ldots, n-1$. The path is closed if the equality $t(e_n) = o(e_1)$ holds, too. For each edge $e \in \mathcal{E}(G)$, let $i_e : \mathcal{E}(G) \to \mathbb{Z}$ denote the unique function such that

$$i_e(f) = \begin{cases} +1 & \text{if } f = e, \\ -1 & \text{if } f = \bar{e}, \\ 0 & \text{otherwise.} \end{cases}$$

To any closed path $e_1, e_2, \ldots, e_n$ we associate the function $\sum_{i=1}^n i_{e_i}$. We define $H_1(G, \mathbb{Z})$ as the abelian group of $\mathbb{Z}$-valued functions on $\mathcal{E}(G)$ generated by these

functions. Let us return to the special case $G = \Gamma\backslash\mathcal{T}$. Let $z(\Gamma)$ denote the cardinality of the center of Γ and let Γ_e be the stabiliser of the edge $e \in \mathcal{E}(\mathcal{T})$ in Γ. Let us quickly recall why Γ_e is finite. Let $v : \mathrm{GL}_2(F_\infty) \to \mathbb{Z}$ be the composition of the determinant and the valuation, and let $\mathrm{GL}_2(F_\infty)_0$ denote its kernel. We claim that every arithmetic group Γ lies in $\mathrm{GL}_2(F_\infty)_0$. Clearly it is enough to show this for $\Gamma(Y)$. The localisation of Y at each prime of A is a free module of rank 2, so the determinant of every element of $\Gamma(Y)$ is a unit at each prime of A, so it is in fact a unit of A. The latter are constants, so they have valuation zero. On the other hand, the stabiliser of e in $\mathrm{GL}_2(F_\infty)_0$ is compact, so Γ_e is finite as the intersection of a compact and a discrete group. We define

$$j_\Gamma : H_1(\Gamma\backslash\mathcal{T}, \mathbb{Z}) \to H_!(\mathcal{T}, \mathbb{Z})^\Gamma$$

as the map $\phi \mapsto \phi^*$ given by the rule $\phi^*(e) = |\Gamma_e|\phi(\tilde{e})/z(\Gamma)$, where $\tilde{e}$ is the image of the edge e in $\mathcal{E}(\Gamma\backslash\mathcal{T})$. It is easy to see that the homomorphism is well-defined, that is, ϕ^* is indeed a harmonic cochain.

Proposition 10.4. *The homomorphism j_Γ is injective with finite cokernel of exponent dividing $q^{\deg(\infty)} - 1$.*

Proof. The injectivity is trivial if the definition above is employed. Gekeler and Reversat [1996, Proposition 6.4.4] proved that the cokernel has index prime to the characteristic p, and if one uses this result, a careful reading of the proof of [Gekeler and Reversat 1996, Lemma 3.3.3] reveals that our proposition above has already been proved there. Here we reproduce their argument for the sake of the reader. Let T be a maximal tree in the connected graph $\Gamma\backslash\mathcal{T}$: such a tree exists by Zorn's lemma. By Serre's structure theorem, the graph $\Gamma\backslash\mathcal{T}$ is the union of a finite graph and finitely many ends, and hence the complement $\mathcal{E}(\Gamma\backslash\mathcal{T}) - \mathcal{E}(T)$ is finite. Let $R = \{\tilde{e}_1, \ldots, \tilde{e}_g\}$ be a set of representatives of $\mathcal{E}(\Gamma\backslash\mathcal{T}) - \mathcal{E}(T)$ modulo orientation, that is, for every edge $e \in \mathcal{E}(\Gamma\backslash\mathcal{T}) - \mathcal{E}(T)$ let exactly one of the edges e and $\overline{e}$ be listed in R. For each edge $\tilde{e}_i \in R$, let c_i denote a closed path consisting of $\tilde{e}_i$ and a path connecting $t(e_i)$ with $o(e_i)$ in T. For any $\phi \in H_!(\mathcal{T}, \mathbb{Z})^\Gamma$, the function

$$\phi - \sum_{i=1}^{g} \frac{\phi(e_i) z(\Gamma)}{|\Gamma_{e_i}|} j_\Gamma(c_i)$$

vanishes identically outside of the maximal tree T, and hence vanishes everywhere. Therefore the cokernel of j_Γ is annihilated by the smallest common multiple of the natural numbers $|\Gamma_{e_i}|/z(\Gamma)$. Since the torsion of the stabiliser of any edge $e \in \mathcal{E}(\mathcal{T})$ in the image of $\mathrm{GL}_2(F_\infty)_0$ in $P\,\mathrm{GL}_2(F_\infty)$ modulo its p-torsion group is a group of order $q^{\deg(\infty)} - 1$, the claim is now clear. □

Notation 10.5. In the rest of the paper we assume that E is a strong Weil curve and $\pi : X_0(\mathfrak{m}) \to E$ is optimal. Let Γ be the arithmetic group:

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A) \,|\, c \in \mathfrak{m} \right\}.$$

One may associate to the strong Weil curve E an element $v_E \in H_!(\mathcal{T}, \mathbb{Z})^\Gamma$ lying in the image of the map j_Γ (for its definition see [Papikian 2007, 3.4]). The set $\mathscr{E}(\mathcal{T})$ can be identified with $\mathrm{GL}_2(F_\infty)/\,\Gamma_\infty Z(F_\infty)$, where Γ_∞ is the Iwahori subgroup:

$$\Gamma_\infty = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{O}_\infty) \,|\, \infty(c) > 0 \right\}.$$

There is a natural map

$$h : \mathscr{E}(\mathcal{T}) \to \mathrm{GL}_2(F) \backslash \mathrm{GL}_2(\mathbb{A}) / \mathbb{K}_0(\mathfrak{m}\infty) Z(\mathbb{A})$$

that for $g \in \mathrm{GL}_2(F_\infty)$ maps the left $\Gamma_\infty Z(F_\infty)$-coset of g to the double coset $\mathrm{GL}_2(F)\mathbf{g}K_0(\mathfrak{m}\infty)Z(\mathbb{A})$ of the unique element $\mathbf{g} \in \mathrm{GL}_2(\mathbb{A})$ such that for every $x \in |\mathscr{C}|$, the x-th component of $\mathbf{g}$ is g if x is ∞, and 1 otherwise. By [Gekeler and Reversat 1996, 9.1], the function v_E lies in the $\mathbb{Q}$-module $\mathbb{Q}(\psi_E \circ h)$ spanned by $\psi_E \circ h$. Let $\tilde{c}(E)$ be the unique nonnegative number such that $v_E = \tilde{c}(E)\psi_E \circ h$. By definition, v_E generates the $\mathbb{Z}$-module $\mathrm{Im}(j_\Gamma) \cap \mathbb{Q}(\psi_E \circ h)$. Hence Proposition 10.4 has the following immediate corollary:

Corollary 10.6. $\tilde{c}(E) \leq (q^{\deg(\infty)} - 1)c(E)^{-1}$.

Using the Riemann hypothesis for the L-function $L(\mathrm{Symm}^2(E), t)$ of the second symmetric square of the Galois representation $H^1(E_{\bar{F}}, \mathbb{Q}_l)$, Papikian [2007, Theorem 4.6 and Proposition 1.3] deduces the following from his main formula for the degree of modular parametrisations of elliptic curves:

Theorem 10.7. *Assume that* $\mathfrak{m}$ *is square-free. Then*

$$\deg(\pi) < \tilde{c}(E)^2 \cdot q^{14g+\deg(\infty)+5} \cdot q^{\deg(\mathfrak{m})} \cdot \deg(\mathfrak{m})^3.$$

Combining Corollary 7.7 with Corollary 10.6 and Theorem 10.7, we obtain the following result:

Theorem 10.8. *Assume that* p *does not divide the order of* $\mathrm{Pic}_0(\mathscr{C})(\mathbb{F}_q)$, *and that* $\mathfrak{m}$ *is square-free. Then*

$$\deg(\pi) < q^{18g+4\deg(\infty)+1} \cdot q^{2\deg(\mathfrak{m})} \cdot \deg(\mathfrak{m})^3.$$

References

[Chinburg 1994] T. Chinburg, "Galois structure of de Rham cohomology of tame covers of schemes", *Ann. of Math.* (2) **139**:2 (1994), 443–490. MR 95h:11125a Zbl 0828.14007

[Deligne 1973] P. Deligne, "Les constantes des équations fonctionnelles des fonctions L", pp. 501–597 in *Modular functions of one variable* (Antwerp, 1972), vol. II, edited by P. Deligne and W. Kuyk, Lecture Notes in Math **349**, Springer, Berlin, 1973. MR 50 #2128 Zbl 0271.14011

[Faber and van der Geer 2004] C. Faber and G. van der Geer, "Complete subvarieties of moduli spaces and the Prym map", *J. Reine Angew. Math.* **573** (2004), 117–137. MR 2005g:14054 Zbl 1075.14023

[Gekeler and Reversat 1996] E.-U. Gekeler and M. Reversat, "Jacobians of Drinfeld modular curves", *J. Reine Angew. Math.* **476** (1996), 27–93. MR 97f:11043 Zbl 0848.11029

[Goldfeld and Szpiro 1995] D. Goldfeld and L. Szpiro, "Bounds for the order of the Tate-Shafarevich group", *Compositio Math.* **97**:1-2 (1995), 71–87. MR 97a:11102 Zbl 0860.11032

[Harder 1974] G. Harder, "Chevalley groups over function fields and automorphic forms", *Ann. of Math.* (2) **100** (1974), 249–306. MR 58 #27799 Zbl 0309.14041

[Illusie 1979] L. Illusie, "Complexe de de Rham–Witt et cohomologie cristalline", *Ann. Sci. École Norm. Sup.* (4) **12**:4 (1979), 501–661. MR 82d:14013 Zbl 0436.14007

[Illusie 1990] L. Illusie, "Ordinarité des intersections complètes générales", pp. 376–405 in *The Grothendieck Festschrift*, vol. II, edited by P. Cartier et al., Progr. Math. **87**, Birkhäuser, 1990. MR 93h:14015 Zbl 0728.14021

[Katz and Messing 1974] N. M. Katz and W. Messing, "Some consequences of the Riemann hypothesis for varieties over finite fields", *Invent. Math.* **23** (1974), 73–77. MR 48 #11117 Zbl 0275.14011

[Lang 1994] S. Lang, *Algebraic number theory*, 2nd ed., Grad. Texts in Math. **110**, Springer, New York, 1994. MR 95f:11085 Zbl 0811.11001

[Laumon 1987] G. Laumon, "Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil", *Inst. Hautes Études Sci. Publ. Math.* 65 (1987), 131–210. MR 88g:14019 Zbl 0641.14009

[Mazur 1972] B. Mazur, "Frobenius and the Hodge filtration", *Bull. Amer. Math. Soc.* **78** (1972), 653–667. MR 48 #8507 Zbl 0258.14006

[Mazur 1973] B. Mazur, "Courbes elliptiques et symboles modulaires", pp. 277–294 in *Séminaire Bourbaki* 1971/1972 (Exposé 414), Lecture Notes in Math. **317**, Springer, Berlin, 1973. MR 55 #2930 Zbl 0276.14012

[Miller 1972] L. Miller, "Curves with invertible Hasse–Witt matrix", *Math. Ann.* **197** (1972), 123–127. MR 47 #3399 Zbl 0235.14009

[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

[Mumford 1969] D. Mumford, "Bi-extensions of formal groups", pp. 307–322 in *Algebraic Geometry (Internat. Colloq.)* (Bombay, 1968), Oxford Univ. Press, London, 1969. MR 41 #1743 Zbl 0216.33101

[Norman and Oort 1980] P. Norman and F. Oort, "Moduli of abelian varieties", *Ann. of Math.* (2) **112**:3 (1980), 413–439. MR 82h:14026 Zbl 0483.14010

[Papikian 2005] M. Papikian, "Pesenti–Szpiro inequality for optimal elliptic curves", *J. Number Theory* **114**:2 (2005), 361–393. MR 2006f:11062 Zbl 1084.11027

[Papikian 2007] M. Papikian, "Analogue of the degree conjecture over function fields", *Trans. Amer. Math. Soc.* **359**:7 (2007), 3483–3503. MR 2008d:11057 Zbl 05140897

[Pesenti and Szpiro 2000] J. Pesenti and L. Szpiro, "Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques", *Compositio Math.* **120**:1 (2000), 83–117. MR 2001c:11063 Zbl 1021.11021

[Rück and Tipp 2000] H.-G. Rück and U. Tipp, "Heegner points and L-series of automorphic cusp forms of Drinfeld type", *Doc. Math.* **5** (2000), 365–444. MR 2001i:11057 Zbl 1012.11039

[Seiler 1987] W. K. Seiler, "Global moduli for elliptic surfaces with a section", *Compositio Math.* **62**:2 (1987), 169–185. MR 88m:14027 Zbl 0624.14023

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015

[Tan 1993] K.-S. Tan, "Modular elements over function fields", *J. Number Theory* **45**:3 (1993), 295–311. MR 95d:11158 Zbl 0802.11026

[Ulmer 2002] D. Ulmer, "Elliptic curves with large rank over function fields", *Ann. of Math.* (2) **155**:1 (2002), 295–315. MR 2003b:11059 Zbl 1109.11314

Communicated by Richard Taylor
Received 2009-03-31 Revised 2009-12-02 Accepted 2009-12-31

a.pal@imperial.ac.uk *Department of Mathematics, Imperial College, 180 Queen's Gate, London, SW7 2AZ, United Kingdom*

ALGEBRA AND NUMBER THEORY 4:5(2010)

Le problème de Bogomolov effectif sur les variétés abéliennes

Aurélien Galateau

On obtient une nouvelle minoration du minimum essentiel en petite codimension sur les variétés abéliennes, sous une conjecture concernant leurs idéaux premiers ordinaires. Cette minoration, déjà connue dans le cas torique depuis les travaux d'Amoroso et David, est optimale « à ε près » en le degré de la sous-variété. La preuve suit la méthode des pentes et est basée sur les propriétés p-adiques des points de torsion des variétés abéliennes.

We give a new lower bound for the essential minimum of subvarieties of abelian varieties with small codimension, under a conjecture about ordinary primes in abelian varieties. This lower bound, known in the toric case through the work of Amoroso and David, is best "up to an ε" in the degree of the subvariety. The proof follows the slope method and is based on the p-adic properties of torsion points in abelian varieties.

1. Introduction

L'objet de ce travail est de minorer le minimum essentiel sur les variétés abéliennes. Une telle minoration est une version quantitative de la conjecture de Bogomolov. Soit C une courbe algébrique de genre $g \geq 2$ définie sur $\overline{\mathbb{Q}}$ et plongée dans sa jacobienne $J(C)$. On note L le fibré canonique et $\hat{h}_L$ la hauteur de Néron–Tate associée. Le théorème suivant a été conjecturé par Bogomolov.

Théorème 1.1 (Ullmo). *Il existe $\varepsilon > 0$ tel que $\{x \in C(\overline{\mathbb{Q}}) : \hat{h}_L(x) \leq \varepsilon\}$ est fini.*

Plus généralement, soit V une sous-variété algébrique d'une variété abélienne A munie d'un fibré L ample et symétrique, et $\hat{h}_L$ la hauteur de Néron–Tate associée à ce fibré (ici et dans toute la suite de cet article, une variété est toujours supposée *irréductible et définie sur* $\overline{\mathbb{Q}}$). On commence par donner un analogue en dimension supérieure de l'hypothèse faite précédemment sur le genre.

MSC2000: primary 11G10; secondary 11J81, 14G40.

Mots-clefs: Bogomolov, variété abélienne, minoration, hauteur, abelian variety, lower bound, height.

Définition 1.2. On dit que V est de torsion si V est la translatée d'une sous-variété abélienne par un point de torsion.

On introduit aussi le minimum essentiel, qui renseigne sur les points de petite hauteur dans V.

Définition 1.3. Le minimum essentiel de V est :

$$\hat{\mu}_L^{\mathrm{ess}}(V) = \inf\{\theta > 0 : \overline{V(\theta)}^Z = V(\overline{\mathbb{Q}})\},$$

où $V(\theta) = \{x \in V(\overline{\mathbb{Q}}), \hat{h}_L(x) \leq \theta\}$ et $\overline{V(\theta)}^Z$ est son adhérence de Zariski.

On peut maintenant donner une généralisation de la conjecture de Bogomolov en dimension supérieure.

Théorème 1.4 (Zhang). *Soit V une sous-variété d'une variété abélienne A. Le minimum essentiel de V est nul si et seulement si V est de torsion.*

Le résultat analogue est vrai si on remplace A par un tore [Zhang 1992] ou plus généralement par une variété semi-abélienne [David et Philippon 2000].

On peut donner une version quantitative de ce résultat. Ceci revient, en dimension générale, à minorer le minimum essentiel d'une variété qui n'est pas de torsion. Par le théorème des minima successifs démontré par Zhang [1995a], il est équivalent de minorer la hauteur d'une telle variété. Depuis les travaux de Bombieri et Zannier (voir [1995] pour le cas torique et [1996] pour le cas abélien), on sait qu'on peut espérer obtenir une borne « uniforme » pour le minimum essentiel, ne dépendant que du degré de V et de la variété abélienne A.

Dans le cas torique, Amoroso et David [2003] donnent une minoration optimale aux facteurs logarithmiques près en le degré de V. Le degré y est remplacé par un invariant plus fin qui apparaît naturellement avec les techniques diophantiennes, l'indice d'obstruction.

Définition 1.5. Soit V une sous-variété stricte de S une variété semi-abélienne munie de L un fibré ample. On définit l'indice d'obstruction de V, noté $\omega_L(V)$, par :

$$\omega_L(V) = \inf \deg_L(Z),$$

où l'infimum est pris sur l'ensemble des hypersurfaces (irréductibles) de S contenant V.

Soit L le fibré associé au plongement standard $\mathbb{G}_m^n \hookrightarrow \mathbb{P}^n$. On obtient une hauteur projective h_L sur les points de $\mathbb{G}_m^n(\overline{\mathbb{Q}})$ et un minimum essentiel $\hat{\mu}_L^{\mathrm{ess}}$ sur les sous-variétés de $\mathbb{G}_m^n(\overline{\mathbb{Q}})$.

Théorème 1.6 (Amoroso, David). *Soit V une sous-variété stricte de $\mathbb{G}_m^n$ de codimension r qui n'est contenue dans aucun translaté d'un sous-tore strict de $\mathbb{G}_m^n$. On a :*

$$\hat{\mu}_L^{\mathrm{ess}}(V) \geq \frac{c(n)}{\omega_L(V)} (\log(3\omega_L(V)))^{-\lambda(r)},$$

où $c(n)$ est un réel strictement positif et $\lambda(r) = (9(3r)^{r+1})^r$.

Dans le cas des variétés abéliennes, on dispose déjà de résultats quantitatifs et inconditionnels, mais la dépendance en le degré n'est pas aussi bonne.

Théorème 1.7 (David, Philippon). *Soit A une variété abélienne de dimension $g \geq 2$ définie sur $\overline{\mathbb{Q}}$, principalement polarisée par un fibré L. Si V est une sous-variété stricte de A qui n'est pas translatée d'une sous-variété abélienne, on a :*

$$\hat{\mu}_L^{\mathrm{ess}}(V) \geq \frac{\min\{1; \mathcal{R}_{\mathrm{inj}}\}^{2(b+1)}}{2^{11g^3}(g-k+1)\deg_L(V)^{2k(b+1)}},$$

où k désigne le nombre minimal de copies de $V - V$ dont la somme est une sous-variété abélienne de A, b la dimension de cette sous-variété abélienne et $\mathcal{R}_{\mathrm{inj}}$ la plus petite norme de Riemann d'une période d'une conjuguée de A.

Au numérateur, on voit apparaître le rayon d'injectivité, qui est relié à $h_L(A)$ (hauteur projective de l'origine dans le plongement associé à $L^{\otimes 16}$) par le lemme « matriciel » de Masser [David et Philippon 2002, lemme 6.8]. Cette minoration est monomiale inverse en le degré, alors que dans le cas torique, elle est linéaire inverse en l'indice d'obstruction (aux facteurs logarithmiques près), ce qui correspond à une minoration en $\deg_L(V)^{-1/\operatorname{codim} V}$.

Remarquons enfin que l'hypothèse du théorème 1.7 (V n'est pas une translatée de sous-variété abélienne stricte) est plus faible que son analogue torique dans le théorème 1.6 (V n'est pas *incluse* dans un translaté de sous-tore strict) ; cette différence se ressent dès qu'on obtient des résultats comparables au théorème 1.6 et on peut préciser la minoration sous l'hypothèse faible, en faisant intervenir la dimension du plus petit translaté de sous-tore strict contenant V [Amoroso et David 2003, corollaire 1.6].

Résultats. Soit A une variété abélienne définie sur K un corps de nombres, et L un fibré ample et symétrique sur A. On considère l'hypothèse suivante sur les idéaux premiers de $\mathbb{O}_K$:

Hypothèse H. *Il existe une densité positive d'idéaux premiers de réduction ordinaire pour A.*

Remarquons que la densité de premiers ordinaires dépend de K, mais qu'elle ne dépend pas d'un modèle si K est fixé, car on peut caractériser ces premiers $\mathfrak{p}$ (parmi les premiers de bonne réduction) en regardant la valuation des valeurs propres de l'action d'un élément de Frobenius $F_{\mathfrak{p}}$ sur un module de Tate fixé. De plus, si A vérifie H, les puissances et les quotients de A vérifient encore H. Si A et A' sont des variétés abéliennes définies sur K et si les premiers ordinaires pour A et pour A' sont de densité 1, les premiers ordinaires de $A \times A'$ sont encore de densité 1.

Il est d'abord nécessaire de supposer que le p-rang est égal au rang de Hasse–Witt pour trouver de bonnes propriétés métriques p-adiques pour A, reliées au type de réduction modulo $\mathfrak{p}$, pour $\mathfrak{p}$ un idéal premier de $\mathbb{O}_K$ divisant un nombre premier p. Des contraintes de nature diophantienne conduisent ensuite à travailler avec des idéaux premiers $\mathfrak{p}$ pour lesquels le p-rang vaut 0 ou g ; en effet, lorsque le p-rang chute, les propriétés métriques obtenues sont plus faibles et on a besoin, en contrepartie, d'un grand nombre de points de torsion se réduisant sur 0 modulo $\mathfrak{p}$. Notre méthode fonctionne donc également avec des premiers pour lesquels le rang de Hasse–Witt est nul, mais en regard du corollaire 2.8 de [Ogus 1982], ce cas est très sporadique.

Le présent article et le suivant [Galateau 2008] sont consacrés à la preuve du théorème :

Théorème 1.8. *Si A vérifie* **H**, *on a la propriété* $\mathbf{P}(A)$ *suivante. Pour toute sous-variété algébrique V stricte de A qui n'est pas contenue dans le translaté d'une sous-variété abélienne stricte de A :*

$$\hat{\mu}_L^{\mathrm{ess}}(V) \geq \frac{C_L(A)}{\omega_L(V)} \left(\log(3 \deg_L(V))\right)^{-\lambda(r)},$$

où $C_L(A)$ est un réel strictement positif ne dépendant que de (A, L), et où $\lambda(r)$ est une constante explicite.

Dans ce travail, on établit d'abord les estimations p-adiques qui sont au cœur de cette approche, puis on adopte le point de vue de la méthode des pentes en vue de la démonstration du théorème 1.8. La preuve s'achève par un argument de descente, devenu classique dans les problèmes de minoration de hauteur. Cet argument comporte des complications techniques, accentuées encore par la spécificité du cas abélien, qui ont tendance à obscurcir l'articulation des arguments. Il nous a donc semblé intéressant de détailler ici le premier cas non trivial, celui de la codimension 2, pour mieux faire apparaître les idées combinatoires sous-jacentes. On explique en conclusion comment appliquer la descente dans le cas général. Ce travail se poursuit dans [Galateau 2008], qui utilise les estimations p-adiques démontrées ici, et donne les détails de la descente en codimension quelconque. Par ailleurs, on a cru utile de donner un autre éclairage sur ce problème en adoptant, dans le second texte, le langage diophantien classique.

L'hypothèse H est l'objet de la conjecture suivante :

Conjecture 1.9 (Serre). *Toute variété abélienne définie sur $\overline{\mathbb{Q}}$ vérifie H.*

Sous cette conjecture, la propriété $\mathbf{P}(A)$ est valide pour toute variété abélienne A définie sur $\overline{\mathbb{Q}}$. On peut conjecturer [Pink 1998, §7] que les premiers ordinaires sont en densité 1, quitte à étendre le corps de définition K de A.

Pour une courbe elliptique E, le résultat est connu. Plus précisément, on sait que la densité de tels idéaux est 1 si E n'est pas CM [Serre 1968, IV, 13], au moins $\frac{1}{2}$

si elle est CM. La validité de H a été étendue aux surfaces abéliennes [Ogus 1982, Corollary 2.9]. Notre théorème s'applique alors sans restriction :

Corollaire 1.10. *Soit C une courbe algébrique incluse dans une surface abélienne A munie d'un fibré L ample et symétrique. Si C n'est pas le translaté d'une courbe elliptique, on a* :

$$\hat{\mu}_L^{\mathrm{ess}}(C) \geq \frac{c_L(A)}{\deg_L(C)} \left(\log(3 \deg_L(C))\right)^{-64},$$

où $c_L(A)$ est un réel strictement positif ne dépendant que de (A, L).

Si A est un produit de courbes elliptiques, ou une variété abélienne CM, notre résultat est encore inconditionnel. Des conditions suffisantes pour que H soit réalisée, portant sur les groupes de monodromie G_l (associés à chaque nombre premier l) de la variété abélienne, ont été données par Noot [1995, §2], puis Pink [1998, §7].

Rappelons que la minoration fine du minimum essentiel permet d'obtenir des résultats en direction des conjectures formulées indépendamment par Bombieri, Masser et Zannier [Bombieri et al. 2007, §5], Zilber [2002] sur les variétés semi-abéliennes, puis Pink [2005, Conjectures 1.2 et 1.3] sur les variétés de Shimura mixtes. Pour S un sous-ensemble de $\mathbb{G}_m^n$, on note :

$$S_\varepsilon = \{xy : x \in S,\, y \in \mathbb{G}_m^n,\, h_L(y) \leq \varepsilon\}.$$

Le théorème 1.6 est ainsi utilisé dans [Habegger 2009] pour démontrer :

Théorème 1.11 (Habegger). *Soit C une courbe algébrique dans $\mathbb{G}_m^n$ qui n'est pas incluse dans le translaté d'un sous-tore strict. Il existe $\varepsilon > 0$ tel que $C \cap \mathscr{H}_\varepsilon$ est fini, où* :

$$\mathscr{H} = \bigcup_{\operatorname{codim} H = 2} H,$$

la réunion portant sur tous les sous-groupes algébriques de $\mathbb{G}_m^n$ ayant la codimension prescrite.

Ce théorème généralise à la fois le théorème 2 de [Bombieri et al. 1999] et la propriété de Bogomolov pour les courbes plongées dans les tores. Récemment, Maurin [2008] a démontré la conjecture de Zilber pour une courbe plongée dans un tore, en utilisant le théorème 1.11 et une inégalité de Vojta uniforme.

Théorème 1.12 (Maurin). *Soit C une courbe algébrique de $\mathbb{G}_m^n$ non incluse dans le translaté d'un sous-tore strict par un point de torsion. Alors $C \cap \mathscr{H}$ est fini.*

Ce théorème optimise le résultat principal de [Bombieri et al. 1999], qui suppose que C n'est pas incluse dans un translaté de sous-tore strict. Dans le cadre abélien, en utilisant des estimations de type Lehmer sur la hauteur des petits points, on sait essentiellement traiter le cas des variétés abéliennes à multiplication complexe

[Viada 2003; Rémond et Viada 2003; Ratazzi 2008; Carrizosa 2009]. Viada [2008; 2009] a récemment utilisé le théorème 1.8 pour établir certains cas particuliers de la conjecture de Zilber–Pink sur les variétés abéliennes.

Théorème 1.13 (Viada). *Soit C une courbe algébrique incluse dans E^g, où E est une courbe elliptique et $g \geq 2$. Si C n'est pas incluse dans le translaté d'une sous-variété abélienne stricte par un point de torsion, il existe $\varepsilon > 0$ tel que $C(\overline{\mathbb{Q}}) \cap \mathscr{H}_\varepsilon$ soit fini.*

Plan de l'article. La deuxième partie est consacrée à la démonstration d'une propriété p-adique obtenue par l'étude du groupe formel d'une variété abélienne en caractéristique p. On commence par faire quelques rappels sur le p-rang d'une variété abélienne, puis sur la théorie des schémas en groupes. On obtient ensuite un résultat métrique p-adique précis, pour les points de p-torsion de A se réduisant sur 0 modulo un idéal premier $\mathfrak{q}$ divisant p dans une extension convenable.

Dans la troisième partie, on rappelle les définitions et résultats généraux de la théorie des pentes. Un premier fait assez inhabituel dans notre application de cette théorie est l'importance des estimations ultramétriques. Dans cette perspective, on utilise une version du théorème des pentes assez précise sur le plan ultramétrique. Puis on introduit les fibrés hermitiens qui seront utiles par la suite et on estime leur pente. La principale difficulté de cette partie réside dans la majoration de la pente maximale du fibré des sections d'un fibré ample sur une sous-variété de A (avec multiplicités), le fibré d'arrivée étant habituellement formé, dans la méthode des pentes, à partir d'un nombre fini de points. Cette majoration est obtenue en suivant une idée figurant dans [Chen 2006]. Les résultats de [Bost et Künnemann 2007] (améliorés par Chen en dimension ≥ 3) sur la pente maximale du produit tensoriel de deux fibrés hermitiens permettent de prendre en compte la multiplicité.

On prend ensuite (quatrième partie) une sous-variété stricte V d'une variété abélienne A qui n'est pas incluse dans un translaté de sous-variété abélienne et on lui associe un fermé de Zariski X en vue de la fin de la preuve ; on construit deux espaces vectoriels E et F et un morphisme de restriction entre ces espaces (paramétrés en fonction de A et de l'indice d'obstruction de X). Puis on fixe les paramètres (degré de l'espace de sections, multiplicités, bornes pour la norme des idéaux premiers utilisés) intervenant dans cette construction et on suppose par l'absurde que le minimum essentiel de X est majoré en fonction de ces paramètres. Dans tout ce paragraphe et les suivants, on travaille avec un plongement étiré, devenu classique dans les travaux diophantiens sur les variétés abéliennes pour passer de la hauteur projective à la hauteur de Néron–Tate.

Dans la cinquième partie, on calcule les rangs et les normes des morphismes susceptibles de rentrer dans l'inégalité des pentes. On écrit ensuite cette inégalité, sous l'hypothèse que le morphisme soit injectif. On parvient rapidement à une contradic-

tion. À ce stade du travail, on a montré que le minimum essentiel de X est correctement minoré modulo l'injectivité du morphisme. On suppose donc par l'absurde, dans la sixième partie, que le morphisme n'est pas injectif. On commence par appliquer un lemme de zéros très général d'Amoroso et David. L'utilisation de ce lemme est suivie d'une phase de dénombrement et d'un argument de descente, qui permettent d'obtenir une contradiction. Le travail sur l'injectivité du morphisme s'effectue après l'inégalité des pentes parce qu'il comporte une itération (dans la phase de descente) qui nécessite d'avoir déjà écrit cette inégalité. On détaille la descente en codimension ≤ 2 et on explique en conclusion comment obtenir le cas général.

Constantes. Le théorème 1.8 montre l'existence d'une constante $C_L(A)$ ne dépendant que de (A, L), qui apparaît dans la minoration du minimum essentiel. Cette constante est explicitable, mais on obtient une borne monomiale inverse en la hauteur de A, plus faible à cet égard que le théorème 1.7 (voir le choix de $C_L(A)$ dans les dernières lignes de la preuve), et en particulier très éloignée des conjectures formulées dans [David et Philippon 2007]. Au cours de ce travail, on introduira des constantes $c_1, \ldots, c_{21}$ ne dépendant que de (A, L). Le choix des paramètres fera intervenir une constante C_0, dépendant uniquement de (A, L) elle aussi, qui sera prise *grande* par rapport aux constantes c_i $(1 \leq i \leq 21)$. La constante $C_L(A)$ s'exprimera alors simplement en fonction de C_0.

2. Un lemme clé p-adique sur les variétés abéliennes

Soit A une variété abélienne définie sur K un corps de nombres et soit $\mathcal{P}_A$ un ensemble de premiers bien choisi en fonction de A. Le but de ce paragraphe est d'établir une inégalité p-adique concernant les points de p-torsion de A, pour $p \in \mathcal{P}_A$. On cherche à montrer, pour les variétés abéliennes, un résultat comparable à l'inégalité suivante, vraie pour tout premier p, toute racine p-ème de l'unité ξ et toute place $v|p$ d'un corps de nombres quelconque contenant ξ :

$$|\xi - 1|_v \leq p^{-1/p}.$$

Cette inégalité, conséquence d'une propriété de ramification bien connue sur les corps cyclotomiques [Ireland et Rosen 1990, Proposition 13.2.7], a un analogue satisfaisant sur les courbes elliptiques pour les premiers de bonne réduction ordinaire, s'il n'y a pas de ramification initiale ; dans le cas des premiers supersinguliers, on doit remplacer $1/p$ par $1/p^2$ [Galateau 2007, 2.4.1]. On s'attend donc à ce que le résultat obtenu sur A dépende de la réduction de A modulo un idéal premier $\mathfrak{p}$ de $\mathbb{O}_K$. Deux invariants apparaissent naturellement : le rang de la matrice de Hasse–Witt et son rang stable (ou p-rang de la variété). On obtient les meilleurs résultats quand ces deux invariants sont égaux. Ce résultat p-adique permettra d'estimer certaines normes ultramétriques apparaissant dans l'inégalité de pentes.

2A. ***Le p-rang d'une variété abélienne.*** On fixe pour ce paragraphe et le suivant un premier p et une variété abélienne A définie sur un corps fini $\mathbb{F}_q \subset k := \overline{\mathbb{F}}_p$.

Proposition 2.1. *Le groupe $A[p]$ des points de p-torsion sur $\overline{\mathbb{F}}_p$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\alpha$, où $0 \leq \alpha \leq g$. Cet entier α est appelé p-rang de A.*

Remarque. Le p-rang de A est aussi appelé rang stable de A (en raison de son lien avec la matrice de Hasse–Witt de A, explicité *infra*, 2B). S'il est égal à g, la variété A est dite *ordinaire*.

On introduit maintenant le morphisme de Frobenius relatif, qu'on notera $\mathfrak{F}$. Sur $\mathrm{Spec}(k)$, on définit $\mathfrak{F}$ comme étant l'identité sur l'espace topologique réduit à un point et l'élévation à la puissance p sur k. On note ensuite $A^{(p)}$ le tiré en arrière de A par l'action du Frobenius $\mathfrak{F}$ sur $\mathrm{Spec}(k)$. Par construction, ce schéma est une variété abélienne.

Définition 2.2. Le morphisme de Frobenius :

$$\mathfrak{F} : A \to A^{(p)}.$$

est défini par l'élévation à la puissance p sur le faisceau structural.

On vérifie que le Frobenius est une isogénie purement inséparable de degré p^g. Cette isogénie nous permet de factoriser la multiplication par p sur A, notée $[p]$.

Lemme 2.3 [Demazure et Grothendieck 1970, VII A.4]. *Il existe une isogénie $\mathfrak{V} : A^{(p)} \to A$, appelée Verschiebung, telle que $[p] = \mathfrak{V} \circ \mathfrak{F}$. De plus, $\mathfrak{V}$ et $\mathfrak{F}$ sont duales l'une de l'autre au sens suivant : si on note $\hat{A}$ la duale de A, on a une décomposition $[p]_{\hat{A}} = \mathfrak{V}_{\hat{A}} \circ \mathfrak{F}_{\hat{A}}$ avec :*

$$\widehat{\mathfrak{V}} = \mathfrak{F}_{\hat{A}} \quad \textit{et} \quad \widehat{\mathfrak{F}} = \mathfrak{V}_{\hat{A}}.$$

Comme le morphisme de Frobenius est purement inséparable, le degré séparable de $\mathfrak{V}$ est égal à p^α. Si $\alpha = g$, l'isogénie $\mathfrak{V}$ est séparable et sa différentielle en 0 est inversible. On veut relier plus généralement α à la différentielle de $\mathfrak{V}$ en 0 ; ceci nous amène à étudier la structure de schéma en groupe du sous-groupe $A[p]$ de A.

2B. ***Schémas en groupe.*** On fait ici quelques rappels sur la théorie des schémas en groupes, suivant [Mumford 1974, III].

Définition 2.4. Un schéma en groupe G sur k est un schéma sur k muni d'un morphisme de multiplication $m : G \times G \to G$, d'un morphisme d'inversion $i : G \to G$ et d'un élément neutre $e : \mathrm{Spec}(k) \to G$ vérifiant les axiomes :

$$\begin{aligned} m \circ (m \times \mathrm{Id}_G) &= m \circ (\mathrm{Id}_G \times m) : G \times G \times G \to G, \\ m \circ (e \times \mathrm{Id}_G) &= j_1 : \mathrm{Spec}(k) \times G \to G, \\ m \circ (\mathrm{Id}_G \times e) &= j_2 : G \times \mathrm{Spec}(k) \to G, \\ e \circ \pi = m \circ (\mathrm{Id}_G \times i) &= m \circ (i \times \mathrm{Id}_G) : G \to G, \end{aligned}$$

où $\pi : G \to \mathrm{Spec}(k)$; $j_1 : \mathrm{Spec}(k) \times G \simeq G$ et $j_2 : G \times \mathrm{Spec}(k)$ sont les isomorphismes canoniques.

Soit G un schéma en groupe. Son algèbre de Lie est le k-espace vectoriel des champs de vecteurs invariants par m et elle est munie de la fonction de Hasse–Witt, qui associe à une dérivation D la dérivation D^p (p-ème itérée de D). C'est une application $\mathbb{F}_p$-linéaire (i.e., additive et linéaire sous la multiplication par un élément de $\mathbb{F}_p$). On définit $\widehat{G}$ le dual (de Cartier) de G d'un schéma en groupe affine $\mathrm{Spec}(R)$ (où R est une k-algèbre de type fini) en munissant le dual R^* de R d'une comultiplication et d'un idéal d'augmentation par dualité.

On suppose maintenant que G est un schéma en groupe fini et commutatif. On dit que G est de type l si l'espace sous-jacent est constitué d'un seul point, et de type r si G est réduit. On dit que G est de type (x, y) si G est de type x et $\widehat{G}$ est de type y. Le schéma G se décompose alors de façon unique en un produit :

$$G = G_{r,r} \times G_{r,l} \times G_{l,r} \times G_{l,l},$$

où $G_{x,y}$ est de type (x, y) (pour plus de détails, voir [Mumford 1974, §14]).

Pour le schéma en groupe $A[p]$ qui nous intéresse ici, le type $G_{r,r}$ est trivial car $A[p]$ est de cardinal une puissance de p. Plus précisément :

Proposition 2.5. *On a l'isomorphisme de schémas en groupes* :

$$A[p] \simeq (\mathbb{Z}/p\mathbb{Z})^\alpha \times (\mu_p)^\alpha \times A[p]_{l,l},$$

où α est le p-rang de A, $\mu_p = \mathrm{Spec}(k[X]/(X^p - 1))$ et $A[p]_{l,l}$ est de type (l, l).

Démonstration. Soit $n \in \mathbb{N}^*$. Compte tenu des structures de groupes de $A[p^n]$ et du dual $\widehat{A[p^n]}$, qui donnent les composantes réduites de ces deux schémas en groupes, et comme le dual du noyau de l'isogénie $[p]$ est le noyau de l'isogénie duale [Mumford 1974, page 143], on a la décomposition :

$$A[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^\alpha \times \left(\widehat{\mathbb{Z}/p^n\mathbb{Z}}\right)^\beta \times A[p^n]_{l,l},$$

pour un certain entier β et un schéma en groupe local $A[p^n]_{l,l}$.

L'algèbre de fonctions associée à $\mathbb{Z}/p^n\mathbb{Z}$ est son algèbre de groupe et, en notant X l'évaluation en $1 \in \mathbb{Z}/p^n\mathbb{Z}$, on voit que l'algèbre duale est isomorphe à :

$$\mathrm{Spec}(k[X]/(X^{p^n} - 1)).$$

On en déduit que $\widehat{\mathbb{Z}/p^n\mathbb{Z}} \simeq \mu_{p^n}$. De plus, α et β sont permutés par passage de A à $\hat{A}$ et puisqu'il existe une isogénie $f : A \to \hat{A}$, en notant K le cardinal de son noyau, on a :

$$f(A[p^n]) \subset \hat{A}[p^n] \quad \text{donc} \quad p^{n\alpha} \leq K p^{n\beta}.$$

En faisant varier n, on obtient $\alpha \leq \beta$. Mais comme la duale de $\hat{A}$ est isomorphe à A [Mumford 1974, page 132], on obtient $\alpha = \beta$. Le résultat suit en prenant $n = 1$. □

Remarque. Les schémas en groupes de type (l, l) sont les plus difficiles à comprendre. Pour plus de détails, voir par exemple [Pink 2004, §16 et §22].

On peut maintenant faire le lien entre la différentielle de $\mathfrak{V}$ en 0 et le p-rang :

Proposition 2.6. *Soit Ψ la différentielle de $\mathfrak{V}$ en 0. Le p-rang de A est le rang de Ψ^g.*

Démonstration. On passe aux algèbres de Lie dans la proposition précédente et on observe que l'application linéaire $[p]^*$ est la multiplication par p, donc est nulle sur $\mathrm{Lie}(A)$. On se limite à la partie locale en 0 :

$$\mathrm{Lie}(A) = \mathrm{Lie}(A[p]) = \mathrm{Lie}(\mu_p)^\alpha \oplus \mathrm{Lie}(A[p]_{l,l}).$$

En prenant comme base de $\mathrm{Lie}(\mu_p)$ la dérivation $X\partial/\partial X$, on observe que la fonction de Hasse–Witt est l'identité sur $\mathrm{Lie}(\mu_p)^\alpha$, alors qu'elle est nilpotente sur la partie locale-locale. De plus, par l'isomorphisme canonique :

$$\mathrm{Lie}\,\hat{A} \simeq H^1(A, \mathcal{O}_A),$$

la fonction de Hasse–Witt correspond à l'application induite par le Frobenius sur $\mathcal{O}_A$ [Mumford 1974, page 148], qui correspond par dualité à la différentielle de $\mathfrak{V}$ sur le tangent en 0. Il existe donc une décomposition $t_A = t_{A,s} + t_{A,n}$ du tangent en 0 laissée stable par Ψ telle que $\Psi_{|t_{A,s}}$ soit un isomorphisme et $\Psi_{|t_{A,n}}$ soit nilpotente ; de plus, l'espace vectoriel $t_{A,s}$ est de dimension α. En itérant g fois l'application Ψ, la partie nilpotente s'annule et on en déduit que le p-rang est le rang de Ψ^g. □

Remarque. On appelle composante semi-simple de Ψ l'espace vectoriel $t_{A,s}$. Cette composante semi-simple est l'image de Ψ^g, donc est définie sur $\mathbb{F}_q$.

Le p-rang d'une variété abélienne n'est pas toujours égal au rang de la matrice de Hasse–Witt. Si on fixe $\alpha \leq g-1$, on peut même montrer [Koblitz 1975, Theorem 7] que sur l'espace de module des variétés abéliennes principalement polarisées de dimension g avec structure de niveau fixée sur k, les variétés abéliennes ayant une matrice de Hasse–Witt de rang $g-1$ sont Zariski-denses dans le fermé des variétés abéliennes dont le p-rang est plus petit que α. Si le p-rang est égal à $g-1$ ou g, il est automatiquement égal au rang de la matrice de Hasse–Witt.

En général, le p-rang et le rang de la matrice de Hasse–Witt sont distincts, et la partie nilpotente fait obstruction pour contrôler efficacement la norme p-adique de tous les paramètres.

