Algebra & Number Theory

Volume 6
2012
No. 6

mathematical sciences publishers

Algebra & Number Theory

msp.berkeley.edu/ant

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

The subscription price for 2012 is US $175/year for the electronic version, and $275/year (+$40 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://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

ALGEBRA AND NUMBER THEORY 6:6 (2012)
dx.doi.org/10.2140/ant.2012.6.1061

The smallest prime that does not split completely in a number field

Xiannan Li

We study the problem of bounding the least prime that does not split completely in a number field. This is a generalization of the classic problem of bounding the least quadratic nonresidue. Here, we present two distinct approaches to this problem. The first is by studying the behavior of the Dedekind zeta function of the number field near 1, and the second by relating the problem to questions involving multiplicative functions. We derive the best known bounds for this problem for all number fields with degree greater than 2. We also derive the best known upper bound for the residue of the Dedekind zeta function in the case where the degree is small compared to the discriminant.

1. Introduction

1.1. ***Historical background.*** Let $\mathcal{N}$ denote the least quadratic nonresidue modulo a prime p. An old and difficult problem in number theory is to find good upper bounds for $\mathcal{N}$. Much work has been done on this problem, and we will only mention a small selection of that here.

The best result known arises from considerations of cancellation in character sums. To be more specific, let χ be the quadratic character with modulus p. Then we say that χ exhibits cancellation at $x = x(p)$ if $\sum_{n \le x} \chi(n) = o(x)$. Thus, the well known bound of Pólya and Vinogradov for character sums implies that cancellation occurs for $x = p^{1/2+o(1)}$; see [Davenport 2000]. Vinogradov [1927] proved that such cancellation implies that the least quadratic nonresidue is $\mathcal{N} \ll p^{1/(2\sqrt{e})+o(1)}$. Burgess [1957] showed that cancellation occurs at $x = p^{1/4+o(1)}$, and this implied that

$$\mathcal{N} \ll p^{1/(4\sqrt{e})+o(1)}, \tag{1}$$

which apart from different quantifications of $o(1)$ is the best result known.

The author is partially supported by a NSERC PGS-D award.
MSC2000: primary 11N60; secondary 11R42.
Keywords: primes, split, number fields, Dedekind zeta function.

Vinogradov conjectured that $\mathcal{N} \ll_\epsilon p^\epsilon$ for any $\epsilon > 0$. This is very reasonable since the Riemann hypothesis for $L(s, \chi)$ implies the stronger bound of

$$\mathcal{N} \ll \log^2 p. \tag{2}$$

The true bound is suspected to be $\mathcal{N} \ll \log p \log\log p$, arising from probabilistic considerations.

1.2. ***Generalization.*** This problem is the same as finding the least prime which does not split completely in a quadratic field. A generalization is to find upper bounds for the least prime which does not split completely in an arbitrary number field. Let K be a number field of degree l with discriminant d_K, $\mathcal{N}$ the least prime which does not split, and let $\zeta_K(s)$ denote its Dedekind zeta function. Then $\zeta_K(s)$ is analytic on the complex plane except for a simple pole at $s = 1$. Moreover, the Euler product

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

holds for $\Re s > 1$, where the product is over prime ideals $\mathfrak{p}$ and $N(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$. We note that, if all integer primes split over K, the Euler product for $\zeta_K(s)$ would be the same as that for $\zeta(s)^l$, where as usual $\zeta(s)$ denotes the Riemann zeta function. Since $\zeta(s)^l$ has a pole of order l at $s = 1$ and $\zeta_K(s)$ has only a simple pole at $s = 1$, we see that not all primes split. This also leads to quantifications of the statement that the least prime which does not split cannot be too large and even suggests that stronger results should be available as l grows. Using this approach, K. Murty [1994] showed, assuming GRH for $\zeta_K(s)$, that $\mathcal{N} \ll ((\log d_K)/(l-1))^2$, which is analogous to (2). Unconditionally, Murty notes in a remark in the same paper that his method would give a bound with a main term that is of the form

$$\mathcal{N} \ll d_K^{\frac{1}{2(l-1)}}. \tag{3}$$

This type of result was explicitly proved later using essentially elementary methods by Vaaler and Voloch [2000]. Their result is that

$$\mathcal{N} \le 26 l^2 d_K^{\frac{1}{2(l-1)}}, \tag{4}$$

provided that

$$d_K \ge \tfrac{1}{8} e^{2(l-1)\max(105,\, 25\log^2 l)}.$$

Vaaler and Voloch note that this result is an improvement on the more general result of Lagarias, Montgomery, and Odlyzko [Lagarias et al. 1979]. The latter condition on the size of d_K is artificial, and there is reason to expect even better results when d_K is small compared to l.

Can this result be improved by some generalization of Vinogradov's method? Interestingly enough, we will show in Theorem 3 that this is not the case. In fact, the best result from Vinogradov's approach is also a bound of the same form. Our Lemma 1 and the discussion immediately preceding it give an alternate fourth proof of the $d_K^{1/(2(l-1))}$ bound.

It thus appears that $d_K^{1/(2(l-1))}$ is a natural barrier. However, using some ideas involving basic information on the zeros of $\zeta_K(s)$, we prove in Theorem 1 a result of the form

$$\mathcal{N} \ll d_K^{\frac{1}{4(l-1)}(1+o(1))}.$$

We also show that approaching the problem with multiplicative functions does pay dividends in some cases, which appear in Theorems 4 and 5, where we derive good bounds for $\mathcal{N}$ in the cases where K is cubic or biquadratic. The idea here is to study how certain multiplicative functions interact with one another and take advantage of the behavior of extremal quadratic characters. The behaviour of extremal quadratic characters has appeared previously in [Diamond et al. 2006], which reproduces unpublished work of Heath-Brown. It is also contained in [Granville and Soundararajan $\geq$ 2012]. In Lemma 12, we quantify what it means for a quadratic character to be almost extremal, which may be of independent interest.

In the cubic case, a consideration of the multiplicative functions involved will immediately generate a bound of $\mathcal{N} \ll d_K^{1/(4\sqrt{e})+\epsilon}$, where $4\sqrt{e} = 6.59\ldots$. By studying almost extremal quadratic characters, we will show a modest improvement, to $\mathcal{N} \ll d_K^{1/6.64}$. We also give the following simple example in the biquadratic case here. Given moduli q_1 and q_2, where for simplicity we assume that $q_1 \asymp q_2 \asymp q$ for some q, the least quadratic nonresidue for either q_1 or q_2 is $\ll q^{(1-\delta)/(4\sqrt{e})}$ for some $\delta > \frac{7}{100}$.

1.3. ***On residues.*** This discussion is related to another interesting problem — that of finding upper bounds on the residue κ of $\zeta_K(s)$ at $s = 1$. We remind the reader that the class number formula relates κ to various algebraic invariants of K. Specifically, let r_1 and $2r_2$ denote the number of real and complex embeddings of K, h the class number, R the regulator, and ω the number of roots of unity. Then

$$\kappa = \frac{2^{r_1}(2\pi)^{r_2} h R}{\omega\sqrt{d_K}}.$$

The best known explicit upper bound is due to Louboutin [2000], who showed that

$$\kappa \leq \left(\frac{e \log d_K}{2(l-1)}\right)^{l-1}. \tag{5}$$

We also refer to [Louboutin 2000; 2001] for applications and connections of this type of result to other questions as well as references to previous works from Siegel

as well as Lavrik and Egorov. We will show a result of the form

$$\kappa \le \Big(\frac{(1+o(1))e^{\gamma}\log d_K}{4l}\Big)^{l-1},$$

when $l/\log d_K = o(1)$ is small, and where $\gamma = 0.577\ldots$ is Euler's constant. See Theorem 2 for the exact result.

1.4. ***Statement of results.*** We consider these problems from two different vantage points. The first is via analysis of L-functions attached to the number field K, and the other stems from Vinogradov's work and work on multiplicative functions as in [Granville and Soundararajan 2001]. It is interesting that the latter method, which gives us the best known bounds in the quadratic case, is not optimal for number fields of large degree. Indeed, the first method will give us the best known upper bounds on the least prime that does not split for number fields of large degree and will also lead to such a result on the residue of the Dedekind zeta function. Specifically, we will show in Section 2:

Theorem 1. *Let K be a number field of degree l and discriminant d_K. Let $\mathcal{N}$ be the least prime that does not split completely in K. Then*

$$\mathcal{N} \ll_{\epsilon} d_K^{\frac{(1+\epsilon)}{4A(l-1)}}.$$

Here $A = \sup_{\lambda\ge 0}\dfrac{1-\frac{l}{l-1}e^{-\lambda}}{\lambda}$ satisfies $A \ge 1-\sqrt{\dfrac{2}{l-1}} = 1+O\Big(\dfrac{1}{\sqrt{l}}\Big) \to 1$ as $l\to\infty$.