Hypothèse. *On suppose maintenant que le p-rang de A est égal au rang de Ψ.*

On choisit un système de paramètres $(x_1, \ldots, x_g)$ associé à une base de différentielles invariantes, tel que $(x_1, \ldots, x_\alpha)$ soit une base de $\mathrm{Im}\,\Psi^g$ (qui est égale à $\mathrm{Im}\,\Psi$). Notons $\widehat{\mathcal{O}}_{0,A}$ le groupe formel associé à A en 0 sur $\mathbb{F}_q$. On a [Hindry et

Silverman 2000, page 268] :

$$\widehat{\mathcal{O}}_{0,A} \simeq \mathbb{F}_q[\![x_1, \ldots, x_g]\!].$$

On note encore $\mathfrak{V} := (\mathfrak{V}_1, \ldots, \mathfrak{V}_g)$ le g-uplet de séries formelles image de l'isogénie $\mathfrak{V}$ dans le groupe formel. On note aussi Φ_α le morphisme de $\mathbb{F}_q[\![x_1, \ldots, x_g]\!]$ qui agit sur les paramètres par :

$$x_i \to x_i \quad \text{si } i \leq \alpha,$$
$$x_i \to x_i^p \quad \text{si } i > \alpha.$$

Corollaire 2.7. *Il existe un g-uplet de séries formelles $\mathbf{U} = (U_1, \ldots, U_g)$ tel que $d\mathbf{U}$ est inversible et $\mathfrak{V}$ se factorise : $\mathfrak{V} = \mathbf{U} \circ \Phi_\alpha$.*

Démonstration. Pour tout entier $1 \leq i \leq g$, comme $\mathfrak{V}$ est une isogénie, la forme différentielle $\mathfrak{V}^* dx_i$ est encore une différentielle invariante, donc se décompose :

$$\mathfrak{V}^* dx_i = \sum_{j=1}^{g} \alpha_{i,j} dx_j,$$

où les $\alpha_{i,j}$ sont constants et donnés par la i-ème colonne de la matrice de Ψ dans la base associée à $(x_1, \ldots, x_g)$. On en déduit par intégration que les seuls termes non-nuls dans les $\mathfrak{V}_i$ sont les termes linéaires ou des monômes en $(x_1^p, \ldots, x_g^p)$. Par choix de la base, les paramètres $(x_{\alpha+1}, \ldots, x_g)$ sont absents de la partie linéaire. On a donc bien la décomposition voulue. L'application Φ_α est purement inséparable et son degré est le rang de :

$$k[\![x_1, \ldots, x_g]\!]/(x_1, \ldots, x_\alpha, x_{\alpha+1}^p, \ldots, x_g^p),$$

donc :

$$\deg \Phi_\alpha = \deg_i \Phi_\alpha = p^{g-\alpha}.$$

En comparant les degrés séparables et inséparables, on voit que $\mathbf{U}$ est séparable, et que sa différentielle est inversible [Lang 2002, VIII, proposition 5.5]. □

2C. ***Retour en caractéristique nulle.*** On traduit maintenant la proposition précédente en un résultat p-adique pour les points de torsion d'une variété abélienne définie sur un corps de nombres. Soit donc A une variété abélienne de dimension g définie sur un corps de nombres K, munie d'un fibré L ample et symétrique, et soit $\mathcal{A}$ un modèle entier de A sur $\mathcal{O}_K$. On peut supposer [Hindry et Silverman 2000, page 105], quitte à considérer $L^{\otimes 3}$, que le fibré L est très ample (et projectivement normal). Rappelons que pour tout nombre premier p, il y a p^{2g} points de p-torsion dans $A(\overline{K})$. Pour un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ de bonne réduction divisant p, la fibre spéciale $\mathcal{A}_\mathfrak{p}$ ne contient plus que p^α points de p-torsion, où α est le p-rang de la fibre spéciale. On fixe à présent une base $(s_i)_i$ de $H^0(A, L)$. Par abus de langage, on dira qu'une constante ne dépend que de A si elle dépend de (A, L) et du choix de cette base.

Précisons d'abord que si $\mathfrak{q}$ est un idéal premier de K' une extension finie de K, dont la projection sur $\mathbb{Z}$ est p, on choisit la normalisation suivante pour la valuation $\mathfrak{q}$-adique :

$$|p|_{\mathfrak{q}} = p^{-n_{\mathfrak{q}}}, \quad \text{où } n_{\mathfrak{q}} \text{ est le degré local } [K'_{\mathfrak{q}} : \mathbb{Q}_p].$$

Cette normalisation permet d'écrire plus simplement la formule du produit, et la hauteur d'un morphisme dans l'inégalité de pentes.

Les premiers de réduction *ordinaire* (i.e., les premiers de bonne réduction pour lesquels le p-rang est égal à g) sont ceux pour lesquels les propriétés métriques sont les meilleures. Dans le cas d'une courbe elliptique E, on sait qu'ils sont de densité 1 si E n'est pas à multiplication complexe ; et qu'ils sont de densité au moins $\frac{1}{2}$ si E est à multiplication complexe. En dimension supérieure, on ne connaît aucun résultat comparable.

Définition 2.8. Soit $\mathcal{Q}$ un sous-ensemble de l'ensemble $\mathcal{P}$ des idéaux premiers de $\mathbb{O}_K$. On dit que $\mathcal{Q}$ a une densité naturelle d si le quotient :

$$\frac{\big|\{\mathfrak{q} \in \mathcal{Q} : \mathbf{N}(\mathfrak{q}) \leq x\}\big|}{\big|\{\mathfrak{p} \in \mathcal{P} : \mathbf{N}(\mathfrak{p}) \leq x\}\big|}$$

tend vers d quand $x \to \infty$.

Remarque. La fonction $\mathbf{N}$ est la norme sur les idéaux (définie dans [Samuel 1967, III, 5]).

Dans toute la discussion qui suit, on omet de préciser les ensembles indexateurs, qui sont toujours finis et dépendent de A. La loi d'addition de A est donnée sur chaque ouvert affine par des polynômes de bi-degré (2, 2) [Lange et Ruppert 1985; David et Philippon 2002, proposition 3.7] dont les coefficients sont de hauteur bornée uniquement en fonction de A. On a donc, si on note $(x_k)_k$ l'ensemble fini de ces coefficients :

$$\forall k : \ |x_k|_{\mathfrak{p}} \leq 1, \tag{2-1}$$

sauf pour un nombre fini d'idéaux premiers $\mathfrak{p}$ (ne dépendant que de A).

Fixons maintenant une base de dérivations algébriques sur A. Quitte à prendre des idéaux premiers $\mathfrak{p}$ de $\mathbb{O}_K$ plus grands qu'une constante ne dépendant que de A, cette base de dérivations sera encore une base de dérivations modulo $\mathfrak{p}$. On a fixé une base $(s_i)_i$ de $H^0(A, L)$ et on note $f_i := s_i/s_0$ la fonction affine sur l'ouvert de A défini par la non-annulation de s_0.

Théorème 2.9. *Il existe une base de dérivations* $(\partial_1, \ldots, \partial_g)$ *sur* A *telle que* :

$$\forall (i, j) : \ \partial_j f_i = \sum_{(k,l)} y_{k,l}^{i,j} f_k f_l,$$

où les $y_{k,l}^{i,j} \in \overline{\mathbb{Q}}$ *sont de hauteur bornée uniquement en fonction de* A.

Démonstration. Le théorème 4.1 de [David 1991] vaut sous l'hypothèse que la polarisation est principale ; le résultat obtenu est alors effectif. L'argument s'adapte sans peine à notre cas. Rappelons-en les étapes.

Soit $(\delta_1, \dots, \delta_g)$ une base de dérivations quelconque en 0. Le fibré L étant très ample, on peut supposer, quitte à renuméroter, que la matrice $(\delta_k s_l)_{1\le k,l\le g}$ est inversible. Il s'agit de la matrice de passage d'une certaine base $(\partial_1, \dots, \partial_g)$ de dérivations en 0 vers $(\delta_1, \dots, \delta_g)$. On a :

$$s_0^2\, \partial_j\Big(\frac{s_i}{s_0}\Big) \in H^0(A, L^{\otimes 2}),$$

et comme le plongement associé à L est projectivement normal, on a l'écriture attendue avec les $y_{k,l}^{i,j}$ dans $\mathbb{C}$. Par construction de la base de dérivations, les $y_{k,l}^{i,j}$ sont en fait dans $\overline{\mathbb{Q}}$. Ces coefficients étant en nombre fini, on peut trouver une borne pour leur hauteur ne dépendant que de A. □

Pour tout idéal premier $\mathfrak{p}$ de $\mathbb{O}_K$ sauf un nombre fini (ne dépendant que de A) :

$$\forall (i, j, k, l) : \ |y_{k,l}^{i,j}|_{\mathfrak{p}} \le 1. \tag{2-2}$$

Par abus de langage, on notera encore $(\partial_1, \dots, \partial_g)$ la base de dérivations en 0 qui en résulte. On ne pourra travailler directement avec cette base de dérivations mais on s'y ramènera grâce à la construction suivante.

Lemme 2.10. *Il existe un ensemble fini $(t_{1,\nu}, \dots, t_{g,\nu})_{\nu\in\mathcal{V}}$ de systèmes de paramètres en* 0 *définis sur des ouverts $(\mathcal{U}_\nu)_{\nu\in\mathcal{V}}$ tels que $A(\overline{K}) = \bigcup_{\nu\in\mathcal{V}} \mathcal{U}_\nu$.*

Démonstration. Si $x \in A(\overline{K})$ est différent de 0, il existe un hyperplan passant par x et évitant 0, défini par l'annulation d'une section $s_x \in H^0(A, L)$, et un hyperplan évitant à la fois x et 0, défini par l'annulation d'une section $s'_x \in H^0(A, L)$. En multipliant un système de paramètres en l'origine quelconque $(t_1, \dots t_g)$ par une puissance tensorielle suffisante de s_x/s'_x, on obtient un nouveau système de paramètres en 0 défini sur un ouvert $\mathcal{U}_x$ contenant x. On conclut par compacité. □

Pour tout $\nu \in \mathcal{V}$, on définit par dualité une base $(\partial_{1,\nu}, \dots, \partial_{g,\nu})$ de dérivations en 0. Comme $\mathcal{V}$ est fini, pour tout idéal premier $\mathfrak{p}$ de $\mathbb{O}_K$ sauf un nombre fini, si on note $(z_m)_m$ les coefficients de toutes les matrices de passage de $(\partial_1, \dots, \partial_g)$ vers les $(\partial_{1,\nu}, \dots, \partial_{g,\nu})_{\nu\in\mathcal{V}}$ (qui sont définis sur une extension finie) :

$$\forall m \ \ \forall \mathfrak{q}|\mathfrak{p} : \ |z_m|_{\mathfrak{q}} \le 1. \tag{2-3}$$

Les premiers de mauvaise réduction pour A sont en nombre fini, ainsi que les premiers de $\mathbb{Z}$ se ramifiant dans $\mathbb{O}_K$. On pose $\mathcal{P}_{A,0}$ l'ensemble des premiers $\mathfrak{p}$ de $\mathbb{O}_K$ de bonne réduction, vérifiant (2-1), (2-2) et (2-3), tels que la base de dérivations algébriques soit encore une base sur $\mathcal{A}_{\mathfrak{p}}$, tels que si $(p) = \mathfrak{p} \cap \mathbb{Z}$, on a $e_{\mathfrak{p}/p} = 1$, et

enfin, tels que :

$$\sum_{\substack{p=\mathfrak{p}_{|\mathbb{Z}} \\ \mathfrak{p}\in\mathscr{P}_{A,0}}} \frac{1}{p^2} \leq \frac{1}{3}.$$

Comme la même somme indexée par $\mathbb{N}^*$ converge, il suffit d'exclure un ensemble fini (absolu) de premiers pour que cette condition soit vérifiée. L'ensemble $\mathscr{P}_{A,0}$ est de densité naturelle égale à 1, et sa construction ne dépend que de A et K.

On fait l'hypothèse suivante sur $\mathscr{A}$:

Hypothèse H′. *Il y a une densité $c_0 > 0$ d'idéaux premiers $\mathfrak{p}$ pour lesquels le p-rang de $\mathscr{A}_\mathfrak{p}$ est égal au rang de la matrice de Hasse–Witt.*

Par le principe des tiroirs de Dirichlet, il existe un entier k tel que la densité naturelle d'idéaux premiers de $\mathscr{P}_{A,0}$ vérifiant H′ et pour lesquels la fibre spéciale a un p-rang égal à k est supérieure ou égale à $c_0/(g+1)$. On choisit un tel entier et on le note α. On note $\mathscr{P}_A$ l'ensemble des idéaux premiers $\mathfrak{p}$ de $\mathscr{P}_{A,0}$ en lesquels la variété $\mathscr{A}_\mathfrak{p}$ a un p-rang égal à α. De plus, quitte à diviser la densité de cet ensemble par $[K : \mathbb{Q}]$, on peut supposer que deux idéaux premiers distincts de $\mathscr{P}_A$ ont des projections distinctes sur $\mathbb{Z}$.

Soit $\mathfrak{p} \in \mathscr{P}_A$ un idéal premier et $(p) = \mathfrak{p} \cap \mathbb{Z}$. Par choix de $\mathscr{P}_A$, la fibre spéciale $\mathscr{A}_\mathfrak{p}$ est lisse. Soit $\Psi_\mathfrak{p}$ la différentielle du Verschiebung sur $\mathscr{A}_\mathfrak{p}$. Par la discussion du paragraphe précédent, on peut trouver une base de paramètres en l'origine de A :

$$t_{\mathfrak{p},1}, \ldots, t_{\mathfrak{p},g}$$

(i.e., dont la projection est une base de $\mathfrak{m}_0/\mathfrak{m}_0^2$, où $\mathfrak{m}_0$ est l'idéal maximal correspondant à l'origine de A) telle que son image par réduction modulo $\mathfrak{p}$:

$$\tilde{t}_{\mathfrak{p},1}, \ldots, \tilde{t}_{\mathfrak{p},g}$$

soit encore une base de paramètres algébriques, avec :

$$\operatorname{Im} \Psi_\mathfrak{p}^g = \operatorname{Vect}(\tilde{t}_{\mathfrak{p},1}, \ldots, \tilde{t}_{\mathfrak{p},\alpha}),$$
$$\operatorname{Ker} \Psi_\mathfrak{p}^g = \operatorname{Vect}(\tilde{t}_{\mathfrak{p},\alpha+1}, \ldots, \tilde{t}_{\mathfrak{p},g}).$$

Ce système de paramètres est défini sur un certain ouvert affine $\mathscr{U}_{\mathbf{t}_\mathfrak{p}}$. On note $\mathbb{O}_\mathfrak{p}$ l'anneau de valuation associé à $\mathfrak{p}$. Il lui correspond par tensorisation :

$$\mathscr{A}_{\mathbb{O}_\mathfrak{p}} := \mathscr{A} \times_{\operatorname{Spec} \mathbb{O}_K} \operatorname{Spec} \mathbb{O}_\mathfrak{p},$$

et la section nulle $\varepsilon_\mathfrak{p}$. On note $\hat{\mathscr{A}}_{\mathbb{O}_\mathfrak{p}}$ le complété le long de $\varepsilon_\mathfrak{p}$ de $\mathscr{A}_{\mathbb{O}_\mathfrak{p}}$. La multiplication par $[p]$ est donnée sur le groupe formel par un g-uplet de séries formelles noté $[\mathbf{p}]$. Par réduction modulo $\mathfrak{p}$, on obtient un g-uplet de séries formelles $[\tilde{\mathbf{p}}]$. La décomposition $[p]_\mathfrak{p} = \mathfrak{V}_\mathfrak{p} \circ \mathfrak{F}_\mathfrak{p}$ de la multiplication par p sur la fibre spéciale induit une décomposition :

$$[\tilde{\mathbf{p}}](\tilde{\mathbf{t}}_\mathfrak{p}) = \mathfrak{V}_\mathfrak{p}(\tilde{\mathbf{t}}_\mathfrak{p}^p),$$

où $\tilde{\mathbf{t}}_\mathfrak{p}^p = (\tilde{t}_{\mathfrak{p},1}^p, \ldots, \tilde{t}_{\mathfrak{p},g}^p)$ est l'image de $\tilde{\mathbf{t}}_\mathfrak{p}$ par le Frobenius.

Proposition 2.11. *Si $P \in \mathcal{U}_{t_\mathfrak{p}}$ est un point de p-torsion se réduisant sur* 0 *modulo* $\mathfrak{q}$, *pour une place* $\mathfrak{q}|\mathfrak{p}$ *dans un corps de définition de* P, *on a* :

$$\forall\, 1 \leq i \leq \alpha : |t_{\mathfrak{p},i}(P)|_\mathfrak{q} \leq p^{-n_\mathfrak{q}/p},$$
$$\forall\, \alpha < i \leq g : |t_{\mathfrak{p},i}(P)|_\mathfrak{q} \leq p^{-n_\mathfrak{q}/p^2}.$$

Démonstration. Soit $P \in \mathcal{U}_{\mathbf{t}_\mathfrak{p}}$ se réduisant sur 0 modulo $\mathfrak{q}$, pour $\mathfrak{q}|\mathfrak{p}$ dans un corps de définition de P. On sait déjà :

$$\forall\, 1 \leq i \leq g :\ |t_{\mathfrak{p},i}(P)|_\mathfrak{q} < 1.$$

De plus, le morphisme $[p]$ en P est donné par le g-uplet de séries formelles $[\mathbf{p}]$ appliquées au système de paramètres [Hindry et Silverman 2000, page 272]. On en déduit que $[\mathbf{p}] \circ \mathbf{t}_\mathfrak{p}(P) = 0$.

D'après le corollaire 2.7, on a une factorisation $\mathfrak{V}_\mathfrak{p} = \mathbf{U}_\mathfrak{p} \circ \Phi_{\alpha,\mathfrak{p}}$, et la différentielle de $\mathbf{U}_\mathfrak{p}$ est inversible. En utilisant la réduction modulo $\mathfrak{p}$ de $[\mathbf{p}]$ et les propriétés de base d'une loi de groupe formel (rappelées dans [Hindry et Silverman 2000, page 269]), on voit que $[\mathbf{p}]$ est donné par :

$$[\mathbf{p}](\mathbf{t}_\mathfrak{p}) = p\mathbf{t}_\mathfrak{p} + \mathbf{G}(\mathbf{t}_\mathfrak{p}) + \mathbf{H} \circ \Phi_\alpha(\mathbf{t}_\mathfrak{p}^p).$$

Le g-uplet de séries formelles $\mathbf{G}$ a ses coefficients dans $\mathfrak{p}\mathbb{O}_\mathfrak{p}$ et ses premiers termes sont quadratiques ; le g-uplet $\mathbf{H}$ a ses coefficients inversibles modulo $\mathfrak{p}$ et sa différentielle est inversible dans $\mathbb{O}_\mathfrak{p}$. Soit $i_0 \in [1, g]$ tel que $|t_{\mathfrak{p},i_0}(P)|_\mathfrak{q}$ soit maximal. En inversant la différentielle, et par choix de i_0, on obtient :

$$t_{\mathfrak{p},i_0}(P)^{p^{n_{i_0}}} \in \mathfrak{p}\mathbb{O}_\mathfrak{q},$$

où $n_{i_0} = 1$ si $i_0 \leq \alpha$ et $n_{i_0} = 2$ sinon. Comme l'indice de ramification $e_{\mathfrak{p}/p}$ vaut 1 et par définition de i_0, on en déduit que pour tout $i \leq g$:

$$|t_{\mathfrak{p},i}(P)|_\mathfrak{q} \leq p^{-n_\mathfrak{q}/p^2}.$$

On est maintenant assuré que les contribution non-linéaires dans $\mathbf{H} \circ \Phi_\alpha(\mathbf{t}_\mathfrak{p}^p)$ ont une norme $\mathfrak{q}$-adique ≤ 1. On obtient donc, cette fois, pour tout $i \leq \alpha$:

$$t_{\mathfrak{p},i}(P)^p \in \mathfrak{p}\mathbb{O}_\mathfrak{q},$$

et la proposition est entièrement démontrée. □

Remarque. Puisque la ramification initiale $e_{\mathfrak{p}/p}$ est égale à 1 et le groupe des points de p-torsion se réduisant sur 0 modulo $\mathfrak{q}$ est galoisien de cardinal inférieur à $p^{2g-\alpha}$, le théorème de Raynaud [1974, corollaire 3.4.4] donne, pour $1 \leq i \leq g$:

$$|t_{\mathfrak{p},i}(P)|_\mathfrak{q} \leq p^{-n_\mathfrak{q}/p^{(2g-\alpha)}}.$$

On suppose maintenant que $\alpha = g$. Soit $(t_1, \ldots, t_g)$ une base de paramètres en 0 dont la réduction modulo $\mathfrak{p}$ est encore une base, et bien définie sur un certain ouvert affine $\mathcal{U}_{\mathbf{t}}$.

Corollaire 2.12. *Si $P \in \mathcal{U}_t$ est un point de p-torsion se réduisant sur 0 modulo $\mathfrak{q}$, pour une place $\mathfrak{q}|\mathfrak{p}$ dans un corps de définition de P :*

$$\forall 1 \leq i \leq g : \ |t_i(P)|_{\mathfrak{q}} \leq p^{-n_{\mathfrak{q}}/p}.$$

3. Théorie des pentes

Dans cette partie, on commence par définir les objets qui apparaissent dans la théorie des pentes, puis on donne les inégalités de pentes dont on se servira par la suite. On finit par estimer les pentes de fibrés qui apparaîtront dans la suite de ce travail.

3A. ***Définitions et inégalité de pentes.*** Le formalisme des pentes a été introduit par Bost [1996b] et s'est développé dans la littérature diophantienne depuis une dizaine d'années. Pour des détails et des exemples d'applications de la théorie des pentes, on renvoie par exemple aux articles de Bost [1996b; 2001] ou à l'article très complet de Gaudron [2006]. Le but de cette partie est donc d'écrire une *inégalité de pentes*. Sous sa forme basique, celle-ci compare les *pentes* de deux $\mathbb{O}_K$-modules hermitiens s'il existe un morphisme ϕ injectif entre eux. On va donc définir le degré arithmétique d'un fibré vectoriel hermitien, puis sa pente, sa pente maximale, et la hauteur d'un morphisme de fibrés.

On note dans ce paragraphe $S = \mathrm{Spec}(\mathbb{O}_K)$, S_0 l'ensemble des points fermés de S et S_∞ l'ensemble des places archimédiennes de $\mathbb{O}_K$; on note enfin $M(K) = S_0 \cup S_\infty$ l'ensemble des places de K. Un fibré vectoriel $\mathscr{E}$ sur S est constant, ce qui mène à la définition suivante :

Définition 3.1. Un fibré vectoriel hermitien sur S est un $\mathbb{O}_K$-module $\mathscr{E}$ de type fini muni d'une collection $\{\|\cdot\|_v\}_{v \in S_\infty}$ telle que pour tout $v \in S_\infty$, $\|\cdot\|_v$ soit une norme hermitienne sur le K_v-espace vectoriel $\mathscr{E}_v = \mathscr{E} \otimes K_v$, invariante par conjugaison complexe.

On notera $\overline{\mathscr{E}}$ le fibré $(\mathscr{E}, \{\|\cdot\|_v\})$, et $\mathscr{E}_K$ (resp. $\mathscr{E}_v$) l'espace vectoriel $\mathscr{E} \otimes_{\mathbb{O}_K} K$ (resp. $\mathscr{E} \otimes_{\mathbb{O}_K} K_v$ pour $v \in S$).

Définition 3.2. Soit $\overline{\mathscr{E}}$ un $\mathbb{O}_K$-fibré hermitien de rang 1 et s un élément non nul de $\mathscr{E}$. Le degré arithmétique (ou arakélovien) normalisé de $\mathscr{E}$ est :

$$\widehat{\deg}\, \overline{\mathscr{E}} = \frac{1}{[K:\mathbb{Q}]} \Big(\log \#(\mathscr{E}/s\mathbb{O}_K) - \sum_{v \in S_\infty} \log \|s\|_v \Big).$$

Si $\overline{\mathscr{E}}$ est un $\mathcal{O}_K$-fibré hermitien de rang r, on pose :

$$\widehat{\deg}\,\overline{\mathscr{E}} = \widehat{\deg}\det\overline{\mathscr{E}},$$

où les normes sur le déterminant sont celles obtenues par puissance tensorielle et quotient à partir de celles de $\mathscr{E}$.

Remarques. La formule du produit montre que cette définition ne dépend pas du choix de s. Si $K = \mathbb{Q}$, le degré d'Arakelov est l'opposé du logarithme du covolume de $\mathscr{E}$ vu comme réseau de $\mathscr{E} \otimes_{\mathbb{Z}} \mathbb{R}$ (voir [Bost et al. 1994, (2.1.13)] pour le cas général).

Définition 3.3. Soit $\overline{\mathscr{E}}$ un fibré hermitien de rang non nul. On définit sa pente par :

$$\hat{\mu}(\overline{\mathscr{E}}) = \frac{\widehat{\deg}\,\overline{\mathscr{E}}}{\operatorname{rg}\mathscr{E}}.$$

Les pentes des sous-modules de $\mathscr{E}$ sont bornées (par l'inégalité d'Hadamard), ce qui justifie la définition :

Définition 3.4. La pente maximale de $\overline{\mathscr{E}}$ est définie par :

$$\hat{\mu}_{\max}(\overline{\mathscr{E}}) = \max \hat{\mu}(\overline{\mathscr{F}}),$$

où $\mathscr{F}$ décrit l'ensemble des sous-fibrés non-nuls de $\mathscr{E}$ munis des métriques déduites de celles de $\mathscr{E}$ par restriction.

Soit ϕ un morphisme entre deux $\mathcal{O}_K$-fibrés $\mathscr{E}$ et $\mathscr{F}$. Si ces fibrés sont hermitiens, pour toute place $v \in M(K)$, on note $\|\phi\|_v$ la norme d'opérateur du morphisme $\phi : \mathscr{E}_v \to \mathscr{F}_v$. On a donc :

$$\|\phi\|_v = \sup_{\substack{x \in \mathscr{E}_v \\ x \neq 0}} \frac{\|\phi(x)\|_v}{\|x\|_v}.$$

Définition 3.5. Si ϕ est un morphisme entre deux $\mathcal{O}_K$-fibrés hermitiens $\overline{\mathscr{E}}$ et $\overline{\mathscr{F}}$, on appelle hauteur de ϕ :

$$h(\phi) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M(K)} \log \|\phi\|_v .$$

On est en mesure d'écrire une première inégalité de pentes :

Lemme 3.6. *Si le morphisme $\phi : \mathscr{E}_K \to \mathscr{F}_K$ est injectif* :

$$\widehat{\deg}\,\overline{\mathscr{E}} \leq \operatorname{rg}\mathscr{E}\left(\hat{\mu}_{\max}(\overline{\mathscr{F}}) + h(\phi)\right).$$

Démonstration. C'est une conséquence de l'inégalité d'Hadamard ; on renvoie à [Chen 2006, page 40], pour plus de détails (où la même convention est faite sur les normes ultramétriques). □

On utilise généralement une version filtrée de cette inégalité. Soit $\phi : \mathscr{E}_K \to \mathscr{F}_K$ une application K-linéaire injective. On suppose qu'il existe une filtration d'espaces vectoriels :

$$\{0\} = \mathscr{F}_{K,N+1} \subset \cdots \subset \mathscr{F}_{K,0} = \mathscr{F}_K.$$

et que les quotients $\mathscr{G}_{K,i} = \mathscr{F}_{K,i}/\mathscr{F}_{K,i+1}$ sont les tensorisations avec K de fibrés hermitiens $\overline{\mathscr{G}}_i$ sur $\operatorname{Spec} \mathbb{O}_K$. On définit une filtration sur $\mathscr{E}_K$ par image réciproque :

$$\mathscr{E}_{K,i} = \phi_K^{-1}(\mathscr{F}_{K,i}),$$

et on considère l'application linéaire naturellement induite sur le quotient :

$$\phi_i : \mathscr{E}_{K,i} \to \mathscr{G}_{K,i}.$$

Lemme 3.7. *Si ϕ est injective, on a l'inégalité* :

$$\widehat{\deg}\, \overline{\mathscr{E}} \leq \sum_{i=0}^{N} \dim(\mathscr{E}_{K,i}/\mathscr{E}_{K,i+1}) \big(\hat{\mu}_{\max}(\overline{\mathscr{G}}_i) + h(\phi_i)\big).$$

Cette version est particulièrement utile dans une preuve de transcendance : la filtration correspond aux différents ensembles et ordres d'annulation d'une fonction auxiliaire.

3B. ***Quelques fibrés hermitiens.*** On peut maintenant préciser les fibrés hermitiens auxquels on compte appliquer la méthode des pentes. Rappelons que A est une variété abélienne munie d'un fibré L ample et symétrique, et définie sur un corps de nombres K.

3B1. *Tangent et espace symétrique.* Quitte à prendre une extension finie de K ne dépendant que de A, on suppose que A admet réduction semi-abélienne sur K. Il existe donc un modèle semi-abélien $\pi : \mathscr{A} \to \operatorname{Spec} \mathbb{O}_K$. On note

$$\varepsilon : \operatorname{Spec} \mathbb{O}_K \to \mathscr{A}$$

la section nulle et on pose :

$$t_{\mathscr{A}} := \varepsilon^* T_{\mathscr{A}/\operatorname{Spec} \mathbb{O}_K},$$

où $T_{\mathscr{A}/\operatorname{Spec} \mathbb{O}_K}$ est le fibré tangent de $\mathscr{A}$ sur $\mathbb{O}_K$. On a une structure de $\mathbb{O}_K$-module de type fini sur $t_{\mathscr{A}}$, qui est un sous-module de l'espace vectoriel tangent de A à l'origine. Si σ est une place complexe de K, il existe un isomorphisme $t_{\mathscr{A}} \otimes_\sigma \mathbb{C} \simeq t_{\mathscr{A}_\sigma}(\mathbb{C})$ et la forme de Riemann ω associée au fibré ample L induit une forme hermitienne $\omega_\sigma \in \bigwedge^{1,1} t_{\mathscr{A}_\sigma}^\vee(\mathbb{C})$. Si ω_σ s'écrit sous la forme :

$$\omega_\sigma = \frac{i}{2} \sum_{1 \leq h,\, l \leq g} a_{h,l}\, f_h^* \wedge \overline{f_l^*},$$

où $(f_1^*, \ldots, f_g^*)$ est la base duale d'une base $(f_1, \ldots, f_g)$ de $t_{\mathscr{A}_\sigma}(\mathbb{C})$, on pose, pour

$(z_1, \dots, z_g) \in \mathbb{C}^g$:

$$\left\| \sum_{i=1}^{g} z_i f_i \right\|_\sigma^2 = \sum_{\substack{1 \le h \\ l \le g}} a_{h,l} z_h \overline{z_l}.$$

Ces métriques font de $t_{\mathcal{A}}$ un fibré vectoriel hermitien et cette structure se transporte par dualité à $t_{\mathcal{A}}^\vee$.

On sait calculer explicitement la pente de $\overline{t_{\mathcal{A}}^\vee}$ en fonction de la hauteur de Faltings de A, de la dimension de l'espace des sections de L sur A, et de la dimension de A [Gaudron 2006, proposition 4.7]. On se donne ici une constante $c_4 > 0$ ne dépendant que de A, L telle que :

$$\hat{\mu}_{\max}(\overline{t_{\mathcal{A}}^\vee}) \le c_4.$$

On a construit une base du tangent (sur $\mathbb{O}_K$) dans laquelle les propriétés $\mathfrak{p}$-adiques de A sont lisibles, pour un grand nombre de premiers $\mathfrak{p}$ de $\mathbb{O}_K$. On souhaiterait pouvoir majorer, en général, la pente maximale associée à des sous-modules du tangent de rang maximal. Soit $\mathcal{W}$ un sous-module de $t_{\mathcal{A}}$ de rang g engendré par des vecteurs $(e_1, \dots, e_g)$; on munit ce module des métriques hermitiennes (issues de la forme de Riemann) de $t_{\mathcal{A}}$ par restriction. On peut majorer la pente maximale de $\overline{\mathcal{W}^\vee}$ en fonction de la hauteur d'une base de $\mathcal{W}$. Soit $c(\mathcal{W}) \ge 1$ tel qu'il existe une base de $\mathcal{W}$ formée d'éléments dont toutes les coordonnées sont dans $\mathbb{O}_K$ et de hauteur plus petite que $c(\mathcal{W})$.

Lemme 3.8. *La pente maximale de $\overline{\mathcal{W}^\vee}$ vérifie* :

$$\hat{\mu}_{\max}(\overline{\mathcal{W}^\vee}) \le c_6 c(\mathcal{W}),$$

pour une constante $c_6 > 0$ ne dépendant que de (A, L).

Démonstration. La valeur absolue du degré normalisé de $\mathcal{W}$ est majorée, à partir de [Bost et al. 1994, (2.1.13)], de l'inégalité d'Hadamard et en prenant une base de $\mathbb{O}_K$ d'éléments dont la hauteur est bornée par $c(\mathcal{W})$:

$$|\widehat{\deg}\ \overline{\mathcal{W}}| \le c_5 c(\mathcal{W}),$$

pour une constante c_5 ne dépendant que de g et de K. En effet, pour les vecteurs à coordonnées dans $\mathbb{O}_K$, il n'y a pas de contribution ultramétrique dans l'expression de la hauteur, et les contributions archimédiennes sont comparables à la norme L^2 sortant de l'inégalité d'Hadamard. Le lemme se déduit immédiatement de cette inégalité et de [Gaudron 2006, (41)]. □

Pour passer aux dérivées d'ordre supérieur, on doit comprendre comment la pente maximale se comporte avec les puissances symétriques. Soit $\overline{\mathcal{E}}$ un fibré hermitien sur $\mathbb{O}_K$. Pour tout m, la puissance symétrique $S^m\mathcal{E}$ est munie d'une structure hermitienne par produit tensoriel puis projection ; on note $S^m\overline{\mathcal{E}}$ le fibré hermitien ainsi obtenu.

Lemme 3.9 [Graftieaux 2001, appendice]. *Pour $\overline{\mathscr{E}}$ un fibré hermitien de rang g :*

$$\hat{\mu}_{\max}(S^m(\overline{\mathscr{E}})) \leq m(\hat{\mu}_{\max}(\overline{\mathscr{E}}) + 2g \log g).$$

La combinaison des deux derniers lemmes donne la proposition suivante.

Proposition 3.10. *On a :*

$$\hat{\mu}_{\max}(S^m(\overline{\mathscr{W}^\vee})) \leq c_7 m c(\mathscr{W}),$$

pour une constante c_7 ne dépendant que de (A, L).

3B2. *L'espace des sections d'un fibré ample sur la variété abélienne.* La variété abélienne A est munie de L un fibré ample et symétrique, et on note $H^0(A, L)$ l'espace des sections sur ce fibré. Si $s \in H^0(A, L)$, on peut définir une métrique à l'aide de la fonction θ associée à s. Pour $x = \exp_A(z)$ et $z \in t_A$, on pose :

$$\|s(x)\| := e^{-(\pi/2)\|z\|^2} |\theta(z)|.$$

Il existe alors, grâce à [Bost 1996a, §4.3], un modèle de (A, L), appelé modèle de Moret-Bailly et noté $(\mathscr{A}, \overline{\mathscr{L}}, 0)$, constitué d'un schéma abélien :

$$\pi : \mathscr{A} \to \operatorname{Spec} \mathbb{O}_K,$$

et d'un fibré hermitien $\overline{\mathscr{L}}$ sur $\mathscr{A}$ vérifiant notamment les propriétés suivantes :

- Il existe un isomorphisme de variétés abéliennes sur $\overline{\mathbb{Q}}$: $i : A \to \mathscr{A}_{\overline{\mathbb{Q}}}$.
- Il existe un isomorphisme de fibrés en droites sur A : $i^*\mathscr{L}_{\overline{\mathbb{Q}}} \to L$.
- L'origine de A se relève en une section $\varepsilon : \operatorname{Spec} \mathbb{O}_K \to \mathscr{A}$.
- Pour toute place σ archimédienne de K, la métrique sur $\mathscr{L} \otimes_\sigma \mathbb{C}$ est la métrique cubiste définie plus haut.

On note $\mathscr{E}$ le $\mathbb{O}_K$-module $H^0(\mathscr{A}, \mathscr{L})$ et on le munit des métriques hermitiennes suivantes aux places archimédiennes : pour tout plongement $\sigma : K \hookrightarrow \mathbb{C}$ et $s \in \mathscr{E} \otimes_\sigma \mathbb{C} \simeq H^0(\mathscr{A}_\sigma, \mathscr{L}_\sigma)$, on pose :

$$\|s\|_{L^2,\sigma} = \Big(\int_{\mathscr{A}_\sigma(\mathbb{C})} \|s(x)\|^2 \, d\mu(x) \Big)^{1/2},$$

où $d\mu$ est la mesure de Haar de masse totale égale à 1 sur $\mathscr{A}_\sigma(\mathbb{C})$. On sait que $\overline{\mathscr{E}}$ est *semi-stable* : sa pente est égale à sa pente maximale [Bost 1996b, 4.2].

Proposition 3.11 [Moret-Bailly 1990; Bost 1996a]. *La pente de $\overline{\mathscr{E}}$ est donnée par la formule suivante :*

$$\hat{\mu}(\overline{\mathscr{E}}) = -\tfrac{1}{2} h_F(A) + \tfrac{1}{4} \log \frac{\chi(A, L)}{(2\pi)^g};$$

où $h_F(A)$ est la hauteur de Faltings de A et $\chi(A, L) = \deg_L(A)/g!$ désigne la caractéristique d'Euler–Poincaré de A.

3B3. *Pente maximale et sous-variétés.* Soit X un fermé de Zariski équidimensionnel de A, de dimension d. On note $\mathscr{X}$ l'adhérence de Zariski de X dans le modèle $\mathscr{A}$ de A qu'on s'est donné précédemment. Soit $\mathscr{W}$ un sous-module du tangent $t_{\mathscr{A}}$, muni de la restriction des métriques hermitiennes provenant de la forme de Riemann. Aux places archimédiennes, on munit :

$$\mathscr{L}^{\otimes M} \otimes S^m(\mathscr{W}^\vee)$$

de la norme obtenue par produit tensoriel de la norme cubiste sur $\mathscr{L} \otimes_\sigma \mathbb{C}$ et de la norme symétrique sur $S^m(\mathscr{W}^\vee) \otimes_\sigma \mathbb{C}$, et on munit le $\mathbb{C}_K$-fibré :

$$\mathscr{H}_m^M := H^0\big(\mathscr{A}, \mathscr{L}^{\otimes M} \otimes S^m(\mathscr{W}^\vee)\big)_{|\mathscr{X}} \subset H^0\big(\mathscr{X}, \mathscr{L}^{\otimes M} \otimes S^m(\mathscr{W}^\vee)\big)$$

de la métrique de Löwner $\|\cdot\|_{L,\sigma}$ associée à la norme du sup, pour toute place archimédienne σ. Il s'agit d'une norme hermitienne proche de la norme du sup dans le sens suivant (voir [Gaudron 2008, 2.2] pour le cas euclidien) :

$$\forall x \in \mathscr{H}_m^M \otimes \mathbb{C} : \ \|x\|_{L,\sigma} \leq \|x\|_{\sup,\sigma} \leq \sqrt{2 \operatorname{rg} \mathscr{H}_m^M}\, \|x\|_{L,\sigma}\,.$$

On souhaite majorer convenablement la pente maximale de $\overline{\mathscr{H}_m^M}$. On étudie d'abord le cas $m = 0$. On notera $h_L(V)$ la hauteur d'une variété V telle qu'elle est définie dans [Bost et al. 1994, partie 3].

Proposition 3.12. *Il existe une constante explicite c_8 ne dépendant que de K telle qu'on ait la majoration suivante pour la pente maximale de $\overline{\mathscr{H}_0^M}$:*

$$\hat{\mu}_{\max}(\overline{\mathscr{H}_0^M}) \leq M \frac{h_{\overline{L}}(X)}{\deg_L(X)} + d\,\log(M+d) + \log \deg_L(X) + \ c_8.$$

Démonstration. On commence par majorer la pente maximale en introduisant la plus petite norme $\varepsilon(\overline{\mathscr{H}_0^M})$ (hermitienne sur la somme orthogonale des $\mathscr{H}_0^M \otimes_\sigma \mathbb{C}$) d'un élément non-nul du réseau $\mathscr{H}_0^M$; voir [Bost et Künnemann 2007, inégalité (3.24) et la majoration de la fonction ψ page 35]. On a :

$$\hat{\mu}_{\max}(\overline{\mathscr{H}_0^M}) \leq -\log \varepsilon(\overline{\mathscr{H}_0^M}) + \tfrac{1}{2} \log \operatorname{rg}_{\mathbb{Z}}(\mathscr{H}_0^M) + \frac{\log|\Delta_K|}{2[K:\mathbb{Q}]}.$$

On majore le terme $-\log \varepsilon(\overline{\mathscr{H}_0^M})$ à l'aide de la théorie de l'intersection arithmétique. On commence par appliquer [Bost et al. 1994, proposition 3.2.1] ; comme L est ample avec $c_1(L)$ définie positive (par [Bost et al. 1994, proposition 3.2.4]), pour une section $s \in H^0(\mathscr{X}, \mathscr{L}^M)$, on a :

$$h_L(\operatorname{div}(s)) = M h_L(X) + \int_{X(\mathbb{C})} \log \|s\|\, c_1(L)^d \geq 0.$$

De plus, comme $c_1(L)$ est définie positive, on a :

$$\int_{X(\mathbb{C})} \log \|s\|\, c_1(L)^d \leq \max_{\sigma \in \Sigma_\infty} \log \|s\|_{\sup,\sigma} \int_{X(\mathbb{C})} c_1(L)^d.$$

Par le théorème de Wirtinger (voir [Griffiths et Harris 1978, page 171]), la dernière intégrale est $\deg_L(X)$. On a donc :

$$-\max_{\sigma\in\Sigma_\infty}\log\|s\|_{\sup,\sigma}\leq M\frac{h_L(X)}{\deg_L(X)}.$$

Soit σ_0 tel que $\|s\|_{\sup,\sigma_0}$ réalise le maximum sur toutes les places archimédiennes. Par choix de la norme de Löwner associée à la norme du sup sur $\mathscr{H}_0^M$, on a :

$$\max_{\sigma\in\Sigma_\infty}\|s\|_{\sup,\sigma}\leq\sqrt{2\operatorname{rg}\mathscr{H}_0^M}\,\|s\|_{L,\sigma_0},$$

et par suite :

$$\begin{aligned}-\log\|s\|&=-\tfrac{1}{2}\log\sum_{\sigma\in\Sigma_\infty}\|s\|_{L,\sigma}^2\leq-\log\|s\|_{L,\sigma_0}\\&\leq-\max_{\sigma\in\Sigma_\infty}\log\|s\|_{\sup,\sigma}+\tfrac{1}{2}\log(2\operatorname{rg}\mathscr{H}_0^M).\end{aligned}$$

On en déduit que :

$$-\log\varepsilon(\overline{\mathscr{H}_0^M})\leq M\frac{h_{\overline{L}}(X)}{\deg_L(X)}+\tfrac{1}{2}\log(2\operatorname{rg}\mathscr{H}_0^M).$$

Il reste à majorer le rang de $\mathscr{H}_0^M$. Le fibré L définit un plongement projectivement normal de A, et les éléments de $\mathscr{H}_0^M$ sont des restrictions à X de sections globales sur A, donc on est en mesure d'appliquer le théorème principal de [Chardin 1989] :

$$\operatorname{rg}_{\mathbb{Z}}\mathscr{H}_0^M\leq[K:\mathbb{Q}]\operatorname{rg}\mathscr{H}_0^M\leq[K:\mathbb{Q}](M+d)^d\deg_L(X).$$

La proposition est entièrement démontrée. □

On peut maintenant majorer la pente maximale du fibré des sections avec multiplicité. Le fibré $\mathscr{W}^\vee$ étant constant, on a l'isomorphisme (isométrique) :

$$\mathscr{H}_m^M\simeq\mathscr{H}_0^M\otimes S^m\mathscr{W}^\vee.$$

Bost a conjecturé que la pente maximale du produit tensoriel est la somme des pentes maximales. Les meilleurs résultats connus dans cette direction sont ceux de Bost et Künnemann [2007], et de Chen [2006], qui a démontré dans sa thèse :

Théorème 3.13. *Soient $\overline{\mathscr{E}}_1,\dots,\overline{\mathscr{E}}_n$ des fibrés hermitiens non-nuls sur* $\operatorname{Spec}\mathcal{O}_K$. *Alors* :

$$\hat{\mu}_{\max}(\overline{\mathscr{E}}_1\otimes\cdots\otimes\overline{\mathscr{E}}_n)\leq\sum_{i=1}^n\big(\hat{\mu}_{\max}(\overline{\mathscr{E}}_i)+\log\operatorname{rg}\mathscr{E}_i\big).$$

Rappelons que par $c(\mathscr{W})$, on désigne une borne ≥ 1 pour la hauteur d'une base entière de $\mathscr{W}$. On peut maintenant démontrer le corollaire suivant :

Corollaire 3.14. *On a la majoration, pour la pente maximale* :

$$\hat{\mu}_{\max}(\overline{\mathscr{H}_m^M})\leq M\frac{h_{\overline{L}}(X)}{\deg_L(X)}+2d\log(M+d)+2\log\deg_L(X)+c_9mc(\mathscr{W}),$$

où c_9 ne dépend que de (A,L).