The dependence on ϵ may be quantified explicitly by

$$\mathcal{N} \ll \Big(\frac{\log d_K}{l}\Big)^2 d_K^{\frac{1+o(1)}{4A(l-1)}}.$$

Here $o(1)$ denotes a quantity that tends to 0 as either l or d_K grows. It is illustrative here to consider two examples. First, if we consider some sequence of number fields such that $d_K \le C^l$ for some constant C, we see that the least prime that does not split must be bounded by a constant. This case does not appear in [Vaaler and Voloch 2000]. Secondly, in the opposite case where $(\log d_K)/l \to \infty$, we obtain $\mathcal{N} \ll d_K^{(1+o(1))/(4A)}$.

Remark 1. The value of A may be calculated for small l. The result above beats the bound $d_K^{1/(2(l-1))}$ when $l \ge 4$. We comment that the best result in the case $l = 2$ is still of the form (1). The best result available in the case $l = 3$ is also not of the form $d_K^{1/(2(l-1))}$ but is the one described below in Theorem 4.

Moreover, we have the following upper bound for the residue of the Dedekind zeta function.

Theorem 2. *Let κ be the residue at $s = 1$ of the Dedekind zeta function of K, and let $d = \log d_K^{1/l}$. Then*

$$\kappa \ll \left(\frac{\left(\frac{1}{4} + B\right) e^{\gamma + \sqrt{2/l}} \log d_K}{l} \right)^{l-1},$$

where $B = (2 \log\log d)/(\log d) + O(1/\log d)$.

In the case where d_K grows faster than an exponential[1] in l, we have $B = o(1)$. Note also that since d_K grows at least exponentially in l, B is usually small. However, the result above is not optimal for d_K very small. Rather, results like those of Hoffstein [1979] and Bessassi [2003] optimize that particular case.

Remark 2. The above results can be made explicit if desired, but we choose not to do so for ease of exposition. Improvements are possible in the coefficient in B above as well as quantifications of the ϵ appearing in Theorem 1.

Also, by applying a result of Stechkin [1970], it is possible to prove the above results more explicitly, but replacing $\frac{1}{4}$ with $(1 - 1/\sqrt{5})/2 = 0.276\ldots > \frac{1}{4}$. See Lemma 1 and environs for details.

The utility of Vinogradov's method in the context of number fields has not been well understood. We show in Section 3:

Theorem 3. *Let K be a number field of degree l and discriminant d_K. Let $f(n)$ be a real multiplicative function satisfying $0 \le f(p) \le l$ on the primes and such that*

$$\sum_n \frac{f(n)}{n^s} = \zeta(s) \sum_n \frac{g(n)}{n^s},$$

valid for $\Re(s) > 1$, for some multiplicative function $g(n)$ such that

$$\sum_{n \le x} g(n) = o(x)$$

for all $x > d_K^{1/2+o(1)}$. Then there exists some $p < d_K^{\frac{1+O(l^{-1/2+\epsilon})}{2(l-1)}}$ such that $f(p) \ne l$.

Moreover, this is essentially the best possible result for large l. To be specific, there exists a real multiplicative function satisfying all the properties above such that $f(p) = l$ for all

$$p < d_K^{\frac{1+O(l^{1/2+\epsilon})}{2(l-1)}}.$$

Thus, the technique behind Theorem 1 is aware of information that cannot be matched solely through the multiplicative functions approach, despite the fact that this approach gives the best known result for the quadratic case $l = 2$.

[1] By this, we mean that the statement $d_K \ll C^l$ is not true for any $C > 0$. An example would be the condition of Vaaler and Voloch immediately following (4).

However, the natural extension of Vinogradov's method and in particular, the structure in [Granville and Soundararajan 2001] has the advantage that it can utilize more information about the interaction between different multiplicative functions. This allows us to improve bounds on $\mathcal{N}$ in the case of cubic and biquadratic fields. Specifically, we will show in Section 4:

Theorem 4. *Let notation be as in Theorem 1. If K is a cubic field, then*

$$\mathcal{N} \ll d_K^{1/6.64}.$$

A similar idea will enable us to show in Section 4 that:

Theorem 5. *Let K be biquadratic with moduli q_1 and q_2. Then*

$$\mathcal{N} \ll (q_1 q_2)^{0.146/2}.$$

Furthermore, if $q_1 \asymp q_2$,

$$\mathcal{N} \ll (q_1 q_2)^{0.141/2}.$$

As we explain in Section 4, these results should be compared to the trivial bounds of $d_K^{1/(4\sqrt{e})+\epsilon}$ in the cubic case and $(q_1 q_2)^{1/(8\sqrt{e})}$ in the biquadratic case. Numerically, the results above are respectable, but have not been completely optimized. We would like to exhibit that an interesting interaction between multiplicative functions leads to better bounds, rather than to push for the best possible numerical result.

1.5. ***Notation.*** In the following, when we write $f = O(g)$, or equivalently $f \ll g$, for functions f and g, we shall mean that there exists a constant C such that $|f| \le C|g|$. In the case where g is a function of ϵ where as usual, ϵ denotes an arbitrary positive number, C is allowed to depend on ϵ. Unless otherwise stated, C is absolute, and in particular, C never depends on the number field K. We will also use $o(1)$ to denote a quantity which tends to 0 as either $d_k \to \infty$ or $l \to \infty$ except in §3, where we are not concerned with uniformity in l and $o(1)$ shall denote a quantity which tends to 0 as $d_K \to \infty$ and $l/\log d_K \to 0$.

2. Working with the Dedekind zeta function

As usual, write $s = \sigma + it$. In this section, we will usually denote by $\rho = \beta + i\gamma$ a zero of the Dedekind zeta function. Let

$$F(s) = \Re \sum_\rho \frac{1}{s-\rho} = \sum_\rho \frac{\sigma-\beta}{(\sigma-\beta)^2+(t-\gamma)^2},$$

defined for all $s \neq \rho$. As before, let $l = r_1 + 2r_2$ denote the degree of K over $\mathbb{Q}$ and r_1 and $2r_2$ be the number of real and complex embeddings of K respectively. Let

$$\xi_K(s) = s(s-1)\Big(\frac{d_K}{4^{r_2}\pi^l}\Big)^{s/2}\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta_K(s).$$

Then $\xi_K(s)$ is entire of order 1 and has a Hadamard product of the form

$$\xi_K(s) = e^{A+Bs} \prod_{\rho} \Big(1 - \frac{s}{\rho}\Big) e^{s/\rho}.$$

Logarithmically differentiating $\xi(s)$ gives that

$$F(s) = \Re\Big(\tfrac{1}{2} \log \frac{d_K}{2^{2r_2}\pi^l} + \frac{\zeta_K'}{\zeta_K}(s) + G(s) + \frac{1}{s} + \frac{1}{s-1}\Big), \tag{6}$$

where

$$G(s) = \Re\Big(\frac{r_1}{2}\frac{\Gamma'}{\Gamma}\Big(\frac{s}{2}\Big) + r_2 \frac{\Gamma'}{\Gamma}(s)\Big).$$

Here we have used that $\Re B = -\Re \sum_\rho \frac{1}{\rho}$. (See (11) in [Davenport 2000, p. 82] in the case of $\zeta(s)$. The proof for the general case is the same.) We have

$$-\frac{\zeta_K'}{\zeta_K}(s) = \sum_{n\geq 1} \frac{\Lambda_K(n)}{n^s},$$

where $\Lambda_K(n) = 0$ if n is not a power of a prime, and $0 \leq \Lambda_K(p^r) \leq l \log p$. Rewriting (6) for $s = \sigma > 1$ gives

$$\sum_{n\geq 1} \frac{\Lambda_K(n)}{n^\sigma} = \frac{1}{2} \log \frac{d_K}{2^{2r_2}\pi^l} + \frac{1}{\sigma - 1} - F(\sigma) + G(\sigma) + \frac{1}{\sigma}. \tag{7}$$

Then $F(\sigma) > 0$ and $\zeta_K'/\zeta_K(\sigma) < 0$ for $\sigma > 1$. This observation led Stark [1975] to his lower bounds on discriminants, and this will be our starting point. Indeed, if we use that $F(\sigma) > 0$ and that $G(\sigma) < 0$ for σ close to 1, we have that, for $1 < \sigma < \frac{5}{4}$,

$$\sum_{n\geq 1} \frac{\Lambda_K(n)}{n^\sigma} \leq \frac{1}{2} \log \frac{d_K}{2^{2r_2}\pi^n} + \frac{1}{\sigma - 1} + 1. \tag{8}$$

Note that $\Lambda_K(n)$ is maximized when n is a prime that splits completely in K, and the inequality above is a statement of the form that $\Lambda_K(n)$ cannot be too large for many n. With some work, this already leads to a bound of the form

$$\mathcal{N} \ll d_K^{\frac{1+O(1/\sqrt{l})}{2(l-1)}},$$

which is similar to the results of [Murty 1994] and [Vaaler and Voloch 2000]. Specifically:

Lemma 1. *Suppose that for some quantity $c > 0$, the bound*

$$\sum_{n\geq 1} \frac{\Lambda_K(n)}{n^\sigma} \leq c \log d_K + \frac{1}{\sigma - 1} \tag{9}$$

holds for all σ *in the range* $1+\dfrac{1}{\log d_K} \le \sigma \le 1+\dfrac{10\sqrt{l}}{\log d_K}$. *Also let*

$$a(\lambda) = \frac{1-\frac{l}{l-1}e^{-\lambda}}{\lambda},$$

and set $A = \sup_{\lambda \ge 0} a(\lambda)$. *Then*

$$\mathcal{N} \ll d_K^{\frac{c}{A(l-1)}(1+o(1))}.$$

Proof. If all primes split completely up to $x > 2$, then $\Lambda_K(n) = l\Lambda(n)$ for all $n \le x$, where $\Lambda(n)$ is the usual von Mangoldt function. Then, by the prime number theorem for $\mathbb{Q}$,

$$\sum_{n\le x} \frac{\Lambda_K(n)}{n^\sigma} = \sum_{n\le x} \frac{l\Lambda(n)}{n^\sigma} = l\left(\int_1^x \frac{1}{t^\sigma}dt + O(1)\right) = \frac{l}{\sigma-1} - \frac{lx^{1-\sigma}}{\sigma-1} + O(l).$$

Thus we have from (9) that

$$\frac{l-1}{\sigma-1} - \frac{lx^{1-\sigma}}{\sigma-1} \le c\log d_K + O(l)$$

Set $\sigma = 1+\dfrac{\lambda}{\log x}$. Then the expression above is the same as

$$\frac{(l-1)(\log x + O(1))}{\lambda}\left(1 - \frac{l}{l-1}e^{-\lambda}\right) \le c\log d_K + O(l).$$

We may assume that $O(1) = o(\log x)$, since otherwise the result is obvious. Rearranging we have

$$\log x \le \frac{c+o(1)}{a(\lambda)(l-1)}\log d_K + O(1).$$

We note that $a(\lambda)$ has a global maximum for $\lambda > 0$. If we let A be that maximum, the result follows immediately. □

A corresponding statement on upper bounds for κ also results from considerations of this type. This conforms to the intuition that in order to maximize κ, we should put as much weight as possible on the small primes in the sum in (8). In other words, the worst-case scenario is when all the small primes split. To this end, we prove the following lemma.

Lemma 2. *Assume that* (9) *holds as in Lemma 1 for some* $\sigma = 1+\dfrac{\alpha}{\log d_K}$, *and that there exists some* T *such that*

$$l\sum_{n\le T}\frac{\Lambda(n)}{n^\sigma} \ge c\log d_K + \frac{1}{\sigma-1}.$$

Then

$$\log\kappa \le c\alpha + l\sum_{n\le T}\frac{\Lambda(n)}{n^\sigma\log n} + \log(\sigma-1).$$

Proof. We first show that

$$\log \zeta_K(\sigma) \le l \sum_{n \le T} \frac{\Lambda(n)}{n^\sigma \log n}. \tag{10}$$

To this end, let

$$S(t) = \sum_{n \le t} \Lambda_K(n)/n^\sigma \quad \text{and} \quad \tilde{S}(t) = \min\left\{ \sum_{n \le t} \frac{l\Lambda(n)}{n^\sigma},\ c \log d_K + \frac{1}{\sigma - 1} \right\}.$$

Essentially, $\tilde{S}(t)$ is the version of $S(t)$ that grows at the fastest rate possible, and visibly $S(t) \le \tilde{S}(t)$. Note also that $\tilde{S}(t) = c \log d_K + 1/(\sigma - 1)$ is constant for $t \ge T$. Since

$$\log \zeta_K(\sigma) = \sum_{n \ge 1} \frac{\Lambda_K(n)}{n^\sigma \log n},$$

by partial summation,

$$\begin{aligned} \log \zeta_K(\sigma) &= \int_1^\infty \frac{S(t)}{t \log^2 t}\, dt \\ &\le \int_1^\infty \frac{\tilde{S}(t)}{t \log^2 t}\, dt = \int_1^T \frac{\tilde{S}(t)}{t \log^2 t}\, dt + \frac{\tilde{S}(T)}{\log T} = l \sum_{n \le T} \frac{\Lambda(n)}{n^\sigma \log n}, \end{aligned}$$

and this proves (10). By (9), we have by integration that

$$\log \kappa - \log(\sigma - 1)\zeta_K(\sigma) \le c(\sigma - 1) \log d_K = c\alpha,$$

as desired. □

Again, since (9) follows from (8) with $c = \frac{1}{2}$, with some work the lemma above gives us a bound roughly of the form

$$\kappa \ll \left(\frac{(1 + o(1))e^\gamma \log d_K}{2(l-1)} \right)^{l-1},$$

at least when d_K is large when compared to l. This is already an improvement over Louboutin's result when $l/\log d_K$ is small.

It is clear from both Lemma 1 and 2 that we gain information on both $\mathcal{N}$ and κ if we were able to extract nontrivial contribution from $F(\sigma)$ in (7). However, the discussion immediately following (7) neglected the contribution of the zeros entirely. We now proceed to rectify that situation. There are a number of possible approaches to this, and the best seems to be due to Heath-Brown [1992] in the case of the Dirichlet L-functions. There are some minor technicalities in our case, which we resolve with the help of the following lemma.

Lemma 3. *Let $\sigma_0 > 1 + 1/\log d_K$ and $\frac{1}{4} < R < \frac{1}{2}$. Let C_1 be the half-circle of radius R centered at σ_0 with real part to the right of σ_0. Let*

$$\mathcal{D} = \log \frac{\log d_K}{l}.$$

Then

$$\frac{1}{\pi R} \int_{C_1} |\log(s-1)\zeta_K(s)| ds \leq l\mathcal{D} + O(l).$$

Proof. Let $s = \sigma + it$, where $\sigma > 1 + \dfrac{1}{\log d_K}$. Then

$$|\log \zeta_K(s)| \leq |\log \zeta_K(\sigma)| \leq \log \zeta_K\Big(1 + \frac{1}{\log d_K}\Big).$$

These inequalities follow upon comparing Dirichlet series and since the coefficients of $\log \zeta_K(\sigma)$ are positive. We now claim that

$$\log \zeta_K\Big(1 + \frac{1}{\log d_K}\Big) \leq l\mathcal{D} + O(l).$$

Our calculations in Lemma 2 gives us this bound almost immediately. Specifically, we have from (8) and (10) in the proof of Lemma 2 that

$$\log \zeta_K(\sigma) \leq l \sum_{n \leq T} \frac{\Lambda(n)}{n^\sigma \log n},$$

provided that

$$l \sum_{n \leq T} \frac{\Lambda(n)}{n^\sigma} \geq \frac{\log d_K}{2} + \frac{1}{\sigma - 1} + 1.$$

Say that $\sigma = 1 + \dfrac{1}{\log d_K}$. Then

$$l \sum_{n \leq T} \frac{\Lambda(n)}{n^\sigma} \geq l e^{-\frac{\log T}{\log d_K}} \sum_{n \leq T} \frac{\Lambda(n)}{n} \geq l e^{-\frac{\log T}{\log d_K}} \log T + O(l).$$

Thus there is some constant[2] C such that

$$l \sum_{n \leq T} \frac{\Lambda(n)}{n^\sigma} \geq \frac{\log d_K}{2} + \frac{1}{\sigma - 1}$$

for $T = d_K^{C/l}$. Hence

$$\log \zeta_K(\sigma) \leq l \log\log T + O(l) = l \log \frac{C \log d_K}{l} + O(l) = l \log \frac{\log d_K}{l} + O(l).$$

Note that our bounds here hold uniformly in d_K and l. □

[2]Later on, we will have a specific value of C when we prove the Theorem 2, but for our present purposes, it suffices to note that this is possible for some absolute constant C.