Démonstration. Le théorème précédent nous montre que :

$$\hat{\mu}_{\max}(\overline{\mathscr{H}_m^M}) \leq \hat{\mu}_{\max}(\overline{\mathscr{H}_0^M}) + \hat{\mu}_{\max}(S^m(\overline{\mathscr{W}^\vee})) + \log(\operatorname{rg} \mathscr{H}_0^M) + \log(\operatorname{rg} S^m(\mathscr{W}^\vee)).$$

Les termes relatifs à $\overline{\mathscr{H}_0^M}$ ont été calculés dans la proposition précédente. Le rang de $S^m(\mathscr{W}^\vee)$ est donné par la formule classique :

$$\operatorname{rg} S^m(\mathscr{W}^\vee) = \binom{m+g-1}{g-1} \leq (m+g)^{g-1},$$

et sa pente maximale a été majorée en 3B1. □

4. Choix des fibrés et du morphisme

On rappelle que A est une variété abélienne définie sur un corps de nombres K, munie d'un fibré L ample et symétrique, qu'on pourra supposer très ample quitte à considérer $L^{\otimes 3}$. Quitte à prendre une extension finie de K (ne dépendant que de A), on prend un modèle de Moret-Bailly $(\mathscr{A}, \mathscr{L}, 0)$ de (A, L), suivant la terminologie de [Bost 1996a]. Ce modèle est en particulier semi-abélien [Gaudron 2006, définition-théorème 4.3]. On suppose de plus que $\mathscr{A}$ vérifie l'hypothèse H. On vérifie aisément que celle-ci implique H′ et on prend $\alpha = g$ dans la définition de $\mathscr{P}_A$.

On prend une sous-variété stricte V de A, de codimension r, qui n'est pas incluse dans le translaté d'une sous-variété abélienne stricte. On pose aussi $X = V + H_0$, où H_0 est un certain sous-groupe fini de A. On va construire un fibré hermitien $\overline{\mathscr{E}}_M$ associé à un espace vectoriel E, une suite de fibrés $\overline{\mathscr{G}}_k$, $k \in I$ (pour un certain ensemble fini I), correspondant à une fibration d'un espace vectoriel F, et un morphisme ϕ de restriction entre E et F. Les $\overline{\mathscr{G}}_k$ seront définis à partir de l'espace des sections d'une puissance de $\mathscr{L}$ sur des modèles entiers de X et de ses translatés par des points de torsion bien choisis. La partie précédente nous permettra de calculer les termes de pentes associés à ces fibrés. À la fin de cette partie, on fixera les paramètres et on supposera par l'absurde que le minimum essentiel de V est majoré en fonction des paramètres.

4A. ***Le plongement étiré.*** Pour éliminer la constante de comparaison entre hauteur projective et hauteur de Néron–Tate sur A, on considère classiquement un plongement étiré. Soit M un entier supérieur ou égal à 1. La multiplication par M sur A est notée $[M]$ et on définit :

$$\psi_M : A \to A \times A, \quad x \mapsto (x, [M]x).$$

Ce plongement a été utilisé pour la première fois par Laurent [1983] pour étudier le problème de Lehmer elliptique. Son principe est le suivant : les techniques

diophantiennes nous renseignent sur la hauteur projective, et le minimum essentiel fait intervenir la hauteur de Néron–Tate associée au plongement. On sait que la différence entre ces deux hauteurs est bornée mais la hauteur de Néron–Tate peut être très petite ; il y a donc une perte d'information sur la hauteur projective. Le plongement étiré multiplie la hauteur par un paramètre assez grand, qui rend négligeable la constante de comparaison.

Soit $L_M := \psi_M^*(\pi_1^* L \otimes \pi_2^* L) \simeq L^{\otimes(M^2+1)}$ et $\mathscr{L}_M := \psi_M^*(\pi_1^*\mathscr{L} \otimes \pi_2^*\mathscr{L})$. On note $\deg_M$ le degré, et $\hat{h}_M$ la hauteur canonique, par rapport au fibré L_M. Le lemme suivant indique la variation de la hauteur et du degré par changement de fibré :

Lemme 4.1. *Si V est une sous-variété de A, on a la variation suivante de la hauteur canonique* :

$$\hat{h}_M(V) = (M^2+1)^{\dim V+1}\hat{h}_L(V);$$

et la formule suivante pour le degré :

$$\deg_M(V) = (M^2+1)^{\dim V}\deg(V).$$

Démonstration. Ces formules sont démontrées, par exemple, dans [Philippon 1995, proposition 7]. □

Dans cette partie et la suivante, on travaillera donc dans le plongement étiré et on notera A_M l'image de A par le plongement ψ_M.

4B. ***Le fibré de départ.*** Commençons par décrire le premier fibré. On pose $\mathscr{E}_M := H^0(\mathscr{A}, \mathscr{L}_M)$. On note aussi E le tensorisé de $\mathscr{E}_M$ avec K. On a vu en 3B2 comment munir ce fibré d'une structure hermitienne et on a donné son degré. On fait une hypothèse qui sera aisément vérifiée par la suite :

$$\log M^2 > 2\Big(\frac{2}{g}h_F(A) + \log(2\pi g!)\Big).$$

Lemme 4.2. *On a la minoration suivante pour le degré normalisé de $\overline{\mathscr{E}_M}$* :

$$\widehat{\deg}\,\overline{\mathscr{E}_M} \geq c_{10}(M^2)^g \log M,$$

pour une constante $c_{10} > 0$ ne dépendant que de A.

Démonstration. En multipliant la pente par le rang, la proposition 3.11 donne :

$$\widehat{\deg}\,\overline{\mathscr{E}_M} = (M^2+1)^g \frac{\deg_L(A)}{g!}\Big(-\tfrac{1}{2}h_F(A) + \tfrac{1}{4}\log\frac{(M^2+1)^g \deg_L(A)}{(2\pi)^g g!}\Big).$$

Notons que la hauteur de Faltings ne dépend que de la classe d'isomorphisme de A. L'hypothèse faite sur les paramètres donne immédiatement le lemme, avec une constante $c_{10} > 0$ ne dépendant que de A et facilement explicitable. □

4C. ***Fibration de l'espace d'arrivée.*** On introduit maintenant la notion de voisinage infinitésimal [Bost 1996a], qui sera défini à partir d'un fermé X de A et d'un ordre de dérivation l. On commence par choisir la base du tangent $(e_1, \ldots, e_g)$ sur A correspondant à la base de dérivations algébriques fixée en 2C. L'action de l'isogénie $[M]$ sur le tangent étant la multiplication par M, on en déduit d'abord une base $(e_1, \ldots, e_{2g})$ de t_{A^2}, puis on pose $f_i = e_i + Me_{g+i}$. La famille $(f_1, \ldots, f_g)$ est une base de l'espace tangent t_{A_M}, image de t_A par l'étirement (voir 3B1) et on note (par abus de langage) $(\partial_1, \ldots, \partial_g)$ la base de dérivations associée. Si $x \in A$, on en déduit par translation une base de dérivations $(\partial_{1,x}, \ldots, \partial_{g,x})$ en x (dans le plongement étiré). On notera aussi par la suite :

$$\partial_x^\lambda = \frac{1}{\prod_{1=i}^g \lambda_i!}\, \partial_{1,x}^{\lambda_1} \cdots \partial_{g,x}^{\lambda_g}.$$

Soit X un fermé de Zariski de A. On définit le schéma $V(X, t_{A_M}, l)$ de la façon suivante :

- si $l = 0$, $V(X, t_{A_M}, l)$ est le sous-schéma réduit de A défini par X ;
- si $l = 1$ et $X = 0$, $V(0, t_{A_M}, 1)$ est le voisinage infinitésimal d'ordre 1 de 0 ;
- si $l \geq 1$, $V(X, t_{A_M}, l)$ est l'image dans A du schéma $X \times V(0, t_{A_M}, 1)^l$ par le morphisme d'addition $A^{l+1} \to A$.

Le schéma $V(X, t_{A_M}, l)$ admet pour support le fermé X et son faisceau d'idéaux $\mathcal{J}$ est défini par :

$$s \in \mathcal{J} \iff \partial_x^\lambda s = 0 \text{ pour tout } x \in X \text{ et tout } \lambda \in \mathbb{N}^g \text{ tel que } \sum_{i=1}^g \lambda_i \leq l.$$

L'espace vectoriel d'arrivée sera formé de sous-espaces de sections sur X et de nombreux translatés de X par des points de torsion, avec multiplicité. On précise d'abord les points de torsion en lesquels on extrapole, et la multiplicité, puis on met un ordre sur cet ensemble. On se donne $T_0 > 0$. Pour $1 \leq n \leq r$ (r étant la codimension de V et de X), on se donne aussi deux nombres positifs T_n (qui correspond à la multiplicité après n extrapolations), et N_n (qui borne les normes des premiers d'extrapolation). Puis on définit les ensembles $\mathcal{P}_n$:

$$\mathcal{P}_n = \big\{\mathfrak{p} \in \mathcal{P}_A : \mathbf{N}(\mathfrak{p}) \in [N_n/2; N_n]\big\}.$$

On note $\mathcal{P}$ l'ensemble des premiers de $\mathbb{Z}$. La projection des $\mathcal{P}_n$ sur $\mathbb{Z}$ est donnée par :

$$\mathcal{P}_{n,\mathbb{Z}} = \{p \in \mathcal{P} : \exists\, \mathfrak{p} \in \mathcal{P}_n, \mathfrak{p} | p\}.$$

Le choix des paramètres sera tel que les ensembles $\mathcal{P}_n$ (resp. $\mathcal{P}_{n,\mathbb{Z}}$) soient disjoints. On note :

$$\mathrm{Tor}_{A,n} = \left\{ \begin{array}{l} P \in A[p] : \ \exists \mathfrak{p} \in \mathcal{P}_n \text{ divisant } p, \text{ tel que pour tout} \\ \mathfrak{q} \in \mathbb{O}_{K(P)} \text{ divisant } \mathfrak{p},\ P \text{ se réduit sur 0 modulo } \mathfrak{q} \end{array} \right\}.$$

On note pour toute la suite K' le corps engendré par K, par un corps de définition de V et par les coordonnées projectives des points de la réunion $\bigcup_{1\leq n\leq r} \mathrm{Tor}_{A,n}$. Les fibrés et les morphismes qu'on va considérer seront tous définis sur K' ; en fait, comme on considère des $\mathbb{O}_K$-fibrés, les calculs de pentes valables sur $\mathbb{O}_K$ se transportent sans changer à $\mathbb{O}_{K'}$, et le corps K' intervient uniquement dans les estimations ultramétriques.

On ordonne les points de $\mathrm{Tor}_{A,n}$ en les classant d'abord selon le plus petit premier p de torsion (pour l'ordre naturel sur $\mathbb{Z}$) puis en choisissant arbitrairement un ordre à p fixé. Pour $i = (i_1, \ldots, i_r)$, où i_n, pour $1 \leq n \leq r$, est un indice dans $[1, |\mathrm{Tor}_{A,n}|]$, on note P_i le point $P_{i_1} + \cdots + P_{i_r}$. On note I l'ensemble de ces multi-indices, qu'on ordonne avec l'ordre lexicographique. On confondra dans la suite l'ensemble I et son image dans $\mathbb{N}$ par l'indexation, et les éléments $i \in I$ pourront être vus comme des entiers via cette identification. On construit, pour $i \in I$, une suite de fermés $X_i = X + P_i$. On pose enfin, pour $i \in I$: $T_{(i)} = T_{n_i}$ et $N_{(i)} = N_{n_i}$, où n_i est le plus grand des j tels que $P_{i_j} \neq 0$.

On définit maintenant :

$$S := \bigcup_{i\in I} V(X_i, t_{A_M}, T_{(i)}) \quad \text{et} \quad F := H^0(A, L_M)_{|S}.$$

On note ϕ le morphisme (surjectif) de restriction de E vers F, et pour $k \in I$ un entier, on pose :

$$S_k = \bigcup_{i\leq k} V(X_i, t_{A_M}, T_{(i)}).$$

Ceci permet de définir F_k, le noyau de la restriction :

$$H^0(A, L_M)_{|S} \to H^0(A, L_M)_{|S_k}.$$

La suite décroissante des F_k est une filtration de F et on en déduit une filtration de E en posant $E_k := \phi^{-1}(F_{k-1})$. Soit aussi $G_k = F_{k-1}/F_k$ et $\phi_k : E_k \to G_k$ l'application linéaire déduite de ϕ et de la projection canonique : $F_{k-1} \to G_k$. En appliquant le lemme des serpents aux deux suites exactes :

$$0 \to F_k \to H^0(A, L_M)_{|S} \to H^0(A, L_M)_{|S_k} \to 0,$$
$$0 \to F_{k-1} \to H^0(A, L_M)_{|S} \to H^0(A, L_M)_{|S_{k-1}} \to 0,$$

on voit que G_k s'identifie au noyau de :

$$H^0(A, L_M)_{|S_k} \to H^0(A, L_M)_{|S_{k-1}}.$$

qui est un sous-espace vectoriel de :

$$H_k := H^0\big(A, \mathrm{Sym}^{T_{(k)}}(t^\vee_{A_M}) \otimes L_M\big)_{|X_k}.$$

Remarque. On a choisi ici de noter Sym le fibré symétrique, pour éviter toute confusion avec le schéma S.

On se donne un modèle entier avec structure hermitienne $\overline{\mathcal{H}}_k$ de H_k comme dans 3B3 et on en déduit un modèle entier avec structure hermitienne $\overline{\mathcal{G}}_k$ de G_k.

Lemme 4.3. *Il existe une constante c_{11} ne dépendant que de A telle que* :

$$\hat{\mu}_{\max}(\overline{\mathcal{G}}_k) \leq c_{11}\big(M^2\hat{\mu}_L^{\mathrm{ess}}(X) + \log \deg_L(X) + T_{(k)}\log(M + T_{(k)})\big).$$

Démonstration. On utilise le corollaire 3.14 pour majorer la pente maximale de $\overline{\mathcal{H}}_k$. En notant h_M la hauteur projective associée à L_M, on commence par remarquer qu'il existe une constante c_{11} ne dépendant que de A telle que :

$$\frac{h_M(X_k)}{\deg_M(X_k)} \leq \frac{\hat{h}_M(X_k)}{\deg_M(X_k)} + c_{11} \leq (M^2+1)\frac{\hat{h}_L(X_k)}{\deg_L(X_k)} + c_{11},$$

en comparant la hauteur projective et la hauteur canonique dans le plongement étiré [David et Philippon 2002, propositions 3.9 et 3.14], puis grâce au lemme 4.1. L'inégalité des minima successifs (démontrée dans [Zhang 1995b, Theorem 5.2]) donne donc, comme $M \geq 1$:

$$\frac{h_M(X_k)}{\deg_M(X_k)} \leq 2gM^2\hat{\mu}_L^{\mathrm{ess}}(X) + c_{11}.$$

Le minimum essentiel, tout comme le degré, n'est pas modifié lorsqu'on translate par des points d'ordre fini. Par choix de la base de dérivation sur $\mathcal{A}_M$, en tenant compte de l'action de $[M]$ sur le tangent et en bornant la hauteur de la base de dérivations algébriques par une constante ne dépendant que de A, on peut choisir :

$$c(t_{\mathcal{A}_M}) \leq \log M + c_{11}.$$

Comme $\overline{\mathcal{G}}_k$ s'injecte isométrique dans $\overline{\mathcal{H}}_k$, on a :

$$\hat{\mu}_{\max}(\overline{\mathcal{G}}_k) \leq \hat{\mu}_{\max}(\overline{\mathcal{H}}_k) \leq c_{11}\big(M^2\hat{\mu}_L^{\mathrm{ess}}(X) + \log \deg_L(X) + T_{(k)}\log(M + T_{(k)})\big),$$

quitte à prendre c_{11} assez grande en fonction de A. □

4D. ***Choix des paramètres et hypothèse sur le minimum essentiel.*** Ce choix doit permettre d'assurer l'injectivité du morphisme ϕ et de contredire l'inégalité des pentes. On suit la stratégie suivante :

– On définit les paramètres M, T_0, N_1 de telle manière que le terme (correspondant au fermé X non-translaté) :

$$\mathrm{rg}\,\mathcal{G}_0\,\big(\hat{\mu}_{\max}(\overline{\mathcal{G}_0}) + h(\phi_0)\big),$$

soit inférieur à $\widehat{\deg}(\overline{\mathcal{E}_M})$.

– Les relations entre les paramètres T_i et N_i sont telles que les contributions des termes suivants dans l'inégalité des pentes soient négatives.
– Le paramètre d'étirement M est pris aussi petit que possible, ce qui permet de montrer que le morphisme ϕ est injectif ; il est aussi choisi de telle sorte que $M^2\hat{\mu}_L^{\mathrm{ess}}(X)$ soit majoré par une constante, ce qui détermine la minoration obtenue pour le minimum essentiel.

On commence par introduire l'indice d'obstruction avec poids $\omega_L(x, X)$; celui-ci permet classiquement de prendre en compte la hauteur des dérivées dans un lemme de Siegel. Il aura un emploi similaire dans le cadre de la théorie des pentes.

Définition 4.4. Soit X un fermé de Zariski strict de A et x un réel positif. On pose :

$$\omega_L(x, X) = \inf\left(x \deg_L(Z)\right)^{1/\operatorname{codim} Z},$$

où l'infimum porte sur l'ensemble des fermés de Zariski (équidimensionnels) stricts de A contenant X.

On utilisera souvent le lemme suivant, qui compare l'indice d'obstruction simple, ne prenant en compte que les hypersurfaces, et l'indice d'obstruction avec poids :

Lemme 4.5. *Soit X un fermé strict (équidimensionnel) de A en codimension r. Il existe une constante c_{12} ne dépendant que de A telle que pour tout réel $x \geq 1$:*

$$c_{12}x^{1/r}\omega_L(X) \leq \omega_L(x, X) \leq x\omega_L(X).$$

Démonstration. L'inégalité de droite est immédiate et celle de gauche est une conséquence de [Chardin 1990, corollaire 2 et exemple 1]. Remarquons qu'un fibré très ample étant fixé, seule la dimension du projectif dans lequel on plonge A intervient dans c_{12}. □

On se donne une constante C_0 ne dépendant que de A, grande devant toutes les constantes du problème, dans un sens explicitable au cours de la preuve. Soit Δ le paramètre :

$$\Delta = C_0^2 \log(3 \deg_L(V)).$$

C'est à partir de ce paramètre, qui est de l'ordre de $\log \deg_L(V)$, qu'on va définir tous les autres paramètres. Son avantage — comparé à $\log(\deg_L(V))$ — est d'être inconditionnellement grand devant les constantes intervenant au cours de la preuve, par choix de C_0.

En vue de la descente, nous introduisons deux paramètres qui permettront d'itérer la construction. Soient donc R et ρ deux entiers strictement positifs tels que :

$$\Delta \geq \log R \quad \text{et} \quad \rho \leq \left(9(2r)^{r+1}\right)^{r-1}.$$

Dans le formalisme des pentes, on regarde la restriction d'une section aux translatés de V par n points de torsion, où $0 \leq n \leq r$. On prend un paramètre T_0 correspondant à la multiplicité initiale et on associe à tout $n \in [1; r]$ des paramètres

spécifiques, à savoir une multiplicité T_n, et une borne N_n pour la norme des premiers de torsion, ce qui détermine un ensemble de premiers $\mathcal{P}_n$. Le lien entre ces paramètres est choisi de telle sorte que la contribution des termes de pente, pour des indices strictement positifs, soient négatifs. On prend d'abord :

$$N_n = \Delta^{\rho(2r)^{r+2-n}}.$$

Chaque N_n est donc négligeable devant le précédent ; les raisons de ce choix seront plus claires au cours de la preuve de la proposition 6.5, qui montrera *quasiment* l'injectivité du morphisme ϕ. Passons à la multiplicité. Par récurrence descendante, pour $0 \leq n \leq r-1$, on pose :

$$T_n = T_{n+1}(N_{n+1}\Delta^2).$$

Puis on pose :

$$T_r = 1.$$

Ces formules déterminent complètement T_0 par itération :

$$T_0 = \Delta^{2r} N_1 \cdots N_r.$$

On finit par le paramètre M. Le but est de prendre M^2 assez grand pour que le premier terme dans la somme de l'inégalité de pentes soit plus petit que le degré de $\overline{\mathscr{E}_M}$. Cette condition s'apparente à celle qu'on obtiendrait par un lemme de Siegel dans une preuve classique de transcendance. Pour montrer l'injectivité de ϕ, on aura au contraire besoin que M^2 ne soit pas trop grand. On choisit donc :

$$M = \left\lfloor (T_0 \omega_L(\Delta T_0, X))^{1/2} \right\rfloor + 1.$$

On rappelle que V est une sous-variété stricte de A qui n'est pas incluse dans un translaté de sous-variété abélienne stricte, et que : $X = V + H_0$, où H_0 est un sous-groupe fini de A. On suppose que le cardinal de H_0 n'est pas trop gros :

$$\log |H_0| \leq \Delta. \tag{4-1}$$

Puis on fait l'hypothèse suivante sur le minimum essentiel de X :

$$\hat{\mu}_L^{\mathrm{ess}}(X) < \frac{\Delta}{T_0 \omega_L(\Delta T_0, X)}. \tag{4-2}$$

5. Utilisation de l'inégalité des pentes

On a déjà calculé le degré de $\overline{\mathscr{E}}_M$ et les pentes maximales. On veut maintenant majorer le rang des $\mathscr{G}_k$ et la hauteur des ϕ_k. Les estimations ultramétriques dans la hauteur des ϕ_k sont le point crucial de la preuve et ont été préparées par la partie 2. Les estimations archimédiennes, enfin, utilisent essentiellement l'inégalité de Cauchy (en plusieurs variables).

5A. ***Majoration du rang.***

5A1. *Nombre de dérivations.* Le calcul du nombre de dérivations est classique dans les preuves de transcendance. Si X est un fermé équidimensionnel plongé par un fibré très ample L dans un espace projectif $\mathbb{P}^n$ sur $\overline{\mathbb{Q}}$, associé à un idéal homogène I, et m un entier, on pose

$$H(X, L^{\otimes m}) := \dim\big[\overline{\mathbb{Q}}[X_0, \dots, X_n]/I\big]_m,$$

où on se restreint à la composante homogène de degré m du quotient. La prise en compte de l'indice d'obstruction avec poids nous amène à faire le raisonnement qui suit avec un fermé équidimensionnel Z_k contenant X_k, de codimension $r' \leq r = \operatorname{codim} X_k$.

Proposition 5.1. *On a l'inégalité suivante* :

$$\operatorname{rg} \mathscr{G}_k \leq \operatorname{rg} \mathscr{H}_k \leq T_{(k)}^{r'} H(Z_k, L_M).$$

Démonstration. La première inégalité est claire. On remarque ensuite que l'inclusion $X_k \subset Z_k$ permet de se ramener à la majoration du rang du fibré $\mathscr{H}_k$, dans lequel on a remplacé X_k par Z_k. Le plongement de A par L_M étant projectivement normal, et les sections considérées étant des restrictions de sections globales sur A, elles appartiennent au quotient $\overline{\mathbb{Q}}[X_0, \dots, X_n]/I(Z_k)$. On applique alors l'« astuce de Philippon–Waldschmidt » (voir [Amoroso et David 2003, lemme 2.5], ou encore [David et Hindry 2000, 5.3]), qui donne :

$$\begin{aligned}\dim H^0\big(A, \operatorname{Sym}^{T_{(k)}}(t_{A_M}^\vee) \otimes L_M\big)_{|Z_k} &\leq \binom{T_{(k)}+r'-1}{r'-1} H\big(Z_k, L_M\big) \\ &\leq T_{(k)}^{r'} H\big(Z_k, L_M\big). \qquad \square\end{aligned}$$

5A2. *Le théorème de Chardin.* Pour majorer $H(Z_k, L_M)$, on ne peut pas se contenter du théorème de Hilbert–Samuel géométrique. Celui-ci donne une estimation asymptotique, ce qui oblige à introduire une constante indéterminée dépendant de Z_k (et par suite de l'indice d'obstruction).

Proposition 5.2. *On a* :

$$H\big(Z_k, L_M\big) \leq \binom{1+g-r'}{g-r'} \deg_M(Z_k).$$

Démonstration. C'est une conséquence du résultat principal de [Chardin 1989], valable pour un fermé équidimensionnel. $\square$

On regroupe les deux derniers résultats dans le corollaire suivant :

Corollaire 5.3. $$\operatorname{rg} \mathscr{G}_k \leq \frac{g(2M^2)^g}{\Delta T_0}.$$

Démonstration. On combine les deux dernières propositions en remarquant que le coefficient binômial apparaissant dans la dernière est inférieur ou égal à g. Puis on obtient, grâce au lemme 4.1 :

$$\operatorname{rg} \mathcal{G}_k \leq g T_{(k)}^{r'} \deg_M(Z_k) \leq g T_{(k)}^{r'} (2M^2)^{g-r'} \deg_L(Z_k).$$

Ceci est vrai pour toute variété Z_k contenant X_k. Soit donc Z_k une sous-variété, de codimension r', telle que (on se ramène à X car le degré est invariant par translation) :

$$\omega_L(\Delta T_0, X) = \left(\Delta T_0 \deg_L(Z_k)\right)^{1/r'}.$$

On a donc, par choix du paramètre M :

$$\operatorname{rg} \mathcal{G}_k \leq \frac{g(2M^2)^g}{\Delta T_0} \left(\frac{T_{(k)}}{T_0} \frac{\omega_L(\Delta T_0, X)}{\omega_L(\Delta T_0, X)} \right)^{r'},$$

et le résultat suit puisque $T_{(k)} \leq T_0$. □

5B. ***Normes ultramétriques des morphismes.*** Soit $k \in I$ un entier. Si $\mathfrak{q}$ est un idéal premier de $\mathbb{O}_{K'}$, la norme $\mathfrak{q}$-adique de ϕ_k est agréablement majorée si la k-ème étape dans la filtration correspond à la translation par certains points de torsion de A.

Proposition 5.4. *Si* $\mathfrak{p} := \mathfrak{q} \cap \mathbb{O}_K \in \bigcup_{1 \leq n \leq r} \mathcal{P}_n$, *on a* :

$$\log \|\phi_k\|_{\mathfrak{q}} \leq 0.$$

Si de plus, en notant $P_k = P_{k_1} + \cdots + P_{k_n}$ *le point associé à* k, *le point* P_{k_n} *est un point de* p*-torsion* (*où* $(p) = \mathfrak{p} \cap \mathbb{Z}$) *se réduisant sur* 0 *mod* $\mathfrak{q}$, *on a* :

$$\log \|\phi_k\|_{\mathfrak{q}} \leq -n_{\mathfrak{q}}(T_{n-1} - T_n) \frac{\log p}{p}.$$

Démonstration. Commençons par l'inégalité faible. Soit s un élément de E_k tel que $\|s\|_{\mathfrak{q}} \leq 1$; soit $\mathcal{X}_k$ le modèle entier de X_k choisi dans la définition de $\mathcal{G}_k$, et x un élément de $\mathcal{X}_k$. Soit aussi $\lambda \in \mathbb{N}^g$ tel que $\sum_{1 \leq i \leq g} \lambda_i \leq T_{(k)}$. On a :

$$\partial_x^\lambda s = \partial^\lambda (s \circ \tau_x).$$

Par définition de $\mathcal{P}_A$, les coefficients de τ_x sont $\mathfrak{p}$-entiers (voir (2-1)). De plus, le choix de $\mathcal{P}_A$ permet aussi que l'opérateur différentiel ∂^λ appliqué en chaque monôme affine s'exprime comme un polynôme en les coordonnées affines à coefficients $\mathfrak{p}$-entiers (par (2-2)). En remarquant que la base de dérivations sur A est algébrique (ce qui fait disparaître les factorielles au dénominateur quand on dérive des polynômes) et que la base de dérivations sur A_M est obtenue par combinaisons linéaires à coefficients entiers des dérivations sur A, on a :

$$|\partial_x^\lambda s|_{\mathfrak{q}} \leq 1.$$

Ceci étant vrai pour tout $x \in \mathscr{X}_k$ et tout $\lambda \in \mathbb{N}^g$ tel que $\sum \lambda_i \leq T_{(k)}$, on en déduit :

$$\|\phi_k(s)\|_{\mathfrak{q}} \leq 1.$$

La première partie de la proposition est donc démontrée en passant au sup sur $s \in E_k$.

Pour l'inégalité forte, on écrit $P_k = P_{k'} + P_{k_n}$ le point de torsion associé à k, où P_{k_n} se réduit sur 0 modulo $\mathfrak{q}$. Pour $x \in \mathscr{X}_k$, on note $x = x' + P_{k_n}$. Soit $\mathbf{t}_\nu = (t_{1,\nu}, \ldots, t_{g,\nu})$ une base de paramètres bien définie en P_{k_n}, suivant le lemme 2.10. On reprend les notations convenues avant la proposition 2.11. L'isomorphisme :

$$\hat{\mathscr{A}}_{\mathbb{O}_{\mathfrak{p}}} \simeq \mathbb{O}_{\mathfrak{p}}[\![t_{1,\nu}, \ldots, t_{g,\nu}]\!],$$

induit une application :

$$H^0(\mathscr{A}_{\mathbb{O}_{\mathfrak{p}}}, \mathbb{O}_{\mathscr{A}_{\mathbb{O}_{\mathfrak{p}}}}) \to \mathbb{O}_{\mathfrak{p}}[\![t_{1,\nu}, \ldots, t_{g,\nu}]\!].$$

Celle-ci associe à l'image d'une section f de $H^0(\mathscr{A}_{\mathbb{O}_{\mathfrak{p}}}, \mathbb{O}_{\mathscr{A}_{\mathbb{O}_{\mathfrak{p}}}})$ son développement de Taylor en 0 :

$$\sum_{\mu \in \mathbb{N}^g} (\partial_\nu^\mu f)\, \mathbf{t}_\nu^\mu.$$

On a, par la proposition 2.11, les majorations suivantes :

$$\forall 1 \leq i \leq g : \ |t_{i,\nu}(P_{k_n})|_{\mathfrak{q}} \leq p^{-n_{\mathfrak{q}}/p}.$$

De plus, pour tout $\mu \in \mathbb{N}^g$, la condition (2-3) garantit :

$$|\partial_\nu^\mu (s \circ \tau_{x'})|_{\mathfrak{q}} \leq 1.$$

La norme étant ultramétrique, ceci suffit à voir que la série de Taylor de $\partial^\lambda(s \circ \tau_{x'})$ converge. On en déduit l'égalité :

$$\partial_x^\lambda s = \sum_{\mu \in \mathbb{N}^g} \partial_\nu^\mu \partial^\lambda (s \circ \tau_{x'}) \mathbf{t}_\nu (P_{k_n})^\mu,$$

Par définition de E_k, s est nulle à un ordre T_{n-1} en x', et cette propriété ne dépend pas du choix de la base de dérivations ; donc si $\partial_\nu^\mu \partial^\lambda (s \circ \tau_{x'}) \neq 0$, on a :

$$\sum_{1 \leq i \leq g} \mu_i + \lambda_i > T_{n-1}.$$

On en déduit :

$$\left| \prod_{i=1}^{g} t_{i,\nu}(P_{k_n})^{\mu_i} \right|_{\mathfrak{q}} \leq p^{-n_{\mathfrak{q}}(T_{n-1} - T_n)/p}.$$

La norme étant ultramétrique, l'inégalité fine de la proposition en résulte. □

5C. ***Normes archimédiennes des morphismes d'évaluation.*** Soit k un entier, et σ une place archimédienne de K'. Tous les ϕ_k sont définis sur K'. Le but de ce paragraphe est de majorer $\|\phi_k\|_\sigma$, par des méthodes d'analyse complexe, en particulier l'inégalité de Cauchy. Cette majoration sera la même pour toutes les places archimédiennes. On suit [Gaudron 2006, paragraphe 5.9].

Proposition 5.5. *Il existe une constante c_{15} ne dépendant que de A telle que* :

$$\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\hookrightarrow\mathbb{C}}\log\|\phi_k\|_\sigma \leq c_{15}T_{(k)}\log M.$$

Démonstration. Soit $s \in E_k \otimes \mathbb{C}$ et $x \in \mathscr{X}_k$. On a alors :

$$\phi_k(s)(x) \in \left(S^{T_{(k)}}t_{\mathscr{A}_M}^\vee \otimes x^*\mathscr{L}_M\right)\otimes_\sigma \mathbb{C},$$

qui est isomorphe (non isométriquement) à :

$$\mathrm{Hom}_{\mathbb{C}}(S^{T_{(k)}}\,t_{\mathscr{A}_{M,\sigma}}, x^*\mathscr{L}_{M,\sigma}).$$

Si on fixe une base d'ouverts affines, l'image de $\phi_k(s)(x)$ par cet isomorphisme est le morphisme qui associe à une dérivation D d'ordre $T_{(k)}$ la valeur de Ds en x (la dérivation D donnant par translation une dérivation en x). On note $\Theta_{T_{(k)}}$ cet isomorphisme qui est défini dans [Gaudron 2006, 4.1], où sa norme d'opérateur, ainsi que celle de son inverse, sont majorées :

$$\|\Theta_{T_{(k)}}\|_\sigma \leq \max_{\substack{\mathbf{i}\in\mathbb{N}^g\\|\mathbf{i}|=T_{(k)}}}\frac{T_{(k)}!}{\mathbf{i}!} \quad\text{et}\quad \|\Theta_{T_{(k)}}^{-1}\|_\sigma \leq 1.$$

On en déduit que :

$$\|\phi_k(s)(x)\|_\sigma \leq \left\|\Theta_{T_{(k)}}\left(\phi_k(s)(x)\right)\right\|_\sigma.$$

Soit $(f_{1,\sigma},\dots,f_{g,\sigma})$ une base de $t_{\mathscr{A}_{M,\sigma}}$ (composée à partir d'une base orthonormée de $t_{\mathscr{A}}$ pour la forme de Riemann induite par σ), correspondant à des dérivations $(\partial_{1,\sigma},\dots,\partial_{g,\sigma})$. Soit D une dérivation d'ordre $T_{(k)}$ le long de $t_{\mathscr{A}_{M,\sigma}}$. On écrit

$$D = \sum_{\substack{\mathbf{i}\in\mathbb{N}^g\\|\mathbf{i}|=T_{(k)}}} d_{\mathbf{i}}\partial_{1,\sigma}^{i_1}\cdots\partial_{g,\sigma}^{i_g}.$$

La norme sur $S^{T_{(k)}}t_{\mathscr{A}_{M,\sigma}}$ est la norme quotient déduite de la projection :

$$t_{\mathscr{A}_{M,\sigma}}^{\otimes T_{(k)}} \to S^{T_{(k)}}\,t_{\mathscr{A}_{M,\sigma}}.$$

On a donc :

$$\|D\|^2 = \sum_{|\mathbf{i}|=T_{(k)}}|d_{\mathbf{i}}|^2\frac{\mathbf{i}!}{T_{(k)}!} \geq \Big(\sum_{|\mathbf{i}|=T_{(k)}}|d_{\mathbf{i}}|\Big)^2 \times g^{-T_{(k)}}.$$

De plus, on a :

$$\|Ds(x)\| \leq \sum_{|\mathbf{i}|=T_{(k)}} |d_{\mathbf{i}}| \left\| (\partial_{1,\sigma}^{i_1} \cdots \partial_{g,\sigma}^{i_g}) s(x) \right\|,$$

et on en déduit :

$$\|\phi_k(s)(x)\|_\sigma \leq g^{T_{(k)}/2} \max_{|\mathbf{i}|=T_{(k)}} \left\| (\partial_{1,\sigma}^{i_1} \cdots \partial_{g,\sigma}^{i_g}) s(x) \right\|.$$

En reprenant la définition de la métrique cubiste, on peut se ramener à la fonction θ correspondant à s ; notons que via le plongement étiré, la section s est une section sur A de degré $\leq 2M^2$. On note $\mathbf{u}$ un logarithme de $\sigma(x)$ ayant une norme hermitienne minimale sur $\mathbb{C}^g$. En tenant compte de l'action de ψ_M sur les dérivations, il vient :

$$\|\phi_k(s)(x)\|_\sigma \leq (Q\sqrt{g})^{T_{(k)}} e^{-3\pi M^2 \|\mathbf{u}\|_\sigma^2} \max_{|\mathbf{i}|=T_{(k)}} \left| \frac{1}{\mathbf{i}!} \left(\frac{\partial}{\partial z} \right)^{\mathbf{i}} \theta(\mathbf{u}+\mathbf{z})_{|\mathbf{z}=0} \right|.$$

De plus, par l'inégalité de Cauchy appliquée à θ, pour tout réel $r_C > 0$ (à ne pas confondre avec r, qui désigne la codimension de V), on a :

$$\max_{|\mathbf{i}|=T_{(k)}} \left| \frac{1}{\mathbf{i}!} \left(\frac{\partial}{\partial z} \right)^{\mathbf{i}} \theta(\mathbf{u}+\mathbf{z})_{|\mathbf{z}=0} \right| \leq \frac{1}{r_C^{T_{(k)}}} \sup_{\|\mathbf{z}\|_\sigma \leq r_C} |\theta(\mathbf{u}+\mathbf{z})|.$$

En revenant aux métriques cubistes, on trouve :

$$\|\phi_k(s)(x)\|_\sigma \leq \left(\frac{M\sqrt{g}}{r_C} \right)^{T_{(k)}} e^{3\pi M^2 (r_C^2 + 2 r_C \|\mathbf{u}\|_\sigma)} \|s\|_{\sup,\sigma}.$$

On choisit alors r_C de façon à optimiser la majoration :

$$r_C = \frac{\sqrt{g}}{M^2 \max\{1, \|\mathbf{u}\|_\sigma\}}.$$

Comme $M^2 \geq \sqrt{g}$ (par le choix des paramètres), cela donne :

$$\|\phi_k(s)(x)\|_\sigma \leq \left(M^3 \max\{1, \|\mathbf{u}\|_\sigma\} \right)^{T_{(k)}} e^{9\pi g} \|s\|_{\sup,\sigma}.$$

La norme sur $\mathcal{G}_k$ étant la norme de Löwner $\|\cdot\|_L$ associée à la norme du sup, elle est plus petite que celle-ci et on a finalement :

$$\|\phi_k(s)\|_{L,\sigma} \leq \left(M^3 \max\{1, \|\mathbf{u}\|_\sigma\} \right)^{T_{(k)}} e^{9\pi g} \|s\|_{\sup,\sigma},$$

Et, vu le choix de la norme L^2 sur $\mathcal{E}_M$:

$$\|\phi_k\|_\sigma \leq \left(M^3 \max\{1, \|\mathbf{u}\|_\sigma\} \right)^{T_{(k)}} e^{9\pi g} \sup_{\substack{s \in \mathcal{E}_M \\ s \neq 0}} \frac{\|s\|_{\sup,\sigma}}{\|s\|_{\mathrm{L}^2,\sigma}}.$$

La remarque 4.18 de [Gaudron 2006] montre que pour une certaine constante c_{13} ne dépendant que de g :

$$\frac{1}{[K':\mathbb{Q}]}\sum_{\sigma:K'\to\mathbb{C}}\log\max\{1,\|\mathbf{u}\|_\sigma\}\leq c_{13}\max\bigl\{1,\log^+h_F(A),\log h^0(A,L)\bigr\}.$$

De plus, d'après la même référence, lemme 4.16, il existe une autre constante c_{14} telle que :

$$\log\sup_{\substack{s\in\mathscr{E}_{M,\sigma}\\ s\neq 0}}\frac{\|s\|_{\sup,\sigma}}{\|s\|_{\mathrm{L}^2,\sigma}}\leq c_{14}\max\bigl\{1,\log^+(h_F(A)),\log(h^0(A,L))\bigr\}\log M^2.$$

La proposition suit en sommant sur les places archimédiennes, pour une constante c_{15} dépendant de A. □

Remarques. On aurait pu choisir différemment le paramètre r_C issu de l'inégalité de Cauchy, en prenant à la place : $r'_C = r_C \times M^2$. On aurait alors obtenu une majoration par $c_{15}(T_{(k)} + M^2)$, qui aurait été plus mauvaise dans notre contexte puisque tous les paramètres sauf M sont logarithmiques en $\deg_L(X)$. Jusqu'à la phase de descente (où cela ne semble plus possible), on pourrait travailler avec des termes en $\log\omega_L(V)$ à la place de $\log\deg_L V$, quitte à améliorer la proposition 3.12.

5D. ***Inégalité de pentes et conséquences.*** Pour pouvoir appliquer le théorème des pentes, on doit s'assurer que le morphisme ϕ est injectif. On y travaillera dans la partie suivante, et on suppose par avance ici cette injectivité.

Contradiction sous l'injectivité de ϕ. On suppose par l'absurde que (4-2) est vérifié. Puisqu'on a aussi supposé que ϕ est injectif, on peut donc utiliser l'inégalité des pentes du lemme 3.7 :

$$\widehat{\deg}\,\overline{\mathscr{E}}_M\leq\sum_{k\in I}\dim(E_k/E_{k+1})\bigl(\hat{\mu}_{\max}(\overline{\mathscr{G}}_k)+h(\phi_k)\bigr).$$

Soit $k>0$ un entier. On veut d'abord montrer que la contribution du k-ème terme dans la somme précédente est négative. On regroupe pour commencer les estimations faites sur le morphisme ϕ_k, à savoir les majorations archimédiennes et ultramétriques. L'entier k est par définition n-lié à tout idéal premier $\mathfrak{q}$ de $\mathbb{O}_{K'}$ au-dessus d'un seul premier $\mathfrak{p}$ de $\mathscr{P}_A$. On note p son image dans $\mathbb{Z}$; on a alors (par les propositions 5.4 et 5.5) :

$$\begin{aligned}h(\phi_k)&=\frac{1}{[K':\mathbb{Q}]}\sum_{v\in M(K')}\log\|\phi_k\|_v\leq c_{15}T_n\log M-\frac{1}{[K':\mathbb{Q}]}\sum_{\mathfrak{q}|\mathfrak{p}}n_{\mathfrak{q}}(T_{n-1}-T_n)\frac{\log p}{p}\\&\leq c_{15}T_n\log M-\frac{1}{[K:\mathbb{Q}]}\bigl(T_{n-1}-T_n\bigr)\frac{\log p}{p},\end{aligned}$$

où on a utilisé l'égalité classique [Lang 1994, II, Corollary 1 to Theorem 2],

$$\sum_{\mathfrak{q}|\mathfrak{p}} n_{\mathfrak{q}} = [K' : K].$$

On majore ensuite :

$$\begin{aligned}
&\hat{\mu}_{\max}(\overline{\mathscr{G}_k}) + h(\phi_k) \\
&\quad \le c_{16}\big(M^2 \hat{\mu}_L^{\mathrm{ess}}(X) + T_n \log(M + T_n) + \log \deg_L(X)\big) - \frac{1}{[K:\mathbb{Q}]} T_{n-1} \frac{\log p}{p} \\
&\quad \le c_{16}\big(M^2 \hat{\mu}_L^{\mathrm{ess}}(X) + T_n \log(M + T_n) + \log \deg_L(X)\big) - \frac{1}{[K:\mathbb{Q}]} T_{n-1} \frac{\log N_n}{N_n},
\end{aligned}$$

pour une constante c_{16} ne dépendant que de A, car $p \le N_n$ et la fonction $\log(x)/x$ est décroissante pour $x \ge 3$. Le choix du paramètre M (voir 4D) et l'hypothèse (4-2) sur le minimum essentiel donnent :

$$M^2 \hat{\mu}_L^{\mathrm{ess}}(X) \le 2\Delta.$$

On a aussi, par l'hypothèse (4-1) et la définition des paramètres :

$$\begin{aligned}
\log(M + T_n) &\le \log\big(2T_0 \omega_L(\Delta T_0, X)\big) \le \log\big(2\Delta T_0^2 \, |H_0| \, \deg_L(V)\big) \\
&\le C_0 \log(\Delta) + \Delta + \log \deg_L(V) \le 2\Delta.
\end{aligned}$$

On en déduit :

$$\hat{\mu}_{\max}(\overline{\mathscr{G}_k}) + h(\phi_k) \le c_{16}\big(2\Delta + 2\Delta T_n + 2\Delta\big) - \frac{T_{n-1}}{N_n} \le 6c_{16}\Delta T_n - \frac{T_{n-1}}{N_n} \le 0,$$

la dernière inégalité résultant de la définition des T_n par récurrence descendante. Il suit, puisque l'estimation qu'on vient de faire est encore valable pour $k = 0$ sans le raffinement ultramétrique :

$$\widehat{\deg}\, \overline{\mathscr{E}_M} \le \dim(E_0/E_1)\big(\hat{\mu}_{\max}(\overline{\mathscr{G}_0}) + h(\phi_0)\big) \le \operatorname{rg} \mathscr{G}_0 \, (5c_{16}\Delta T_0).$$

On a pu remplacer $\dim(E_0/E_1)$ par $\operatorname{rg}(\mathscr{G}_0)$ en utilisant l'injectivité de ϕ, et parce que la hauteur est majorée par un terme positif. En combinant le lemme 4.2 (par le choix des paramètres que $\log M$ est plus grand que n'importe quelle constante) et le corollaire 5.3 avec $k = 0$, on obtient :

$$c_{10}(M)^{2g} \log M \le \frac{g(2M^2)^g}{\Delta T_0}(5c_{16}\Delta T_0),$$

et on rappelle que $c_{10} > 0$. On en déduit la contradiction suivante :

$$\log M \le \frac{5g2^g c_{16}}{c_{10}}. \qquad \square$$

6. Lemme de zéros et injectivité du morphisme

Il nous reste à assurer l'injectivité du morphisme de restriction. On procède par l'absurde, en commençant par écrire un lemme de zéros. Une étude combinatoire (paragraphe 6B) nous amène à une « quasi-contradiction » (paragraphe 6C). On conclut par un argument de descente sur des variétés (paragraphe 6D), qu'on détaille ici en petite codimension $r \leq 2$.

6A. ***Lemme de zéros.*** Le lemme de zéros dont on a besoin ici s'inscrit dans la tradition des théorèmes démontrés par Philippon [1995], dont on reprend le formalisme. Ce lemme est l'analogue abélien du théorème utilisé dans [Amoroso et David 2003], à une différence près : on prend en compte les multiplicités, et ce à l'aide de la notion de dessous d'escalier, qui permet d'envisager des multiplicités différenciées selon les directions. Dans le cas qui nous intéresse, il est utile d'envisager la multiplicité finale dans le lemme de zéros. On ne fait pas usage, cependant, de multiplicités différentes selon les directions.

Remarque. On a pris la multiplicité finale T_r dans l'inégalité de pentes égale à 1 mais la multiplicité finale dans le lemme de zéros est un certain T_{r_0}, pour $r_0 \leq r$, et n'est pas forcément nulle.

Soient $Z = \sum_i n_i \cdot Z_i$ et $Z' = \sum_i n'_i \cdot Z_i$ deux cycles algébriques (quitte à rajouter des zéros, on peut supposer que la somme porte sur les mêmes composantes). On définit leur *réunion*, notée $Z \cup Z'$, comme le cycle $\sum \max_i\{n_i, n'_i\} \cdot Z_i$. Le *degré* du cycle $\sum_i n_i \cdot Z_i$ sera l'entier $\sum_i n_i \deg_L(Z_i)$. Soit A une variété abélienne munie d'un fibré L ample. On considère la base de dérivations sur A définie en 4C. Un ensemble $E \subset \mathbb{N}^g$ est un escalier si pour tout $\beta \in E$, on a $\beta + \mathbb{N}^g \subset E$. Un sous-ensemble de $\mathbb{N}^g$ est un dessous d'escalier s'il est le complémentaire d'un escalier. Si W est le dessous d'un escalier E de $\mathbb{N}^g$, et si on a des indices $1 \leq i_1 < \cdots < i_r \leq g$, on note $\mathscr{C}_{i_1,\ldots,i_r}(W)$ l'enveloppe convexe dans $\mathbb{R}^r_+$ de la trace de E sur la r-face de $\mathbb{N}^g$ définie par $(i_1, \ldots, i_r)$.

On appelle aussi ensemble pondéré un sous-ensemble Σ de $\mathbb{N}^g \times A$ tel que pour tout $x \in A$, l'ensemble $W_{x,\Sigma} = (\mathbb{N}^g \times \{x\}) \cap \Sigma$ soit un dessous d'escalier (éventuellement vide). On appelle support de Σ, noté $\mathrm{Supp}(\Sigma)$, sa projection sur A. Si Σ et Σ' sont deux ensembles pondérés, on définit $\Sigma + \Sigma'$ comme l'ensemble des couples $(x + x', \lambda + \lambda')$, pour $(x, \lambda) \in \Sigma$, et $(x', \lambda') \in \Sigma'$; c'est aussi un ensemble pondéré. On a $E + \varnothing = \varnothing$ et si E est un sous-ensemble de A, on l'identifie à l'ensemble pondéré $\{0\} \times E$.

On dit que $f \in H^0(A, L)$ s'annule sur un ensemble pondéré Σ si pour tout $(x, \lambda) \in \Sigma$, on a $\partial_x^\lambda f = 0$. Si V est une sous-variété de codimension r de A et W un dessous d'escalier, on pose :

$$m_W(V) = r! \max_{\substack{x \in V \\ 1 \leq i_1 < \cdots < i_r \leq g}} \mathrm{vol}\big(\mathbb{R}^r_+ \setminus \mathscr{C}_{i_1,\ldots,i_r}(W)\big);$$

le maximum porte sur $x \in X$ et les r-faces de $\mathbb{N}^g$ telles que $(\partial_{i_1,x}, \dots, \partial_{i_r,x})$ forment une base du quotient $t_{A,x}/t_{V,x}$.

Théorème 6.1. *Soit V une sous-variété de A, de codimension r, $\tilde{M} \geq 1$ un entier et $\Sigma_0, \dots, \Sigma_r$ des ensembles pondérés finis à support dans $A(\overline{K})$ tels que pour tout $1 \leq n \leq r$:*

$$\mathrm{Supp}(\Sigma_n) = \bigcup_{l=1\dots s_n} H_{n,l},$$

où les $H_{n,l}$ sont des sous-groupes de $A(\overline{K})$; et pour tout $x \in \mathrm{Supp}(\Sigma_n)$, W_{x,Σ_n} ne dépend pas de x. Soit de plus $f \in H^0(A, L^{\otimes \tilde{M}})$, non nulle, qui s'annule sur $V + \Sigma_0 + \cdots + \Sigma_r$. Alors il existe une constante c_{17} ne dépendant que de A, deux entiers $1 \leq r_0 \leq r_1 \leq r$, des indices $j_0, \dots, j_{r_0-1}$ avec $1 \leq j_l \leq s_l$ pour $l = 0 \dots r_0 - 1$, et des sous-variétés algébriques Z_j $(j = 1, \dots, s_{r_0})$ strictes de A, de codimension r_1, contenant au moins une composante isolée de

$$\mathrm{Supp}\big(H_{0,j_0} + \cdots + H_{r_0-1,j_{r_0-1}} + \Sigma_{r_0} + \cdots + \Sigma_r + V\big),$$

telles que :

$$\deg_L \left(\bigcup_{x \in H_{0,j_0} + \cdots + H_{r_0-1,j_{r_0-1}}} \bigcup_{\substack{j=1\dots s_{r_0} \\ y \in H_{r_0,j}}} m_{W_{y,\Sigma_{r_0}}}(x+y+Z_j) \cdot (x+y+Z_j) \right) \leq c_{17} \tilde{M}^{r_1}.$$

Démonstration. Il s'agit d'un cas particulier du résultat principal de [Galateau 2009], énoncé dans le cadre plus général des groupes algébriques commutatifs. □

6B. ***Degré d'une sous-variété obstructrice.*** On reprend les hypothèses et notations des parties 4 et 5 et on rappelle que :

$$X = V + H_0,$$

où V est une variété et H_0 est un sous-groupe fini de A. On suppose enfin que le cardinal $|H_0|$ est premier à tous les premiers des $\mathcal{P}_{n,\mathbb{Z}}$, pour $1 \leq n \leq r$. Si p est un nombre premier de $\bigcup_{1 \leq n \leq r} \mathcal{P}_{n,\mathbb{Z}}$ et $\mathfrak{p} | p$ dans $\mathbb{C}_K$, on désigne par $\mathrm{Ker}[p]_{\mathfrak{p}}$ le groupe des points de p-torsion se réduisant sur 0 modulo $\mathfrak{p}$.

Si $l = \prod_{n=1}^{r} p_n$ avec $p_n \in \mathcal{P}_{n,\mathbb{Z}} \cup \{1\}$ pour tout $1 \leq n \leq r$, on note :

$$\mathrm{Ker}[l]^* = \bigoplus_n \mathrm{Ker}[p_n]_{\mathfrak{p}_n}.$$

Cette somme est bien directe car le choix des paramètres implique que les $\mathcal{P}_{n,\mathbb{Z}}$ sont deux-à-deux disjoints. Notre but, jusqu'à la fin de cette partie, sera de démontrer la proposition suivante, pour un bon choix du fermé X (dont dépend la construction du morphisme) :

Proposition 6.2. *Le morphisme $\phi : E \to F$ est injectif.*

On va supposer que ce n'est pas le cas et obtenir une contradiction en appliquant le lemme de zéros du paragraphe précédent. Celui-ci permet de majorer le degré d'une réunion de sous-variétés. On souhaite se ramener à une seule sous-variété obstructrice, et utiliser le fait que la réunion est largement distincte. On y arrive par un travail sur le stabilisateur, dont on rappelle la définition :

Définition 6.3. Si Z est un fermé inclus dans A, on appelle stabilisateur de Z, noté $\mathrm{Stab}(Z)$, le groupe :

$$\{x \in A : x + Z = Z\} = \bigcap_{x \in Z} (Z - x).$$

On a les propriétés suivantes (voir [Amoroso et David 1999, 2], qui se transpose immédiatement aux variétés abéliennes) :

$$\dim \mathrm{Stab}(Z) \leq \dim Z, \quad \deg_L(\mathrm{Stab}(Z)) \leq \deg_L(Z)^{\dim Z+1}.$$

Proposition 6.4. *Il existe une constante c_{19}, des entiers $r_0 \leq r_1 \leq r$ strictement positifs, un entier $l \in \mathcal{P}_{1,\mathbb{Z}} \cdots \mathcal{P}_{r_0,\mathbb{Z}}$, et une sous-variété Z stricte de A, de codimension r_1 contenant un translaté de V par un point de torsion, tels que* :

$$T_{r_0}^{r_1} |\mathcal{P}_{r,\mathbb{Z}}| \, \frac{|H_0|}{|H_0 \cap \mathrm{Stab}(Z)|} \, \frac{l^g}{|\mathrm{Ker}[l]^* \cap \mathrm{Stab}(Z)|} \deg_L(Z) \leq c_{19} M^{2r_1} \Delta .$$

Pour simplifier les calculs qui viennent, on pose :

$$f(H_0, Z) = \frac{|H_0|}{|\mathrm{Stab}(Z) \cap H_0|}.$$

Démonstration. Si le morphisme ϕ n'est pas injectif, il existe une section $f \in H^0(A, L^{\otimes M^2+1})$ qui s'annule sur $\bigcup_{i \in I} V(X_i, t_A, T_{(i)})$. Par définition des voisinages infinitésimaux, ceci implique que f s'annule sur $X + \Sigma_1 + \cdots + \Sigma_r$, où l'ensemble Σ_n, pour $1 \leq n \leq r$, est pondéré de support :

$$\mathrm{Supp}(\Sigma_n) = \mathrm{Tor}_{A,n} = \bigcup_{\mathfrak{p} \in \mathcal{P}_n} \mathrm{Ker}[p]_{\mathfrak{p}};$$

et de dessous d'escalier ne dépendant pas de $x \in \mathrm{Supp}(\Sigma_n)$ défini par :

$$\sum_{k=1}^{g} \lambda_k \leq T_n.$$

Il existe donc, par le théorème précédent, deux entiers r_0 et r_1 tels que $r_0 \leq r_1 \leq r$, des couples d'idéaux premiers $(p_1, \mathfrak{p}_1), \ldots, (p_{r_0-1}, \mathfrak{p}_{r_0-1})$ avec $\mathfrak{p}_n \in \mathcal{P}_n$ (pour $1 \leq n \leq r_0 - 1$) et des sous-variétés strictes $Z_{\mathfrak{p}}$ de A (pour tout $\mathfrak{p} \in \mathcal{P}_{r_0}$), de codimension

r_1, tels que :

$$\deg_L\left(\bigcup_{\mathfrak{p}\in\mathcal{P}_{r_0}}\ \bigcup_{\zeta\in\bigoplus_n \mathrm{Ker}[p_n]_{\mathfrak{p}_n}\oplus H_0} m_{W_{\zeta_{r_0},\Sigma_{r_0}}}(\zeta+Z_{\mathfrak{p}})\cdot(\zeta+Z_{\mathfrak{p}})\right)\leq 2^{r_1}c_{17}M^{2r_1},$$

où on a écrit $\mathfrak{p}_{r_0}=\mathfrak{p}$, pour unifier l'écriture dans la somme directe, et où ζ_{r_0} est la composante selon r_0 de ζ dans la somme directe. De plus, pour tout $\mathfrak{p}\in\mathcal{P}_{r_0}$, la variété $Z_{\mathfrak{p}}$ contient un translaté de V par un point de torsion.

La multiplicité se calcule immédiatement. Soit $\mathfrak{p}\in\mathcal{P}_{r_0}$ et

$$\zeta\in H_0\oplus\bigoplus_n \mathrm{Ker}[p_n]_{\mathfrak{p}_n};$$

on a :

$$m_{W_{\zeta_{r_0},\Sigma_{r_0}}}(\zeta+Z_{\mathfrak{p}})=r_1!\,T_{r_0}^{r_1}\mathrm{vol}(\{u_1+\cdots+u_{r_1}<1\})=T_{r_0}^{r_1}.$$

Cette multiplicité ne dépend pas de la variété dans la réunion, donc on peut la mettre en facteur.

Les entiers r_0 et r_1 sont déjà déterminés ; posons $l_0=p_1\cdots p_{r_0-1}$. Choisissons, pour tout premier $p\in\mathcal{P}_{r_0,\mathbb{Z}}$, un idéal premier $\mathfrak{p}$ de $\mathcal{P}_{r_0}$ divisant p tel que la quantité :

$$\frac{f(H_0,Z_{\mathfrak{p}})(l_0p)^g}{\left|\mathrm{Ker}[l_0p]^*\cap\mathrm{Stab}(Z_{\mathfrak{p}})\right|}\deg_L(Z_{\mathfrak{p}})$$

soit minimale parmi les premiers de $\mathcal{P}_{r_0}$divisant p. Prenons aussi $\mathfrak{p}_{r_0}\in\mathcal{P}_{r_0}$ (et p_{r_0}) tels que cette même quantité soit minimale parmi tous les premiers de $\mathcal{P}_{r_0}$. On pose $l=l_0p_{r_0}$ et $Z=Z_{\mathfrak{p}_{r_0}}$. Il suffit donc de majorer cette quantité pour obtenir la proposition. Rappelons que la somme :

$$\mathrm{Ker}[l_0]^*=\bigoplus_{n=1}^{r_0-1}\mathrm{Ker}[p_n]_{\mathfrak{p}_n}$$

est bien directe car, les premiers p_n étant deux-à-deux distincts, on peut écrire une relation de Bézout entre un des p_n et tous les autres. On partitionne $\mathcal{P}_{r_0,\mathbb{Z}}$ en introduisant la relation d'équivalence suivante :

$$p\sim p'\iff \text{il existe } \gamma\in H_0\oplus\mathrm{Ker}[l_0]^*\oplus\bigoplus_{p_i\in\mathcal{P}_{r_0,\mathbb{Z}}}\mathrm{Ker}[p_i]_{\mathfrak{p}_i}\text{ tel que }\gamma+Z_{\mathfrak{p}}=Z_{\mathfrak{p}'},$$

et on note $(\mathscr{C}_1,\ldots,\mathscr{C}_s)$ les différentes classes d'équivalence associées. Si p et p' appartiennent à des classes différentes, les réunions

$$\bigcup_{\zeta\in H_0\oplus\mathrm{Ker}[l_0]^*\oplus\mathrm{Ker}[p]_{\mathfrak{p}}}\zeta+Z_{\mathfrak{p}}$$

n'ont aucune composante en commun et on peut additionner les degrés. Le choix d'un seul idéal de $\mathcal{P}_{r_0}$ au-dessus d'un nombre premier restreint la réunion. On a

donc :

$$T_{r_0}^{r_1}\sum_{j=1}^{s}\deg_L\left(\bigcup_{p\in\mathscr{C}_j}\ \bigcup_{\zeta\in H_0\oplus\mathrm{Ker}[l_0]^*\oplus\mathrm{Ker}[p]_{\mathfrak{p}}}\zeta+Z_{\mathfrak{p}}\right)\leq 2^{r_1}c_{17}M^{2r_1}.$$

Soit $p\in\mathscr{P}_{r_0,\mathbb{Z}}$ et soit $\mathfrak{p}$ l'idéal qui lui est associé ; le stabilisateur de $Z_{\mathfrak{p}}$ ne dépend que de la classe d'équivalence de p puisque si p' (associé à $\mathfrak{p}'$) est dans la même classe que p, $Z_{\mathfrak{p}'}$ est un translaté de $Z_{\mathfrak{p}}$. On appelle $\mathscr{S}_j$ le stabilisateur commun aux $Z_{\mathfrak{p}}$, pour $\mathfrak{p}$ associé à $p\in\mathscr{C}_j$. Dans chaque classe $\mathscr{C}_j$, on fixe un premier $\rho_j\in\mathscr{C}_j$ et on note Z_{ρ_j} la variété qui lui est associée. Pour tout autre premier $p\in\mathscr{C}_j$, il existe donc des éléments $\alpha_p\in\bigoplus_{p_i\in\mathscr{P}_{r_0,\mathbb{Z}}}\mathrm{Ker}[p_i]_{\mathfrak{p}_i}$ et $\eta_p\in H_0\oplus\mathrm{Ker}[l_0]^*$ tels que :

$$\alpha_p+\eta_p+Z_{\mathfrak{p}}=Z_{\rho_j}.$$

Remarquons que la somme est directe car tous les p_i sont distincts. Soient $p\neq p'$ dans la même classe $\mathscr{C}_j$; soient $\omega_p\in\mathrm{Ker}[p]_{\mathfrak{p}}$ et $\omega_{p'}\in\mathrm{Ker}[p']_{\mathfrak{p}'}$. Si les réunions

$$\bigcup_{\zeta\in H_0\oplus\mathrm{Ker}[l_0]^*}\zeta+\omega_\xi+Z_\xi \tag{6-1}$$

pour $\xi=p$ et $\xi=p'$ ont au moins une composante commune, c'est qu'il existe un élément $\eta_{p,p'}\in H_0\oplus\mathrm{Ker}[l_0]^*$ tel que :

$$\omega_p+Z_p=\eta_{p,p'}+\omega_{p'}+Z_{p'}.$$

On en déduit, grâce aux deux dernières égalités, que :

$$x=\alpha_p-\omega_p-\alpha_{p'}+\omega_{p'}+(\eta_p-\eta_{p'}+\eta_{p,p'})\in\mathscr{S}_j.$$

On note $\alpha_p^{p_i}$ la composante selon p_i de α_p. On remarque que : $\alpha_p^p-\alpha_{p'}^p-\omega_p\in\mathrm{Ker}[p]_{\mathfrak{p}}$. De même, $\alpha_{p'}^{p'}-\alpha_p^{p'}-\omega_{p'}\in\mathrm{Ker}[p']_{\mathfrak{p}'}$ et $\eta_{p'}-\eta_p+\eta_{p,p'}\in H_0\oplus\mathrm{Ker}[l_0]^*$. Le nombre p est premier à p', à l_0, à H_0 et à tous les autres premiers de $\mathscr{P}_{r_0,\mathbb{Z}}$. Il existe donc une relation de Bézout :

$$up+vl_0\prod_{p_i\neq p\in\mathscr{P}_{r_0,\mathbb{Z}}}p_i=1.$$

On en déduit que :

$$\left[vl_0\prod_{p_i\neq p\in\mathscr{P}_{r_0,\mathbb{Z}}}p_i\right]x=\left[vl_0\prod_{p_i\neq p\in\mathscr{P}_{r_0,\mathbb{Z}}}p_i\right](\alpha_p^p-\alpha_{p'}^p-\omega_p)=\alpha_p^p-\alpha_{p'}^p-\omega_p\in\mathscr{S}_j,$$

puisqu'il suit de sa définition que le stabilisateur est stable sous la multiplication par n, quel que soit $n\in\mathbb{N}$. Par contraposition, si :

$$\omega_p\in\mathrm{Ker}[p]_{\mathfrak{p}}\setminus(\alpha_p^p-\alpha_{p'}^p-\mathscr{S}_j)\quad\text{et}\quad\omega_{p'}\in\mathrm{Ker}[p']_{\mathfrak{p}'}\setminus(\alpha_{p'}^{p'}-\alpha_p^{p'}+\mathscr{S}_j),$$

les réunions (6-1) n'ont pas de composantes communes. Il suit :

$$\deg_L\Big(\bigcup_{p\in\mathscr{C}_j}\ \bigcup_{\zeta\in H_0\oplus\mathrm{Ker}[l_0]^*}\ \bigcup_{\xi\in\mathrm{Ker}[p]_{\mathfrak{p}}}\zeta+\xi+Z_{\mathfrak{p}}\Big)$$
$$\geq\sum_{p\in\mathscr{C}_j}\deg_L\Big(\bigcup_{\zeta\in H_0\oplus\mathrm{Ker}[l_0]^*}\ \bigcup_{\xi\in\mathrm{Ker}[p]_{\mathfrak{p}}\setminus\bigcup_i(\alpha_p^p-\alpha_{p_i}^p+\mathscr{S}_j)}\zeta+\xi+Z_{\mathfrak{p}}\Big).$$

Fixons j et $p\in\mathscr{C}_j$. On va calculer le degré de la réunion totale en fonction de $\deg_L(Z_{\mathfrak{p}})$. Par choix de l'ensemble $\mathscr{P}_A$, il y a p^g points se réduisant sur 0 mod $\mathfrak{p}$, et il y a l_0^g points dans $\mathrm{Ker}[l_0]^*$. Il en résulte :

$$\deg_L\Big(\bigcup_{\zeta\in H_0\oplus\mathrm{Ker}[l_0]^*}\ \bigcup_{\xi\in\mathrm{Ker}[p]_{\mathfrak{p}}}\zeta+\xi+Z_{\mathfrak{p}}\Big)=\frac{f(H_0,Z_{\mathfrak{p}})(l_0p)^g}{\big|\mathscr{S}_j\cap\mathrm{Ker}[l_0p]^*\big|}\deg_L(Z_{\mathfrak{p}}).\quad(6\text{-}2)$$

A cette réunion, il faut retrancher :

$$\deg_L\Big(\bigcup_{\zeta\in H_0\oplus\mathrm{Ker}[l_0]^*}\ \bigcup_{\xi\in\bigcup_i(\alpha_p^p-\alpha_{p_i}^p+\mathscr{S}_j)}\zeta+\xi+Z_{\mathfrak{p}}\Big)\leq\frac{f(H_0,Z_{\mathfrak{p}})|\mathscr{C}_j|l_0^g}{\big|\mathscr{S}_j\cap\mathrm{Ker}[l_0]^*\big|}\deg_L(Z_{\mathfrak{p}}).$$

En effet, il y a au plus $|\mathscr{C}_j|$ points de la forme $\alpha_{p_i}^p$. Notons $\tilde{\mathscr{C}}_j$ le sous-ensemble de $\mathscr{C}_j$ formé des p divisant $[\mathscr{S}_j:\mathscr{S}_j^0]$, où $\mathscr{S}_j^0$ désigne la composante connexe de l'identité dans $\mathscr{S}_j$. Si $p\notin\tilde{\mathscr{C}}_j$, les dénominateurs des deux dernières formules sont égaux et on a :

$$\deg_L\Big(\bigcup_{\zeta\in H_0\oplus\mathrm{Ker}[l_0]^*}\ \bigcup_{\xi\in\mathrm{Ker}[p]_{\mathfrak{p}}\setminus\bigcup_i(\alpha_p^p-\alpha_{p_i}^p+\mathscr{S}_j)}\zeta+\xi+Z_{\mathfrak{p}}\Big)$$
$$\geq\Big(1-\frac{|\mathscr{C}_j|}{p^2}\Big)\frac{f(H_0,Z_{\mathfrak{p}})(l_0p)^g}{\big|\mathscr{S}_j\cap\mathrm{Ker}[l_0p]^*\big|}\deg_L(Z_{\mathfrak{p}}).$$

Le quotient $1/p^2$ provient du fait que la « partie discrète » du stabilisateur de $Z_{\mathfrak{p}}$ est triviale et que sa composante connexe en 0 est un groupe algébrique de codimension $\geq r+1\geq 2$. En fixant j, on somme sur l'ensemble des p ; en tenant compte de la définition de Z, on obtient :

$$\deg_L\Big(\bigcup_{p\in\mathscr{C}_j}\ \bigcup_{\zeta\in H_0\oplus\mathrm{Ker}[l_0]^*}\ \bigcup_{\xi\in\mathrm{Ker}[p]_{\mathfrak{p}}}\zeta+Z_{\mathfrak{p}}\Big)$$
$$\geq\Big(|\mathscr{C}_j\setminus\tilde{\mathscr{C}}_j|-|\mathscr{C}_j|\sum_{p\in\mathscr{C}_j}\frac{1}{p^2}\Big)\frac{f(H_0,Z)(l)^g}{\big|\mathrm{Ker}[l]^*\cap\mathrm{Stab}(Z)\big|}\deg_L(Z)$$
$$\geq\big(\tfrac{2}{3}|\mathscr{C}_j|-|\tilde{\mathscr{C}}_j|\big)\frac{f(H_0,Z)(l)^g}{\big|\mathrm{Ker}[l]^*\cap\mathrm{Stab}(Z)\big|}\deg_L(Z),$$

par la définition de l'ensemble $\mathcal{P}_A$. On a plus directement, par (6-2) et la définition de Z :

$$\deg_L\left(\bigcup_{p\in\mathscr{C}_j}\ \bigcup_{\zeta\in H_0\oplus\mathrm{Ker}[l_0]^*}\ \bigcup_{\xi\in\mathrm{Ker}[p]_{\mathfrak{p}}}\zeta+Z_{\mathfrak{p}}\right)\geq\frac{f(H_0,Z)(l)^g}{\left|\mathrm{Ker}[l]^*\cap\mathrm{Stab}(Z)\right|}\deg_L(Z).$$

On doit donc estimer le nombre de premiers divisant $[\mathcal{S}_j:\mathcal{S}_j^0]$. Or :

$$|\tilde{\mathscr{C}}_j|\leq\frac{\log[\mathcal{S}_j:\mathcal{S}_j^0]}{\log 3}\leq\log\deg_L(\mathcal{S}_j)\leq c_{18}\Delta,$$

pour une constante c_{18}. On a ici majoré le degré du stabilisateur en fonction de celui de la variété [Hindry 1988, lemme 6], puis on a utilisé le lemme de zéros pour majorer $\deg_L(Z_{\rho_j})$, et on a majoré $\log M$ à l'aide du choix des paramètres. Par l'inégalité $\max\{x-y;1\}\geq x/2y$ pour $x\geq 0$ et $y\geq 1$, on obtient :

$$\max\{\tfrac{2}{3}|\mathscr{C}_j|-|\tilde{\mathscr{C}}_j|,1\}\geq\frac{|\mathscr{C}_j|}{3c_{18}\Delta}.$$

La proposition suit en sommant sur les classes d'équivalence. □

6C. ***Un premier pas vers l'injectivité.*** Le choix des paramètres va donner une inégalité « presque absurde" ; on ne pourra cependant pas conclure, car il manquera une hypothèse de coprimalité sur des objets construits simultanément pendant la phase diophantienne.

Proposition 6.5. *On suppose que X n'est pas incluse dans le translaté d'une sous-variété abélienne et que son minimum essentiel est majoré de la façon suivante* :

$$\hat{\mu}_L^{\mathrm{ess}}(X)\omega_L(X)<\frac{1}{\Delta^{8\rho(2r)^{r+1}}}.$$

Alors il existe une sous-variété stricte Z de codimension $r_1\leq r$ contenant un translaté de V par un point de torsion et un entier $l>0$ tels que :

– *L'entier l est premier avec R et* :

$$l\leq\Delta^{2\rho(2r)^{r+1}}.$$

– *De plus, on a l'inégalité* :

$$\left(\frac{f(H_0,Z)l^g}{\left|\mathrm{Ker}[l]^*\cap\mathrm{Stab}(Z)\right|}\deg_L(Z)\right)^{1/r_1}<\Delta^{-\rho}l\omega_L(l,X).$$

Démonstration. On commence par montrer que la contrainte portant ici sur le minimum essentiel est plus forte que l'hypothèse (4-2). Si (4-2) n'est pas vérifiée :

$$\hat{\mu}_L^{\mathrm{ess}}(X)\geq\frac{\Delta}{T_0\omega_L(\Delta T_0,X)}\geq\frac{1}{T_0^2\omega_L(X)},$$

par application du lemme 4.5. De plus, par les choix de paramètres faits en 4D :

$$T_0^2 \leq \Delta^{2r} \prod_{n=1}^{r} N_n^4 \leq \Delta^{8\rho(2r)^{r+1}},$$

ce qui contredit l'hypothèse de la proposition. Pour démontrer cette inégalité, on a d'abord utilisé :

$$N_1 \cdots N_r \leq \Delta^{\rho[(2r)^2+\cdots+(2r)^{r+1}]}; \tag{6-3}$$

puis on a majoré l'exposant comme suit :

$$\sum_{j=2}^{r+1}(2r)^j \leq -r + \sum_{j=1}^{r+1}(2r)^j \leq 2(2r)^{r+1} - r,$$

par l'inégalité :

$$1 + x + \cdots + x^h \leq 2x^h \quad \text{pour } h \in \mathbb{N} \text{ et } x \geq 2.$$

La proposition précédente nous donne donc l'existence de trois entiers strictement positifs r_0, r_1, l avec $r_0 \leq r_1 \leq r$ et $l \in \mathcal{P}_{1,\mathbb{Z}} \cdots \mathcal{P}_{r_0,\mathbb{Z}}$, et une sous-variété algébrique Z stricte de A, de codimension r_1, contenant un translaté de V par un point de torsion, telle que :

$$T_{r_0}^{r_1} |\mathcal{P}_{r_0,\mathbb{Z}}| \, \frac{f(H_0, Z) l^g}{\left|\mathrm{Ker}[l]^* \cap \mathrm{Stab}(Z)\right|} \deg_L(Z) \leq c_{19} M^{2r_1} \Delta.$$

Par construction des $\mathcal{P}_{n,\mathbb{Z}}$, l'entier l est premier avec R et on a les inégalités :

$$2^{-r_0} N_1 \cdots N_{r_0} \leq l \leq N_1 \cdots N_{r_0}.$$

Et le premier point suit, par la même majoration que (6-3).

Reste à prouver la seconde inégalité. Le théorème des nombres premiers et le choix de l'ensemble $\mathcal{P}_A$ font que, pour une certaine constante $c_{20} > 0$ ne dépendant que de A :

$$|\mathcal{P}_{r_0,\mathbb{Z}}| \geq c_{20} \frac{N_{r_0}}{\log N_{r_0}} - \frac{\log R}{\log 2}.$$

Par définition des N_n et de Δ, on a $\log N_{r_0} \leq \Delta^{1/2}$ pour C_0 assez grand dans la définition de Δ. On a aussi :

$$N_{r_0} \geq \Delta^9 \geq \log(R)^2.$$

On a encore, pour C_0 assez grand, $\frac{1}{2} c_{20} \Delta^{1/2} \geq 1$, le facteur $\frac{1}{2}$ correspondant au terme en $\log R$. On en déduit :

$$|\mathcal{P}_{r_0,\mathbb{Z}}| \geq \Delta^{\rho(2r)^{r+2-r_0}-1}.$$

Par [Amoroso et David 2003, lemme 2.4], comme $l \leq N_1 \cdots N_r \leq \Delta T_0$, on a :

$$\omega_L(\Delta T_0, X) \leq \frac{\Delta T_0}{l} \omega_L(l, X).$$

Puis :

$$\begin{aligned}\left(\frac{f(H_0,Z)l^g}{\left|\mathrm{Ker}[l]^*\cap\mathrm{Stab}(Z)\right|}\deg_L(Z)\right)^{1/r_1} &\le \frac{c_{19}M^2\Delta^{1/r_1}}{|\mathcal{P}_{r_0,\mathbb{Z}}|^{1/r_1}T_{r_0}}\\ &\le 2c_{19}\frac{T_0\omega_L(\Delta T_0,X)\Delta^{1/r_1}}{|\mathcal{P}_{r_0,\mathbb{Z}}|^{1/r_1}T_{r_0}}\\ &\le 2c_{19}\frac{\Delta T_0^2\Delta^{1/r_1}}{l|\mathcal{P}_{r_0,\mathbb{Z}}|^{1/r_1}T_{r_0}}\omega_L(l,X).\end{aligned}$$

Or on a :

$$\frac{T_0}{T_{r_0}}\le\Delta^{2r_0}N_1\cdots N_{r_0}\le(2\Delta)^{2r_0}l,$$

et on en déduit :

$$\left(\frac{f(H_0,Z)l^g}{\left|\mathrm{Ker}[l]^*\cap\mathrm{Stab}(Z)\right|}\deg_L(Z)\right)^{1/r_1}\le c_{21}\frac{l\Delta^{2r+1+1/r_1}N_{r_0+1}\cdots N_r}{|\mathcal{P}_{r_0,\mathbb{Z}}|^{1/r_1}}\omega_L(l,X).$$

L'exposant h de Δ dans cette dernière majoration est borné par :

$$\begin{aligned}h &:= 4r+2\rho\big((2r)^2+\cdots+(2r)^{r+1-r_0}\big)-\big(\rho(2r)^{r+2-r_0}-2\big)/r_1.\\ &\le 2\rho\big((2r)+\cdots+(2r)^{r+1-r_0}\big)-2\rho(2r)^{r+1-r_0}\\ &\le 2\rho(r-r_0)(2r)^{r-r_0}+\rho(2r)^{r+1-r_0}-2\rho(2r)^{r+1-r_0}\\ &\le -2\rho r_0(2r)^{r-r_0}\le -2\rho.\end{aligned}$$

On a donc finalement :

$$\left(\frac{f(H_0,Z)l^g}{\left|\mathrm{Ker}[l]^*\cap\mathrm{Stab}(Z)\right|}\deg_L(Z)\right)^{1/r_1}<\Delta^{-\rho}l\omega_L(l,X),$$

en faisant disparaître les constantes avec Δ^ρ, et le résultat suit. □

On notera dorénavant :

$$\left|\mathrm{Ker}[l]^*\cap\mathrm{Stab}(Z)\right|=\lambda(Z,l).$$

Remarque. Posons $X=V$ et $H_0=\{0\}$. Si on savait assurer la coprimalité entre l et $[\mathrm{Stab}(Z):\mathrm{Stab}(Z)^0]$, on pourrait déjà clore la preuve, car on aurait :

$$\lambda(Z,l)\le l^{\dim\mathrm{Stab}(Z)^0}\le l^{(g-r_1-1)},$$

la deuxième inégalité provenant du fait que V n'est pas inclus dans un translaté de sous-variété abélienne. La variété Z contenant un translaté de V par un point de torsion, on a de plus :

$$\omega_L(l,V)\le(l\deg_L(Z))^{1/r_1},$$

et une contradiction suivrait immédiatement.

6D. ***Itération et descente.*** Pour conclure, on est donc amené à itérer la dernière proposition, suivant une stratégie de descente désormais classique dans les minorations de hauteur par voie diophantienne. On détaille ici la descente en codimension $r \leq 2$, où la technicité est moins grande et ne cache pas les idées combinatoires en jeu.

Démonstration du théorème 1.8 en codimension $r \leq 2$. Soit V une sous-variété stricte de A qui n'est pas incluse dans un translaté de sous-variété abélienne de A, de codimension $r \leq 2$. On rappelle que :

$$\Delta = C_0^2 \log(3 \deg_L(V)),$$

et on suppose :

$$\omega_L(V)\hat{\mu}_L^{\mathrm{ess}}(V) < \Delta^{-(16(2r)^{r+1})^r}. \tag{6-4}$$

Première étape. Pour utiliser la proposition 6.5, on doit définir :

$$\rho_1 = (9(2r)^{r+1})^{r-1} \quad \text{et} \quad R_1 = [\mathrm{Stab}(V) : \mathrm{Stab}(V)^0].$$

On a, en tenant compte des propriétés du stabilisateur suivant la définition6.3 :

$$\log R_1 \leq \log \deg_L(\mathrm{Stab}(V)) \leq g \log(3 \deg_L(V)) \leq \Delta.$$

Si le morphisme ϕ n'est pas injectif, on applique la proposition 6.5 avec $X = V$, ce qui donne l'existence d'un entier l_1 et d'une sous-variété Z_1 de A, stricte et de codimension k_1, contenant un translaté de V par un point x_1, et telle que :

$$\left(\frac{l_1^g \deg_L(Z_1)}{\lambda(Z_1, l_1)}\right)^{1/k_1} < \Delta^{-\rho_1} l_1 \omega_L(l_1, V).$$

On peut supposer que V est de codimension 2 et que Z_1 est une hypersurface. Sinon, on aurait $Z_1 = x_1 + V$, l'entier l_1 serait premier à

$$[\mathrm{Stab}(V) : \mathrm{Stab}(V)^0] = [\mathrm{Stab}(Z_1) : \mathrm{Stab}(Z_1)^0],$$

et la remarque suivant la preuve de la proposition 6.5 montre qu'on aurait une contradiction.

Deuxième étape. On itère maintenant la proposition 6.5 en posant :

$$V_1 = \bigcup_{x \in \mathrm{Stab}(Z_1) \cap \mathrm{Ker}[l_1]^*} x + V, \qquad \rho_2 = (9(2r)^{r+1})^{r-2},$$

$$R_2 = [\mathrm{Stab}(V) : \mathrm{Stab}(V)^0] \times [\mathrm{Stab}(Z_1) : \mathrm{Stab}(Z_1)^0] \times l_1.$$

La dernière condition permet que le cardinal de H_0 soit premier à tous les premiers des $\mathcal{P}_{i,\mathbb{Z}}$ dans la phase combinatoire. On vérifie une nouvelle fois (par les majorations du degré de Z_1 et de l_1 données par la proposition 6.5) que :

$$\log R_2 \leq g \log(3\omega_L(V)) + g^2 \log \omega_L(V) + 3 \log l_1 \leq \Delta.$$

L'hypothèse (4-1) est satisfaite pour les mêmes raisons (on a $|H_0| \leq l_1^{2g}$). On doit aussi majorer $\omega_L(V_1)\hat{\mu}_L^{\mathrm{ess}}(V_1)$. Le minimum essentiel de V_1 est celui de V. Comme $x_1 + V_1 \subset Z_1$ (par définition de ces deux variétés), l'inégalité sur le degré de Z_1 donne :

$$\omega_L(V_1) \leq l_1 \omega_L(l_1, V) \leq l_1^2 \omega_L(V). \tag{6-5}$$

On obtient donc :

$$\begin{aligned}\omega_L(V_1)\hat{\mu}_L^{\mathrm{ess}}(V_1) &\leq l_1^4 \omega_L(V)\hat{\mu}_L^{\mathrm{ess}}(V) \leq \Delta^{-(16(2r)^{r+1})^r + 8\rho_1(2r)^{r+1}} \\ &\leq \Delta^{\rho_2(2r)^{(r+1)}(-16+8)} \leq \Delta^{-8\rho_2(2r)^{r+1}}.\end{aligned}$$

Par (6-5), on a enfin :

$$C_0 \log(3\omega_L(V_1)) \leq \Delta\,.$$

La proposition 6.5 avec $H_0 = \mathrm{Stab}(Z_1) \cap \mathrm{Ker}[l_1]^*$ donne l'existence d'une variété Z_2 de codimension k_2 contenant un translaté $x_2 + V$, telle que :

$$\left(\frac{f(H_0, Z_2) l_2^g \deg_L(Z_2)}{\lambda(Z_2, l_2)}\right)^{1/k_2} < \Delta^{-\rho_2} l_2 \omega_L(l_2, V_1).$$

Or, Z_2 contient les translatés de $x_2 + V$ par les points de $H_0 \cap \mathrm{Stab}(Z_2)$. On a :

$$\deg_L\Big(\bigcup_{x \in H_0/(H_0 \cap \mathrm{Stab} Z_2)} x + Z_2\Big) \leq f(H_0, Z_2) \deg_L(Z_2);$$

et cette réunion, notée Z_2', contient un translaté de V_1. Si Z_2 est de codimension 2, on a $Z_2 = x_2 + V$, et on en déduit que l_2 est premier à $[\mathrm{Stab}(Z_2) : \mathrm{Stab}(Z_2)^0]$. Il suit :

$$\big(l_2 \deg_L(Z_2')\big)^{1/2} \leq \Delta^{-\rho_2} \omega_L(l_2, V_1),$$

ce qui est absurde, puisque Z_2' contient un translaté de V_1.

Les deux variétés Z_1 et Z_2 sont donc des hypersurfaces, qui contiennent toutes deux un translaté de V, de codimension 2. Quitte à translater ces deux variétés (ce qui est sans conséquences sur le degré et le stabilisateur), on suppose que $V \subset Z_1 \cap Z_2$. Il reste à comparer Z_1 et Z_2 pour finir la preuve.

Cas 1. L'intersection $Z_1 \cap Z_2$ est de codimension 1. Les deux hypersurfaces (irréductibles) sont donc égales. Par construction, Z_1 contient V_1 et on a :

$$\omega_L(V_1) \leq \deg_L(Z_1) \leq \deg_L(Z_2).$$

En outre, l'égalité des variétés nous montre que l_2 est premier à la partie discrète du stabilisateur de Z_2, et comme cette hypersurface n'est pas incluse dans un translaté de variété abélienne (puisque cette propriété est vraie pour $V \subset Z_2$) :

$$\omega_L(V_1) \leq \Delta^{-\rho_2} l_2^{(2-g)} \lambda(Z_2, l_2) \omega_L(V_1) \leq \Delta^{-\rho_2} \omega_L(V_1).$$

On obtient donc une contradiction.

Cas 2. L'intersection $Z_1 \cap Z_2$ est de codimension 2. Dans ce cas, cette intersection contient V, mais elle contient aussi les translatés de V par les points de $H_0 \cap \mathrm{Stab}(Z_2)$. Comme ce groupe est de cardinal une puissance de l_1, la partie discrète du stabilisateur de V n'intervient pas et on a :

$$\deg_L\Big(\bigcup_{x\in H_0\cap \mathrm{Stab}(Z_2)} x+V\Big) \geq \frac{|H_0\cap \mathrm{Stab}(Z_2)|}{l_1^{(\dim V-1)}}\deg_L(V) = \frac{\lambda(Z_1,l_1)l_1^{(3-g)}}{f(H_0,Z_2)}\deg_L(V).$$

On a utilisé au passage le fait que V n'était pas un translaté de variété abélienne. Par le théorème de Bézout, il vient :

$$\begin{aligned}\frac{\lambda(Z_1,l_1)l_1^{(3-g)}}{f(H_0,Z_2)}\deg_L(V) &\leq \deg_L(Z_1)\deg_L(Z_2)\\ &\leq \Delta^{-\rho_1}\frac{\lambda(Z_1,l_1)l_1^{(1-g)}}{f(H_0,Z_2)}l_2^4\omega_L(l_1,V)\omega_L(V_1).\end{aligned}$$

La majoration des termes en l_2 a été grossière car ceux-ci sont négligeables devant Δ^{ρ_1} par la majoration de l_2 suivant la proposition 6.5. On en déduit :

$$\deg_L(V) \leq \Delta^{-\rho_1}l_1^{-2}l_2^4\omega_L(l_1,V)\omega_L(V_1).$$

Par (6-5), on trouve :

$$l_1\deg_L(V) \leq \Delta^{-\rho_1}l_2^4\omega_L(l_1,V)^2 \leq \Delta^u\omega_L(l_1,V)^2,$$

et le réel u vérifie :

$$u \leq -\rho_1 + 8\rho_2(2r)^{r+1} < 0.$$

C'est à nouveau une contradiction.

Fin de la preuve. On a donc démontré par l'absurde que la proposition 6.2 était vraie, soit avec $X = V$, soit avec $X = V_1$. Il en résulte dans les deux cas que V contredit la majoration (6-4). On en déduit :

$$\hat{\mu}_L^{\mathrm{ess}}(V) \geq \frac{C_L(A)}{\omega_L(V)}\big(\log(3\deg_L(V))\big)^{-\lambda(r)},$$

où $\lambda(r) = (16(2r)^{(r+1)})^r$ et $C_L(A) = 1/C_0^{2\lambda(r)}$, qui ne dépend que de A. □

Conclusion. Expliquons pour finir quelles modifications il convient d'apporter à ce travail pour traiter la descente en codimension générale, suivant [Galateau 2008]. La principale difficulté rencontrée dans le cas abélien est l'absence, en général, d'un relèvement du morphisme de Frobenius en caractéristique nulle. On est donc amené à le reconstituer combinatoirement, en considérant le translaté d'une variété V par certains sous-groupes de torsion. La phase de descente, lorsqu'on travaille avec des fermés réductibles, est particulièrement délicate et nécessite la définition de nouveaux indices d'obstructions.