Lemma 4. *Assume that*

$$1+\frac{1}{\log d_K} < \sigma_0 \le 1+\frac{10\sqrt{l}}{\log d_K} \quad \textit{and} \quad \mathcal{D} = \log\frac{\log d_K}{l}.$$

Then

$$-\frac{\zeta_K'}{\zeta_K}(\sigma_0) \le \left(\tfrac{1}{4}+o(1)\right)\log d_K + \frac{1}{\sigma_0-1} + 2l\mathcal{D} + O(l)$$

uniformly in σ_0.

Proof. Let $f(s) = (s-1)\zeta_K(s)$. Let C_R denote the circle of radius R with center σ_0 with no zeros of $f(s)$ on C_R. Then $f(s)$ is analytic and we apply Lemma 3.2 in [Heath-Brown 1992] to get that

$$-\Re\frac{f'}{f}(\sigma_0) = \sum_\rho{}' \left(\frac{1}{\sigma_0-\rho} - \frac{\sigma_0-\rho}{R^2}\right) - \frac{1}{\pi R}\int_0^{2\pi} \cos\theta \log\left|f(\sigma_0+Re^{i\theta})\right| d\theta$$

where $\sum'$ denotes a sum over all zeros of f within C_R. This is related to Jensen's formula and we refer the reader to [Heath-Brown 1992] for a proof.

We now need to bound the integral above, which we split into two ranges. The first is when $0 \le \theta \le \pi/2$ and $3\pi/2 \le \theta \le 2\pi$. The second is when $\pi/2 \le \theta \le 3\pi/2$. In the first range Lemma 3 tells us that

$$\frac{1}{\pi R}\int_{C_1} \log\left|f(\sigma_0+Re^{i\theta})\right| \le l\mathcal{D} + O(l).$$

In the second range, we use the convexity bound $\zeta_K(\sigma+it) \ll d_K^{(1-\sigma)/2} e^{l\mathcal{D}+Cl}$ for some $C > 0$. Since $\cos\theta \le 0$, we have

$$\begin{aligned}\cos\theta \log\left|f(\sigma_0+Re^{i\theta})\right| &\ge \cos\theta\frac{1-\sigma_0-R\cos\theta}{2}\log d_K(1+o(1)) + \cos\theta(l\mathcal{D}+Cl)\\ &\ge -\cos\theta\frac{R\cos\theta}{2}\log d_K(1+o(1)) + \cos\theta(l\mathcal{D}+Cl).\end{aligned}$$

Here we have used that $1-\sigma_0 = o(1)$. Now, we may assume that $2/\pi < R < 1$ so the contribution of the second term to the integral is at most $l\mathcal{D} + Cl$.

The contribution of the first term to the integral is at most

$$\frac{\log d_K + o(1)}{2\pi R}\left(\int_{\pi/2}^{3\pi/2} R\cos^2\theta d\theta + o(1)\right) = \left(\tfrac{1}{4}+o(1)\right)\log d_K.$$

Hence

$$\begin{aligned}-\frac{\zeta_K'}{\zeta_K}(\sigma_0) &\le \frac{1}{\sigma_0-1} - \Re\sum_\rho{}'\left(\frac{1}{\sigma_0-\rho} - \frac{\sigma_0-\rho}{R^2}\right) + \frac{1+o(1)}{4}\log d_K + 2l\mathcal{D} + O(l)\\ &\le \frac{1}{\sigma_0-1} + \frac{1+o(1)}{4}\log d_K + 2l\mathcal{D} + O(l),\end{aligned}$$

where we have used that

$$\Re\Big(\frac{1}{\sigma_0-\rho}-\frac{\sigma_0-\rho}{R^2}\Big)=(\sigma_0-\beta)\Big(\frac{1}{|\sigma_0-\rho|^2}-\frac{1}{R^2}\Big)\geq 0. \qquad \square$$

2.1. ***Proof of Theorem 1.*** Theorem 1 now follows immediately from Lemma 1 and Lemma 4 with $c=\frac{1}{4}+o(1)+(2l\mathcal{D}+O(l))/\log d_K$, where $\mathcal{D}=\log(\log d_K/l)$ as before. For $d=d_K^{1/l}$ we have

$$\frac{2l\mathcal{D}+O(l)}{\log d_K}=2\frac{\log\log d}{\log d}+O\Big(\frac{1}{\log d}\Big).$$

Also

$$d_K^{\frac{2\log\log d+O(1)}{(l-1)\log d}}\ll(\log d)^2.$$

We further need to verify that

$$A=\sup_{\lambda\geq 0}\frac{1-\frac{l}{l-1}e^{-\lambda}}{\lambda}\geq 1-\sqrt{\frac{2}{l-1}}.$$

We have

$$\frac{1-\frac{l}{l-1}e^{-\lambda}}{\lambda}=\frac{1-e^{-\lambda}}{\lambda}-\frac{e^{-\lambda}}{(l-1)\lambda}\geq 1-\frac{\lambda}{2}-\frac{1}{(l-1)\lambda}=1-\sqrt{\frac{2}{l-1}},$$

upon setting $\lambda=\sqrt{2/(l-1)}$.

2.2. ***Proof of Theorem 2.*** It remains to prove the upper bound on the residue κ in Theorem 2. As before, set $d=\log d_K^{1/l}$. We already have from Lemma 2 that with $\sigma=1+\alpha/\log d_K$ and for any T such that $l\sum_{n\leq T}\Lambda(n)/n^\sigma\geq c\log d_K+1/(\sigma-1)$ with $c=\frac{1}{4}+2\log\log d/\log d+O(1/\log d)+o(1)$, then

$$\begin{aligned}\log\kappa &\leq c\alpha+l\sum_{n\leq T}\frac{\Lambda(n)}{n^\sigma\log n}+\log(\sigma-1)\\ &\leq c\alpha+\log(\sigma-1)+l\Big(\log\log T+\gamma+\frac{2}{\log^2 T}\Big),\end{aligned}$$

where the latter line follows from taking logarithms in [Rosser and Schoenfeld 1962, (3.27)]. Set $\alpha=4\sqrt{l}$ and recall that $\sigma=1+\alpha/\log d_K$. We need to find the smallest admissible value of T. Let $S(x)=\sum_{n\leq x}\Lambda(n)/n=\log x-C+E(x)$ for some constant C. From [Rosser and Schoenfeld 1962], we know that $-1/\log x<E(x)<1/\log x$. We have

$$\begin{aligned}\sum_{n\leq T}\frac{\Lambda(n)}{n^\sigma}&=\int_{2^-}^{T}\frac{1}{x^{\sigma-1}}d(S(x))=\int_{2^-}^{T}\frac{1}{x^\sigma}dx+\frac{E(T)}{T^{\sigma-1}}\\ &=\frac{1}{\sigma-1}(2^{\sigma-1}-T^{\sigma-1})+\frac{E(T)}{T^{\sigma-1}}=\log T+\frac{E(T)}{T^{\sigma-1}}+O((\sigma-1)T^{\sigma-1})\end{aligned}$$

We see easily that $T \ll d_K^{1/l}$, so $(\sigma-1)T^{\sigma-1} = o(1)$. Thus

$$\log T = \frac{\log d_K}{l}\Big(c + \frac{1}{\alpha}\Big) + R(T),$$

where $|R(T)| < 1/\log T$. If $\log T \geq (\log d_K)/(4l)$, we may absorb $R(T)$ into the $O(l/\log d_K)$ term inside c and write

$$\log T = \frac{\log d_K}{l}\Big(c + \frac{1}{\alpha}\Big).$$

Otherwise, $\log T \leq \dfrac{\log d_K}{4l} \leq \dfrac{\log d_K}{l}\Big(c + \dfrac{1}{\alpha}\Big)$. Either way, we have

$$\kappa \leq \exp(\sqrt{l})\frac{4\sqrt{l}}{\log d_K}(e^\gamma \log T)^l \leq \frac{4e^\gamma c}{\sqrt{l}}\Big(ce^{\gamma+2/\sqrt{l}}\,\frac{\log d_K}{l}\Big)^{l-1},$$

where we have written $c + 1/\alpha \leq ce^{1/c\alpha}$. Let $B = \dfrac{2\log\log d}{\log d} + O\Big(\dfrac{l}{\log d}\Big)$. Then we have also

$$\kappa \ll \Big(\big(\tfrac{1}{4} + B\big)e^{\gamma+2/\sqrt{l}}\,\frac{\log d_K}{l}\Big)^{l-1}$$

Since d_K grows at least as fast as an exponential in l, B is always bounded. As mentioned before, we are most interested here in the case when d grows, so that $B = o(1)$.