Pour préparer au mieux cette descente, on rajoute une information d'ordre combinatoire dans la phase de transcendance. Plus précisément, en insérant un principe de tiroirs de Dirichlet dans le lemme de zéros, on montre que le fermé Z donné par la proposition 6.5 peut être choisi de telle sorte qu'il contienne une proportion « raisonnable » de composantes irréductibles de X ; on perd en contrepartie l'irréductibilité de Z. À quelques détails près dans le choix des paramètres, on obtient alors [Galateau 2008, proposition 5.1], sur laquelle s'articule la descente finale.

Remerciements

Je souhaite remercier chaleureusement Sinnou David, qui m'a patiemment initié au problème de Bogomolov au cours de mon doctorat, et Eric Gaudron pour sa minutieuse relecture et ses conseils. Pendant la rédaction de ce travail, j'ai pu bénéficier des explications d'Antoine Chambert-Loir, Huayi Chen, Richard Pink, Hugues Randriam et Emmanuel Ullmo. Je remercie enfin le rapporteur dont les commentaires m'ont permis d'améliorer significativement cet article.

References

[Amoroso et David 1999] F. Amoroso et S. David, "Le problème de Lehmer en dimension supérieure", *J. Reine Angew. Math.* **513** (1999), 145–179. MR 2001a:11116 Zbl 1011.11045

[Amoroso et David 2003] F. Amoroso et S. David, "Minoration de la hauteur normalisée dans un tore", *J. Inst. Math. Jussieu* **2**:3 (2003), 335–381. MR 2004m:11101 Zbl 1041.11048

[Bombieri et Zannier 1995] E. Bombieri et U. Zannier, "Algebraic points on subvarieties of $\mathbf{G}_m^n$", *Internat. Math. Res. Notices* 7 (1995), 333–347. MR 96h:11061 Zbl 0848.11030

[Bombieri et Zannier 1996] E. Bombieri et U. Zannier, "Heights of algebraic points on subvarieties of abelian varieties", *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **23**:4 (1996), 779–792. MR 98j:11043 Zbl 0897.11020

[Bombieri et al. 1999] E. Bombieri, D. Masser et U. Zannier, "Intersecting a curve with algebraic subgroups of multiplicative groups", *Int. Math. Res. Not.* **1999**:20 (1999), 1119–1140. MR 2001c:11081 Zbl 0938.11031

[Bombieri et al. 2007] E. Bombieri, D. Masser et U. Zannier, "Anomalous subvarieties — structure theorems and applications", *Int. Math. Res. Not.* **2007**:19 (2007), ID rnm057. MR 2008k:11060 Zbl 1145.11049

[Bost 1996a] J.-B. Bost, "Intrinsic heights of stable varieties and abelian varieties", *Duke Math. J.* **82**:1 (1996), 21–70. MR 97j:14025 Zbl 0867.14010

[Bost 1996b] J.-B. Bost, "Périodes et isogenies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz)", pp. 115–161 dans *Séminaire Bourbaki,* 1994/95 (exposé 795), Astérisque **237**, 1996. MR 98k:11073 Zbl 0936.11042

[Bost 2001] J.-B. Bost, "Algebraic leaves of algebraic foliations over number fields", *Publ. Math. Inst. Hautes Études Sci.* 93 (2001), 161–221. MR 2002h:14037 Zbl 1034.14010

[Bost et Künnemann 2007] J. B. Bost et K. Künnemann, "Hermitian vector bundles and extension groups on arithmetic varieties, I: Geometry of numbers", prépubl., 2007. arXiv math.NT/0701343

[Bost et al. 1994] J.-B. Bost, H. Gillet et C. Soulé, "Heights of projective varieties and positive Green forms", *J. Amer. Math. Soc.* **7**:4 (1994), 903–1027. MR 95j:14025 Zbl 0973.14013

[Carrizosa 2009] M. Carrizosa, "Petits points et multiplication complexe", *Int. Math. Res. Not.* **2009**:16 (2009), 3016–3097. MR 2533796 Zbl 1176.11025

[Chardin 1989] M. Chardin, "Une majoration de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique", *Bull. Soc. Math. France* **117**:3 (1989), 305–318. MR 90m:13021 Zbl 0709.13007

[Chardin 1990] M. Chardin, *Contributions à l'algèbre commutative effective et à la théorie de l'élimination*, Thèse de Doctorat, Université Paris VI, 1990.

[Chen 2006] H. Chen, *Positivité en géométrie algébrique et en géométrie d'Arakelov*, Thèse de Doctorat, Université Paris XI, 2006.

[David 1991] S. David, "Fonctions thêta et points de torsion des variétés abéliennes", *Compositio Math.* **78**:2 (1991), 121–160. MR 92d:11061 Zbl 0741.14025

[David et Hindry 2000] S. David et M. Hindry, "Minoration de la hauteur de Néron–Tate sur les variétés abéliennes de type C.M.", *J. Reine Angew. Math.* **529** (2000), 1–74. MR 2001j:11054 Zbl 0993.11034

[David et Philippon 2000] S. David et P. Philippon, "Sous-variétés de torsion des variétés semi-abéliennes", *C. R. Acad. Sci. Paris Sér. I Math.* **331**:8 (2000), 587–592. MR 2001k:14084 Zbl 0972.11059

[David et Philippon 2002] S. David et P. Philippon, "Minorations des hauteurs normalisées des sous-variétés de variétés abeliennes, II", *Comment. Math. Helv.* **77**:4 (2002), 639–700. MR 2004a:11055 Zbl 1030.11026

[David et Philippon 2007] S. David et P. Philippon, "Minorations des hauteurs normalisées des sous-variétés des puissances des courbes elliptiques", *Int. Math. Res. Pap.* 3 (2007), ID rpm006. MR 2008h:11068 Zbl 1163.11049

[Demazure et Grothendieck 1970] M. Demazure et A. Grothendieck (éditeurs), *Schémas en groupes, I: Propriétés générales des schémas en groupes*, Lecture Notes in Mathematics **151**, Springer, Berlin, 1970. MR 43 #223a

[Galateau 2007] A. Galateau, *Problème de Bogomolov sur les variétés abéliennes*, Thèse de Doctorat, Université Paris VI, 2007.

[Galateau 2008] A. Galateau, "Une minoration du minimum essentiel sur les variétés abéliennes", prépublication, 2008. À paraître dans *Comment. Math. Helv.* arXiv 0807.0171

[Galateau 2009] A. Galateau, "Un théorème de zéros dans les groupes algébriques commutatifs. D'après Amoroso et David", prépublication, 2009, Voir http://www.math.unibas.ch/~galateau/zeros.pdf.

[Gaudron 2006] É. Gaudron, "Formes linéaires de logarithmes effectives sur les variétés abéliennes", *Ann. Sci. École Norm. Sup.* (4) **39**:5 (2006), 699–773. MR 2008a:11084 Zbl 1111.11038

[Gaudron 2008] É. Gaudron, "Pentes des fibrés vectoriels adéliques sur un corps global", *Rend. Semin. Mat. Univ. Padova* **119** (2008), 21–95. MR 2009j:11107 Zbl 05582423

[Graftieaux 2001] P. Graftieaux, "Formal groups and the isogeny theorem", *Duke Math. J.* **106**:1 (2001), 81–121. MR 2002f:14055 Zbl 1064.14045

[Griffiths et Harris 1978] P. Griffiths et J. Harris, *Principles of algebraic geometry*, Wiley, New York, 1978. MR 80b:14001 Zbl 0408.14001

[Habegger 2009] P. Habegger, "A Bogomolov property for curves modulo algebraic subgroups", *Bull. Soc. Math. France* **137**:1 (2009), 93–125. MR 2010d:11071 Zbl 05558321

[Hindry 1988] M. Hindry, "Autour d'une conjecture de Serge Lang", *Invent. Math.* **94**:3 (1988), 575–603. MR 89k:11046 Zbl 0638.14026

[Hindry et Silverman 2000] M. Hindry et J. H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics **201**, Springer, New York, 2000. MR 2001e:11058 Zbl 0948.11023

[Ireland et Rosen 1990] K. Ireland et M. Rosen, *A classical introduction to modern number theory*, 2ème éd., Graduate Texts in Math. **84**, Springer, New York, 1990. MR 92e:11001 Zbl 0712.11001

[Koblitz 1975] N. Koblitz, "p-adic variation of the zeta-function over families of varieties defined over finite fields", *Compositio Math.* **31**:2 (1975), 119–218. MR 54 #2658 Zbl 0332.14008

[Lang 1994] S. Lang, *Algebraic number theory*, 2ème éd., Graduate Texts in Mathematics **110**, Springer, New York, 1994. MR 95f:11085 Zbl 0811.11001

[Lang 2002] S. Lang, *Algebra*, 3rd éd., Graduate Texts in Mathematics **211**, Springer, New York, 2002. MR 2003e:00003 Zbl 0984.00001

[Lange et Ruppert 1985] H. Lange et W. Ruppert, "Complete systems of addition laws on abelian varieties", *Invent. Math.* **79**:3 (1985), 603–610. MR 86f:14029 Zbl 0577.14035

[Laurent 1983] M. Laurent, "Minoration de la hauteur de Néron–Tate", pp. 137–151 dans *Seminar on number theory* (Paris, 1981/1982), édité par M.-J. Bertin, Progr. Math. **38**, Birkhäuser, Boston, 1983. MR 85e:11048 Zbl 0521.14010

[Maurin 2008] G. Maurin, "Courbes algébriques et équations multiplicatives", *Math. Ann.* **341**:4 (2008), 789–824. MR 2009g:14026 Zbl 1154.14017

[Moret-Bailly 1990] L. Moret-Bailly, "Sur l'équation fonctionnelle de la fonction thêta de Riemann", *Compositio Math.* **75**:2 (1990), 203–217. MR 92a:14049 Zbl 0728.14039

[Mumford 1974] D. Mumford, , 2éme éd., Tata Institute of Fundamental Research Studies in Mathematics **5**, Oxford University Press, London, 1974. MR 2010e:14040 Zbl 0326.14012

[Noot 1995] R. Noot, "Abelian varieties — Galois representation and properties of ordinary reduction", *Compositio Math.* **97**:1-2 (1995), 161–171. MR 97a:11093 Zbl 0868.14021

[Ogus 1982] A. Ogus, *Hodge cycles and crystalline cohomology*, Lecture Notes in Mathematics **900**, Springer, Berlin, 1982. MR 84m:14046 Zbl 0538.14010

[Philippon 1995] P. Philippon, "Sur des hauteurs alternatives, III", *J. Math. Pures Appl.* (9) **74**:4 (1995), 345–365. MR 97a:11098 Zbl 0878.11025

[Pink 1998] R. Pink, "l-adic algebraic monodromy groups, cocharacters, and the Mumford–Tate conjecture", *J. Reine Angew. Math.* **495** (1998), 187–237. MR 98m:11060 Zbl 0920.14006

[Pink 2004] R. Pink, "Finite group schemes", notes de cours, 2004, Voir http://www.math.ethz.ch/~pink/FiniteGroupSchemes.html.

[Pink 2005] R. Pink, "A common generalization of the conjectures of André–Oort, Manin–Mumford and Mordell–Lang", prépublication, 2005, Voir www.math.ethz.ch/~pink/ftp/AOMMML.pdf.

[Ratazzi 2008] N. Ratazzi, "Intersection de courbes et de sous-groupes et problèmes de minoration de dernière hauteur dans les variétés abéliennes C.M.", *Ann. Inst. Fourier* (*Grenoble*) **58**:5 (2008), 1575–1633. MR 2009m:11096 Zbl 1156.11025

[Raynaud 1974] M. Raynaud, "Schémas en groupes de type $(p, \dots, p)$", *Bull. Soc. Math. France* **102** (1974), 241–280. MR 54 #7488 Zbl 0325.14020

[Rémond et Viada 2003] G. Rémond et E. Viada, "Problème de Mordell–Lang modulo certaines sous-variétés abéliennes", *Int. Math. Res. Not.* **2003**:35 (2003), 1915–1931. MR 2004h:11054 Zbl 1072.11038

[Samuel 1967] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris, 1967. MR 35 #6643 Zbl 0146.06402

[Serre 1968] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968. MR 41 #8422 Zbl 0186.25701

[Viada 2003] E. Viada, "The intersection of a curve with algebraic subgroups in a product of elliptic curves", *Ann. Sc. Norm. Super. Pisa Cl. Sci.* (5) **2**:1 (2003), 47–75. MR 2004c:11099 Zbl .11314 Zbl 1170.11314

[Viada 2008] E. Viada, "The intersection of a curve with a union of translated codimension-two subgroups in a power of an elliptic curve", *Algebra Number Theory* **2**:3 (2008), 249–298. MR 2009f:11079 Zbl 1168.11024

[Viada 2009] E. Viada, "Nondense subsets of varieties in a power of an elliptic curve", *Int. Math. Res. Not.* **2009**:7 (2009), 1213–1246. MR 2010d:14031 Zbl 1168.14030

[Zhang 1992] S. Zhang, "Positive line bundles on arithmetic surfaces", *Ann. of Math.* (2) **136**:3 (1992), 569–587. MR 93j:14024 Zbl 0788.14017

[Zhang 1995a] S. Zhang, "Positive line bundles on arithmetic varieties", *J. Amer. Math. Soc.* **8**:1 (1995), 187–221. MR 95c:14020 Zbl 0861.14018

[Zhang 1995b] S. Zhang, "Small points and adelic metrics", *J. Algebraic Geom.* **4**:2 (1995), 281–300. MR 96e:14025 Zbl 0861.14019

[Zilber 2002] B. Zilber, "Exponential sums equations and the Schanuel conjecture", *J. London Math. Soc.* (2) **65**:1 (2002), 27–44. MR 2002m:11104 Zbl 1030.11073

Communicated by Bjorn Poonen
Received 2009-06-25 Revised 2009-11-16 Accepted 2009-12-20

aurelien.galateau@math.u-psud.fr

Mathematisches Institut, Universität Basel, Rheinsprung, 21, CH-4051 Basel, Switzerland

Bâtiment 425, Université Paris-Sud, 91405 Orsay, France
http://www.math.u-psud.fr/~galateau

ALGEBRA AND NUMBER THEORY 4:5(2010)

Transverse quiver Grassmannians and bases in affine cluster algebras

Grégoire Dupont

Sherman, Zelevinsky and Cerulli constructed canonically positive bases in cluster algebras associated to affine quivers having at most three vertices. Their constructions involve cluster monomials and normalized Chebyshev polynomials of the first kind evaluated at a certain "imaginary" element in the cluster algebra. Using this combinatorial description, it is possible to define for any affine quiver Q a set $\mathcal{B}(Q)$, which is conjectured to be the canonically positive basis of the acyclic cluster algebra $\mathcal{A}(Q)$.

In this article, we provide a geometric realization of the elements in $\mathcal{B}(Q)$ in terms of the representation theory of Q. This is done by introducing an analogue of the Caldero–Chapoton cluster character, where the usual quiver Grassmannian is replaced by a constructible subset called the *transverse quiver Grassmannian*.

1. Introduction

Cluster algebras were introduced by Fomin and Zelevinsky [2002; 2003; 2007; Berenstein et al. 2005] in order to define a combinatorial framework for studying positivity in algebraic groups and canonical bases in quantum groups. Since then, cluster algebras have found applications in various areas of mathematics, such as Lie theory, combinatorics, Teichmüller theory, Poisson geometry and quiver representations.

MSC2000: primary 16G99; secondary 13F99.

Keywords: cluster algebras, canonical bases, Chebyshev polynomials, cluster characters, quiver Grassmannians.

A (coefficient-free) cluster algebra $\mathscr{A}$ is a commutative $\mathbb{Z}$-algebra equipped with a distinguished set of generators, called *cluster variables*, gathered into possibly overlapping sets of fixed cardinality, called *clusters*. Monomials in variables belonging all to the same cluster are called *cluster monomials*. According to the *Laurent phenomenon* [Fomin and Zelevinsky 2002], it is known that $\mathscr{A}$ is a subalgebra of $\mathbb{Z}[\boldsymbol{c}^{\pm 1}]$ for any cluster $\boldsymbol{c}$ in $\mathscr{A}$. A nonzero element $y \in \mathscr{A}$ is called *positive* if y belongs to $\mathbb{Z}_{\geq 0}[\boldsymbol{c}^{\pm 1}]$ for any cluster $\boldsymbol{c}$ in $\mathscr{A}$. Following [Cerulli 2009], a $\mathbb{Z}$-basis $\mathscr{B} \subset \mathscr{A}$ is called *canonically positive* if the semiring of positive elements in $\mathscr{A}$ coincides with the set of $\mathbb{Z}_{\geq 0}$-linear combinations of elements of $\mathscr{B}$. Note that if such a basis exists, it is unique.

The problems of existence and description of a canonically positive basis in an arbitrary cluster algebra are still wide open. Both problems were first solved in the particular case of cluster algebras of finite type $\mathbb{A}_2$ and affine type $\tilde{\mathbb{A}}_{1,1}$ by Sherman and Zelevinsky [2004]. It was later extended by Cerulli [2009] for cluster algebras of affine type $\tilde{\mathbb{A}}_{2,1}$. To the best of the author's knowledge, these are the only known constructions of canonically positive bases in cluster algebras.

Using categorifications of acyclic cluster algebras with cluster categories and cluster characters, it is possible to rephrase Sherman–Zelevinsky and Cerulli constructions in order to place them in the more general context of acyclic cluster algebras associated to arbitrary affine quivers.

If Q is an acyclic quiver and $\boldsymbol{u}$ is a Q_0-tuple of indeterminates over $\mathbb{Z}$, we denote by $\mathscr{A}(Q)$ the acyclic cluster algebra with initial seed $(Q, \boldsymbol{u})$. We denote by $\mathscr{C}_Q$ the associated *cluster category* (over the field $\boldsymbol{k}$ of complex numbers) and by $X_? : \mathrm{Ob}(\mathscr{C}_Q) \to \mathbb{Z}[\boldsymbol{u}^{\pm 1}]$ the *Caldero–Chapoton map* on $\mathscr{C}_Q$, also called the (canonical) *cluster character* (see Section 2 for details). When Q is an affine quiver with positive minimal imaginary root δ, we set

$$\mathscr{B}(Q) = \mathscr{M}(Q) \sqcup \{F_n(X_\delta)X_R \mid n \geq 1 \text{ and } R \text{ is a regular rigid } \boldsymbol{k}Q\text{-module}\},$$

where $\mathscr{M}(Q)$ denotes the set of cluster monomials in $\mathscr{A}(Q)$, F_n denotes the n-th normalized Chebyshev polynomial of the first kind and X_δ is the evaluation of $X_?$ at any quasisimple module in a homogeneous tube of the Auslander–Reiten quiver $\Gamma(\boldsymbol{k}Q\text{-mod})$ of $\boldsymbol{k}Q$-mod.

If Q is of type $\tilde{\mathbb{A}}_{1,1}$ or $\tilde{\mathbb{A}}_{2,1}$, the set $\mathscr{B}(Q)$ coincides with the canonically positive basis constructed in [Sherman and Zelevinsky 2004] and [Cerulli 2009], respectively. It was conjectured in [Dupont 2010, Conjecture 7.10] that, for any affine quiver Q, the set $\mathscr{B}(Q)$ is the canonically positive basis of $\mathscr{A}(Q)$. Using the *generic basis*, it is possible to prove that, for any affine quiver Q, the set $\mathscr{B}(Q)$ is a $\mathbb{Z}$-basis in $\mathscr{A}(Q)$ [Dupont 2008; Ding et al. 2009]. Nevertheless, it is not known if this basis is the canonically positive basis in general.

An essential problem in investigating this question is that the elements of the form $F_n(X_\delta)X_R$ are defined combinatorially, and as yet have no representation-theoretic or geometric interpretation. The aim of this article is to provide such an interpretation.

Extending the idea of Caldero and Chapoton [2006], for any integrable bundle $\mathcal{F}$ on $\mathrm{rep}_{\boldsymbol{k}}(Q)$ (see Section 4 for definitions), we define a map $\theta_{\mathcal{F}}$, called the *character associated to* $\mathcal{F}$, from the set of objects in $\mathcal{C}_Q$ to the ring $\mathbb{Z}[\boldsymbol{u}^{\pm 1}]$. With this terminology, the Caldero–Chapoton map $X_?$ is the character θ_{Gr}, where $\mathrm{Gr}: M \mapsto \mathrm{Gr}(M)$ denotes the integrable bundle of quiver Grassmannians.

For any indecomposable $\boldsymbol{k}Q$-module M, we introduce a constructible subset $\mathrm{Tr}(M) \subset \mathrm{Gr}(M)$, called the *transverse quiver Grassmannian*. We prove that the bundle $\mathrm{Tr} : M \mapsto \mathrm{Tr}(M)$ is integrable on $\mathrm{rep}_{\boldsymbol{k}}(Q)$ and that the elements in $\mathcal{B}(Q)$ can be described using the associated character θ_{Tr}. More precisely, we prove that for any $l \geq 1$,

$$F_l(X_\delta) = \theta_{\mathrm{Tr}}(M),$$

where M is any indecomposable $\boldsymbol{k}Q$-module with dimension vector $l\delta$. It turns out that θ_{Tr}, unlike θ_{Gr}, is independent of the tube containing M. In particular, it takes the same values if M belongs to a homogeneous or to an exceptional tube. This is surprising since the usual quiver Grassmannians of two indecomposable modules of dimension $l\delta$ belonging to tubes of different ranks are in general completely different.

Moreover, if R is an indecomposable regular rigid $\boldsymbol{k}Q$-module, then

$$F_l(X_\delta)X_R = \theta_{\mathrm{Tr}}(M),$$

where M is the unique indecomposable $\boldsymbol{k}Q$-module of dimension $l\delta + \mathbf{dim}\, R$.

As a consequence, we obtain the following description of the set $\mathcal{B}(Q)$:

$$\mathcal{B}(Q) = \left\{ \theta_{\mathrm{Tr}}(M \oplus R) \;\middle|\; \begin{array}{l} M \text{ is an indecomposable (or zero) regular } \boldsymbol{k}Q\text{-module,} \\ R \text{ is any rigid object in } \mathcal{C}_Q \text{ such that } \mathrm{Ext}^1_{\mathcal{C}_Q}(M, R) = 0 \end{array} \right\}.$$

This paper is organized as follows. In Section 2, we start by recalling several results concerning Chebyshev and generalized Chebyshev polynomials. Then we recall necessary background on cluster categories and cluster characters associated to acyclic and especially affine quivers. Finally, we recall the known results concerning constructions of bases in affine cluster algebras.

In Section 3, we use the combinatorics of generalized Chebyshev polynomials to prove relations for cluster characters associated to regular $\boldsymbol{k}Q$-modules when Q is an affine quiver with minimal imaginary root δ. These relations are generalizations of the *difference property* [Dupont 2008], used to compute the difference between cluster characters evaluated at indecomposable modules of dimension vector δ in different tubes.

Section 4 introduces the notions of integrable bundles on $\mathrm{rep}_{\boldsymbol{k}}(Q)$ and associated characters for any acyclic quiver. With this terminology, the Caldero–Chapoton map is the character associated to the quiver Grassmannian bundle. For affine quivers, we introduce the integrable bundle Tr of the Grassmannian of transverse submodules and see that it coincides with the Caldero–Chapoton map on rigid objects in the cluster category.

In Section 5, we prove that the elements in $\mathcal{B}(Q)$ can be expressed as values of the character θ_{Tr} associated to the integrable bundle Tr of $\mathrm{rep}_{\boldsymbol{k}}(Q)$. This provides a geometrization of the set $\mathcal{B}(Q)$.

In Section 6, we illustrate some of our results for quivers of affine types $\tilde{\mathbb{A}}_{1,1}$ and $\tilde{\mathbb{A}}_{2,1}$, putting [Sherman and Zelevinsky 2004; Cerulli 2009] into context.

2. Background, notation and terminology

Given a quiver Q, we denote by Q_0 its set of arrows and by Q_1 its set of vertices. We always assume that Q_0, Q_1 are finite sets and that the underlying unoriented graph of Q is connected. A quiver is called *acyclic* if it does not contain any oriented cycles.

We now fix an acyclic quiver Q and a Q_0-tuple $\boldsymbol{u} = (u_i \mid i \in Q_0)$ of indeterminates over $\mathbb{Z}$. We denote by $\mathcal{A}(Q)$ the coefficient-free cluster algebra with initial seed $(Q, \boldsymbol{u})$.

Chebyshev polynomials and their generalizations. Chebyshev (respectively generalized Chebyshev) polynomials are orthogonal polynomials in one variable (respectively several variables) playing an important role in the context of cluster algebras associated to representation-infinite quivers [Sherman and Zelevinsky 2004; Caldero and Zelevinsky 2006] (respectively [Dupont 2009; 2010]). We recall some basic results concerning these polynomials.

For any $l \geq 0$, the *l-th* (*normalized*) *Chebyshev polynomial of the first kind* is the polynomial F_l in $\mathbb{Z}[x]$ defined inductively by

$$F_0(x) = 2, \quad F_1(x) = x, \quad \text{and} \quad F_l(x) = xF_{l-1}(x) - F_{l-2}(x) \quad \text{for any } l \geq 2.$$

F_l is characterized by the following identity in $\mathbb{Z}[t, t^{-1}]$:

$$F_l(t + t^{-1}) = t^l + t^{-l}.$$

These polynomials first appeared in the context of cluster algebras in [Sherman and Zelevinsky 2004].

For any $l \geq 0$, the *l-th* (*normalized*) *Chebyshev polynomial of the second kind* is the polynomial S_l in $\mathbb{Z}[x]$ defined inductively by

$$S_0(x) = 1, \quad S_1(x) = x, \quad \text{and} \quad S_l(x) = xS_{l-1}(x) - S_{l-2}(x) \quad \text{for any } l \geq 2.$$

S_l is characterized by the following identity in $\mathbb{Z}[t, t^{-1}]$:

$$S_l(t + t^{-1}) = \sum_{k=0}^{n} t^{n-2k}.$$

Chebyshev polynomials of the Second kind first appeared in the context of cluster algebras in [Caldero and Zelevinsky 2006]. For any $l \geq 1$, $S_l(x)$ is the polynomial given by

$$S_l(x) = \det \begin{bmatrix} x & 1 & & (0) \\ 1 & x & \ddots & \\ & \ddots & \ddots & \ddots \\ & & \ddots & \ddots & 1 \\ (0) & & & 1 & x \end{bmatrix},$$

where the matrix is tridiagonal in $M_l(\mathbb{Z}[x])$. The two kinds of Chebyshev polynomials are related by

$$F_l(x) = S_l(x) - S_{l-2}(x)$$

for any $l \geq 1$, with the convention that $S_{-1}(x) = 0$.

Fix a family $\{x_i \mid i \geq 1\}$ of indeterminates over $\mathbb{Z}$. For any $l \geq 0$, the *l-th generalized Chebyshev polynomial* is the polynomial in $\mathbb{Z}[x_1, \ldots, x_l]$ defined inductively by $P_0 = 1$, $P_1(x_1) = x_1$, and

$$P_l(x_1, \ldots, x_l) = x_l P_{l-1}(x_1, \ldots, x_{l-1}) - P_{l-2}(x_1, \ldots, x_{l-2}) \quad \text{for any } l \geq 2.$$

Equivalently,

$$P_l(x_1, \ldots, x_l) = \det \begin{bmatrix} x_l & 1 & & (0) \\ 1 & x_{l-1} & \ddots & \\ & \ddots & \ddots & \ddots \\ & & \ddots & \ddots & 1 \\ (0) & & & 1 & x_1 \end{bmatrix},$$

where the matrix is tridiagonal in $M_l(\mathbb{Z}[x_1, \ldots, x_l])$. These polynomials first appeared in the context of cluster algebras in [Dupont 2009] under the name of *generalized Chebyshev polynomials of infinite rank*, and similar polynomials also arose in the context of cluster algebras in [Yang and Zelevinsky 2008; Dupont 2010].

Cluster categories and cluster characters. Let $\boldsymbol{k}Q$-mod be the category of finitely generated left-modules over the path algebra $\boldsymbol{k}Q$ of Q. As usual, this category will be identified with the category $\mathrm{rep}_{\boldsymbol{k}}(Q)$ of finite-dimensional representations of Q over $\boldsymbol{k}$.

For any vertex $i \in Q_0$, we denote by S_i the simple module associated to i, by P_i its projective cover, and by I_i its injective hull. We denote by $\langle -, - \rangle$ the

homological Euler form defined on $\boldsymbol{k}Q$-mod by

$$\langle M, N\rangle = \dim \mathrm{Hom}_{\boldsymbol{k}Q}(M, N) - \dim \mathrm{Ext}^1_{\boldsymbol{k}Q}(M, N)$$

for any two $\boldsymbol{k}Q$-modules M, N. Since Q is acyclic, $\boldsymbol{k}Q$ is a finite-dimensional hereditary algebra, and therefore $\langle -, -\rangle$ is well-defined on the Grothendieck group $K_0(\boldsymbol{k}Q\text{-mod})$.

For any $\boldsymbol{k}Q$-module M, the dimension vector of M is

$$\mathbf{dim}\, M = (\dim \mathrm{Hom}_{\boldsymbol{k}Q}(P_i, M))_{i\in Q_0} \in \mathbb{N}^{Q_0}.$$

Viewed as a representation of Q, $\mathbf{dim}\, M = (\dim M(i))_{i\in Q_0}$ where $M(i)$ is the $\boldsymbol{k}$-vector space at vertex i in the representation M of Q. The dimension vector map **dim** induces an isomorphism of abelian groups

$$\mathbf{dim} : K_0(\boldsymbol{k}Q\text{-mod}) \xrightarrow{\sim} \mathbb{Z}^{Q_0}$$

sending the class of the simple S_i to the i-th vector of the canonical basis of $\mathbb{Z}^{Q_0}$.

The *cluster category* was introduced in [Buan et al. 2006] (see also [Caldero et al. 2006] for Dynkin type $\mathbb{A}$) in order to define a categorical framework for studying the cluster algebra $\mathcal{A}(Q)$. Let $D^b(\boldsymbol{k}Q\text{-mod})$ be the bounded derived category of $\boldsymbol{k}Q$-mod with shift functor [1] and Auslander–Reiten translation τ. The *cluster category* is the orbit category $\mathcal{C}_Q$ of the auto-functor $\tau^{-1}[1]$ in $D^b(\boldsymbol{k}Q\text{-mod})$. It is a 2-Calabi–Yau triangulated category. The set of isoclasses of indecomposable objects in $\mathcal{C}_Q$ can be identified with the union of the set of isoclasses of indecomposable $\boldsymbol{k}Q$-modules and the set of isoclasses of shifts of indecomposable projective $\boldsymbol{k}Q$-modules [Keller 2005; Buan et al. 2006]. In particular, every object M in $\mathcal{C}_Q$ can be uniquely (up to isomorphism) decomposed into

$$M = M_0 \oplus P_M[1],$$

where M_0 is a $\boldsymbol{k}Q$-module and P_M is a projective $\boldsymbol{k}Q$-module.

Given a representation M of Q, the *quiver Grassmannian of* M is the set $\mathrm{Gr}(M)$ of all subrepresentations of M. For any element $\boldsymbol{e} \in \mathbb{Z}^{Q_0}$, the set

$$\mathrm{Gr}_{\boldsymbol{e}}(M) = \{N \text{ submodule of } M \mid \mathbf{dim}\, N = \boldsymbol{e}\}$$

is a projective variety. We denote by $\chi(\mathrm{Gr}_{\boldsymbol{e}}(M))$ its Euler characteristic with respect to the singular cohomology with rational coefficients.

Definition 2.1 [Caldero and Chapoton 2006]. The *Caldero–Chapoton map* is the map

$$X_? : \mathrm{Ob}(\mathcal{C}_Q) \to \mathbb{Z}[\boldsymbol{u}^{\pm 1}]$$

defined by:

- For any $i \in Q_0$,
$$X_{P_i[1]} = u_i.$$
- If M is an indecomposable $\boldsymbol{k}Q$-module, then
$$X_M = \sum_{\boldsymbol{e} \in \mathbb{N}^{Q_0}} \chi(\mathrm{Gr}_{\boldsymbol{e}}(M)) \prod_{i \in Q_0} u_i^{-\langle \boldsymbol{e}, S_i \rangle - \langle S_i, \mathbf{dim}\, M - \boldsymbol{e} \rangle}. \tag{2-1}$$
- For any two objects M, N in $\mathscr{C}_Q$,
$$X_{M \oplus N} = X_M X_N.$$

Note that (2-1) also holds for decomposable modules.

Caldero and Keller [2006, Theorem 4] proved that $X_?$ induces a 1-1 correspondence between the set of isoclasses of indecomposable rigid objects (that is, without self-extensions) in $\mathscr{C}_Q$ and the set of cluster variables in $\mathscr{A}(Q)$. Moreover, $X_?$ induces a 1-1 correspondence between the set of isoclasses of cluster-tilting objects in $\mathscr{C}_Q$ and the set of clusters in $\mathscr{A}(Q)$. In particular, we have the following description of cluster monomials in $\mathscr{A}(Q)$:

$$\mathscr{M}(Q) = \{X_M \mid M \text{ is rigid in } \mathscr{C}_Q\}.$$

For any $\boldsymbol{d} = (d_i)_{i \in Q_0} \in \mathbb{Z}^{Q_0}$, we set $\boldsymbol{u}^{\boldsymbol{d}} = \prod_{i \in Q_0} u_i^{d_i}$. For any Laurent polynomial $L \in \mathbb{Z}[\boldsymbol{u}^{\pm 1}]$, the *denominator vector* of L is the Q_0-tuple $\mathrm{den}(L) \in \mathbb{Z}^{Q_0}$ such that there exists a polynomial $P(u_i \mid i \in Q_0)$ not divisible by any u_i such that

$$L = \frac{P(u_i \mid i \in Q_0)}{\boldsymbol{u}^{\mathrm{den}(L)}}.$$

We define the dimension vector map $\mathbf{dim}_{\mathscr{C}_Q}$ on $\mathscr{C}_Q$ by setting $\mathbf{dim}_{\mathscr{C}_Q} M = \mathbf{dim}\, M$ if M is a $\boldsymbol{k}Q$-module and $\mathbf{dim}_{\mathscr{C}_Q} P_i[1] = -\mathbf{dim}\, S_i$ and extending by additivity. Note that, for any $\boldsymbol{k}Q$-module M, we have $\mathbf{dim}\, M = \mathbf{dim}_{\mathscr{C}_Q}(M)$; we will abuse notation and write $\mathbf{dim}\, M$ for any object in $\mathscr{C}_Q$. Caldero and Keller's denominator theorem [2006, Theorem 3] relates the denominator vector of the character with the dimension vector of the corresponding object in the cluster category:

$$\mathrm{den}(X_M) = \mathbf{dim}\, M,$$

for any object M in $\mathscr{C}_Q$.

Representation theory of affine quivers. We shall briefly recall some well-known facts concerning the representation theory of affine quivers. We refer the reader to [Simson and Skowroński 2007; Ringel 1984] for details.

We now fix an affine quiver Q, that is, an acyclic quiver of type $\tilde{\mathbb{A}}_n$, $(n \geq 1)$, $\tilde{\mathbb{D}}_n$, $(n \geq 4)$, $\tilde{\mathbb{E}}_n$, $(n = 6, 7, 8)$. We will say that a quiver is of affine type $\tilde{\mathbb{A}}_{r,s}$ if it is an orientation of an affine diagram of affine type $\tilde{\mathbb{A}}_{r+s-1}$, with r arrows going

clockwise and s arrows going counterclockwise. Let $\mathfrak{g}_Q$ denote the Kac–Moody algebra associated to Q.

We denote by $\Phi_{>0}$ the set of *positive roots* of $\mathfrak{g}_Q$, by $\Phi^{\mathrm{re}}_{>0}$ the set of positive *real roots* and by $\Phi^{\mathrm{im}}_{>0}$ the set of positive *imaginary roots*. Since Q is affine, there exists a unique $\delta \in \Phi_{>0}$ such that $\Phi^{\mathrm{im}}_{>0} = \mathbb{Z}_{>0}\delta$. We always identify the root lattice of $\mathfrak{g}_Q$ with $\mathbb{Z}^{Q_0}$ by sending the i-th simple root of $\mathfrak{g}_Q$ to the i-th vector of the canonical basis of $\mathbb{Z}^{Q_0}$.

According to Kac's theorem, for any $\boldsymbol{d} \in \mathbb{N}^{Q_0}$, there exists an indecomposable representation M such that $\mathbf{dim}\, M = \boldsymbol{d}$ if and only if $\boldsymbol{d} \in \Phi_{>0}$. Moreover, this representation is unique up to isomorphism if and only if $\boldsymbol{d} \in \Phi^{\mathrm{re}}_{>0}$. A positive root $\boldsymbol{d}$ is called a *Schur root* if there exists a (necessarily indecomposable) representation M of Q such that $\mathbf{dim}\, M = \boldsymbol{d}$ and $\mathrm{End}_{\boldsymbol{k}Q}(M) \simeq \boldsymbol{k}$.

We define a partial order $\leq$ on the root lattice by setting

$$\boldsymbol{e} \leq \boldsymbol{f} \quad \Longleftrightarrow \quad e_i \leq d_i \text{ for any } i \in Q_0,$$

and we set

$$\boldsymbol{e} \lneqq \boldsymbol{f} \quad \text{if } \boldsymbol{e} \leq \boldsymbol{f} \text{ and } \boldsymbol{e} \neq \boldsymbol{f}.$$

The Auslander–Reiten quiver $\Gamma(\boldsymbol{k}Q\text{-mod})$ of $\boldsymbol{k}Q$-mod contains infinitely many connected components. There exists a connected component containing all the projective (resp. injective) modules, called the *preprojective* (resp. *preinjective*) component of $\Gamma(\boldsymbol{k}Q\text{-mod})$ and denoted by $\mathcal{P}$ (resp. $\mathcal{I}$). The other components are called *regular*. A $\boldsymbol{k}Q$-module M is called *preprojective*, *preinjective*, or *regular* if each indecomposable direct summand of M belongs to a component with the same property.

It is convenient to introduce the so-called *defect form* on $\mathbb{Z}^{Q_0}$. It is given by

$$\partial_? : \mathbb{Z}^{Q_0} \to \mathbb{Z}, \quad \boldsymbol{e} \mapsto \partial_{\boldsymbol{e}} = \langle \delta, \boldsymbol{e} \rangle .$$

By definition, the defect ∂_M of a $\boldsymbol{k}Q$-module M is the defect $\partial_{\mathbf{dim}\, M}$ of its dimension vector. It is well-known that an indecomposable $\boldsymbol{k}Q$-module M is preprojective, preinjective, or regular depending on whether ∂_M is negative, positive or zero.

The regular components in $\Gamma(\boldsymbol{k}Q\text{-mod})$ form a $\mathbb{P}^1(\boldsymbol{k})$-family of tubes. Thus, for every tube $\mathcal{T}$, there exists an integer $p \geq 1$, called the *rank* of $\mathcal{T}$, such that $\mathcal{T} \simeq \mathbb{Z}\mathbb{A}_\infty/(\tau^p)$. The tubes of rank 1 are called *homogeneous*, while those of rank $p > 1$ are called *exceptional*. At most three tubes are exceptional in $\Gamma(\boldsymbol{k}Q\text{-mod})$. It is well-known that the full subcategory of $\boldsymbol{k}Q$-mod formed by the objects in any tube $\mathcal{T}$ is standard, that is, isomorphic to the mesh category of $\mathcal{T}$. It is also known that there are neither morphisms nor extensions between pairwise distinct tubes.

An indecomposable regular $\boldsymbol{k}Q$-module M is called *quasisimple* if it is at the mouth of the tube, or equivalently, if it does not contain any proper regular submodule. For any quasisimple module R in a tube $\mathcal{T}$ and any integer $l \geq 1$, we denote by

$R^{(l)}$ the unique indecomposable $\boldsymbol{k}Q$-module with quasisocle R and quasilength l. For any indecomposable regular $\boldsymbol{k}Q$-module $R^{(l)}$, we denote by

$$\operatorname{qsoc} R^{(l)} = R$$

the *quasisocle* of M and by

$$\operatorname{qrad} R^{(l)} = R^{(l-1)}$$

the quasiradical of M with the convention that $R^{(0)} = 0$.

For any indecomposable regular $\boldsymbol{k}Q$-module M, we have

$$M \text{ is rigid} \iff \mathbf{dim}\, M \lneqq \delta; \quad \operatorname{End}_{\boldsymbol{k}Q}(M) \simeq \boldsymbol{k} \iff \mathbf{dim}\, M \leq \delta.$$

Cluster characters associated to modules in tubes are known to be governed by the combinatorics of generalized Chebyshev polynomials. More precisely, it is proved in [Dupont 2009, Theorem 5.1] that for any quasisimple module M in a tube $\mathcal{T}$, we have

$$X_{M^{(l)}} = P_l(X_M, X_{\tau^{-1}M}, \ldots, X_{\tau^{-l+1}M}).$$

In particular, if $\mathcal{T}$ is homogeneous, we get $X_{M^{(l)}} = S_l(X_M)$, recovering a result of [Caldero and Zelevinsky 2006].

In [Dupont 2009, Theorem 7.2], generalized Chebyshev polynomials provide multiplication formulas for cluster characters associated to indecomposable regular $\boldsymbol{k}Q$-modules. The following theorem will be essential in the proofs.

Theorem 2.2 [Dupont 2009]. *Let Q be an affine quiver and $\mathcal{T}$ be a tube of rank p in $\Gamma(\boldsymbol{k}Q\text{-mod})$. Let $R_i, i \in \mathbb{Z}$ denote the quasisimple modules in $\mathcal{T}$ ordered such that $\tau R_i \simeq R_{i-1}$ and $R_{i+p} \simeq R_i$ for any $i \in \mathbb{Z}$. Let $m, n > 0$ be integers and $j \in [0, p-1]$. Then, for every $k \in \mathbb{Z}$ such that $0 < j + kp \leq n$ and $m \geq n - j - kp$, we have the identity*

$$X_{R_j^{(m)}} X_{R_0^{(n)}} = X_{R_0^{(m+j+kp)}} X_{R_j^{(n-j-kp)}} + X_{R_0^{(j+kp-1)}} X_{R_{n+1}^{(m+j+kp-n-1)}}.$$

Bases in affine cluster algebras. We shall now review some results concerning the construction of $\mathbb{Z}$-bases in cluster algebras associated to affine quivers. In this section, Q still denotes an affine quiver with positive minimal imaginary root δ.

If M, N are quasisimple modules in distinct homogeneous tubes, then $X_M = X_N$; see [Dupont 2008], for example. We denote this common value by X_δ, and call it the *generic variable of dimension* δ, as in that earlier paper.

Theorem 2.3 [Dupont 2008; Ding et al. 2009]. *Let Q be an affine quiver. Then*

$$\mathcal{G}(Q) = \mathcal{M}(Q) \sqcup \left\{ X_\delta^l X_R \mid l \geq 1, R \text{ is a regular rigid } \boldsymbol{k}Q\text{-module} \right\}$$

is a $\mathbb{Z}$-basis of $\mathcal{A}(Q)$.

Moreover, den *induces a* 1-1 *correspondence from $\mathcal{G}(Q)$ to $\mathbb{Z}^{Q_0}$.*

The set $\mathcal{G}(Q)$ is called the *generic basis* of $\mathcal{A}(Q)$.

Since F_l and S_l are monic polynomials of degree l, it follows that, for any affine quiver Q, the sets

$$\mathcal{B}(Q) = \mathcal{M}(Q) \sqcup \{F_l(X_\delta)X_R \mid l \geq 1,\ R \text{ is a regular rigid } \boldsymbol{k}Q\text{-module}\}$$

and

$$\mathcal{C}(Q) = \mathcal{M}(Q) \sqcup \{S_l(X_\delta)X_R \mid l \geq 1,\ R \text{ is a regular rigid } \boldsymbol{k}Q\text{-module}\}$$

are $\mathbb{Z}$-bases of the cluster algebra $\mathcal{A}(Q)$.

When Q is the Kronecker quiver, $\mathcal{B}(Q)$ coincides with the canonically positive basis constructed in [Sherman and Zelevinsky 2004] and $\mathcal{C}(Q)$ coincides with the basis constructed in [Caldero and Zelevinsky 2006]. When Q is a quiver of affine type $\tilde{\mathbb{A}}_{2,1}$, the basis $\mathcal{B}(Q)$ is the canonically positive basis of $\mathcal{A}(Q)$ constructed in [Cerulli 2009].

Since $X_\delta = X_M$ for any quasisimple module M in a homogeneous tube, it follows that $S_l(X_\delta) = X_{M^{(l)}}$ for any $l \geq 0$, so the set $\mathcal{C}(Q)$ has an interpretation in terms of the cluster character $X_?$. No such interpretation had been known for the set $\mathcal{B}(Q)$; this paper provides one.

The map $\phi : \mathcal{G}(Q) \to \mathcal{B}(Q)$ preserving cluster monomials and sending $X_\delta^l X_R$ to $F_l(X_\delta)X_R$ for any $l \geq 1$ and any rigid regular module R is a 1-1 correspondence. We denote by

$$\mathfrak{b}_? : \mathbb{Z}^{Q_0} \xrightarrow{1:1} \mathcal{B}(Q), \quad \boldsymbol{d} \mapsto \mathfrak{b}_{\boldsymbol{d}}$$

the 1-1 correspondence obtained by composing the bijection above with the one provided in Theorem 2.3.

3. Difference properties of higher orders

Here Q still denotes an affine quiver with positive minimal imaginary root δ.

The difference property. In [Dupont 2008] we introduced the *difference property*, which relates the possibly different values of cluster characters evaluated at different indecomposable representations of dimension δ. The difference property was crucial in that article. It is also an essential ingredient in this one, since transverse Grassmannians will arise precisely from difference properties of higher orders.

This difference property was established in [Dupont 2008] for affine type $\tilde{\mathbb{A}}$ and in [Ding et al. 2009] in general. It can be expressed as follows:

Theorem 3.1 [Dupont 2008; Ding et al. 2009]. *If Q is an affine quiver and M is any indecomposable module of dimension δ, then*

$$\mathfrak{b}_\delta = X_\delta = X_M - X_{\operatorname{qrad} M / \operatorname{qsoc} M},$$

with the convention that $X_{\operatorname{qrad} M / \operatorname{qsoc} M} = 0$ if M is quasisimple.

Higher-difference properties. The aim of this section is to provide an analogue of Theorem 3.1 for $\mathfrak{b}_{\boldsymbol{d}}$ when $\boldsymbol{d}$ is any positive root with zero defect. We will first consider the imaginary roots and then the real roots of defect zero.

We fix a tube $\mathcal{T}$ in $\Gamma(\boldsymbol{k}Q\text{-mod})$ of rank $p \geq 1$. The quasisimples of $\mathcal{T}$ are denoted by R_i, with $i \in \mathbb{Z}/p\mathbb{Z}$, ordered so that $\tau R_i \simeq R_{i-1}$ for any $i \in \mathbb{Z}/p\mathbb{Z}$. Note that for any $l \geq 1$ and $0 \leq k \leq p-1$ and any $i \in \mathbb{Z}/p\mathbb{Z}$, we have $\mathbf{dim}\, R_i^{(lp)} = l\delta \in \Phi_{>0}^{\mathrm{im}}$ and $\mathbf{dim}\, R_i^{(lp+k)} \in \Phi_{>0}^{\mathrm{re}}$ if $k \neq 0$.

The following technical lemma will be used in the proof of Proposition 3.3:

Lemma 3.2. *With the notation above, for any $l \geq 1$,*

$$X_{R_0^{(lp-1)}} X_{R_1^{(p-1)}} = X_{R_0^{(p-1)}} X_{R_1^{(lp-1)}}.$$

Proof. We first notice that generalized Chebyshev polynomials are symmetric in the sense that for every $i \in \mathbb{Z}$ and $n \geq 1$,

$$P_n(x_i, \ldots, x_{i+n-1}) = P_n(x_{i+n-1}, \ldots, x_i).$$

If $l = 1$, the result is obvious. We thus fix some $l \geq 2$. For technical convenience, we denote by R_i, $i \in \mathbb{Z}$ the quasisimple modules in $\mathcal{T}$ and we assume that $R_i \simeq R_{i+p}$ for every $i \in \mathbb{Z}$. Consider the morphism of $\mathbb{Z}$-algebras

$$\begin{aligned} \phi : \mathbb{Z}[X_{R_0}, \ldots, X_{R_{lp-1}}] &\to \mathbb{Z}[X_{R_0}, \ldots, X_{R_{lp-1}}] \\ X_{R_i} &\mapsto X_{R_{lp-1-i}} \qquad \text{for all } i = 0, \ldots, lp-1. \end{aligned}$$

It is well-defined since $X_{R_0}, \ldots, X_{R_{p-1}}$ are known to be algebraically independent over $\mathbb{Z}$ (see for example [Dupont 2009]).

According to Theorem 2.2, we have

$$X_{R_1^{(p-1)}} X_{R_0^{(lp-1)}} = X_{R_0^{(p)}} X_{R_1^{(lp-2)}} - X_{R_{p+1}^{((l-1)p-2)}}.$$

According to [Dupont 2009, Theorem 5.1], each of the $X_{R_j}^{(k)}$ appearing above lies in $\mathbb{Z}[X_{R_0}, \ldots, X_{R_{lp-1}}]$. We can thus apply ϕ and we get

$$\phi(X_{R_1^{(p-1)}})\phi(X_{R_0^{(lp-1)}}) = \phi(X_{R_0^{(p)}})\phi(X_{R_1^{(lp-2)}}) - \phi(X_{R_{p+1}^{((l-1)p-2)}}). \tag{3-1}$$

We now compute these images under ϕ.

$$\begin{aligned} \phi(X_{R_1^{(p-1)}}) &= \phi(P_{p-1}(X_{R_1}, \ldots, X_{R_{p-1}})) \\ &= P_{p-1}(\phi(X_{R_1}), \ldots, \phi(X_{R_{p-1}})) = P_{p-1}(X_{R_{lp-2}}, \ldots, X_{R_{(l-1)p}}) \\ &= P_{p-1}(X_{R_{(l-1)p}}, \ldots, X_{R_{lp-2}}) = X_{R_{(l-1)p}^{(p-1)}} = X_{R_0^{(p-1)}}; \end{aligned}$$

$$\begin{aligned}
\phi(X_{R_0^{(lp-1)}}) &= \phi(P_{lp-1}(X_{R_0},\dots,X_{R_{lp-2}})) \\
&= P_{lp-1}(\phi(X_{R_0}),\dots,\phi(X_{R_{lp-2}})) = P_{lp-1}(X_{R_{lp-1}},\dots,X_{R_1}) \\
&= P_{lp-1}(X_{R_1},\dots,X_{R_{lp-1}}) = X_{R_1^{(lp-1)}};
\end{aligned}$$

$$\begin{aligned}
\phi(X_{R_0^{(p)}}) &= \phi(P_p(X_{R_0},\dots,X_{R_{p-1}})) = P_p(\phi(X_{R_0}),\dots,\phi(X_{R_{p-1}})) \\
&= P_p(X_{R_{lp-1}},\dots,X_{R_{(l-1)p}}) = P_p(X_{R_{(l-1)p}},\dots,X_{R_{lp-1}}) \\
&= X_{R_{(l-1)p}^{(p)}} = X_{R_0^{(p)}};
\end{aligned}$$

$$\begin{aligned}
\phi(X_{R_1^{(lp-2)}}) &= \phi(P_{lp-2}(X_{R_1},\dots,X_{R_{lp-2}})) \\
&= P_{lp-2}(\phi(X_{R_1}),\dots,\phi(X_{R_{lp-2}})) = P_{lp-2}(X_{R_{lp-2}},\dots,X_{R_1}) \\
&= P_{lp-2}(X_{R_1},\dots,X_{R_{lp-2}}) = X_{R_1^{(lp-2)}};
\end{aligned}$$

$$\begin{aligned}
\phi(X_{R_{p+1}^{((l-1)p-2)}}) &= \phi(P_{(l-1)p-2}(X_{R_{p+1}},\dots,X_{R_{lp-2}})) \\
&= P_{(l-1)p-2}(\phi(X_{R_{p+1}}),\dots,\phi(X_{R_{lp-2}})) \\
&= P_{(l-1)p-2}(X_{R_{(l-1)p-2}},\dots,X_{R_1}) \\
&= P_{(l-1)p-2}(X_{R_1},\dots,X_{R_{(l-1)p-2}}) = X_{R_1^{((l-1)p-2)}}.
\end{aligned}$$

Substituting in (3-1), we get

$$\begin{aligned}
X_{R_0^{(p-1)}} X_{R_1^{(lp-1)}} &= X_{R_0^{(p)}} X_{R_1^{(lp-2)}} - X_{R_1^{((l-1)p-2)}} \\
&= X_{R_0^{(p)}} X_{R_1^{(lp-2)}} - X_{R_{p+1}^{((l-1)p-2)}} = X_{R_1^{(p-1)}} X_{R_0^{(lp-1)}}.
\end{aligned}$$

□

We can now prove some higher-difference properties for imaginary roots.

Proposition 3.3. *Fix $l \geq 1$. Then for any indecomposable representation M in* $\mathrm{rep}_k(Q, l\delta)$, *we have*

$$\mathfrak{b}_{l\delta} = F_l(X_\delta) = X_M - X_{\operatorname{qrad} M/\operatorname{qsoc} M},$$

with the convention that $X_{\operatorname{qrad} M/\operatorname{qsoc} M} = 0$ if M is quasisimple.

Proof. We first treat the case where M is an indecomposable representation of dimension $l\delta$ in a homogeneous tube. It is not necessary to prove it separately but in this particular case, the proof is straightforward. We write $M = R^{(l)}$ for some quasisimple module R in a homogeneous tube. If $l = 1$, the proposition follows from Theorem 3.1. If $l \geq 2$, $\operatorname{qrad} M/\operatorname{qsoc} M \simeq R^{(l-2)}$, so that

$$\begin{aligned}
X_M - X_{\operatorname{qrad} M/\operatorname{qsoc} M} &= X_{R^{(l)}} - X_{R^{(l-2)}} \\
&= S_l(X_R) - S_{l-2}(X_R) = F_l(X_R) = F_l(X_\delta).
\end{aligned}$$

We now assume that M is an indecomposable representation of dimension $l\delta$ in an exceptional tube $\mathcal{T}$ of rank $p \geq 2$. We denote by $R_0, \ldots, R_{p-1}$ the quasisimples in $\mathcal{T}$ ordered such that $\tau R_i \simeq R_{i-1}$ for any $i \in \mathbb{Z}/p\mathbb{Z}$. We can thus write $M \simeq R_i^{(lp)}$ for some $i \in \mathbb{Z}/p\mathbb{Z}$. Without loss of generality, we assume that $i = 0$. In order to simplify the notation, for any $l \geq 1$, we write

$$\Delta_l = X_{R_0^{(lp)}} - X_{R_1^{(lp-2)}}.$$

We thus have to prove that for any $l \geq 1$,

$$\Delta_l = F_l(X_\delta).$$

The central tool in this proof is Theorem 2.2. According to Theorem 3.1, we have

$$X_\delta = X_{R_0^{(p)}} - X_{R_1^{(p-2)}},$$

so the proposition holds for $l = 1$.

We now prove it for $l = 2$. We have

$$\begin{aligned} F_2(X_\delta) = X_\delta^2 - 2 &= (X_{R_0^{(p)}} - X_{R_1^{(p-2)}})^2 - 2 \\ &= X_{R_0^{(p)}}^2 + X_{R_1^{(p-2)}}^2 - 2X_{R_0^{(p)}} X_{R_1^{(p-2)}} - 2, \end{aligned}$$

but according to the almost split multiplication formula [Caldero and Chapoton 2006, Proposition 3.10], we have

$$X_{R_0^{(p-1)}} X_{R_1^{(p-1)}} = X_{R_0^{(p)}} X_{R_1^{(p-2)}},$$

so

$$F_2(X_\delta) = X_{R_0^{(p)}}^2 - 2X_{R_0^{(p-1)}} X_{R_1^{(p-1)}} + X_{R_1^{(p-2)}}^2.$$

But, according to Theorem 2.2, we have

$$X_{R_0^{(p)}}^2 = X_{R_0^{(p)}} X_{R_0^{(p)}} = X_{R_0^{(2p)}} + X_{R_0^{(p-1)}} X_{R_1^{(p-1)}},$$

so that finally

$$F_2(X_\delta) = X_{R_0^{(2p)}} - X_{R_0^{(p-1)}} X_{R_1^{(p-1)}} + X_{R_1^{(p-2)}}^2.$$

Thus,

$$\begin{aligned} F_2(X_\delta) = \Delta_2 &\iff -X_{R_1^{(2p-2)}} = X_{R_1^{(p-2)}}^2 - X_{R_0^{(p-1)}} X_{R_1^{(p-1)}} \\ &\iff X_{R_1^{(2p-2)}} + X_{R_1^{(p-2)}}^2 - X_{R_0^{(p-1)}} X_{R_1^{(p-1)}} = 0. \end{aligned}$$

But

$$X_{R_1^{(2p-2)}} = -X_{R_1^{(p-3)}} X_{R_0^{(p-1)}} + X_{R_1^{(p-2)}} X_{R_{p-1}^{(p)}},$$

so

$$F_2(X_\delta) = \Delta_2 \iff X^2_{R_1^{(p-2)}} + X_{R_1^{(p-2)}} X_{R_{p-1}^{(p)}} - X_{R_0^{(p-1)}} X_{R_1^{(p-1)}} - X_{R_0^{(p-1)}} X_{R_1^{(p-3)}} = 0$$
$$\iff X_{R_1^{(p-2)}} \left[X_{R_1^{(p-2)}} + X_{R_{p-1}^{(p)}} \right] - X_{R_0^{(p-1)}} \left[X_{R_1^{(p-3)}} + X_{R_1^{(p-1)}} \right] = 0.$$

Theorem 2.2 gives

$$X_{R_{p-1}} X_{R_0^{(p-1)}} = X_{R_1^{(p-2)}} + X_{R_{p-1}^{(p)}} \quad \text{and} \quad X_{R_1^{(p-2)}} X_{R_{p-1}} = X_{R_1^{(p-3)}} + X_{R_1^{(p-1)}},$$

so

$$F_2(X_\delta) = \Delta_2$$

and the proposition is proved for $l = 2$.

For $l > 2$, we will use the three-term relations for first kind Chebyshev polynomials

$$F_l(x) = x F_{l-1}(x) - F_{l-2}(x).$$

Thus, it is enough to prove that for any $l \geq 2$,

$$\Delta_{l+1} = \Delta_1 \Delta_l - \Delta_{l-1}.$$

In order to simplify our notation, we denote by LHS the left side of the equality above and by RHS the right side. We thus have

$$\begin{aligned} \text{RHS} &= (X_{R_0^{(p)}} - X_{R_1^{(p-2)}})(X_{R_0^{(lp)}} - X_{R_1^{(lp-2)}}) - (X_{R_0^{((l-1)p)}} - X_{R_1^{((l-1)p-2)}}) \\ &= X_{R_0^{(p)}} X_{R_0^{(lp)}} - X_{R_0^{(p)}} X_{R_1^{(lp-2)}} - X_{R_1^{(p-2)}} X_{R_0^{(lp)}} \\ &\quad + X_{R_1^{(p-2)}} X_{R_1^{(lp-2)}} - X_{R_0^{((l-1)p)}} + X_{R_1^{((l-1)p-2)}}. \end{aligned}$$

But, according to the multiplication theorem, we get

$$X_{R_0^{(p)}} X_{R_0^{(lp)}} = X_{R_0^{((l+1)p)}} + X_{R_0^{(p-1)}} X_{R_1^{(lp-1)}},$$

so

$$\text{LHS} = \text{RHS} \iff X_{R_0^{(p-1)}} X_{R_1^{(lp-1)}} - X_{R_0^{(p)}} X_{R_1^{(lp-2)}} - X_{R_1^{(p-2)}} X_{R_0^{(lp)}}$$
$$+ X_{R_1^{(p-2)}} X_{R_1^{(lp-2)}} - X_{R_0^{((l-1)p)}} + X_{R_1^{((l-1)p-2)}} + X_{R_1^{((l+1)p-2)}} = 0.$$

Applying the multiplication theorem, we get

$$X_{R_0^{(lp-2)}} X_{R_{lp-2}^{(p)}} = X_{R_0^{((l+1)p-2)}} + X_{R_0^{(lp-3)}} X_{R_{lp-1}^{(p-1)}},$$

so

$$X_{R_1^{((l+1)p-2)}} = X_{R_1^{(lp-2)}} X_{R_{p-1}^{(p)}} - X_{R_1^{(lp-3)}} X_{R_0^{(p-1)}},$$

and thus

$$\text{LHS} = \text{RHS} \iff X_{R_0^{(p-1)}} X_{R_1^{(lp-1)}} - X_{R_0^{(p)}} X_{R_1^{(lp-2)}} - X_{R_1^{(p-2)}} X_{R_0^{(lp)}} + X_{R_1^{(p-2)}} X_{R_1^{(lp-2)}}$$
$$- X_{R_0^{((l-1)p)}} + X_{R_1^{((l-1)p-2)}} + X_{R_1^{(lp-2)}} X_{R_{p-1}^{(p)}} - X_{R_1^{(lp-3)}} X_{R_0^{(p-1)}} = 0.$$

But

$$X_{R_0^{(p)}} X_{R_1^{(lp-2)}} = X_{R_0^{(lp-1)}} X_{R_1^{(p-1)}} + X_{R_1^{((l-1)p-2)}};$$

hence,

$$\begin{aligned}
\mathrm{LHS} = \mathrm{RHS} \iff\ & X_{R_0^{(p-1)}} X_{R_1^{(lp-1)}} - X_{R_0^{(lp-1)}} X_{R_1^{(p-1)}} \\
& - X_{R_1^{(p-2)}} X_{R_0^{(lp)}} + X_{R_1^{(p-2)}} X_{R_1^{(lp-2)}} \\
& - X_{R_0^{((l-1)p)}} + X_{R_1^{(lp-2)}} X_{R_{p-1}^{(p)}} - X_{R_1^{(lp-3)}} X_{R_0^{(p-1)}} = 0 \\
\iff\ & X_{R_0^{(p-1)}} X_{R_1^{(lp-1)}} - X_{R_0^{(lp-1)}} X_{R_1^{(p-1)}} \\
& - X_{R_1^{(p-2)}} X_{R_0^{(lp)}} - X_{R_0^{((l-1)p)}} - X_{R_1^{(lp-3)}} X_{R_0^{(p-1)}} \\
& + X_{R_1^{(lp-2)}} \left(X_{R_1^{(p-2)}} + X_{R_{p-1}^{(p)}} \right) = 0.
\end{aligned}$$

Theorem 2.2 gives

$$X_{R_{p-1}} X_{R_0^{(p-1)}} = X_{R_1^{(p-2)}} + X_{R_{p-1}^{(p)}},$$

so

$$\begin{aligned}
\mathrm{LHS} = \mathrm{RHS} \iff\ & X_{R_0^{(p-1)}} \left(X_{R_1^{(lp-1)}} - X_{R_1^{(lp-3)}} + X_{R_1^{(lp-2)}} X_{R_{p-1}} \right) \\
& - X_{R_0^{((l-1)p)}} - X_{R_0^{(lp-1)}} X_{R_1^{(p-1)}} - X_{R_1^{(p-2)}} X_{R_0^{(lp)}} = 0.
\end{aligned}$$

The three-term relation for generalized Chebyshev polynomials gives

$$X_{R_1^{(lp-1)}} = X_{R_{p-1}} X_{R_1^{(lp-2)}} - X_{R_1^{(lp-3)}}.$$

Thus

$$\begin{aligned}
&\mathrm{LHS} = \mathrm{RHS} \\
&\quad \iff 2X_{R_0^{(p-1)}} X_{R_1^{(lp-1)}} - \left(X_{R_0^{((l-1)p)}} + X_{R_0^{(lp-1)}} X_{R_1^{(p-1)}} + X_{R_0^{(lp)}} X_{R_1^{(p-2)}} \right) = 0.
\end{aligned}$$

Theorem 2.2 gives

$$X_{R_0^{(p-1)}} X_{R_1^{(lp-1)}} = X_{R_0^{(lp)}} X_{R_1^{(p-2)}} + X_{R_0^{((l-1)p)}},$$

so we finally get

$$\mathrm{LHS} = \mathrm{RHS} \iff X_{R_0^{(p-1)}} X_{R_1^{(lp-1)}} - X_{R_0^{(lp-1)}} X_{R_1^{(p-1)}} = 0.$$

The second equality holds by Lemma 3.2, so we have proved that for any $l \geq 2$,

$$\Delta_{l+1} = \Delta_1 \Delta_l - \Delta_{l-1}.$$

Since we know that $\Delta_1 = X_\delta$ and $\Delta_2 = F_2(X_\delta)$, it follows that $\Delta_l = F_l(X_\delta)$ for any $l \geq 1$. □

We are now able to prove the general difference property:

Theorem 3.4. *Let Q be an affine quiver, $\mathcal{T}$ be a tube of rank $p \geq 1$ in $\Gamma(\boldsymbol{k}Q\text{-mod})$. For any $l \geq 1$ and any $0 \leq k \leq p-1$, we have*

$$\mathfrak{b}_{l\delta+\mathbf{dim}\, R_0^{(k)}} = X_{R_0^{(k)}} F_l(X_\delta) = X_{R_0^{(lp+k)}} - X_{R_{k+1}^{(lp-k-2)}},$$

with the convention that $X_{R_0^{(-1)}} = 0$.

Proof. The first equality follows from

$$\mathrm{den}(X_{R_0^{(k)}} X_\delta^l) = \mathbf{dim}\, R_0^{(k)} + l\delta,$$

so

$$\mathfrak{b}_{l\delta+\mathbf{dim}\, R_0^{(k)}} = X_{R_0^{(k)}} F_l(X_\delta).$$

We now prove that

$$X_{R_0^{(k)}} F_l(X_\delta) = X_{R_0^{(lp+k)}} - X_{R_{k+1}^{(lp-k-2)}},$$

with the convention that $X_{R_0^{(-1)}} = 0$.

We denote by LHS the left side and by RHS the right side of this equation.

$$\begin{aligned}\mathrm{LHS} &= X_{R_0^{(k)}}\left(X_{R_k^{(lp)}} - X_{R_{k+1}^{(lp-2)}}\right) = X_{R_0^{(k)}} X_{R_k^{(lp)}} - X_{R_0^{(k)}} X_{R_{k+1}^{(lp-2)}} \\ &= X_{R_0^{(lp+k)}} + X_{R_0^{(k-1)}} X_{R_{k+1}^{(lp-1)}} - X_{R_0^{(k)}} X_{R_{k+1}^{(lp-2)}}.\end{aligned}$$

If $l = 1$ and $k = p-1$, we get

$$\mathrm{LHS} = X_{R_0^{(lp+k)}} + X_{R_0^{(p-2)}} X_{R_0^{(p-1)}} - X_{R_0^{(p-1)}} X_{R_0^{(p-2)}} = X_{R_0^{(lp+k)}} = \mathrm{RHS}.$$

Otherwise, LHS = RHS if and only if

$$X_{R_{k+1}^{(lp-k-2)}} = X_{R_0^{(k)}} X_{R_{k+1}^{(lp-2)}} - X_{R_0^{(k-1)}} X_{R_{k+1}^{(lp-1)}}. \tag{3-2}$$

Using the three-term recurrence relations for generalized Chebyshev polynomials, we have

$$X_{R_0^{(k)}} = X_{R_{k-1}} X_{R_0^{(k-1)}} - X_{R_0^{(k-2)}} \quad \text{and} \quad X_{R_{k+1}^{(lp-1)}} = X_{R_{lp+k-1}} X_{R_{k+1}^{(lp-2)}} - X_{R_{k+1}^{(lp-3)}},$$

so that, replacing in the right side of (3-2), we get

$$X_{R_0^{(k)}} X_{R_{k+1}^{(lp-2)}} - X_{R_0^{(k-1)}} X_{R_{k+1}^{(lp-1)}} = X_{R_0^{(k-1)}} X_{R_{k+1}^{(lp-3)}} - X_{R_0^{(k-2)}}.$$

Thus, by induction, we get

$$X_{R_0^{(k)}} X_{R_{k+1}^{(lp-2)}} - X_{R_0^{(k-1)}} X_{R_{k+1}^{(lp-1)}} = X_{R_0} X_{R_{k+1}^{(lp-k-1)}} - X_{R_{k+1}^{(lp-k)}}.$$

Now, the three-term recurrence relation gives

$$X_{R_{k+1}^{(lp-k)}} = X_{R_{k+1+lp-k-1}} X_{R_{k+1}^{(lp-k-1)}} - X_{R_{k+1}^{(lp-k-2)}} = X_{R_0} X_{R_{k+1}^{(lp-k-1)}} - X_{R_{k+1}^{(lp-k-2)}},$$

and thus

$$X_{R_0} X_{R_{k+1}^{(lp-k-1)}} - X_{R_{k+1}^{(lp-k)}} = X_{R_{k+1}^{(lp-k-2)}},$$

proving that (3-2) holds. □

As a corollary, for any positive root $\boldsymbol{d}$ with defect zero, we obtain a description of $\mathfrak{b}_{\boldsymbol{d}}$ as a certain difference of cluster characters:

Corollary 3.5. *Let Q be an affine quiver and $\boldsymbol{d}$ be a positive root with defect zero. Let M be any indecomposable representation of dimension $\boldsymbol{d}$. Then there exists a quasisimple module R_0 in a tube of rank $p \geq 1$, an integer $0 \leq k \leq p-1$, and an integer $l \geq 0$ such that $\boldsymbol{d} = l\delta + \mathbf{dim}\, R_0^{(k)}$. Moreover, for any such R_0, k, l, we have*

$$\mathfrak{b}_{\boldsymbol{d}} = X_{R_0^{(k)}} F_l(X_\delta) = X_{R_0^{(lp+k)}} - X_{R_{k+1}^{(lp-k-2)}},$$

where R_i, with $i \in \mathbb{Z}/p\mathbb{Z}$, are the quasisimple modules in $\mathcal{T}$ ordered such that $\tau R_i \simeq R_{i-1}$ for every $i \in \mathbb{Z}/p\mathbb{Z}$.

4. Integrable bundles on $\mathrm{rep}_{\boldsymbol{k}}(Q)$ and their characters

In the previous section, we obtained a realization of the elements $\mathfrak{b}_{\boldsymbol{d}}$ associated to defect zero roots as differences of cluster characters. The aim of this section is to introduce a new map θ_{Tr} such that these elements correspond precisely to values of θ_{Tr}.

Unless otherwise specified, Q denotes an arbitrary acyclic quiver in this section.

Integrable bundles. For any $\boldsymbol{d} \in \mathbb{N}^{Q_0}$, the representation variety $\mathrm{rep}_{\boldsymbol{k}}(Q, \boldsymbol{d})$ of dimension $\boldsymbol{d}$ is the set of all representations M of Q with dimension vector $\boldsymbol{d}$. Note that

$$\mathrm{rep}_{\boldsymbol{k}}(Q, \boldsymbol{d}) \simeq \prod_{i \to j \in Q_1} \mathrm{Hom}_{\boldsymbol{k}}(\boldsymbol{k}^{d_i}, \boldsymbol{k}^{d_j}),$$

so that $\mathrm{rep}_{\boldsymbol{k}}(Q, \boldsymbol{d})$ is an affine irreducible variety.

Definition 4.1. Let Q be any acyclic quiver. An *integrable bundle* on $\mathrm{rep}_{\boldsymbol{k}}(Q)$ is a map

$$\mathcal{F} : M \mapsto \mathcal{F}(M) \subset \mathrm{Gr}(M)$$

defined on the set of indecomposable objects in $\mathrm{rep}_{\boldsymbol{k}}(Q)$ such that for any $M \in \mathrm{rep}_{\boldsymbol{k}}(Q)$,

- for any $\boldsymbol{e} \in \mathbb{N}^{Q_0}$, $\mathcal{F}_{\boldsymbol{e}}(M) = \mathcal{F}(M) \cap \mathrm{Gr}_{\boldsymbol{e}}(M)$ is constructible, and
- if $M \simeq N$ in $\mathrm{rep}_{\boldsymbol{k}}(Q)$, then $\chi(\mathcal{F}_{\boldsymbol{e}}(M)) \simeq \chi(\mathcal{F}_{\boldsymbol{e}}(N))$ for any $\boldsymbol{e} \in \mathbb{N}^{Q_0}$.

Remark 4.2. Note that, if $\mathscr{F}$ is an integrable bundle on $\mathrm{rep}_{\boldsymbol{k}}(Q)$, then the family $(\chi(\mathscr{F}_{\boldsymbol{e}}(M)))_{\boldsymbol{e}\in\mathbb{N}^{Q_0}}$ has finite support.

Example 4.3. The map $M \mapsto \mathrm{Gr}(M)$ is an integrable bundle called the *quiver Grassmannian bundle*.

For any $\boldsymbol{k}Q$-module M and any submodule $U \subset M$, we set

$$\mathrm{Gr}^U(M) = \{N \in \mathrm{Gr}(M) \mid U \text{ is a submodule of } N\}.$$

This is a constructible subset in the quiver Grassmannian $\mathrm{Gr}(M)$.

If Q is an affine quiver, we define another integrable bundle Tr as follows. Let M be an indecomposable $\boldsymbol{k}Q$-module. If M is rigid, we set $\mathrm{Tr}(M) = \mathrm{Gr}(M)$. If M is not rigid, it is regular and we can thus write $M = R_0^{(lp+k)}$ for some quasisimple module R_0 in a tube of rank $p \geq 1$, $l \geq 1$ and $0 \leq k \leq p-1$. There exists a nonzero monomorphism $\imath : R_0^{(lp-1)} \to R_0^{(lp)}$ such that

$$\mathrm{Hom}_{\boldsymbol{k}Q}(R_0^{(lp-1)}, R_0^{(lp)}) \simeq \boldsymbol{k}\imath.$$

The set $\imath(\mathrm{Gr}^{R_0^{(k+1)}}(R_0^{(lp-1)}))$ is a constructible subset of $\mathrm{Gr}(R_0^{(lp)})$, and since

$$\mathrm{Hom}_{\boldsymbol{k}Q}(R_0^{(lp-1)}, R_0^{(lp)}) \simeq \boldsymbol{k}\imath,$$

it does not depend on the choice of $\imath$. We can thus identify $\mathrm{Gr}^{R_0^{(k+1)}}(R_0^{(lp-1)})$ with a constructible subset of $\mathrm{Gr}(R_0^{(lp)})$. With these notations and identifications, we set

$$\mathrm{Tr}(M) = \mathrm{Gr}(M) \setminus \mathrm{Gr}^{R_0^{(k+1)}}(R_0^{(lp-1)}).$$

Note that if $l = 0$, M is rigid and we recover the equality $\mathrm{Tr}(M) = \mathrm{Gr}(M)$.

For every dimension vector $\boldsymbol{e} \in \mathbb{N}^{Q_0}$ and any indecomposable $\boldsymbol{k}Q$-module M, the *transverse quiver Grassmannian of M* (of dimension $\boldsymbol{e}$) is the constructible subset of $\mathrm{Gr}_{\boldsymbol{e}}(M)$

$$\mathrm{Tr}_{\boldsymbol{e}}(M) = \{N \in \mathrm{Tr}(M) \mid \mathbf{dim}\, N = \boldsymbol{e}\}.$$

The map

$$\mathrm{Tr} : M \mapsto \mathrm{Tr}(M) \subset \mathrm{Gr}(M)$$

is an integrable bundle on $\mathrm{rep}_{\boldsymbol{k}}(Q)$.

Character associated to an integrable bundle. Extending an idea of Caldero and Chapoton, we associate to any integrable bundle on $\mathrm{rep}_{\boldsymbol{k}}(Q)$ a map from the set of objects in $\mathscr{C}_Q$ to the ring $\mathbb{Z}[\boldsymbol{u}^{\pm 1}]$ of Laurent polynomials in the initial cluster of $\mathscr{A}(Q)$.

Definition 4.4. Let $\mathscr{F}$ be an integrable bundle on $\mathrm{rep}_{\boldsymbol{k}}(Q)$. The *character associated to $\mathscr{F}$* is the map

$$\theta_{\mathscr{F}}(?) : \mathrm{Ob}(\mathscr{C}_Q) \to \mathbb{Z}[\boldsymbol{u}^{\pm 1}]$$

given by:

- If $M \simeq P_i[1]$ for some $i \in Q_0$, then $\theta_{\mathscr{F}}(P_i[1]) = u_i$.
- If M is an indecomposable $\boldsymbol{k}Q$-module, then

$$\theta_{\mathscr{F}}(M) = \sum_{\boldsymbol{e} \in \mathbb{N}^{Q_0}} \chi(\mathscr{F}_{\boldsymbol{e}}(M)) \prod_{i \in Q_0} u_i^{-\langle \boldsymbol{e}, S_i \rangle - \langle S_i, \mathbf{dim}\, M - \boldsymbol{e} \rangle}.$$

- $\theta_{\mathscr{F}}(M \oplus N) = \theta_{\mathscr{F}}(M)\theta_{\mathscr{F}}(N)$ for any two objects M, N in $\mathscr{C}_Q$.

We now prove that θ_{Tr} coincides with $X_?$ on the set of rigid objects in $\mathscr{C}_Q$. In particular, this will allow us to realize cluster monomials in terms of θ_{Tr}.

Lemma 4.5. *Let Q be an affine quiver. Then, for any rigid object M in $\mathscr{C}_Q$, we have $\theta_{\mathrm{Tr}}(M) = X_M$. In particular,*

$$\mathscr{M}(Q) = \{\theta_{\mathrm{Tr}}(M) \mid M \text{ is rigid in } \mathscr{C}_Q\}.$$

Proof. Let M be a rigid object in $\mathscr{C}_Q$. We write

$$M = P_{i_1}[1] \oplus \cdots \oplus P_{i_r}[1] \oplus M_1 \oplus \cdots \oplus M_s,$$

where each P_{i_j} is an indecomposable projective $\boldsymbol{k}Q$-module and each M_i is an indecomposable module. Also, since M is rigid, each M_i is a rigid $\boldsymbol{k}Q$-module and thus $\mathrm{Tr}(M_i) = \mathrm{Gr}(M_i)$ for any $i \in \{1, \ldots, s\}$. In particular, it follows that $\theta_{\mathrm{Tr}}(M_i) = X_{M_i}$ for any $i \in \{1, \ldots, s\}$. Then

$$\begin{aligned}
\theta_{\mathrm{Tr}}(M) &= \theta_{\mathrm{Tr}}(P_{i_1}[1] \oplus \cdots \oplus P_{i_r}[1] \oplus M_1 \oplus \cdots \oplus M_s) \\
&= \theta_{\mathrm{Tr}}(P_{i_1}[1]) \cdots \theta_{\mathrm{Tr}}(P_{i_r}[1]) \theta_{\mathrm{Tr}}(M_1) \cdots \theta_{\mathrm{Tr}}(M_s) \\
&= u_{i_1} \cdots u_{i_r} X_{M_1} \cdots X_{M_s} \\
&= X_{P_{i_1}[1] \oplus \cdots \oplus P_{i_r}[1] \oplus M_1 \oplus \cdots \oplus M_s} = X_M.
\end{aligned}$$

The second assertion follows directly from Caldero and Keller's realization of cluster monomials:

$$\mathscr{M}(Q) = \left\{X_M \mid M \text{ is rigid in } \mathscr{C}_Q\right\} = \left\{\theta_{\mathrm{Tr}}(M) \mid M \text{ is rigid in } \mathscr{C}_Q\right\}. \qquad \square$$

5. A geometrization of $\mathscr{B}(Q)$

We now relate the character θ_{Tr} with the difference properties obtained in Section 3. This will provide a realization of the elements in $\mathscr{B}(Q)$ in terms of θ_{Tr}.

From difference properties to θ_{Tr}. Using Theorem 3.4, we first deduce a realization in terms of θ_{Tr} of the elements in $\mathscr{B}(Q)$ corresponding to positive roots.

Theorem 5.1. *Let $\boldsymbol{d}$ be any positive root. Then $\mathfrak{b}_{\boldsymbol{d}} = \theta_{\mathrm{Tr}}(M)$, where M is any indecomposable representation of dimension $\boldsymbol{d}$.*

Proof. If $\boldsymbol{d}$ is a positive root with nonzero defect, then $\boldsymbol{d}$ is real and there exists a unique indecomposable representation M in $\mathrm{rep}_{\boldsymbol{k}}(Q, \boldsymbol{d})$. Moreover, this representation has to be preprojective or preinjective. In both cases, it is rigid and thus $\mathfrak{b}_{\boldsymbol{d}} = X_M = \theta_{\mathrm{Tr}}(M)$. We can thus assume that $\boldsymbol{d} \in \mathbb{N}^{Q_0}$ is a root with defect zero.

Let M be an indecomposable representation in $\mathrm{rep}_{\boldsymbol{k}}(Q, \boldsymbol{d})$. It is necessarily contained in a tube $\mathcal{T}$ of rank $p \geq 1$. We denote by R_i, with $i \in \mathbb{Z}/p\mathbb{Z}$, the quasisimple modules in $\mathcal{T}$ ordered such that $\tau R_i \simeq R_{i-1}$ for any $i \in \mathbb{Z}/p\mathbb{Z}$. We can write $\boldsymbol{d} = l\delta + \boldsymbol{n}$, where $\boldsymbol{n}$ is either a real Schur root or zero. If $\boldsymbol{n} \neq 0$, there exists a unique indecomposable representation N in $\mathrm{rep}_{\boldsymbol{k}}(Q, \boldsymbol{n})$. In any case, if $M \simeq R_0^{(lp+k)}$ with $l \geq 0$ and $0 \leq k \leq p-1$, N is the rigid representation $R_0^{(k)}$ (still with the convention that $R_0^{(0)} = 0$) and

$$\mathfrak{b}_{\boldsymbol{d}} = X_{R_0^{(k)}} F_l(X_\delta).$$

Now, according to Theorem 3.4, we have

$$X_{R_0^{(k)}} F_l(X_\delta) = X_{R_0^{(lp+k)}} - X_{R_{k+1}^{(lp-k-2)}}.$$

For any $\boldsymbol{e} \in \mathbb{N}^{Q_0}$, the map $\mathrm{Gr}_{\boldsymbol{e}}^{R_0^{(k+1)}}(R_0^{(lp-1)}) \to \mathrm{Gr}_{\boldsymbol{e}-\mathbf{dim}\, R_0^{(k+1)}}(R_{k+1}^{(lp-k-2)})$ given by

$$U \mapsto U/R_0^{(k+1)}$$

is an algebraic isomorphism, and we denote by $c_{\boldsymbol{e}} \in \mathbb{Z}$ the common value of the Euler characteristics of these constructible sets. Fix now some $\boldsymbol{e} \in \mathbb{N}^{Q_0}$; the monomial corresponding to $\boldsymbol{e}$ in $X_{R_0^{(lp+k)}}$ is

$$c_{\boldsymbol{e}} \prod_i u_i^{-\langle \boldsymbol{e}, S_i\rangle - \left\langle S_i, \mathbf{dim}\, R_0^{(lp+k)} - \boldsymbol{e}\right\rangle},$$

and the monomial corresponding to $\boldsymbol{e} - \mathbf{dim}\, R_0^{(k+1)}$ in $X_{R_{k+1}^{(lp-k-2)}}$ is

$$c_{\boldsymbol{e}} \prod_i u_i^{-\left\langle \boldsymbol{e}-\mathbf{dim}\, R_0^{(k+1)}, S_i\right\rangle - \left\langle S_i, \mathbf{dim}\, R_{k+1}^{(lp-k-2)} + \mathbf{dim}\, R_0^{(k+1)} - \boldsymbol{e}\right\rangle}.$$

We now prove that these monomials are the same. For any $i = 0, \ldots, p-1$, we set $r_i = \mathbf{dim}\, R_i$ and we denote by c the Coxeter transformation on $\mathbb{Z}^{Q_0}$ induced by the Auslander–Reiten translation. We recall that for any $\beta, \gamma \in \mathbb{Z}^{Q_0}$, we have $\langle \gamma, c(\beta)\rangle = -\langle \beta, \gamma \rangle$. With this notation, we have

$$\mathbf{dim}\, R_0^{(k+1)} = r_0 + \cdots + r_k \quad \text{and} \quad \mathbf{dim}\, R_{k+1}^{(lp-k-2)} = (l-1)\delta + r_{k+1} + \cdots r_{p-2},$$

so

$$\mathbf{dim}\, R_0^{(k+1)} + \mathbf{dim}\, R_{k+1}^{(lp-k-2)} = l\delta - r_{p-1}.$$

We now compute the exponents:

$$\begin{aligned}
-\langle \boldsymbol{e}, S_i\rangle - \left\langle S_i, \mathbf{dim}\, R_0^{(lp+k)} - \boldsymbol{e}\right\rangle &= -\langle \boldsymbol{e}, S_i\rangle - \langle S_i, l\delta + r_0 + \cdots + r_{k-1} - \boldsymbol{e}\rangle \\
&= -\langle \boldsymbol{e}, S_i\rangle - \langle S_i, l\delta - \boldsymbol{e}\rangle - \langle S_i, r_0 + \cdots + r_{k-1}\rangle \\
&= -\langle \boldsymbol{e}, S_i\rangle - \langle S_i, l\delta - \boldsymbol{e}\rangle - \langle r_1 + \cdots + r_k, S_i\rangle\,; \\
-\left\langle \boldsymbol{e} - \mathbf{dim}\, R_0^{(k+1)}, S_i\right\rangle - \left\langle S_i, \mathbf{dim}\, R_{k+1}^{(lp-k-2)} + \mathbf{dim}\, R_0^{(k+1)} - \boldsymbol{e}\right\rangle & \\
= -\langle \boldsymbol{e}, S_i\rangle + \langle r_0 + \cdots + r_k, S_i\rangle + \left\langle S_i, r_{p-1}\right\rangle - \langle S_i, l\delta - \boldsymbol{e}\rangle & \\
= -\langle \boldsymbol{e}, S_i\rangle - \langle S_i, l\delta - \boldsymbol{e}\rangle + \langle r_1 + \cdots + r_k, S_i\rangle\,. &
\end{aligned}$$

Thus the two monomials are the same. It follows that

$$\begin{aligned}
&X_{R_0^{(lp+k)}} - X_{R_{k+1}^{(lp-k-2)}} \\
&\quad = \sum_{\boldsymbol{e}} \chi(\mathrm{Gr}_{\boldsymbol{e}}(R_0^{(lp+k)})) \prod_i u_i^{-\langle \boldsymbol{e}, S_i\rangle - \langle S_i, l\delta - \boldsymbol{e}\rangle - \langle r_1 + \cdots + r_k, S_i\rangle} \\
&\qquad\quad - \sum_{\boldsymbol{e}} \chi\left(\mathrm{Gr}_{\boldsymbol{e} - \mathbf{dim}\, R_0^{(k+1)}}(R_{k+1}^{(lp-k-2)})\right) \prod_i u_i^{-\langle \boldsymbol{e}, S_i\rangle - \langle S_i, l\delta - \boldsymbol{e}\rangle - \langle r_1 + \cdots + r_k, S_i\rangle} \\
&\quad = \sum_{\boldsymbol{e}} \chi\left(\mathrm{Gr}_{\boldsymbol{e}}(R_0^{(lp+k)}) \setminus \mathrm{Gr}_{\boldsymbol{e}}^{R_0^{(k+1)}}(R_0^{(lp-1)})\right) \prod_i u_i^{-\langle \boldsymbol{e}, S_i\rangle - \langle S_i, l\delta - \boldsymbol{e}\rangle - \langle r_1 + \cdots + r_k, S_i\rangle} \\
&\quad = \sum_{\boldsymbol{e}} \chi(\mathrm{Tr}_{\boldsymbol{e}}(R_0^{(lp+k)})) \prod_i u_i^{-\langle \boldsymbol{e}, S_i\rangle - \left\langle S_i, \mathbf{dim}\, R_0^{(lp+k)} - \boldsymbol{e}\right\rangle}. \qquad \square
\end{aligned}$$

Realization of $\mathcal{B}(Q)$ in terms of θ_{Tr}. Summing up the previous results, we deduce the following geometric description of $\mathcal{B}(Q)$:

Theorem 5.2. *Let Q be an affine quiver. Then*

$$\mathcal{B}(Q) = \left\{ \theta_{\mathrm{Tr}}(M \oplus R) \;\middle|\; \begin{array}{l} M \text{ is an indecomposable (or zero) regular } \boldsymbol{k}Q\text{-module,} \\ R \text{ is any rigid object in } \mathcal{C}_Q \text{ such that } \mathrm{Ext}^1_{\mathcal{C}_Q}(M, R) = 0 \end{array} \right\}.$$

Proof. We denote by $\mathcal{S}$ the right side of the claimed equality. By definition,

$$\mathcal{B}(Q) = \mathcal{M}(Q) \sqcup \{F_l(X_\delta) X_R \mid l \geq 1,\ R \text{ is a regular rigid } \boldsymbol{k}Q\text{-module}\}.$$

We first prove that $\mathcal{S} \subset \mathcal{B}(Q)$. Let R be a rigid object in $\mathcal{C}_Q$; then $\theta_{\mathrm{Tr}}(R)$ is a cluster monomial by Lemma 4.5. Fix now M to be an indecomposable regular $\boldsymbol{k}Q$-module in a tube $\mathcal{T}$ such that $\mathrm{Ext}^1_{\mathcal{C}_Q}(M, R) = 0$. If M is rigid, then $M \oplus R$ is rigid in $\mathcal{C}_Q$, and $\theta_{\mathrm{Tr}}(M)\theta_{\mathrm{Tr}}(R) = \theta_{\mathrm{Tr}}(M \oplus R)$ is a cluster monomial by Lemma 4.5. Now, if M is nonrigid, then $\boldsymbol{d} = \mathbf{dim}\, M$ is a positive root of defect zero, and thus $\theta_{\mathrm{Tr}}(M) = \mathfrak{b}_{\boldsymbol{d}}$ by Theorem 5.1. Thus, there exists $l \geq 1$ and N an indecomposable

rigid (or zero) module in $\mathcal{T}$ such that $\boldsymbol{d} = l\delta + \mathbf{dim}\, N$. According to Theorem 5.1,

$$\begin{aligned}\theta_{\mathrm{Tr}}(M \oplus R) &= \theta_{\mathrm{Tr}}(M)\theta_{\mathrm{Tr}}(R) = \mathfrak{b}_{l\delta+\mathbf{dim}\, N}\theta_{\mathrm{Tr}}(R) = F_l(X_\delta)X_N\theta_{\mathrm{Tr}}(R)\\ &= F_l(X_\delta)\theta_{\mathrm{Tr}}(N)\theta_{\mathrm{Tr}}(R) = F_l(X_\delta)\theta_{\mathrm{Tr}}(N \oplus R).\end{aligned}$$

Since $\mathrm{Ext}^1_{\mathscr{C}_Q}(M, R) = 0$, we have $\mathrm{Ext}^1_{\boldsymbol{k}Q}(M, R) = 0$ and $\mathrm{Ext}^1_{\boldsymbol{k}Q}(R, M) = 0$. Thus, it follows easily that $\mathrm{Ext}^1_{\boldsymbol{k}Q}(N, R) = 0$ and $\mathrm{Ext}^1_{\boldsymbol{k}Q}(R, N) = 0$, so $N \oplus R$ is a rigid regular $\boldsymbol{k}Q$-module. In particular, $\theta_{\mathrm{Tr}}(N \oplus R) = X_{N\oplus R}$ and thus

$$\theta_{\mathrm{Tr}}(M \oplus R) = F_l(X_\delta)X_{N\oplus R} \in \mathcal{B}(Q).$$

Conversely, fix an element in $\mathcal{B}(Q)$. If x is a cluster monomial, then according to Lemma 4.5, there exists some rigid object M in $\mathscr{C}_Q$ such that $x = \theta_{\mathrm{Tr}}(M)$. Thus, $x \in \mathcal{S}$. Fix now some regular rigid $\boldsymbol{k}Q$-module R and some integer $l \geq 1$. Then the direct summands of R belong to exceptional tubes. We fix an indecomposable $\boldsymbol{k}Q$-module M of dimension vector $l\delta$ in a homogeneous tube. Then $\mathrm{Ext}^1_{\mathscr{C}_Q}(M, R) = 0$. According to Theorem 5.1, we have $F_l(X_\delta)X_R = \theta_{\mathrm{Tr}}(M)X_R$, but R is rigid, so $X_R = \theta_{\mathrm{Tr}}(R)$. Thus,

$$F_l(X_\delta)X_R = \theta_{\mathrm{Tr}}(M)\theta_{\mathrm{Tr}}(R) = \theta_{\mathrm{Tr}}(M \oplus R) \in \mathcal{S}. \qquad \square$$

6. Examples

We shall now study two examples corresponding to cases where it is known that $\mathcal{B}(Q)$ is the canonically positive basis in $\mathcal{A}(Q)$.