3. On multiplicative functions

3.1. ***Preliminaries.*** Let $\zeta_K(s) = \sum_{n\geq 1} a(n)/n^s$ be the Dirichlet series for $\zeta_K(s)$. For this section, let $f(n)$ be the multiplicative function such that

$$\frac{\zeta_K(s)}{\zeta(s)} = \zeta_K(s)\prod_p\left(1 - \frac{1}{p^s}\right) = \sum_n \frac{f(n)}{n^s},$$

for $\Re s > 1$. At primes, $f(p) = a(p) - 1$. We first note that $f(n)$ exhibits cancellation at $d_K^{1/2+o(1)}$. This argument is a standard one wherein we examine the Dirichlet series

$$D(s) := \frac{\zeta_K(s)}{\zeta(s)} = \sum_{n\geq 1}\frac{f(n)}{n^s}.$$

Then the standard zero-free region for $\zeta(s)$ is sufficient to find cancellation using Perron's formula.

The question of bounding the least nonsplit prime can be converted to a more general question involving $f(n)$. To be precise, knowing that $f(n)$ exhibits cancellation at $d_K^{1/2+o(1)}$, what is the maximum y such that $f(p) = l - 1$ for all $p \leq y$?

We now collect some facts about multiplicative functions that will be useful for the remainder of this section. Since the applications will be towards proving Theorems 3, 4 and 5, we will not take the same care to prove uniformity in l as in

the previous results. The following material is essentially culled from [Granville and Soundararajan 2001]; the results there are proved for the case where $|f(n)| \le 1$, but the proofs extend to our case with very minor modifications. We summarize below the results and the required modifications to the proofs.

Let $f(n)$ be the multiplicative function defined above, with $-1 \le f(p) \le k := l-1$, where we recall that l is the degree of our number field K. Fix some $y \ge 2$ such that $f(p) = k$ for all $p \le y$. This implies that all y smooth numbers n satisfy $f(n) = d_k(n)$, where the latter is the number of ways of writing n as a product of k numbers. Then define

$$\sigma(u) = \frac{1}{y^u \log^{k-1} y} \sum_{n \le y^u} f(n)$$

and

$$P(u) = \frac{1}{y^u} \sum_{p \le y^u} f(p) \log p.$$

There are two related ways to express the relationship between $\sigma(u)$ and $P(u)$.

First say that $\tilde{\sigma}$ satisfies the convolution equation

$$u\tilde{\sigma}(u) = \tilde{\sigma} * P(u) = \int_0^u \tilde{\sigma}(u-t) P(t)\, dt, \tag{11}$$

for $u > 1$ subject to $\tilde{\sigma}(u) = u^{k-1}$ for $u \le 1$. Then for our case, we will have $\tilde{\sigma}(u) = \sigma(u) + o(1)$. The proof of this when $|f(n)| \le 1$ is contained in [Granville and Soundararajan 2001, Section 4], and the proof for our case is almost the same. There (proof of Proposition 4.1), one defines the multiplicative function $g(n)$ by $g(p^k) = f(p^k) - f(p^{k-1})$ for all prime powers. The nonnegative function $|g(n)|$ still satisfies the hypothesis of Theorem 2 in [Halberstam and Richert 1979], which gives

$$\sum_{n \le x} |g(n)| \le k \frac{x}{\log x} \sum_{n \le x} \frac{|g(n)|}{n} \left(1 + O\left(\frac{1}{\log x}\right)\right).$$

The only modification in the proofs thereafter is to replace error terms of the form $O(A)$ by $O(kA)$.

Next, we also have an inclusion-exclusion relationship. To be specific, let

$$I_j(u) = \int_{\substack{t_1+\cdots+t_j \le u \\ t_i \ge 1}} \left(\frac{u - \sum_{i=1}^j t_i}{u}\right)^{k-1} \prod_{i=1}^j \frac{k - P(t_i)}{t_i}\, dt_1 \cdots dt_j. \tag{12}$$

Then

$$\tilde{\sigma}(u) = u^{k-1} \sum_{j=0}^{\infty} \frac{(-1)^j}{j!} I_j(u), \tag{13}$$

where we set $I_0 = 1$. This sum is finite since $I_j(u) = 0$ for $u \le j$.

(We digress briefly to elucidate this inclusion-exclusion relationship. We have $\tilde{\sigma}(u) \le u^{k-1} + o(1)$, since $f(n) \le d_k(n)$. Now, if $p \ge y$, note that

$$\sum_{\substack{n \le y^u \\ p \mid n \\ p \ge y}} 1 = \Bigg(\sum_{\substack{n \le y^u \\ p \mid n,\ p^2 \nmid n \\ p \ge y}} 1 \Bigg)(1 + O(1/y)),$$

so

$$\begin{aligned}
\sum_{n \le y^u} f(n) &\ge y^u \log^{k-1}(y^u)(1+o(1)) - \sum_{y \le p \le y^u} \sum_{\substack{n \le y^u \\ p \mid n}} (d_k(n) - f(n)) \\
&\ge y^u \log^{k-1}(y^u)(1+o(1)) - \sum_{y \le p \le y^u} \sum_{m \le y^u/p} d_k(m)(k - f(p)) \\
&\ge y^u \log^{k-1}(y^u)(1+o(1)) - \sum_{y \le p \le y^u} (k - f(p)) \frac{y^u}{p} \left(\log \frac{y^u}{p} \right)^{k-1}.
\end{aligned}$$

An appropriate application of summation by parts brings this to

$$\sigma(u) \ge u^{k-1}(1 - I_1(1) + o(1)),$$

and one can derive (13) in this manner. However, we will relate this independently to the convolution equation (11).)

Now, for fixed $P(t)$, the solution $\tilde{\sigma}(u)$ to (11) is unique by the same proof as Theorem 3.3 in [Granville and Soundararajan 2001]. Thus to prove (13), it suffices to show that

$$u^{k-1} \sum_{j=0}^{\infty} \frac{(-1)^j}{j!} I_j(u)$$

satisfies the convolution (11). The calculation here is similar to [ibid., Lemma 3.2] and the main step is checking that

$$k * J_j(u) = u J_j(u) - j((k-P) * J_{j-1})(u), \tag{14}$$

where $J_j(u) = u^{k-1} I_j(u)$. This is because (14) immediately implies that

$$u \sum_{j=1}^{\infty} \frac{(-1)^j}{j!} J_j(u) + u^k = u^k + k * \sum_{j=1}^{\infty} \frac{(-1)^j}{j!} J_j(u) - \sum_{j=0}^{\infty} \frac{(-1)^j}{j!} ((k-P) * J_{j-1})(u)$$

which becomes (13) upon noting that $u^k = k * J_0$.

Some of the details in proving (14) differ slightly from those in [Granville and Soundararajan 2001], so we will provide the proof in the lemma below.

Lemma 5. *For $J_j(u)$ defined as above, $k * J_j(u) = u I_j(u) - j((k-P) * J_{j-1})(u)$.*

Proof. For notational convenience, set $S = \sum_{i=1}^{j} t_i$. Then

$$\begin{aligned}
k * J_j(u) &= \int_0^u k \int_{\substack{S\le t\\ t_i\ge 1}} (t-S)^{k-1} \prod_{i=1}^{j} \frac{k-P(t_i)}{t_i}\, dt_1\cdots dt_j\, dt \\
&= \int_{\substack{S\le u\\ t_i\ge 1}} \prod_{i=1}^{j} \frac{k-P(t_i)}{t_i} \int_S^u k(t-S)^{k-1}\, dt\, dt_1\cdots dt_j \\
&= \int_{\substack{S\le u\\ t_i\ge 1}} \prod_{i=1}^{j} \frac{k-P(t_i)}{t_i} (u-S)^{k-1}(u-S)\, dt_1\cdots dt_j \\
&= u J_j(u) - j \int_{\substack{t_1+\cdots+t_{j-1}\\ \le u-t_j\le u\\ t_i\ge 1}} t_j \prod_{i=1}^{j} \frac{k-P(t_i)}{t_i} \Big(u - t_j - \sum_{i=1}^{j-1} t_i\Big)^{k-1} dt_1\cdots dt_j \\
&= u J_j(u) - j(k-P) * J_{j-1}(u). \qquad \square
\end{aligned}$$

Henceforth, by an abuse of notation, we write $\sigma(u)$ for $\tilde{\sigma}(u)$ as well, and suppress the $o(1)$ error. Frequently, it will be useful to know that the minimal value of $P(t)$ gives the earliest cancellation in $\sigma(t)$. The following proposition tells us this. For an alternate proof, see also [Granville and Soundararajan 2001, Lemma 3.4].

Proposition 1. *Suppose that we have two multiplicative functions f and $f^\sharp$. Let*

$$P(u) = \frac{1}{y^u} \sum_{p\le y^u} f(p)\log p \quad \text{and} \quad P^\sharp(u) = \frac{1}{y^u} \sum_{p\le y^u} f^\sharp(p)\log p.$$

Define $\sigma(u)$ and $\sigma^\sharp(u)$ to be the solutions to (11) *for $P(u)$ and $P^\sharp(u)$ respectively. Further suppose that $P(u) = P^\sharp(u)$ for $u \le 1$, and that $P(u) \le P^\sharp(u)$ always. Let u_0 be the first zero of $\sigma(u)$. Then $0 \le \sigma(u) \le \sigma^\sharp(u)$ for $u \le u_0$.*

Proof. We use $I_j(u)$ and $I_j^\sharp(u)$ to denote the various integrals defined as in (12). Further let $1_{(a,a+\epsilon)}(t)$ be the indicator function of the small interval $(a, a+\epsilon)$. Without loss of generality, it suffices to prove the result in the case where $P^\sharp(t) = P(t) + \delta 1_{(a,a+\epsilon)}(t)$ for all $\delta > 0$, all $a > 1$ and ϵ arbitrarily small. This is because linear combinations of functions of the form $\delta 1_{(a,a+\epsilon)}(t)$ are L^2 dense. For notational convenience, set

$$S(t,u) = S(t) = \frac{k-P(t)}{t} \quad \text{and} \quad Q(t,u) = Q(t) = \frac{\delta 1_{(a,a+\epsilon)}(t)}{t}.$$

We may also assume that $u > 1+a$, since otherwise $\sigma(u) = \sigma^\sharp(u)$. Now fix some $1+a < u < u_0$, and say that $N \ge u$ is the smallest such integer. We have

$$\begin{aligned}
&\sigma^\sharp(u)-\sigma(u)\\
&\quad= u^{k-1}\sum_{j=0}^{N}\frac{(-1)^j}{j!}(I_j^\sharp(u)-I_j(u))\\
&\quad= \sum_{j=1}^{N}\Bigg(\frac{(-1)^j}{j!}\\
&\qquad\qquad\times\int_{\substack{t_1+\cdots+t_j\le u\\ t_i\ge 1}}\Big(u-\sum_{i=1}^{j}t_i\Big)^{k-1}\Big(\prod_{i=1}^{j}(S(t_i)-Q(t_i))-\prod_{i=1}^{j}S(t_i)\Big)\,dt_1\cdots dt_j\Bigg)\\
&\quad= \sum_{j=1}^{N}\frac{(-1)^{j-1}}{(j-1)!}\big(\mathcal{T}_j+O(\epsilon^2)\big),
\end{aligned}$$

where

$$\mathcal{T}_j=\int_{\substack{t_1+\cdots+t_j\le u\\ t_i\ge 1}}Q(t_1)\Big(u-\sum_{i=1}^{j}t_i\Big)^{k-1}\prod_{i=2}^{j}S(t_i)\,dt_1\cdots dt_j.$$

Here, we have used that integrals containing two factors of Q like

$$\int_{\substack{t_1+\cdots+t_j\le u\\ t_i\ge 1}}Q(t_1)Q(t_2)\prod_{i=3}^{j}S(t_i)\,dt_1\cdots dt_j$$

are $O(\epsilon^2)$. The terms containing one factor of Q are the same by symmetry. We now note that

$$\begin{aligned}
\mathcal{T}_j&=\int_a^{a+\epsilon}Q(t_1)\Big(u-\sum_{i=1}^{j}t_i\Big)^{k-1}\int_{\substack{t_1+\cdots+t_j\le u\\ t_i\ge 1}}\prod_{i=2}^{j}S(t_i)\,dt_1\cdots dt_j\\
&=\int_a^{a+\epsilon}Q(t_1)\,dt_1\left(\int_{\substack{t_2+\cdots+t_j\le u-a\\ t_i\ge 1}}\Big(u-a-\sum_{i=2}^{j}t_i\Big)^{k-1}\prod_{i=2}^{j}S(t_i)\,dt_2\cdots dt_j+O(\epsilon)\right)\\
&=\int_a^{a+\epsilon}Q(t_1)\,dt_1\left(u^{k-1}I_{j-1}(u-a)+O(\epsilon)\right).
\end{aligned}$$

Here the $O(\epsilon)$ arises from replacing instances of t_1 by a and using that $a\le t_1\le a+\epsilon$. Combining the above with the previous equation gives us

$$\sigma^\sharp(u)-\sigma(u)=\int_a^{a+\epsilon}Q(t_1)\,dt_1\Big(\frac{u^{k-1}}{(u-a)^{k-1}}\sigma(u-a)+O(\epsilon)\Big).$$

If we pick ϵ to be sufficiently small, the latter is positive since $\int_a^{a+\epsilon}Q(t_1)\,dt_1>0$ and $\sigma(u-a)>0$. □

Remark 3. Actually, wherever we use this result, we have $f^\sharp(p) \geq f(p)$. When this is true, there is an alternative argument, which we now sketch. Let $g(n)$ be the multiplicative function defined by $f^\sharp = f * g$, that is, $f^\sharp(n) = \sum_{d|n} f(d)g(n/d)$. Then since $f^\sharp(p) = f(p) + g(p)$, we must have $g(p) \geq 0$. Hence

$$\sum_{n\leq x} f^\sharp(n) = \sum_{n\leq x} \sum_{d|n} f(d)g(n/d) = \sum_{d\leq x} f(d) \sum_{n\leq x/d} g(n).$$

One may then argue that the contribution from values of g on the prime powers is benign and so the latter is an upper bound for $\sum_{n\leq x} f(n)$.

3.2. ***Generalization of Vinogradov's method.*** By Proposition 1, we only need consider the case where $P(u) = k$ for $u \leq 1$, and $P(u) = -1$ otherwise.

By the convolution (11), we get that $\sigma(u)$ satisfies the following differential difference equation:

$$u\sigma'(u) + (1-k)\sigma(u) + (k+1)\sigma(u-1) = 0. \tag{15}$$

Lemma 6. *Let u_0 be a zero of $\sigma(u)$. Then $u_0 \gg k/\log k$.*

Proof. Without loss of generality, we may suppose that u_0 is minimal. By a change of variables $\tau(u) = \sigma(u)u^{1-k}$, we derive from (15) that

$$\tau'(u) = -(k+1)\Big(1 - \frac{1}{u}\Big)^k \tau(u-1).$$

We see immediately that τ is positive and decreasing on $[0, u_0)$, so $-\tau'(u) \leq (k+1)(1-1/u)^k \ll (k+1)e^{-k/u}$. The result follows since by mean value theorem, $1 \ll (u_0 - 1)(k+1)e^{-k/u}$ for some $u \in [1, u_0)$. □

This allows us to say that cancellation occurs later than $k/\log k$ but we require finer analysis in order to obtain that it must occur very near k. For this, we use the saddle-point method.