The $\tilde{\mathbb{A}}_{1,1}$ case. Let Q be the Kronecker quiver, that is, the affine quiver of type $\tilde{\mathbb{A}}_{1,1}$ with the orientation

$$Q: \qquad 1 \rightrightarrows 2$$

and minimal imaginary root $\delta = (11)$.

For any $\lambda \in \boldsymbol{k}$, we set

$$M_\lambda: \qquad \boldsymbol{k} \underset{\lambda}{\overset{1}{\rightrightarrows}} \boldsymbol{k}$$

and

$$M_\infty: \qquad \boldsymbol{k} \underset{1}{\overset{0}{\rightrightarrows}} \boldsymbol{k}.$$

It is well-known that every tube in $\Gamma(\boldsymbol{k}Q\text{-mod})$ is homogeneous and that the family $\{M_\lambda \mid \lambda \in \boldsymbol{k} \sqcup \{\infty\}\}$ is a complete set of representatives of pairwise nonisomorphic quasisimple $\boldsymbol{k}Q$-modules.

For any $n \geq 1$, the indecomposable representations of quasilength n are given by

$$M_\lambda^{(n)}: \qquad \boldsymbol{k}^n \underset{J_n(\lambda)}{\overset{1}{\rightrightarrows}} \boldsymbol{k}^n$$

for any $\lambda \in \boldsymbol{k}$ and

$$M_\infty^{(n)} : \qquad \boldsymbol{k}^n \underset{1}{\overset{J_n(0)}{\rightrightarrows}} \boldsymbol{k}^n \ ,$$

where $J_n(\lambda) \in M_n(\boldsymbol{k})$ denotes the Jordan block of size n associated to the eigenvalue λ. Quiver Grassmannians and transverse quiver Grassmannians of indecomposable representations with quasilength 2 are described in Table 1.

Note that $\boldsymbol{k}Q$-mod contains no regular rigid modules. It follows that in this case

$$\mathcal{B}(Q) = \mathcal{M}(Q) \sqcup \{\theta_{\mathrm{Tr}}(M) \mid M \text{ is an indecomposable regular } \boldsymbol{k}Q\text{-module}\}.$$

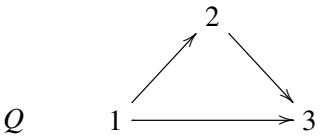
According to [Sherman and Zelevinsky 2004], this set is the canonically positive basis of $\mathcal{A}(Q)$.

From Table 1, we see that for any $\lambda \in \boldsymbol{k} \sqcup \{\infty\}$,

$$\theta_{\mathrm{Tr}}(M_\lambda^{(2)}) = \theta_{\mathrm{Gr}}(M_\lambda^{(2)}) - 1 = X_{M_\lambda^{(2)}} - 1 = S_2(X_{M_\lambda}) - 1 = F_2(X_{M_\lambda}) = \mathfrak{b}_{2\delta}.$$

This illustrates Theorem 5.1.

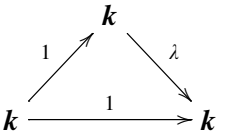
The $\tilde{\mathbb{A}}_{2,1}$ case. We now consider the quiver Q of affine type $\tilde{\mathbb{A}}_{2,1}$ equipped with the orientation



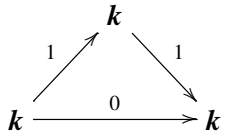
$\boldsymbol{e}$	$\mathrm{Gr}_{\boldsymbol{e}}(M_\lambda^{(2)})$	$\mathrm{Tr}_{\boldsymbol{e}}(M_\lambda^{(2)})$	$\boldsymbol{u}^{\langle -\boldsymbol{e}, S_i\rangle - \langle S_i, 2\delta - \boldsymbol{e}\rangle}$
(00)	$\{0\}$	$\{0\}$	u_1^2/u_2^2
(01)	$\mathbb{P}^1 \times \{S_2\}$	$\mathbb{P}^1 \times \{S_2\}$	$1/u_2^2$
(02)	$\{S_2 \oplus S_2\}$	$\{S_2 \oplus S_2\}$	$1/(u_1^2u_2^2)$
(11)	$\{M_\lambda\}$	$\varnothing$	1
(12)	see caption		$1/u_1^2$
(22)	$\{M_\lambda^{(2)}\}$	$\{M_\lambda^{(2)}\}$	u_2^2/u_1^2

Table 1. Grassmannians and transverse Grassmannians of indecomposable modules of quasilength 2 in type $\tilde{\mathbb{A}}_{1,1}$. Here λ takes values in $\boldsymbol{k} \cup \{0, \infty\}$. For $e = (12)$, the values of both $\mathrm{Gr}_{(12)}(M_\lambda^{(2)})$ and $\mathrm{Tr}_{(12)}(M_\lambda^{(2)})$ are $\{P_1, M_\lambda \oplus S_2\}$ if $\lambda \in \{0, \infty\}$, and $\mathbb{P}^1 \times \{M_\lambda \oplus S_2\}$ otherwise.

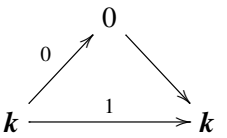
The minimal imaginary root of Q is $\delta = (111)$. For any $\lambda \in \boldsymbol{k}$, we set

M_λ 

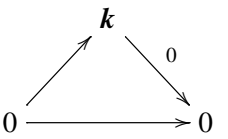
and

M_∞ 

Further, $\Gamma(\boldsymbol{k}Q\text{-mod})$ contains exactly one exceptional tube $\mathcal{T}$ of rank 2, whose quasisimples are

R_0 

and

$R_1 \simeq S_2$ 

The set $\{M_\lambda \mid \lambda \in \boldsymbol{k} \sqcup \{\infty\}\} \sqcup \{R_0^{(2)}\}$ is a complete set of representatives of pairwise nonisomorphic indecomposable representations in $\mathrm{rep}_{\boldsymbol{k}}(Q, \delta)$. For any $\lambda \neq 0, \infty$, M_λ is a quasisimple $\boldsymbol{k}Q$-module in a homogeneous tube. Moreover, $M_0 = R_1^{(2)}$ and M_∞ is quasisimple in a homogeneous tube.

Quiver Grassmannians and transverse quiver Grassmannians of indecomposable representations of dimension δ are described in Table 2. For simplicity, we only listed the dimension vectors that lead to nonempty quiver Grassmannians.

In Table 2, we observe that $X_{M_\lambda} = X_{M_0} - 1 = X_{M_\infty} - 1$, illustrating Theorem 3.1. Also, we see that $\theta_{\mathrm{Tr}}(M_\lambda) = \theta_{\mathrm{Tr}}(M_0) = \theta_{\mathrm{Tr}}(M_\infty)$ for any $\lambda \in \boldsymbol{k} \setminus \{0\}$ so that the transverse character does not depend on the chosen tube. Moreover,

$$\theta_{\mathrm{Tr}}(M_\lambda) = X_{M_\lambda} = F_1(X_\delta),$$

illustrating Theorem 5.1.

Remark 6.1. Table 2 justifies the terminology *transverse submodule*. Indeed, we see that, given two indecomposable regular modules M and N having the same dimension vectors, the submodules U in $\mathrm{Tr}(M)$ are those having a corresponding submodule in $\mathrm{Gr}(N)$. In some sense, we can see U as a submodule "common" to M and N. This is why we call it *transverse*.

$\boldsymbol{e}$	$\mathrm{Gr}_{\boldsymbol{e}}(M_\lambda)$	$\mathrm{Tr}_{\boldsymbol{e}}(M_\lambda)$	$\mathrm{Gr}_{\boldsymbol{e}}(R_0^{(2)})$	$\mathrm{Tr}_{\boldsymbol{e}}(R_0^{(2)})$	$\boldsymbol{u}^{\langle -\boldsymbol{e}, S_i\rangle - \langle S_i, \delta - \boldsymbol{e}\rangle}$
(000)	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	u_1/u_3
(001)	$\{S_3\}$	$\{S_3\}$	$\{S_3\}$	$\{S_3\}$	$1/(u_2u_3)$
(010)	see caption		$\varnothing$	$\varnothing$	1
(011)	see caption		$\{P_2\}$	$\{P_2\}$	$1/(u_1u_2)$
(101)	$\varnothing$	$\varnothing$	$\{R_0\}$	$\varnothing$	1
(111)	$\{M_\lambda\}$	$\{M_\lambda\}$	$\{R_0^{(2)}\}$	$\{R_0^{(2)}\}$	u_3/u_1

Table 2. Grassmannians and transverse Grassmannians for quasilength 2 in type $\tilde{\mathbb{A}}_{2,1}$. Here λ takes values in $\boldsymbol{k} \cup \{0, \infty\}$. For $e = (010)$, all entries are $\varnothing$ except that $\mathrm{Gr}_{010}(M_0) = \{S_2\}$. For $e = (011)$, all entries equal $\{P_2\}$, apart from that $\mathrm{Gr}_{(011)}(M_0)$ and $\mathrm{Tr}_{(011)}(M_0)$, which equal $\{S_2 \oplus S_3\}$.

As suggested by Bernhard Keller, this notion of transversality should have a more precise meaning in the context of deformation theory. Some connections are known at this time, and this will be discussed in a forthcoming article.

Acknowledgements

This paper was written while the author was at the university of Sherbrooke as a CRM-ISM postdoctoral fellow under the supervision of the Ibrahim Assem, Thomas Brüstle and Virginie Charette. He would like to thank Giovanni Cerulli Irelli for motivating the investigation of higher-difference properties during his stay at the University of Padova in June 2009. This was the starting point of this work. He would also like to thank the rest of the algebra group of Padova for their kind hospitality. Finally, he would like to thank Bernhard Keller, Philippe Caldero and Frédéric Chapoton for interesting discussions on the topic.

References

[Berenstein et al. 2005] A. Berenstein, S. Fomin, and A. Zelevinsky, "Cluster algebras, III: Upper bounds and double Bruhat cells", *Duke Math. J.* **126**:1 (2005), 1–52. MR 2005i:16065 Zbl 1135.16013

[Buan et al. 2006] A. B. Buan, R. Marsh, M. Reineke, I. Reiten, and G. Todorov, "Tilting theory and cluster combinatorics", *Adv. Math.* **204**:2 (2006), 572–618. MR 2007f:16033 Zbl 1127.16011

[Caldero and Chapoton 2006] P. Caldero and F. Chapoton, "Cluster algebras as Hall algebras of quiver representations", *Comment. Math. Helv.* **81**:3 (2006), 595–616. MR 2008b:16015 Zbl 1119.16013

[Caldero and Keller 2006] P. Caldero and B. Keller, "From triangulated categories to cluster algebras, II", *Ann. Sci. École Norm. Sup.* (4) **39**:6 (2006), 983–1009. MR 2008m:16031 Zbl 1115.18301

[Caldero and Zelevinsky 2006] P. Caldero and A. Zelevinsky, "Laurent expansions in cluster algebras via quiver representations", *Mosc. Math. J.* **6**:3 (2006), 411–429, 587. MR 2008j:16045 Zbl 1133.16012

[Caldero et al. 2006] P. Caldero, F. Chapoton, and R. Schiffler, "Quivers with relations arising from clusters (A_n case)", *Trans. Amer. Math. Soc.* **358**:3 (2006), 1347–1364. MR 2007a:16025 Zbl 1137.16020

[Cerulli 2009] G. Cerulli Irelli, "Canonically positive basis of cluster algebras of type $A_2^{(1)}$", preprint, 2009. arXiv 0904.2543v2

[Ding et al. 2009] M. Ding, J. Xiao, and F. Xu, "Integral bases of cluster algebras and representations of tame quivers", preprint, 2009. arXiv 0901.1937v1

[Dupont 2008] G. Dupont, "Generic variables in acyclic cluster algebras", preprint, 2008. arXiv 0811.2909v1

[Dupont 2009] G. Dupont, "Cluster multiplication in regular components via generalized Chebyshev polynomials", preprint, 2009. arXiv 0801.3964v2

[Dupont 2010] G. Dupont, "Quantized Chebyshev polynomials and cluster characters with coefficients", *J. Algebraic Combin.* **31**:4 (2010), 501–532.

[Fomin and Zelevinsky 2002] S. Fomin and A. Zelevinsky, "Cluster algebras, I: Foundations", *J. Amer. Math. Soc.* **15**:2 (2002), 497–529. MR 2003f:16050 Zbl 1021.16017

[Fomin and Zelevinsky 2003] S. Fomin and A. Zelevinsky, "Cluster algebras, II: Finite type classification", *Invent. Math.* **154**:1 (2003), 63–121. MR 2004m:17011 Zbl 1054.17024

[Fomin and Zelevinsky 2007] S. Fomin and A. Zelevinsky, "Cluster algebras, IV: Coefficients", *Compos. Math.* **143**:1 (2007), 112–164. MR 2008d:16049 Zbl 1127.16023

[Keller 2005] B. Keller, "On triangulated orbit categories", *Doc. Math.* **10** (2005), 551–581. MR 2007c :18006 Zbl 1086.18006

[Ringel 1984] C. M. Ringel, *Tame algebras and integral quadratic forms*, Lecture Notes in Mathematics **1099**, Springer, Berlin, 1984. MR 87f:16027 Zbl 0546.16013

[Sherman and Zelevinsky 2004] P. Sherman and A. Zelevinsky, "Positivity and canonical bases in rank 2 cluster algebras of finite and affine types", *Mosc. Math. J.* **4**:4 (2004), 947–974, 982. MR 2006c:16052 Zbl 1103.16018

[Simson and Skowroński 2007] D. Simson and A. Skowroński, *Elements of the representation theory of associative algebras*, vol. II, London Mathematical Society Student Texts **71**, Cambridge University Press, 2007. MR 2009f:16001 Zbl 1129.16001

[Yang and Zelevinsky 2008] S.-W. Yang and A. Zelevinsky, "Cluster algebras of finite type via Coxeter elements and principal minors", *Transform. Groups* **13**:3-4 (2008), 855–895. MR 2009j:13029 Zbl 1177.16010

Communicated by Andrei Zelevinsky
Received 2009-10-26 Revised 2010-03-17 Accepted 2010-04-16

gregoire.dupont@usherbrooke.ca

Université de Sherbrooke, Département de Mathématiques, 2500 Boulevard de l'université, Sherbrooke J1K 2R1, Canada
http://pages.usherbrooke.ca/gdupont2

ALGEBRA AND NUMBER THEORY 4:5(2010)

Connected gradings and the fundamental group

Claude Cibils, María Julia Redondo and Andrea Solotar

The main purpose of this paper is to provide explicit computations of the fundamental groups of several algebras. For this purpose, given a k-algebra A, we consider the category of all connected gradings of A by a group G and we study the relation between gradings and Galois coverings. This theoretical tool gives information about the fundamental group of A, which allows its computation using complete lists of gradings.

1. Introduction

We provide explicit computations of the intrinsic fundamental groups of some algebras. For this, we study in detail the relation between gradings and Galois coverings of each algebra considered as a k-linear category with one object. Particular attention is paid to matrix algebras, since the problem of classifying gradings of these algebras has been extensively treated in the literature [Aljadeff et al. 2010; Bahturin et al. 2001; Bahturin and Zaicev 2002; Bahturin and Shestakov 2001; Boboc 2003; Boboc and Dăscălescu 2001; 2006; 2007; Caenepeel et al. 2002; Chun and Lee 2007; Dăscălescu et al. 1999; Khazal et al. 2003].

We recall that the intrinsic fundamental group of an algebra was defined in [Cibils et al. 2007] using Galois coverings. We make use of an equivalence between the category of Galois coverings and its full subcategory with objects obtained from the smash product construction, which is deeply attached to connected gradings. We replace algebras by linear categories over a base ring: a category over a ring k is considered as an algebra with several objects [Mitchell 1972], and a k-algebra A can be viewed as a k-category with a single object and endomorphism ring equal to A. Note that in [Green 1983; Green and Marcos 1994], a relation between gradings

MSC2000: primary 16W50; secondary 16S50.

Keywords: grading, Galois covering, fundamental group.

This work has been supported by the projects UBACTY, PIP-CONICET, PICT-ANPCyT, and MATHAMSUD. Redondo and Solotar are research members of CONICET (Argentina). Solotar is a Regular Associate of the ICTP Associate Scheme.

and coverings is established for quivers with relations. In this paper we consider an intrinsic context, where the categories are not given by a presentation.

When computing the fundamental group of an algebra, one faces the problem of classifying and organizing its connected gradings. The methods we introduce allow the computation of the fundamental groups of matrix algebras, triangular matrix algebras, group algebras and diagonal algebras. We restrict to connected gradings and prove that the matrix algebras do not admit a universal grading. Indeed, there exist at least two nonisomorphic Galois coverings or, equivalently, two nonisomorphic connected gradings that are simply connected, in the sense that they have no nontrivial Galois coverings. In particular, this confirms that the fundamental group of an algebra takes into account the matrix structure; in other words, it is not a Morita invariant.

In Section 2, we show that the connectedness of gradings is the right notion that corresponds to the connectedness of the associated smash product. We recall the concept of Galois covering and observe that the smash product construction gives examples of Galois coverings. We describe in detail the morphisms between smash coverings.

In Section 3, we make an explicit comparison between Galois coverings and smash coverings of a k-category $\mathcal{B}$. More precisely, we provide an equivalence between the category $\mathrm{Gal}(\mathcal{B}, b_0)$ of Galois coverings of $\mathcal{B}$ and its full subcategory $\mathrm{Gal}^{\#}(\mathcal{B}, b_0)$, whose objects are the smash product coverings. We consider the fundamental group defined in [Cibils et al. 2007] using Galois coverings and show that we can restrict to smash coverings when computing the fundamental group $\pi_1(\mathcal{B}, b_0)$.

In the subsequent sections, we focus on the description of connected gradings of certain algebras in order to compute their fundamental groups. As a rule, we wonder about the existence of a universal grading, since when such a grading exists, the grading group is isomorphic to the fundamental group of the algebra.

In Section 4, we consider matrix algebras, proving that there is no universal covering by providing two nonisomorphic simply connected gradings. Despite the fact that they appear to be very different in nature, we show that they have a unique largest common nontrivial quotient. Using the classification of gradings of $M_2(k)$ given in [Khazal et al. 2003] and of $M_3(k)$ given in [Boboc and Dăscălescu 2007], we compute the fundamental groups of these algebras in the cases where the field is algebraically closed of characteristic different from 2 and 3, respectively. Using analogous methods and the classification in [Bahturin and Zaicev 2002], we compute the fundamental group of $M_p(k)$, where p is prime and k an algebraically closed field of characteristic zero, which is the direct product of the free group on $p-1$ generators with the cyclic group of order p. We compute the fundamental group of triangular matrix algebras, using results in [Valenti and Zaicev 2007],

without any hypothesis on the characteristic of the field k. The fundamental group in this case is the free group on $n-1$ generators.

In Section 5, we first prove that the natural grading of a group algebra is simply connected. Next we consider in detail the group algebra of the cyclic group of order p, where p is a prime, in the case of a field of characteristic p. This algebra is isomorphic to the truncated polynomial algebra $k[x]/(x^p)$, and we show that it does not admit a universal grading. Nevertheless, we provide a complete description of its connected gradings, and we conclude that the fundamental group of the truncated polynomial algebra in characteristic p is the product of the infinite cyclic group and the cyclic group of order p.

Finally, in Section 6 we consider the group algebra kG, for G an abelian group of order n and k a field with enough n-th roots of unity or, equivalently, the algebra k^E of all maps from E to k, where E is a set with n elements. In the case where n is not square-free, we show that k^n has no universal covering. A special case occurs when $n=2$ and k is a field of characteristic different from 2: there exists a universal covering. More precisely, we prove that there is only one nontrivial group providing a connected grading of the set algebra k^2, namely the cyclic group of order 2, which in turn is the fundamental group of this algebra.

We end the paper by computing the fundamental group of the set algebras k^3 and k^4, using a description of all the gradings of k^E given in [Dăscălescu 2008]. In the case where k is a field containing all roots of unity of order 2 and 3, we prove that $\pi_1(k^3) = C_2 \times C_3$, while if k contains all roots of unity of order 3 and 4, we obtain

$$\pi_1(k^4) = (C_2 * C_2) \times C_6 \times C_4 \times C_2.$$

A detailed study of Dăscălescu's classification and the relations among the grading groups, together with the techniques presented in this paragraph, should lead to the computation of the fundamental group for arbitrary diagonal algebras.

2. Gradings and coverings

Let k be a commutative ring and let $\mathcal{B}$ be a small category such that each morphism set ${}_y\mathcal{B}_x$ from an object x to an object y is endowed with a k-module structure such that composition of morphisms is k-bilinear. Such a category is called a k-category; note that each endomorphism k-module ${}_x\mathcal{B}_x$ is a k-algebra and ${}_y\mathcal{B}_x$ is a ${}_y\mathcal{B}_y$-${}_x\mathcal{B}_x$-bimodule. Each k-algebra A provides in this way a single object k-category.

In [Cibils and Marcos 2006; Green 1983] it was shown that connected group gradings and Galois coverings are in one-to-one correspondence. We recall the definition of these categories and, even if they are not equivalent, we make precise the relation between them.

Definition 2.1. A *grading* X of a k-category $\mathcal{B}$ by a group Γ is given by a direct sum decomposition of each k-module of morphisms

$$ {}_y\mathcal{B}_x = \bigoplus_{s\in\Gamma} X^s({}_y\mathcal{B}_x), $$

such that $X^t({}_z\mathcal{B}_y)X^s({}_y\mathcal{B}_x) \subset X^{ts}({}_z\mathcal{B}_x)$. The *homogeneous component* of degree s from x to y is the k-module $X^s({}_y\mathcal{B}_x)$.

Next we consider *connected* gradings, in order to establish the correspondence with Galois coverings. We use the following notation: given a morphism f, its source object is denoted by $s(f)$ and its target object by $t(f)$.

We will also make use of walks. For this purpose we consider the set of formal pairs (f, ε) as *morphisms with sign*, where f is a morphism in $\mathcal{B}$ and $\varepsilon \in \{-1, 1\}$. We extend source and target maps to this set:

$$ s(f, 1) = s(f), s(f, -1) = t(f), t(f, 1) = t(f), t(f, -1) = s(f). $$

Definition 2.2. Let $\mathcal{B}$ be a k-category. A nonzero *walk* in $\mathcal{B}$ is a sequence of nonzero morphisms with signs $(f_n, \varepsilon_n) \dots (f_1, \varepsilon_1)$ such that

$$ s(f_{i+1}, \varepsilon_{i+1}) = t(f_i, \varepsilon_i). $$

We say that this walk goes from $s(f_1, \varepsilon_1)$ to $t(f_n, \varepsilon_n)$.

A nonzero walk $\alpha = (f_n, \varepsilon_n) \dots (f_1, \varepsilon_1)$ is called *homogeneous* if each f_i is a homogeneous morphism in the graded category $\mathcal{B}$. We shall denote by $\deg f$ the degree of a homogeneous morphism f. We define the *degree* of a homogeneous nonzero walk α:

$$ \deg \alpha = (\deg f_n)^{\varepsilon_n} \dots (\deg f_1)^{\varepsilon_1}. $$

As expected, a k-category $\mathcal{B}$ is called *connected* if any two objects of $\mathcal{B}$ can be joined by a nonzero walk. Moreover, a Γ-grading of $\mathcal{B}$ is *connected* if given any two objects in $\mathcal{B}$ and any element $g \in \Gamma$, they can be joined by a nonzero homogeneous walk of degree g. Of course, if a grading of a k-category is connected, then the underlying category is connected. Conversely, the following easy result holds.

Lemma 2.3. *Let $\mathcal{B}$ be a connected k-category equipped with a Γ-grading and let x_0 be an object of $\mathcal{B}$. Assume there exist homogeneous walks of any degree from x_0 to itself. Then the grading is connected.*

The definition of a connected grading restricts to algebras as follows. First recall that the *support* of a grading X of a k-algebra A by a group Γ is

$$ \operatorname{Supp} X = \{s \in \Gamma \mid X^s A \neq 0\}. $$

If the category has only one object, the following result describes the notion of a connected grading of an algebra. Note that [Dăscălescu 2008] gives the name *faithful* to this kind of grading.

Proposition 2.4. *Let A be a k-algebra and X be a Γ-grading of A. The grading is connected if and only if* Supp X *is a set of generators of* Γ.

Proof. Consider the k-category $\mathcal{B}_A$ with a single object $*$ such that ${}_*(\mathcal{B}_A)_* = A$. Assume that the grading is connected. Then for any element g of Γ, there is a homogeneous nonzero walk $\alpha = (f_n, \varepsilon_n) \dots (f_1, \varepsilon_1)$ such that $\deg \alpha = g$, which precisely means that Supp X generates Γ. Conversely, let $g \in \Gamma$. Since Supp X generates Γ, we have that $g = g_n^{\varepsilon_n} \dots g_1^{\varepsilon_1}$ where $g_i \in \operatorname{Supp} X$ and $\varepsilon_i = \pm 1$. Let $a_n, \dots, a_1$ be nonzero homogeneous elements of A such that $\deg a_i = g_i$. Then $(a_n, \varepsilon_n) \dots (a_1, \varepsilon_1)$ is a nonzero closed homogeneous walk from $*$ to itself, of degree g. □

Remark 2.5. Clearly each Γ-grading of an algebra provides a unique connected grading by restricting Γ to the subgroup generated by the support.

We recall now the smash product category associated to a grading, as defined in [Cibils and Marcos 2006]. This construction is compatible with the one in the algebra case, in the sense that for a finite group Γ and a Γ-graded algebra A, we recover the smash product $A\#\Gamma$ given in that reference.

Definition 2.6. Let X be a Γ-grading of the k-category $\mathcal{B}$. The objects of the *smash product category* $\mathcal{B}\#\Gamma$ are $\mathcal{B}_0 \times \Gamma$, while the module of morphisms from (b, g) to (c, h) is ${}^{h^{-1}g}X_c\mathcal{B}_b$. In other words, morphisms are provided by homogeneous components, and composition in $\mathcal{B}\#\Gamma$ is given by the original composition in $\mathcal{B}$. The composition of morphisms is well-defined, as an immediate consequence of the definition of a graded category.

Remark 2.7. Consider this definition for a single object k-category $\mathcal{B}_A$ associated to a k-algebra A, and write $A\#\Gamma = \mathcal{B}_A\#\Gamma$. Then the set of objects of $A\#\Gamma$ is Γ, while the morphisms from g to h are the homogeneous elements of degree $h^{-1}g$. If Γ is finite, the matrix algebra obtained as the direct sum of all the morphisms of this category is precisely the smash product algebra of [Cibils and Marcos 2006].

Proposition 2.8. *$\mathcal{B}\#\Gamma$ is a connected category if and only if the Γ-grading of $\mathcal{B}$ is connected.*

Proof. Note first that there is a canonical functor $F : \mathcal{B}\#\Gamma \to \mathcal{B}$ given on objects by $F(b, g) = b$, while, on morphisms, F is the inclusion map of homogeneous components. Assume that $\mathcal{B}\#\Gamma$ is connected and let b and c be objects of $\mathcal{B}$ and g in Γ. Consider the objects $(b, 1_\Gamma)$ and (c, g) in $\mathcal{B}\#\Gamma$. Let $\alpha = (f_n, \varepsilon_n) \dots (f_1, \varepsilon_1)$ be a nonzero walk from $(b, 1_\Gamma)$ to (c, g). Each f_i is a homogeneous morphism in $\mathcal{B}$, by definition of $\mathcal{B}\#\Gamma$.

Note also that the target in $\mathcal{B}\#\Gamma$ of (f_1, ε_1) is $(t(f_1, \varepsilon_1), (\deg f_1)^{-\varepsilon_1})$. Moreover, the target in $\mathcal{B}\#\Gamma$ of (f_2, ε_2) is $(t(f_2, \varepsilon_2), (\deg f_1)^{-\varepsilon_1}(\deg f_2)^{-\varepsilon_2})$. Thus we get

$$g = (\deg f_1)^{-\varepsilon_1}(\deg f_2)^{-\varepsilon_2} \dots (\deg f_n)^{-\varepsilon_n},$$

so α is a homogeneous nonzero walk from b to c of degree g.

Conversely, assume that the Γ-grading of $\mathcal{B}$ is connected. Let (b, g) and (c, h) be objects of $\mathcal{B}\#\Gamma$, and consider $\alpha = (f_n, \varepsilon_n) \dots (f_1, \varepsilon_1)$ a homogeneous nonzero walk in $\mathcal{B}$ from b to c of degree $h^{-1}g$. Then α provides a nonzero walk from (b, g) to (c, h). □

Coverings of k-categories were introduced in [Bongartz and Gabriel 1982] in order to study representation theory. We recall the definition given in [Cibils et al. 2007]. First we define the star $\mathrm{St}_{b_0}\mathcal{B}$ at an object b_0 of a k-category $\mathcal{B}$ as the direct sum of all k-modules of morphisms with source or target b_0. A k-functor $F : \mathcal{C} \to \mathcal{B}$ induces a k-linear map $F : \mathrm{St}_x\mathcal{C} \to \mathrm{St}_{Fx}\mathcal{B}$ for any object x of $\mathcal{C}$.

Definition 2.9. Let $\mathcal{C}$ and $\mathcal{B}$ be k-categories. A k-functor $F : \mathcal{C} \to \mathcal{B}$ is a *covering* if it is surjective on objects and if F induces k-isomorphisms between the corresponding stars. More precisely, for each $b_0 \in \mathcal{B}_0$ and each x in the nonempty fiber $F^{-1}(b_0)$, the map

$$F^x_{b_0} : \mathrm{St}_x\mathcal{C} \to \mathrm{St}_{b_0}\mathcal{B}$$

provided by F is a k-isomorphism.

A morphism from a covering $F : \mathcal{C} \to \mathcal{B}$ to a covering $G : \mathcal{D} \to \mathcal{B}$ is a pair of k-linear functors (H, J), where $H : \mathcal{C} \to \mathcal{D}$, $J : \mathcal{B} \to \mathcal{B}$ are such that J is an isomorphism, J is the identity on objects, and $GH = JF$.

We consider, within the group of automorphisms of a covering $F : \mathcal{C} \to \mathcal{B}$, the subgroup $\mathrm{Aut}_1 F$ of invertible endofunctors G of $\mathcal{C}$ such that $FG = F$.

Let $b \in \mathcal{B}$ and let $F^{-1}(b)$ be the corresponding fiber. This fiber is nonempty by definition, and $\mathrm{Aut}_1 F$ acts freely on it [Le Meur 2007; Cibils et al. 2007].

Definition 2.10. A covering $F : \mathcal{C} \to \mathcal{B}$ of k-categories is a *Galois covering* if $\mathcal{C}$ is connected and if $\mathrm{Aut}_1 F$ acts transitively on some fiber.

Remark 2.11. One can prove that for a Galois covering F, the group $\mathrm{Aut}_1 F$ acts transitively on any fiber [Le Meur 2007; Cibils et al. 2007].

As an example of Galois coverings, we have those coming from the smash product construction: if X is a Γ-grading of the k-category $\mathcal{B}$, the functor $\mathcal{B}\#\Gamma \to \mathcal{B}$, given by $(b, g) \mapsto b$ and the inclusion on morphisms, is a Galois covering with Γ as group of automorphisms.

It is useful to observe that the evident action of Γ on the smash product category $\mathcal{B}\#\Gamma$ is given as follows. The action on objects is given by the left action of Γ on

itself. It is a free action. Observe that for any $u \in \Gamma$, a morphism from (b, g) to (c, h) is also a morphism from (b, ug) to (c, uh) since $h^{-1}g = (uh)^{-1}ug$.

We now consider Galois coverings together with a fixed object as follows. Given a k-category $\mathcal{B}$ and a fixed object b_0 of $\mathcal{B}$, the objects of the category $\mathrm{Gal}(\mathcal{B}, b_0)$ are Galois coverings $F : \mathcal{C} \to \mathcal{B}$. Morphisms are Galois covering morphisms $(H, J) : F_1 \to F_2$, where $H : \mathcal{C}_1 \to \mathcal{C}_2$ and $J : \mathcal{B} \to \mathcal{B}$ is an isomorphism that is the identity on objects.

We proved in [Cibils et al. 2007] that a morphism (H, J) induces a unique group epimorphism $\lambda_H : \mathrm{Aut}_1 F_1 \to \mathrm{Aut}_1 F_2$ verifying $Hf = \lambda_H(f)H$, for all $f \in \mathrm{Aut}_1 F_1$.

The following proposition describes morphisms of smash coverings in terms of the corresponding λ.

Proposition 2.12. *Let $b_0 \in \mathcal{B}$, and let $F_1 : \mathcal{B}\#G_1 \to \mathcal{B}$ and $F_2 : \mathcal{B}\#G_2 \to \mathcal{B}$ be Galois coverings associated to connected gradings X_1 and X_2 of $\mathcal{B}$ with groups G_1 and G_2. Given a morphism of coverings $(H, J) : F_1 \to F_2$ in $\mathrm{Gal}(\mathcal{B}, b_0)$, there exists a map $h : G_1 \to G_2$ such that $H(b_0, g) = (b_0, h(g))$ for all $g \in G_1$. Moreover, h is a G_1-morphism and $h(g) = \lambda_H(g)h(1)$, where $\lambda_H : G_1 \to G_2$ is the group morphism associated to H.*

Proof. It is clear that $H(b_0, g) = (b_0, g')$ for some $g' \in G_2$, since $b_0 = JF(b_0, g) = FH(b_0, g)$. We write $h(g) = g'$.

We have thus obtained that given $b_0 \in \mathcal{B}$, the morphism H induces a map

$$h : F_1^{-1}(b_0) \to F_2^{-1}(b_0).$$

Moreover, $F_i^{-1}(b_0)$ is a G_i-set ($i = 1, 2$), by identifying G_i with $\mathrm{Aut}_1 F_i$, and λ_H makes $F_2^{-1}(b_0)$ a G_1-set; more precisely, if $f \in G_1$ and $y \in F_2^{-1}(b_0)$, then $f \cdot y = \lambda_H(f) \cdot y$. We assert that h is a morphism of G_1-sets. For this purpose, take $x \in F_1^{-1}(b_0)$ and $f \in G_1$; then

$$\begin{aligned}(b_0, h(f \cdot x)) &= H(b_0, f \cdot x) = Hf(b_0, x)\\ &= \lambda_H(f)H(b_0, x) = \lambda_H(f)(b_0, h(x)) = (b_0, \lambda_H(f)h(x)).\end{aligned}$$

Finally, $h(g) = h(g \cdot 1) = \lambda_H(g)h(1)$. □

3. The fundamental group

In [Cibils et al. 2007], we defined the fundamental group of a connected k-category using Galois coverings. Our purpose is to relate this fundamental group to connected gradings. Let us recall the definition given in [Cibils et al. 2007]. Considering the fiber functor

$$\Phi : \mathrm{Gal}(\mathcal{B}, b_0) \to \mathsf{Sets}$$

given by $\Phi(F) = F^{-1}(b_0)$, we have defined $\pi_1(\mathcal{B}, b_0) = \mathrm{Aut}\,\Phi$.

To study the fundamental group we introduce the full subcategory $\mathrm{Gal}^{\#}(\mathcal{B}, b_0)$ of $\mathrm{Gal}(\mathcal{B}, b_0)$ whose objects are the smash product Galois coverings $F : \mathcal{B}\#\Gamma \to \mathcal{B}$.

Theorem 3.1. *The categories* $\mathrm{Gal}^{\#}(\mathcal{B}, b_0)$ *and* $\mathrm{Gal}(\mathcal{B}, b_0)$ *are equivalent.*

Proof. It is immediate from [Cibils and Marcos 2006], since any Galois covering $F : \mathcal{C} \to \mathcal{B}$ is isomorphic to the Galois covering $\mathcal{B}\#\mathrm{Aut}_1 F \to \mathcal{B}$. Note that the grading of $\mathcal{B}$ by $\mathrm{Aut}_1 F$ is not canonical; it depends on a choice of an object in each fiber. □

The next proposition shows that we can restrict to the subcategory $\mathrm{Gal}^{\#}(\mathcal{B}, b_0)$ of $\mathrm{Gal}(\mathcal{B}, b_0)$ when considering the fundamental group $\pi_1(\mathcal{B}, b_0)$.

Proposition 3.2. *Let* $F : \mathcal{C} \to \mathcal{D}$ *be an equivalence of categories,* $\Phi_{\mathcal{C}} : \mathcal{C} \to \mathsf{Sets}$, $\Phi_{\mathcal{D}} : \mathcal{D} \to \mathsf{Sets}$ *such that* $\Phi_{\mathcal{D}} F = \Phi_{\mathcal{C}}$. *Then there exists an isomorphism* $F^* : \mathrm{Aut}\,\Phi_{\mathcal{D}} \to \mathrm{Aut}\,\Phi_{\mathcal{C}}$.

Proof. Recall that an element $\tau \in \mathrm{Aut}\,\Phi_{\mathcal{D}}$ is an invertible natural transformation, that is, a family of invertible set maps $\tau_d : \Phi_{\mathcal{D}}(d) \to \Phi_{\mathcal{D}}(d)$ for every object d in $\mathcal{D}$, which are compatible with morphisms in $\mathcal{D}$. Since F is a functor, it is clear that $F^*(\tau)$ defined by $F^*(\tau)_c = \tau_{F(c)}$ is an element in $\mathrm{Aut}\,\Phi_{\mathcal{C}}$.

Let $\tau \in \mathrm{Aut}\,\Phi_{\mathcal{D}}$ be such that $F^*(\tau) = \mathrm{id}$. Since F is dense, for any object d in $\mathcal{D}$ there exists c in $\mathcal{C}$ with an isomorphism $\alpha : d \to F(c)$; the naturality of τ induces the commutative diagram

$$\begin{array}{ccc} \Phi_{\mathcal{D}}(d) & \xrightarrow{\tau_d} & \Phi_{\mathcal{D}}(d) \\ \downarrow{\scriptstyle \Phi_{\mathcal{D}}(\alpha)} & & \downarrow{\scriptstyle \Phi_{\mathcal{D}}(\alpha)} \\ \Phi_{\mathcal{D}}(F(c)) & \xrightarrow{\tau_{F(c)}} & \Phi_{\mathcal{D}}(F(c)). \end{array}$$

Since $\tau_{F(c)} = \mathrm{id}$ for all $c \in \mathcal{C}$, this implies that $\tau_d = \mathrm{id}$, and hence $\tau = \mathrm{id}$.

In order to prove that F^* is surjective, let $\sigma \in \mathrm{Aut}\,\Phi_{\mathcal{C}}$ and consider $\hat{\sigma}$ defined in the following way. For any object d in $\mathcal{D}$, we choose c and an isomorphism $\alpha : d \to F(c)$; in the case where $d = F(c)$, we choose $\alpha = \mathrm{id}$. Now we define $\hat{\sigma}_d$ such that the following diagram is commutative:

$$\begin{array}{ccc} \Phi_{\mathcal{D}}(d) & \xrightarrow{\hat{\sigma}_d} & \Phi_{\mathcal{D}}(d) \\ \downarrow{\scriptstyle \Phi_{\mathcal{D}}(\alpha)} & & \downarrow{\scriptstyle \Phi_{\mathcal{D}}(\alpha)} \\ \Phi_{\mathcal{C}}(c) = \Phi_{\mathcal{D}}(F(c)) & \xrightarrow{\sigma_c} & \Phi_{\mathcal{D}}(F(c)) = \Phi_{\mathcal{C}}(c). \end{array}$$

Since F is full, we have that $\hat{\sigma}$ is a natural transformation and $F^*(\hat{\sigma}) = \sigma$. □

Corollary 3.3. *Let* $\Phi^{\#} : \mathrm{Gal}^{\#}(\mathcal{B}, b_0) \to \mathsf{Sets}$ *be the functor given by*

$$\Phi(F : \mathcal{B}\#G \to \mathcal{B}) = F^{-1}(b_0) = G.$$

Then $\pi_1(\mathcal{B}, b_0) \cong \operatorname{Aut} \Phi^{\#}$.

Corollary 3.4. *If* $\mathcal{B}$ *only admits the trivial connected grading, then* $\pi_1(\mathcal{B}, b_0) = 1$.

An advantage of considering $\mathrm{Gal}^{\#}(\mathcal{B}, b_0)$ instead of $\mathrm{Gal}(\mathcal{B}, b_0)$ is explained by the following proposition, which describes the automorphisms of the fiber functor.