3.3. ***The saddle-point method.*** Let $\hat{\sigma}(s) = \int_0^\infty \sigma(t)e^{-st}dt$ denote the Laplace transform of $\sigma(t)$. In Lemma 7, we will show that $\hat{\sigma}(s)$ can be analytically continued to all of $\mathbb{C}$. Thus, by Laplace inversion,

$$\sigma(u) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \hat{\sigma}(s)e^{us}\, dt \tag{16}$$

where $s = x + it$ for fixed x. The idea of the saddle-point method is that the integral for $\sigma(u)$ above is dominated by a small interval where the argument of the integrand changes slowly. First, we need to obtain a workable form for $\hat{\sigma}(s)$. Our approach will be similar to the analysis of the classic Dickman's function in [Tenenbaum 1995, Section 5.4].

Lemma 7. *We have*

$$\hat{\sigma}(s) = (k-1)!\, s e^{(k+1)(I(-s)+\gamma)} = \frac{(k-1)!}{s^k} e^{-(k+1)J(s)},$$

where γ is Euler's constant and

$$I(s) = \int_0^s \frac{e^t - 1}{t}\, dt, \quad J(s) = \int_0^\infty \frac{e^{-(s+t)}}{s+t}\, dt.$$

Note that $J(s)$ only has holomorphic extension to $\mathbb{C} \setminus (-\infty, 0]$; the purpose of writing $\hat{\sigma}(s)$ in terms of $I(-s)$ is to analytically continue the transform to all of $\mathbb{C}$.

Proof. A change of variables $t = v/s$ in the definition of the Laplace transform gives us that

$$s\hat{\sigma}(s) = \int_0^\infty e^{-v} \sigma(v/s)\, dv.$$

Differentiating both sides with respect to s gives

$$\begin{aligned}
\frac{d}{ds} s\hat{\sigma}(s) &= \frac{1}{s} \int_0^\infty e^{-v} (-(v/s)\sigma'(v/s))\, dv \\
&= \frac{1}{s} \int_0^\infty e^{-v} \left((k+1)\sigma\left(\frac{v}{s} - 1\right) - (k-1)\sigma(v/s) \right) dv \\
&= (k+1)e^{-s}\hat{\sigma}(s) - (k-1)\hat{\sigma}(s),
\end{aligned}$$

upon changing variables again. Solving this differential equation for $s\hat{\sigma}(s)$ gives

$$s\hat{\sigma}(s) = C \frac{e^{-(k+1)J(s)}}{s^{k-1}},$$

for some constant C. We have $\lim_{s\to\infty} J(s) = 0$, so

$$\lim_{s\to\infty} s^k \hat{\sigma}(s) = C.$$

On the other hand,

$$\lim_{s\to\infty} s^k \hat{\sigma}(s) = \lim_{s\to\infty} s^{k-1} \int_0^\infty e^{-v} \left(\frac{v}{s}\right)^{k-1} dv = \int_0^\infty e^{-v} v^{k-1} dv = (k-1)!\,,$$

from which it follows that $C = (k-1)!$. Note that the first line follows from the fact that $\sigma(t) = t^{k-1}$ for $t \le 1$, and that e^{-v} decreases rapidly.

By [Tenenbaum 1995, Lemma 7.1 of Section 5.4], we have

$$-J(s) = I(-s) + \gamma + \log s$$

for $s \in \mathbb{C} \setminus (-\infty, 0]$, and this concludes the proof. □

In order to apply the saddle-point method, we first collect some information on the extrema of the integrand in (16). In the sequel, we let $W(x)$ denote the Lambert W function, defined by $x = W(x)e^{W(x)}$. We remind the reader that there exist two real branches of $W(x)$ when $x \geq -1/e$, which we denote by W_0 and W_{-1}, where they are distinguished by $W_0(0) = 0$ and $W_{-1}(0) = -\infty$.

Lemma 8. *Let $\Phi(s) = \hat{\sigma}(s)e^{us}$ and let $\xi(u) = -W((-(k+1)e^{-k/u})/u) - k/u$, where W is a branch of the Lambert W function. Then $\Phi'(\xi) = 0$. If $|u-k| \geq 2\sqrt{k}$, then we may pick $\xi(u)$ to be real. In particular, we pick*

$$\xi(u) = \begin{cases} -W_0\Big(\dfrac{-(k+1)e^{-k/u}}{u}\Big) - k/u & \text{for } u \leq k - 2\sqrt{k}, \\ -W_{-1}\Big(\dfrac{-(k+1)e^{-k/u}}{u}\Big) - k/u & \text{for } u > k + 2\sqrt{k}. \end{cases} \tag{17}$$

For this choice of $\xi(u)$, if $|u-k| \gg k^{1/2+\epsilon}$, then $\xi(u) \gg k^{-1/2+\epsilon}$. Moreover, $\xi(u) < 0$ for $u < k - 2\sqrt{k}$ and $\xi(u) > 0$ for $u > k - 2\sqrt{k}$.

Proof. We have that

$$\frac{d}{ds}(se^{(k+1)I(-s)}e^{us}) = e^{(k+1)I(-s)}e^{us}(1 + s(u - (k+1)I'(-s))),$$

and this is 0 when $s = -\xi(u)$ where $\xi(u)$ satisfies

$$(k+1)e^{\xi(u)} = k + u\xi(u).$$

In other words,

$$\xi(u) = -W\Big(\frac{-(k+1)e^{-k/u}}{u}\Big) - k/u, \tag{18}$$

Note that

$$\frac{-(k+1)e^{-k/u}}{u} \geq -1/e \iff (k+1) \leq ue^{(k-u)/u}.$$

We first verify that the latter holds for all $|u-k| \geq 2\sqrt{k}$. Indeed, a little calculus tells us that the function $ue^{(k-u)/u}$ has a global minimum on $[0, \infty)$ at $u = k$. Since it is decreasing on $[0, k)$ and increasing on $[k, \infty)$, it suffices to check the assertion for $|u-k| = 2\sqrt{k}$. But for $|u-k| = 2\sqrt{k}$, we have

$$\begin{aligned} ue^{(k-u)/u} &= k + \frac{(k-u)^2}{2u} + \frac{(k-u)^3}{3!\,u^2} + \cdots \\ &\geq k + \Big(\frac{1}{2} - \frac{1}{3!}\Big)\frac{(k-u)^2}{u} \geq k + \frac{4}{3} > k+1. \end{aligned}$$

Now let $u = k + E$, where $|E| > 2\sqrt{k}$. We examine two cases. First, when $E < 0$, we know that $-W_0(x) \leq 1$ for all $x \leq 0$ so

$$\xi(u) \leq 1 - \frac{k}{k+E} = \frac{E}{k+E} < 0.$$

Next, when $E > 0$, we know that $-W_{-1}(x) \geq 1$ for all $x \leq 0$ so

$$\xi(u) \geq 1 - \frac{k}{k+E} = \frac{E}{k+E} > 0.$$

Note that $|E/(k+E)| \gg 1/k^{1/2-\epsilon}$ if $|E| \gg k^{1/2+\epsilon}$, and that $\xi(u)$ shares the same sign with E. □

Remark 4. To motivate the definition of $\xi(u)$ in this lemma, note that k/u is close to satisfying the equation defining $W(-(k+1)e^{-k/u}/u)$, so k/u must sometimes be close to one of the branches. The idea here is to take the other branch. The sign change for $\xi(u)$ occurs near $u = k$, and this is also when the branches converge to the same value at $-1/e$.

We now need to estimate $\sigma(u)$ by Laplace inversion of $\hat{\sigma}(s)$ on the $\Re s = \Re\xi$ line. For this purpose, we collect the following estimates.