Proposition 3.5. *Let* $\sigma \in \operatorname{Aut} \Phi^{\#}$, *and let* G *be a group grading the category* $\mathcal{B}$ *in a connected way. The map* $\sigma_G : G \to G$ *is given by* $\sigma_G(x) = xg$, *where* $g \in G$ *is uniquely determined.*

Proof. Consider a covering $F : \mathcal{B}\#G \to \mathcal{B}$. Each $g \in G$ induces an automorphism of the covering F, which is the identity on $\mathcal{B}$ and the left action of G on itself. We shall denote it by l_g. Given $\sigma \in \operatorname{Aut} \Phi^{\#}$, we get a map $\sigma_G : G \to G$. It must make the diagram

$$\begin{array}{ccc} G & \xrightarrow{\sigma_G} & G \\ {\scriptstyle \widetilde{l_g}}\downarrow & & \downarrow{\scriptstyle \widetilde{l_g}} \\ G & \xrightarrow{\sigma_G} & G \end{array}$$

commutative, where $\widetilde{l_g}$ is induced by l_g. So, for all $x \in G$, we get $\sigma_G(g_0 x) = g_0 \sigma_G(x)$. Taking $x = 1$ we obtain $\sigma_G(g_0) = g_0 \sigma_G(1)$. Note that g_0 is an arbitrary element of G. □

4. The fundamental group of matrix and triangular algebras

Let k be a field containing a primitive n-th root of unity q, and let $M_n(k)$ be the k-algebra of $n \times n$ matrices. The problem of classifying all the gradings of $M_n(k)$ is not solved. Lists of gradings have been described by several authors [Aljadeff et al. 2010; Bahturin et al. 2001; Bahturin and Zaicev 2002; Boboc 2003; Boboc and Dăscălescu 2001; 2006; Caenepeel et al. 2002; Dăscălescu et al. 1999], and the complete lists for $n = 2$ and $n = 3$ are obtained in [Khazal et al. 2003; Boboc and Dăscălescu 2007].

We consider connected gradings of the algebra $M_n(k)$. In the case of a nonconnected grading, we shall restrict to the subgroup generated by the support, in order to study the unique associated connected grading.

We briefly recall the definition of the universal covering of a k-category.

Definition 4.1. A *universal covering* $U : \mathcal{U} \to \mathcal{B}$ is an object in $\mathrm{Gal}(\mathcal{B})$ such that for any Galois covering $F : \mathcal{C} \to \mathcal{B}$, and for any $u_0 \in \mathcal{U}_0$, $c_0 \in \mathcal{C}_0$ with $U(u_0) = F(c_0)$, there exists a unique morphism $(H, 1)$ from U to F verifying $H(u_0) = c_0$.

Theorem 4.2 [Cibils et al. 2007, Theorem 4.6]. *Suppose that a connected* k*-category* $\mathcal{B}$ *admits a universal covering* U. *Then*

$$\pi_1(\mathcal{B}, b_0) \simeq \operatorname{Aut}_1 U.$$

Definition 4.3. A connected k-category is *simply connected* if its only connected grading is the trivial grading. A connected grading is *simply connected* if the corresponding Galois covering is simply connected.

We will prove that there is no universal cover for $M_n(k)$. Indeed there exist at least two nonisomorphic connected gradings of $M_n(k)$ that provide simply connected Galois coverings. Recall that a covering is simply connected if it admits no proper Galois covering.

Proposition 4.4 [Bahturin et al. 2001; Chun and Lee 2007]. *There exists a connected $C_n \times C_n$-grading of $M_n(k)$.*

Proof. The algebra $M_n(k)$ has a well-known presentation

$$M_n(k) = k\{x, y\}/\langle x^n = 1, y^n = 1, yx = qxy\rangle,$$

where

$$x = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \qquad y = \begin{pmatrix} q & 0 & 0 & \cdots & 0 \\ 0 & q^2 & 0 & \cdots & 0 \\ 0 & 0 & q^3 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & q^n \end{pmatrix},$$

with q a primitive n-th root of unity. We provide a connected grading of $k\{x, y\}$ by assigning degree $(t, 1)$ to x and degree $(1, t)$ to y, where t is a generator of C_n. The group is abelian and the order of the generators is n, and hence the ideal of relations is homogeneous. Since the support coincides with $C_n \times C_n$, the grading is connected. □

Proposition 4.5. *Let $\mathcal{C}$ be a k-category with a finite set of objects and one-dimensional vector spaces of morphisms between any pair of objects b and c, denoted by ${}_c\mathcal{C}_b = k\ {}_c f_b$, verifying*

$$({}_d f_c)({}_c f_b) = q_{d,c,b}\ ({}_d f_b)$$

for any triple of objects of $\mathcal{C}$, where $q_{d,c,b} \in k^*$ are the structure constants. Then $\mathcal{C}$ is simply connected.

Proof. Let G be a group providing a grading of the category $\mathcal{C}$. As noted above, we consider connected gradings. Since all the k-vector spaces of morphisms are one-dimensional, they are homogeneous. Let ${}_c s_b$ be the degree of ${}_c\mathcal{C}_b$. Note that for each object b we have ${}_b\mathcal{C}_b = k$; hence ${}_b s_b = 1$ and ${}_b s_c = {}_c s_b^{-1}$. We assert that any nonzero homogeneous closed walk has degree 1. Indeed, since composition of nonzero morphisms is nonzero in $\mathcal{C}$, and since ${}_b s_c = {}_c s_b^{-1}$, a nonzero homogeneous closed walk at b can be replaced by a nonzero endomorphism of b with the same degree. Since endomorphisms of b have degree 1, the assertion is proved. Recall that a grading is connected if for any pair of objects, any group element appears

as the degree of a nonzero homogeneous walk between them. Since the grading is connected, the group is trivial. □

Corollary 4.6. *Let $\mathscr{C}$ be a category as above. Then $\pi_1(\mathscr{C}) = 1$.*

Let ${}_jE_i$ be the matrix whose entries are zero, except the (j, i) entry, which equals 1. We recall that a *good grading* of a matrix algebra is a grading where the elementary matrices ${}_jE_i$, also called *matrix units*, are homogeneous; see for instance [Dăscălescu et al. 1999]. Note that the k-category $\mathscr{M}_n(k)$ associated to a matrix algebra with respect to the idempotent elementary matrices ${}_iE_i$ is precisely a category as in the proposition above, where all the structure constants equal 1.

Clearly good gradings of $M_n(k)$ and gradings of the k-category $\mathscr{M}_n(k)$ coincide.

Corollary 4.7. *Let G be a group providing a good grading of a matrix algebra, and assume that the corresponding grading of the k-category $\mathscr{M}_n(k)$ is connected. Then G is trivial.*

Remark 4.8. A good grading by a nontrivial group G of a matrix algebra $M_n(k)$ can be connected when $M_n(k)$ is viewed as a category with a single object. This means that the support of the grading generates G. Corollary 4.7 makes precise that the corresponding grading of the k-category $\mathscr{M}_n(k)$ will not be connected.

Theorem 4.9. *The connected grading of the matrix algebra $M_n(k)$ by the group $C_n \times C_n$ of Proposition 4.4 is simply connected.*

Proof. We will prove that the Galois covering $\mathscr{C} = M_n(k)\#(C_n \times C_n)$ is simply connected. The category $\mathscr{C} = M_n(k)\#(C_n \times C_n)$ has set of objects $C_n \times C_n = \{a^i b^j \mid 0 \le i, j \le n-1\}$ and

$$ {}_{a^s b^l}\mathscr{C}_{a^i b^j} = X^{a^{i-s} b^{j-l}} M_n(k) = k(x^{i-s} y^{j-l}). $$

Hence the k-vector spaces of morphisms are one-dimensional with basis elements

$$ {}_{(s,l)}f_{(i,j)} = x^{i-s} y^{j-l} $$

and

$$ {}_{(u,v)}f_{(s,l)}\,{}_{(s,l)}f_{(i,j)} = x^{s-u} y^{l-v} x^{i-s} y^{j-l} = q^{l+i-v-s}\,{}_{(u,v)}f_{(i,j)}. $$

Finally, Proposition 4.5 asserts that such categories are simply connected. □

Each time a universal covering exists, the fundamental group is isomorphic to its Galois group. Clearly, if there exist at least two nonisomorphic simply connected coverings, there is no universal covering.

We will now show that this is the case for $M_n(k)$, that is, there exists at least another simply connected grading of $M_n(k)$. For this purpose we first provide another presentation of the matrix algebra as a quotient of a path algebra.

Proposition 4.10. *Let Q be the quiver with n vertices labelled $1, \dots, n$, and arrows x_i from i to $i+1$ as well as reverse arrows y_i from $i+1$ to i for $1 \leq i < n$. We denote by $e_1, \dots, e_n$ the idempotents of the path algebra kQ corresponding to the vertices. Let I be the two-sided ideal of kQ generated by $y_i x_i - e_i$ and $x_i y_i - e_{i+1}$ for $1 \leq i < n$. Then kQ/I is isomorphic to $M_n(k)$.*

Proof. Consider the morphism of algebras $\varphi : kQ \to M_n(k)$ given by $\varphi(e_i) = {}_iE_i$, $\varphi(x_i) = {}_{i+1}E_i$ and $\varphi(y_i) = {}_iE_{i+1}$, which is well-defined by the universal property of path algebras, which are in fact tensor algebras over the semisimple commutative algebra given by the length zero paths. This map is surjective, since the matrices ${}_jE_i$ are clearly images of paths of Q. Also $I \subset \operatorname{Ker}\varphi$ and $\dim_k kQ/I \leq n^2$. □

Let F_{n-1} be the free group on $n-1$ generators $s_1, \dots, s_{n-1}$. First we introduce an F_{n-1} grading of kQ as follows: for $1 \leq i \leq n$, let $\deg e_i = 1$, while for $1 \leq i \leq n-1$ we set $\deg x_i = s_i$ and $\deg y_i = (s_i)^{-1}$. The path algebra is a free algebra on the set of arrows with respect to the semisimple subalgebra of vertices, so this provides a well-defined grading of kQ. More precisely, the degree of any path is the corresponding product of the degrees of the arrows. Since the ideal I is homogeneous with respect to this grading, we obtain a grading of kQ/I, and hence of $M_n(k)$. Note that this grading, considered as a grading of the algebra $M_n(k)$, that is, as a grading of the single object category with endomorphism algebra $M_n(k)$, is connected, since the generators of the free group are in the support.

Proposition 4.11. *The F_{n-1}-grading of $M_n(k)$ just described is simply connected.*

Proof. The set of objects of $M_n(k)\#F_{n-1}$ is F_{n-1}. For $j > i$, let ${}_js_i = s_{j-1} \dots s_{i+1}s_i$. There is a one-dimensional vector space of morphisms from a word w in F_{n-1} considered as an object of $M_n(k)\#F_{n-1}$ to each object ${}_js_iw$ with basis vector denoted by ${}_jE_i{}^w$. Similarly, for $j < i$ there is a one-dimensional vector space of morphisms from w to ${}_js_i^{-1}w$, with basis ${}_jE_i{}^w$. From w to w, the n-dimensional vector space of morphisms has basis $\{{}_1E_1{}^w, \dots, {}_nE_n{}^w\}$. Note that the endomorphism algebra of each object is the n-dimensional diagonal algebra $k({}_1E_1{}^w) \times \cdots \times k({}_nE_n{}^w)$. Consider now a grading of this category by a group G. Since the spaces of morphisms between different objects are one-dimensional, they are homogeneous. This fact implies that for each object w, the subvector space $k\,({}_iE_i{}^w)$ is homogeneous, since

$${}_iE_j{}^{({}_js_iw)}\,{}_jE_i{}^w = {}_iE_i{}^w.$$

Observe that an idempotent homogeneous element necessarily has degree 1, so each endomorphism algebra has trivial grading (all elements have degree 1). As a consequence,

$$\deg\left({}_iE_j{}^{({}_js_iw)}\right) = \left(\deg {}_jE_i^w\right)^{-1}.$$

Moreover, for $j > i$,

$$\deg({}_jE_i{}^w) = \deg\big({}_jE_{j-1}{}^{({}_{j-1}s_i w)}\big) \cdots \deg({}_{i+2}E_{i+1}{}^{s_i w})\ \deg({}_{i+1}E_i{}^w).$$

For $j < i$, the statement is analogous considering the inverses of the degrees above. This complete description of any possible grading of the smash category shows that any closed homogeneous nonzero walk has degree 1. Consequently the grading is connected only if the group is trivial. □

The complete list of good gradings of a matrix algebra is obtained in [Caenepeel et al. 2002]. In order to compute the fundamental groups of matrix algebras, we make this classification explicit using Proposition 4.10.

Theorem 4.12. *There is a one-to-one correspondence between good connected G-gradings of $M_n(k)$ and maps $\{1, \dots, n-1\} \to G$ such that the image generates G.*

Proof. Let m be a map from $\{1, \dots, n-1\}$ to G. We obtain a grading of the algebra kQ defined in Proposition 4.10 as before, namely $\deg({}_{i+1}E_i) = m(i)$ and $\deg({}_iE_{i+1}) = m(i)^{-1}$. The ideal of relations of Proposition 4.10 is homogeneous and we obtain a good grading of $M_n(k)$. If the image of m generates G, then the grading is connected. Conversely, consider a good connected grading of $M_n(k)$ by a group G. The image of the map $m : \{1, \dots, n-1\} \to G$ given by $m(i) = \deg({}_{i+1}E_i)$ generates G. □

Note that relaxing the connectedness requirement for good gradings is equivalent to removing the condition that the image of each map m generates G. In [Caenepeel et al. 2002], the algebra $M_n(k)$ is viewed as the endomorphism algebra of a vector space V, and good gradings are obtained from a grading of V, considering graded endomorphisms as homogeneous components.

Definition 4.13. The *quotient* of a G-grading X of a category $\mathcal{B}$ by a normal subgroup N of G is a G/N-grading X/N of $\mathcal{B}$, where the homogeneous component of degree α is

$$(X/N)^\alpha{}_c\mathcal{B}_b = \bigoplus_{g \in \alpha} X^g{}_c\mathcal{B}_b.$$

Observe that if X is connected then X/N is also connected.

The corresponding functor between the smash product coverings is precisely the canonical projection obtained through the quotient of $\mathcal{B}\#G \to \mathcal{B}$ by N.

Proposition 4.14. *Any good connected G-grading of $M_n(k)$ is a quotient of the F_{n-1}-grading considered before.*

Proof. Let $m_0 : \{1, \dots, n-1\} \to F_{n-1}$ be the map corresponding to this grading, given by $m_0(i) = s_i$, and let $m : \{1, \dots, n-1\} \to G$ be another map such that the image of m generates G. Then the group homomorphism given by $s_i \mapsto m(i)$ is a surjective group morphism. □

We recall that a simply connected grading is a grading that is maximal in the sense that it is not isomorphic to a proper quotient of a connected grading.

Proposition 4.15. *Let k be a field containing a primitive n-th root of unity. The grading by $C_n \times C_n$ of Proposition 4.4 and the grading by the free group of Proposition 4.11 have a unique maximal common quotient C_n-grading.*

Proof. We denote by X the grading by $C_n \times C_n$ and we observe that the vector space X^1 of homogeneous elements of trivial degree is one-dimensional. Let Y be the grading by F_{n-1}: observe that Y^1 is the n-dimensional subalgebra of diagonal matrices. Assume that Z is a common quotient of X and Y, and let N be the normal subgroup of $C_n \times C_n$ that provides Z as a quotient of X. Since Z is a quotient of Y, clearly Z^1 contains at least Y^1, the diagonal matrices. Observe that the elementary diagonal matrices are homogeneous for X, and consequently their degrees must be elements of N in order to become trivial. The set of degrees of the diagonal matrices for X is precisely $1 \times C_n$. Hence $1 \times C_n$ is the smallest subgroup of $C_n \times C_n$ that has a chance to meet a quotient of Y; let $N = 1 \times C_n$. In fact we assert that X/N is already a good grading; in other words, elementary matrices are homogeneous. Indeed, consider the n-dimensional subvector space E of $M_n(k)$ with basis $\{{}_2E_1, {}_3E_2, \ldots, {}_nE_{n-1}, {}_1E_n\}$. Recall that x is the circulant matrix, which is the sum of all the previous basis vectors of E, while y is the diagonal matrix made with powers of the primitive root of unity q. Then the set $\{x, xy, xy^2, \ldots, xy^{n-1}\}$ is clearly contained in E. Also the elements xy^i, for $0 \le i \le n-1$, are homogeneous for the grading X, of different degrees (t, t^i) where t is the generator of C_n. Hence they are linearly independent and they form a basis of E. Finally we observe that for X/N, all these elements have the same degree $\overline{(t, 1)}$, and hence E is contained in the set of homogeneous elements of degree $\overline{(t, 1)}$ of X/N.

Consequently, each elementary matrix is homogeneous for X/N. Considering Y, we obtain X/N as the quotient Y/M, where M is the smallest normal subgroup of F_{n-1} such that in F_{n-1}/M all the generators of F_{n-1} are equal, and this element is of order n. □

Theorem 4.16. *Let k be an algebraically closed field.*

(1) *If* $\mathrm{char}(k) \neq 2$, *then* $\pi_1 M_2(k) \simeq \mathbb{Z} \times C_2$.

(2) *If* $\mathrm{char}(k) \neq 3$, *then* $\pi_1 M_3(k) \simeq F_2 \times C_3$.

Proof. Under these assumptions, the classifications of [Khazal et al. 2003; Boboc and Dăscălescu 2001] show that all gradings are good gradings or quotients of the one given by Proposition 4.4. The latter and the grading by the free group have a common quotient described in Proposition 4.15. Recall that we have proved that all good gradings of $M_n(k)$ are quotients of the F_{n-1}-grading. We now prove the first assertion. We construct two inverse group morphisms between $\pi_1 M_2(k)$ and

$F_1 \times C_2$. Let $\sigma \in \operatorname{Aut} \Phi^{\#}$, where $\Phi^{\#} : \operatorname{Gal}^{\#}(M_2(k)) \to \mathrm{Sets}$ is the fiber functor. Consider the good F_1-grading of $M_2(k)$. By Proposition 3.5, the map σ_{F_1} verifies $\sigma_{F_1}(x) = xg$ for some uniquely determined $g \in F_1$. Analogously, the $C_2 \times C_2$-grading provides $\sigma_{C_2 \times C_2}$ and an element (t^a, t^b), where $C_2 = \langle t \rangle$. The compatibility condition obtained when considering the maximal common quotient C_2 says that t^a equals the class of g in C_2. We associate the pair (g, t^b) to σ.

Conversely, given $(g, t^b) \in F_1 \times C_2$, we will construct $\sigma \in \operatorname{Aut} \Phi^{\#}$ associated to it. One needs to have maps $\sigma_G : G \to G$ for each group G providing a connected grading of $M_2(k)$. Using the classification of the gradings given in [Khazal et al. 2003] and Proposition 4.15, it is sufficient to describe σ_{F_1} and $\sigma_{C_2 \times C_2}$. Fix $\sigma_{F_1}(x) = xg$ and $\sigma_{C_2 \times C_2}(x) = x(\overline{g}, t^b)$. Note that these maps satisfy the compatibility condition. Of course, for the other quotients G of F_1 or of $C_2 \times C_2$, the map σ_G is uniquely determined thanks to the quotient compatibility conditions.

The proof of the second statement is completely analogous. □

Next we prove a generalization of the preceding theorem for matrices of prime size. Consider an algebraically closed field k of characteristic zero. The main result — Theorem 5.1 — of [Bahturin and Zaicev 2002] states that any grading of $M_n(k)$ by a group G is a tensor product of gradings, in the sense that there exists a decomposition $n = n_1 n_2$, a fine grading of $M_{n_1}(k)$ by a subgroup G_1 of order n_1^2, and a good G-grading of $M_{n_2}(k)$ such that $M_n(k)$ is isomorphic as a G-graded algebra to the tensor product algebra $M_{n_1}(k) \otimes M_{n_2}(k)$ that is obtained as an induced grading. The construction of an induced grading resembles a tensor construction, but is well-defined only in the case where one of the graded algebras involved is a matrix algebra with a good grading [Bahturin and Zaicev 2002].

Proposition 4.17. *Let p be a prime and k be an algebraically closed field of characteristic zero. Let X be a maximal connected grading by a group G of $M_p(k)$. Then either the group G is isomorphic to $C_p \times C_p$ and the grading is fine as in Proposition 4.4, or the grading is a good grading given by $m : \{1, \ldots, p-1\} \to G$ such that* $\mathrm{Im}(m)$ *generates G.*

Proof. Since p is a prime, [Bahturin and Zaicev 2002, Theorem 5.1] shows that the grading is either good, or fine with group of order p^2. We already know that good connected gradings are as described in Proposition 4.14. If the grading is fine, the order p^2 of the group is precisely the dimension of the matrix algebra, and hence $\operatorname{Supp} X = G$. Moreover, for fine gradings of matrix algebras, homogeneous nonzero elements are invertible by Corollary 2.7 of the same article. Then we assert that the group is not cyclic: indeed, if G has a generator t of order p^2, let x be a nonzero element of degree p^2, and thus invertible. Note that $X^1 M_p(k) = k$. Hence $x^{p^2} \in k$ and $x^{p^2} \neq 0$, and we can normalize x by dividing it by a scalar in order to obtain $x' \in X^t M_p(k)$ such that $x'^{p^2} = 1$. Then $M_p(k)$ would be isomorphic to the

group algebra of the cyclic group of order p^2, which is false since (for instance) the former is commutative.

Consequently, a fine connected grading of $M_p(k)$ is given by $C_p \times C_p$. As before, $\operatorname{Supp} X = G$ for dimensional reasons. Let t be a generator of C_p and let x and y be nonzero elements of degree $(t, 1)$ and $(1, t)$ respectively. Again, x and y are invertible and we normalize them in order to have $x^p = y^p = 1$. They do not commute, since otherwise the algebra would be the commutative algebra $k(C_p \times C_p)$. In fact, xy and yx are both nonzero and have common degree (t, t). Hence they differ by a scalar: $yx = qxy$. Moreover $q^p = 1$, since $x = y^p x = q^p xy^p = q^p x$. Then q is a primitive root of unity and the grading corresponds to the grading of Proposition 4.4. □

Theorem 4.18. *Let k be an algebraically closed field of characteristic zero, and let p be a prime. Then*

$$\pi_1 M_p(k) \simeq F_{p-1} \times C_p.$$

The proof is completely analogous to the proof of Theorem 4.16.

We end this section with a computation of the fundamental group of triangular matrix algebras, based on [Valenti and Zaicev 2007].

A grading of an upper triangular matrix algebra $T_n(k)$ is *good* if the elementary matrices ${}_jE_i$ are homogeneous. Clearly any good grading is completely determined by assigning group elements to subdiagonal elementary matrices ${}_{i+1}E_i$, since the idempotents ${}_iE_i$ necessarily have trivial degree. In other words, a good grading is determined as before by a map $m : \{1, \dots, n-1\} \to G$. The grading is connected if and only if $\operatorname{Im} m$ generates G. As before, any good connected grading is a quotient of the grading given by the free group F_{n-1} on a set $\{s_1, \dots, s_{n-1}\}$ and a map m such that $\operatorname{Im} m = \{s_1, \dots, s_{n-1}\}$.

Theorem 7 of [Valenti and Zaicev 2007] states that any grading of a triangular algebra is good, without any hypothesis concerning the field. As an immediate consequence we obtain:

Theorem 4.19. *Let k be a field and let $T_n(k)$ be the algebra of triangular matrices of size n. Then*

$$\pi_1 T_n(k) \simeq F_{n-1}.$$

5. The fundamental group of truncated polynomial algebras

In this section we compute the fundamental group of the group algebra of the cyclic group of order p in characteristic p, that is, we compute the fundamental group of $k[x]/(x^p)$.

Proposition 5.1. *Let G be a finite group and let k be any field. The usual G-grading of the group algebra kG is simply connected.*

Proof. The Galois covering $kG\#G$ has G as set of objects and, given $s, t \in G$,

$$ {}_t(kG\#G)_s = k(t^{-1}s). $$

The composition is given by the product of G. In other words, all k-vector spaces of morphisms are one-dimensional and all of the structure constants are 1. By Proposition 4.5, this category is simply connected. □

Remark 5.2. As a consequence of this proof, we recover the Cohen–Montgomery duality theorem for coactions [Cohen and Montgomery 1984]: the algebras $kG\#G$ and $M_{|G|}(k)$ are isomorphic. The algebra associated to a finite object category is obtained as the direct sum of all the vector spaces of morphisms. In particular, if all the vector spaces of morphisms are one-dimensional, we get the matrix algebra. Hence the algebra associated to the category $kG\#G$ is $M_{|G|}(k)$. On the other hand, it was proved in [Cibils and Marcos 2006] that the algebra corresponding to the categorical smash product by a finite group is precisely the usual smash product algebra.

Next we provide an example of a path k-algebra of a quiver with admissible relations, which does not admit a universal cover when the field is of characteristic p. The quiver is a loop, and the relation is given by the p-th power of the loop. There are at least two simply connected coverings by smash categories. One of them is not a covering of "quivers with relations" in the sense of [Gabriel 1981].

Proposition 5.3. *Let k be a field of characteristic p. The truncated polynomial algebra $k[x]/(x^p)$ does not admit a universal covering.*

Proof. First, note that $k[x]/(x^p)$ is isomorphic to the k-group algebra of the cyclic group C_p of order p, and hence the preceding proposition provides a simply connected covering with group C_p. Note that this covering is the category with p vertices, where all vector spaces of morphisms are one-dimensional and all the structure constants are 1.

On the other hand, consider the usual $\mathbb{Z}$-grading of $k[x]$. Since (x^p) is a homogeneous ideal — this holds in any characteristic — it induces a grading in $k[x]/(x^p)$. For this grading, $[k[x]/(x^p)]\#\mathbb{Z}$ is the category that has $\mathbb{Z}$ as set of objects, one-dimensional vector spaces of morphisms from i to j if $0 \leq j - i < p$, and 0 otherwise. In other words, the morphisms in the category are generated by morphisms from i to $i + 1$ for each integer i, with relations such that any composition of p generators is zero. As a consequence of this description, each grading of $[k[x]/(x^p)]\#\mathbb{Z}$ is freely determined by assigning a degree to the one-dimensional vector space of morphisms from i to $i + 1$. Hence, any homogeneous nonzero closed walk has trivial degree.

Recall that by the definition of a connected grading, any element of the group should be the degree of a homogeneous walk between objects. Then the unique

group that grades this smash product category in a connected way is the trivial one. As a consequence, this covering category is simply connected. Finally note that the Galois coverings are not isomorphic, since their groups of automorphisms are not isomorphic. In this way we have constructed two nonisomorphic simply connected coverings. □

It is well-known and easy to prove that the trivial homogeneous component of any grading always contains the ground field k.

A grading is called *fine* if the dimension of each homogeneous component is at most one; see for instance [Bahturin et al. 2001].

Theorem 5.4. *Let k be a field of characteristic p and let $A = k[x]/(x^p)$. There are two types of connected gradings of A, with no common quotient except the trivial one. The first type corresponds to the group algebra case, and its grading group is C_p. In the second one, the grading group is either $\mathbb{Z}$ or any of its quotients.*

Proof. Let X be a connected basic grading of A. There are two cases, according to the existence of an invertible homogeneous element of nontrivial degree. First we suppose that there exists an invertible homogeneous element a of degree $s \neq 1$. We write $a = a_0 + a_+$, where $a_0 \in k^*$ and $a_+ \in (x)$, and we normalize a in order to have $a_0 = 1$. Since the characteristic of k is p, we obtain that $a^p = 1$ and p is the order of a. For $i < p$ we infer that $a^i \neq 0$, and thus $X^{s^i} A \neq 0$. Moreover, $X^{s^i} A \neq X^{s^j} A$ for $i \neq j$, $i, j < p$. Also $1 = a^p \in X^{s^p} A$ implies $s^p = 1$. Since the grading is connected, by computing dimensions we deduce that the group is cyclic of order p, and the grading is fine.

As a second case, assume that all homogeneous elements of nontrivial degree belong to the maximal ideal (x):

$$\bigoplus_{s \in G,\, s \neq 1} X^s A \subseteq (x).$$

Consider now the usual valuation ν on A: namely, for $f \neq 0$ we have that $\nu(f)$ is the smallest exponent of x appearing in f. Of course $\nu(f) = 0$ if and only if f is invertible. The valuation ν has the following properties:

- $\nu(f+g) \geq \inf\{\nu(f), \nu(g)\}$ for f, g, $f + g \neq 0$.
- $\nu(fg) = \nu(f) + \nu(g)$ for f, g, $fg \neq 0$.

Then for $f \neq 0$ we obtain $f = x^{\nu(f)} u$, where u is invertible.

Assume first that there exists a homogeneous $g_1 \in X^1 A$ of valuation 1, that is, $g_1 = x + u$ with $u \in (x^2)$. Since $g_1^{p-1} = x^{p-1}$ and g_1^{p-1} is homogeneous, we infer that x^{p-1} is homogeneous of degree 1. Now, $g_1^{p-2} = x^{p-2} + \lambda x^{p-1}$, so $x^{p-2} = g_1^{p-2} - \lambda x^{p-1}$ and thus x^{p-2} is homogeneous of degree 1. If we continue with this procedure, we finally get that x is homogeneous of degree 1 and the

grading is trivial. Finally, assume $\nu(g_1) \geq 2$ for any homogeneous $g_1 \in X^1 A$. We claim that there exists a homogeneous f of valuation 1. If not, for any $g \in (x)$ we have $\nu(g) \geq 2$, by decomposing g as a sum of its homogeneous components and using the property of a valuation just discussed, which is clearly false since $\nu(x) = 1$. Now $\nu(f^i) = i$ for $i < p$. Since $f^i \in X^{s^i} A$, the latter is not zero. For dimensional reasons, we infer that the support of the grading is $\{1, s, \ldots, s^{p-1}\}$, which generates a cyclic group. □

Corollary 5.5. *Let k be a field of characteristic p. Then $\pi_1(k[x]/(x^p)) = \mathbb{Z} \times C_p$.*

6. The fundamental group of diagonal algebras

Let E be a finite set and k a field. The diagonal algebra k^E is the vector space of maps from E to k with pointwise multiplication. Next we consider connected gradings of diagonal algebras [Dăscălescu 2008; Bichon 2008]. The following result shows that any abelian group with the cardinality of a given set grades the diagonal algebra in a connected way, if the field contains enough roots of unity.

Proposition 6.1. *Let E be a finite set of order n, and let k be a field with enough n-th roots of unity. Let G be any abelian group of order n. Then there is a simply connected G-grading of k^E.*

Proof. We first sketch the proof of the following well-known result. Let G be any abelian group of order n, E a set of cardinal n, and k a field containing n different n-th roots of unity; then the algebras kG and k^E are isomorphic. First assume that G is cyclic. Let t be a generator of G and let μ_n be the set of n-th roots of unity in k. Note that under our assumptions p does not divide n in the case where k is a field of characteristic $p > 0$. Then the set

$$\left\{ e_\zeta = \frac{1}{n} \sum_{i=0}^{n-1} \zeta^i t^i \right\}_{\zeta \in \mu_n}$$

is a complete set of orthogonal idempotents of kG and has n elements. This set provides a new basis of kG, proving that kG is isomorphic to $\bigoplus_{\zeta \in \mu_n} k e_\zeta$, which in turn is identified with k^E through a bijection between E and μ_n by considering the Dirac masses in k^E.

For an arbitrary abelian group G of order n, note that G is a direct product of finite cyclic groups. Note also that a group algebra $k(G_1 \times G_2)$ is isomorphic to $kG_1 \otimes kG_2$, while the algebras $k^{E_1 \times E_2}$ and $k^{E_1} \otimes k^{E_2}$ are also isomorphic. The previous case provides the required isomorphism.

Next we prove the statement of the proposition. Consider the algebra k^E, an arbitrary abelian group G of order n, and an algebra isomorphism between kG and k^E as before. The usual G-grading of kG provides a grading of k^E by transporting

the structure through the isomorphism. Consequently any abelian group of order n provides a simply connected grading of the algebra k^E. □

Corollary 6.2. *Let n be a nonsquare free positive integer and let k be a field as above. The algebra k^n does not admit a universal covering.*

Proof. If n is not square-free, there exist at least two nonisomorphic groups of order n. Proposition 6.1 provides at least two nonisomorphic simply connected coverings, so k^n does not admit a universal cover. Moreover, each abelian group G of order n provides a simply connected grading through the isomorphism of k^n with kG. □

The following result is based on the fact that $k \times k$ admits precisely one connected grading. We provide a proof of this, which is also a particular case of Dăscălescu's classification [2008] (see also [Bichon 2008]).

Proposition 6.3. *Let k be a field of characteristic different from 2. The fundamental group $\pi_1(k \times k)$ is cyclic of order 2.*

Proof. Let X be a connected G-grading of $k \times k$ for some group G. The trivial homogeneous component $X^1(k \times k)$ contains the unit of the algebra. If $X^1(k \times k) = k \times k$, then the group is trivial since the support of X is just the trivial element of G and the grading is connected. Otherwise there is exactly one more nonzero homogeneous component $X^s(k \times k)$ that is one-dimensional. Note that s has to generate G. We prove that s is of order 2. Let (x, y) be a nonzero element of degree s. Clearly $(x, y)^2 \neq 0$, and also $(x, y)^2 \in X^{s^2}(k \times k)$. Since there are only two homogeneous components, we infer that $X^{s^2}(k \times k) = X^1(k \times k)$ or $X^{s^2}(k \times k) = X^s(k \times k)$. In the first case $s^2 = 1$, while in the second case $s = 1$. Consequently, there are precisely two connected gradings and the fundamental group is cyclic of order two. □

Lemma 6.4. *Let A and B be algebras with connected G_A and G_B-gradings X and Y. Then the algebra $C = A \times B$ has a natural $(G_A * G_B)$-connected grading Z. As a consequence, all quotients of $G_A * G_B$ grade C connectedly.*

Proof. Consider the following subspaces of C:

$$\begin{aligned} Z^1 C &= X^1 A \times Y^1 B, \\ Z^s C &= X^s A \times 0, && \text{if } s \neq 1 \text{ and } s \in G_A, \\ Z^t C &= 0 \times Y^t B, && \text{if } t \neq 1 \text{ and } t \in G_B, \\ Z^w C &= 0, && \text{in the remaining cases.} \end{aligned}$$

The support of the grading Z is the union of the supports of X and Y. These supports generate G_A and G_B respectively, and hence the support of Z generates $G_A * G_B$. □

Example 6.5. Let E_5 be a set with five elements. There exists a connected C_6-grading of k^{E_5}.

Indeed, let E_2 and E_3 be sets with two and three elements respectively. Then $k^{E_5} \cong k^{E_2} \times k^{E_3}$ and we consider the previous fine and connected gradings given by C_2 and C_3 of k^{E_2} and k^{E_3} respectively. Lemma 6.4 shows that the product group $C_2 * C_3$ grades the product algebra k^{E_5} in a connected way, as well as any of its quotients, in particular C_6.

This example is the basis of the general procedure developed by Dăscălescu in order to describe all the connected gradings of a diagonal algebra. We rephrase one of his results.

Lemma 6.6 [Dăscălescu 2008, Lemma 1]. *Let k^n be a diagonal algebra. Any connected G-grading with one-dimensional trivial homogeneous component is given by the usual G-grading of kG, where G is any abelian group of order n.*

Note that Dăscălescu calls *ergodic* a grading with one-dimensional trivial homogeneous component. For $n = 2$, a nontrivial grading has to be ergodic, and hence we recover the fact that there is only one nontrivial grading of $k \times k$ as in Proposition 6.3.

Theorem 5 of [Dăscălescu 2008] provides a description of all the gradings of k^E, which is based on ergodic ones. We shall use it in order to compute $\pi_1(k^n)$ for small values of n. In order to state his result, we fist consider the following specific connected gradings of a diagonal algebra, modeled on Example 6.5.

Roughly speaking, the specific gradings are free product gradings of connected ergodic ones based on a product algebra decomposition of a diagonal algebra. Note that connected ergodic gradings of diagonal algebras are classified by Lemma 6.6.

More precisely, let $A = k^E$ be a diagonal algebra and let $M_1, \ldots, M_s$ be a partition of E. Let A_{M_i} be the algebra $A.e_{M_i}$, where

$$e_{M_i} = \sum_{x \in M_i} \delta_x$$

with δ_x the Dirac mass at x. It is easy to prove that any direct product decomposition of k^E is obtained in this way. Let H_i be an abelian group of order $\#(M_i)$, and finally let X_i be the corresponding H_i-ergodic grading of A_{M_i}. Then by Lemma 6.4, the group $H_1 * \cdots * H_s$ provides a connected grading of $A = A_{M_1} \times \cdots \times A_{M_s}$, which we call specific.

Theorem 6.7 [Dăscălescu 2008]. *Let E be a finite set and let k be a field containing all roots of unity of order less than or equal to $\#E$. Any connected grading of k^E is a quotient of a specific grading.*

Corollary 6.8. *Let k be a field containing all roots of unity of order* 2 *and* 3. *Then* $\pi_1(k^3) = C_2 \times C_3$.

Group	Dimension of the trivial component	Dimensions of other components
$\{1\}$	4	0
$C_2 * C_2$	2	1, 1
C_3	2	1, 1
C_2	3	1
C_4	1	1, 1, 1
$C_2 \times C_2$	1	1, 1, 1

Proof. The two nontrivial partitions of $\{1, 2, 3\}$ provide connected gradings by C_2 and C_3. Clearly they do not have nontrivial common quotients. □

Theorem 6.9. *Let k be a field containing all roots of unity of order* 2, 3 *and* 4. *Then* $\pi_1(k^4) = (C_2 * C_2) \times C_4 \times C_2 \times C_2 \times C_3 = (C_2 * C_2) \times C_6 \times C_4 \times C_2$.

Proof. The specific gradings of k^4 are given by the partitions of the set $\{1, 2, 3, 4\}$ as shown in the table above. An inspection of the possible common quotients, taking into account the structure of the groups and the dimension of the trivial homogeneous components, shows that the C_2-grading is a quotient of the $C_2 * C_2$-grading. Moreover, there is no other nontrivial common quotient. □

Acknowledgement

We thank S. Dăscălescu for a valuable exchange during the preparation of this work.

References

[Aljadeff et al. 2010] E. Aljadeff, D. Haile, and M. Natapov, "Graded identities of matrix algebras and the universal graded algebra", *Trans. Amer. Math. Soc.* **362**:6 (2010), 3125–3147. MR 2592949

[Bahturin and Shestakov 2001] Y. Bahturin and I. Shestakov, "Gradings of simple Jordan algebras and their relation to the gradings of simple associative algebras", *Comm. Algebra* **29**:9 (2001), 4095–4102. MR 2002h:17033 Zbl 1054.17025

[Bahturin and Zaicev 2002] Y. A. Bahturin and M. V. Zaicev, "Group gradings on matrix algebras", *Canad. Math. Bull.* **45**:4 (2002), 499–508. MR 2003h:16046 Zbl 1022.16032

[Bahturin et al. 2001] Y. A. Bahturin, S. K. Sehgal, and M. V. Zaicev, "Group gradings on associative algebras", *J. Algebra* **241**:2 (2001), 677–698. MR 2002h:16067 Zbl 0988.16033

[Bichon 2008] J. Bichon, "Algebraic quantum permutation groups", *Asian-Eur. J. Math.* **1**:1 (2008), 1–13. MR 2009c:16112 Zbl 1170.16028

[Boboc 2003] C. Boboc, "Gradings of matrix algebras by the Klein group", *Comm. Algebra* **31**:5 (2003), 2311–2326. MR 2004e:16029 Zbl 1030.16025

[Boboc and Dăscălescu 2001] C. Boboc and S. Dăscălescu, "Gradings of matrix algebras by cyclic groups", *Comm. Algebra* **29**:11 (2001), 5013–5021. MR 2002h:16068 Zbl 1002.16039

[Boboc and Dăscălescu 2006] C. Boboc and S. Dăscălescu, "Good gradings of matrix algebras by finite abelian groups of prime index", *Bull. Math. Soc. Sci. Math. Roumanie* (*N.S.*) **49(97)**:1 (2006), 5–11. MR 2006m:16034 Zbl 1108.16037

[Boboc and Dăscălescu 2007] C. Boboc and S. Dăscălescu, "Group gradings on $M_3(k)$", *Comm. Algebra* **35**:9 (2007), 2654–2670. MR 2008k:16054 Zbl 1152.16031

[Bongartz and Gabriel 1982] K. Bongartz and P. Gabriel, "Covering spaces in representation-theory", *Invent. Math.* **65**:3 (1982), 331–378. MR 84i:16030 Zbl 0482.16026

[Caenepeel et al. 2002] S. Caenepeel, S. Dăscălescu, and C. Năstăsescu, "On gradings of matrix algebras and descent theory", *Comm. Algebra* **30**:12 (2002), 5901–5920. MR 2003h:16047 Zbl 1019.16030

[Chun and Lee 2007] J.-H. Chun and J. Lee, "Abelian group gradings on full matrix rings", *Comm. Algebra* **35**:10 (2007), 3095–3102. MR 2008j:16086 Zbl 1129.16034

[Cibils and Marcos 2006] C. Cibils and E. N. Marcos, "Skew category, Galois covering and smash product of a k-category", *Proc. Amer. Math. Soc.* **134**:1 (2006), 39–50. MR 2006e:18003 Zbl 1098.18002

[Cibils et al. 2007] C. Cibils, M. J. Redondo, and A. Solotar, "The intrinsic fundamental group of a linear category", preprint, 2007. arXiv 0706.2491

[Cohen and Montgomery 1984] M. Cohen and S. Montgomery, "Group-graded rings, smash products, and group actions", *Trans. Amer. Math. Soc.* **282**:1 (1984), 237–258. MR 85i:16002 Zbl 0533.16002

[Dăscălescu 2008] S. Dăscălescu, "Group gradings on diagonal algebras", *Arch. Math.* (*Basel*) **91**:3 (2008), 212–217. MR 2009f:16075 Zbl 05500568

[Dăscălescu et al. 1999] S. Dăscălescu, B. Ion, C. Năstăsescu, and J. Rios Montes, "Group gradings on full matrix rings", *J. Algebra* **220**:2 (1999), 709–728. MR 2000g:16048 Zbl 0947.16028

[Gabriel 1981] P. Gabriel, "The universal cover of a representation-finite algebra", pp. 68–105 in *Representations of algebras* (Puebla, 1980), edited by M. Auslander and E. Lluis, Lecture Notes in Math. **903**, Springer, Berlin, 1981. MR 83f:16036 Zbl 0481.16008

[Green 1983] E. L. Green, "Graphs with relations, coverings and group-graded algebras", *Trans. Amer. Math. Soc.* **279**:1 (1983), 297–310. MR 85a:16033 Zbl 0536.16001

[Green and Marcos 1994] E. L. Green and E. d. N. Marcos, "Graded quotients of path algebras: a local theory", *J. Pure Appl. Algebra* **93**:2 (1994), 195–226. MR 95f:16052 Zbl 0811.16010

[Khazal et al. 2003] R. Khazal, C. Boboc, and S. Dăscălescu, "Group gradings of $M_2(K)$", *Bull. Austral. Math. Soc.* **68**:2 (2003), 285–293. MR 2004i:16060 Zbl 1047.16023

[Le Meur 2007] P. Le Meur, "The universal cover of an algebra without double bypass", *J. Algebra* **312**:1 (2007), 330–353. MR 2008c:16026 Zbl 1124.16015

[Mitchell 1972] B. Mitchell, "Rings with several objects", *Advances in Math.* **8** (1972), 1–161. MR 45 #3524 Zbl 0232.18009

[Valenti and Zaicev 2007] A. Valenti and M. V. Zaicev, "Group gradings on upper triangular matrices", *Arch. Math.* (*Basel*) **89**:1 (2007), 33–40. MR 2009f:16054 Zbl 1151.16042

Communicated by Dave Benson
Received 2009-11-24 Accepted 2010-04-01

Claude.Cibils@math.univ-montp2.fr
Institut de mathématiques et de modélisation de Montpellier I3M, UMR 5149, Université Montpellier 2, F-34095 Montpellier cedex 5, France
http://www.math.univ-montp2.fr/~cibils/

mredondo@uns.edu.ar
Departamento de Matemática, Universidad Nacional del Sur, Avenida Leandro N. Alem 1253, B8000CPB Bahía Blanca, Argentina
http://inmabb.criba.edu.ar/gente/mredondo/

asolotar@dm.uba.ar
Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón 1, C1428EGA Buenos Aires, Argentina
http://mate.dm.uba.ar/~asolotar

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 and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in ANT are usually in English, but articles written in other languages are welcome.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@mathscipub.org with details about how your graphics were generated.

White Space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 4 No. 5 2010

1937-0652(2010)4:5;1-E