Lemma 9. *Let ξ be as in Lemma 8. Write $s = -\xi + i\tau$, with τ real, and assume $1 < u \leq 10k$ with $|k-u| \gg k^{1/2+\epsilon}$. Then for $|\tau| \geq k + u|\xi|$,*

$$\hat{\sigma}(s) = \frac{(k-1)!}{s^{k-1}}\Big(1 + O\Big(\frac{u\xi+k}{|s|}\Big)\Big). \tag{19}$$

Moreover, there exists $c > 0$ such that for $|\tau| \leq \pi$,

$$\hat{\sigma}(s) \ll (k-1)!\, s e^{(k+1)(\gamma+I(\xi))} e^{-c\frac{k+1}{|\xi|+1}\tau^2}, \tag{20}$$

and for $|\tau| > \pi$,

$$\hat{\sigma}(s) \ll (k-1)!\, s e^{(k+1)(\gamma+I(\xi))} e^{-c\frac{k+1}{|\xi|+1}}. \tag{21}$$

Proof. The first bound follows from $\hat{\sigma}(s) = ((k-1)!/s^{k-1})e^{-(k+1)J(s)}$, and the bound $J(s) \ll |e^{\xi}/s| = |(u\xi+k)/((k+1)s)|$. For the other two cases, set $H(\tau) = I(\xi) - I(-s) = \int_0^1 (e^{h\xi}/h)(1 - e^{-i\tau h})\, dh$. We extract the real part to get that

$$\Re H(\tau) = \int_0^1 \frac{e^{h\xi}}{h}(1 - \cos\tau h)\, dh$$

For (20), note that $1 - \cos h\tau \geq 2\tau^2 h^2/\pi^2$ for $|\tau| \leq \pi$. By the calculation in [Tenenbaum 1995, Lemma 8.2],

$$\Re H(\tau) \geq \frac{\tau^2}{2\pi^2}\left|\int_0^1 e^{h\xi} dh\right| \gg \frac{\tau^2}{|\xi|+1}.$$

From this and Lemma 7, we have (20).

To prove the third bound, (21), observe that

$$\Re H(\tau) = \int_0^1 \frac{e^{h\xi}}{h}(1 - \cos\tau h)\, dh \gg \frac{1}{|\xi|+1}.$$

The last inequality follows from considering an open set $E \subset [0,1]$ of small measure outside of which $(1-\cos\tau h) \gg 1$. One may make E small enough so that $\int_E e^{h\xi}\,dh$ is bounded by $\int_{[0,1]\setminus E} e^{h\xi}\,dh$. This is possible since $\xi \le C$ for some absolute constant C for u in the specified range. This is true in the case $u < k$ because $-W_0(x) \le 1$ for $x \le 0$ and it is true for $u > k$ since the argument inside W_{-1} is bounded away from 0 when $u \le 10k$. □

We now apply the bounds above to obtain an estimate for $\sigma(t)$. Set

$$\delta = \sqrt{\frac{\log^3(k+1)}{c(k+1)}}$$

where c is the constant appearing in Lemma 9. Let $K(u) = 1/(2\pi)\int_{-\delta}^{\delta} \hat{\sigma}(s)e^{us}d\tau$, and $H(u) = 1/(2\pi)\int_{\mathbb{R}\setminus[-\delta,\delta]} \hat{\sigma}(s)e^{us}d\tau$. As above, we have written $s = -\xi + i\tau$. We know that $\sigma(u) = K(u) + H(u)$, and we first find an upper bound for $H(u)$.

Lemma 10. *Assume $k \ge 3$ and $u \gg k/\log k$ with $|k-u| \gg k^{1/2+\epsilon}$. Then*

$$H(u) \ll (k-1)!\, e^{(k-1)(\gamma+I(\xi))} \frac{1}{(k+1)^{\log^2 k}}.$$

Proof. First note by (18) that $\xi \ll \log k$ when $u \gg k/\log k$. Now, we split the integral in the definition of $H(u)$ into 3 ranges. First, when $\delta < |\tau| \le \pi$, we have by (20) that the integral is

$$\begin{aligned}
&\ll (k-1)!\, e^{(k-1)(\gamma+I(\xi))} \int_{\delta}^{\infty} e^{-c(k+1)\tau^2/\log k} d\tau \\
&\ll (k-1)!\, e^{(k-1)(\gamma+I(\xi))} \frac{1}{(\sqrt{k+1})^{1-\epsilon}} \int_{\log^{3/2}(k+1)}^{\infty} e^{-\tau^2} d\tau \\
&\ll (k-1)!\, e^{(k-1)(\gamma+I(\xi))} \frac{1}{(k+1)^{\log^2 k}}.
\end{aligned}$$

Next, when $\pi < |\tau| \le k + u|\xi|$, we get by (21) that the integral is

$$\ll (k-1)!\, e^{(k-1)(\gamma+I(\xi))} e^{-k^{1-\epsilon}},$$

where we have used that $u \ll k$. Lastly, for $|\tau| \ge k + u|\xi|$, we get by (19) that the integral is

$$\ll (k-1)!\, \frac{1}{k^{k-1}},$$

which is tiny. □

Now we are ready to evaluate $K(u)$.

Lemma 11. *Suppose that $k \ge 3$ and $k/\log k \ll u \le 10k$ with $|k-u| \gg k^{1/2+\epsilon}$. Then*

$$K(u) = \frac{-(k-1)!\,\xi e^{(k+1)(\gamma+I(\xi))-u\xi}}{\sqrt{2\pi(k+1)I''(\xi)}}\Big(1 + O\Big(\frac{1}{(k+1)^{\epsilon}}\Big)\Big).$$

Proof. We first examine the Taylor expansion of $I(-s)$ about ξ. First note that

$$I'(\xi) = \frac{e^{\xi}-1}{\xi} = \frac{u}{k+1} - \frac{1}{(k+1)\xi},$$

as before. Thus

$$I(-s) = I(\xi) - \frac{i\tau u}{k+1} + \frac{i\tau}{(k+1)\xi} - \frac{\tau^2 I''(\xi)}{2} + O(\tau^3).$$

Since $1/(k^{1/2-\epsilon}) \ll \xi \ll \log k$ for $k/\log k \ll u \le 10k$, we have for $|\tau| \le \delta$ that

$$e^{(k+1)I(-s)+us} = e^{(k+1)I(\xi)-u\xi-(k+1)\frac{\tau^2 I''(\xi)}{2}}\Big(1 + O\Big(\frac{1}{k^{\epsilon}}\Big)\Big),$$

and so

$$\begin{aligned} K(u) &= (k-1)!\, e^{(k+1)(\gamma+I(\xi))-u\xi}\int_{-\delta}^{\delta} e^{-(k+1)(\tau^2 I''(\xi))/2}(-\xi+i\tau)\,d\tau\,\Big(1+O\Big(\frac{1}{k^{\epsilon}}\Big)\Big) \\ &= -(k-1)!\,\xi e^{(k+1)(\gamma+I(\xi))-u\xi}\int_{-\delta}^{\delta} e^{-(k+1)(\tau^2 I''(\xi))/2}\,d\tau\,\Big(1+O\Big(\frac{1}{k^{\epsilon}}\Big)\Big), \end{aligned}$$

by symmetry. Note that

$$I''(\xi) = \frac{\xi e^{\xi} - e^{\xi} + 1}{\xi^2}.$$

Then for u in the range specified, $1/\log^2 k \ll I''(\xi) \ll 1$. We also have

$$\begin{aligned} \int_{-\delta}^{\delta} e^{-(k+1)\tau^2 I''(\xi)/2}d\tau &= \int_{-\infty}^{\infty} e^{-(k+1)\tau^2 I''(\xi)/2}d\tau + O\Big(\frac{1}{\sqrt{I''(\xi)}(k+1)^{3/2}}\Big) \\ &= \sqrt{\frac{2\pi}{(k+1)I''(\xi)}}\Big(1+O\Big(\frac{1}{(k+1)^{1/2}}\Big)\Big), \end{aligned}$$

as desired. □

Proposition 2. *Say that $k \ge 3$ and $k/\log k \ll u \le 10k$ with $|u-k| \gg k^{1/2+\epsilon}$. Then*

$$\sigma(u) = \frac{-(k-1)!\,\xi e^{(k+1)(\gamma+I(\xi))-u\xi}}{\sqrt{2\pi(k+1)I''(\xi)}}\Big(1+O\Big(\frac{1}{(k+1)^{\epsilon}}\Big)\Big)$$

Moreover, by Lemma 8, the first zero of $\sigma(u)$ must be $k + O(k^{1/2+\epsilon})$.

Proof. The expression for $\sigma(u) = K(u) + H(u)$ follows directly from Lemmas 10 and 11. Note that $I''(\xi) \gg 1/\log^2 k$ for u in the range specified. The last assertion follows from noting that $\sigma(u)$ changes sign when ξ changes sign, and the fact that by Lemma 6, the first zero of $\sigma(u)$ must be $\gg k/\log k$. □

Finally, we note that Theorem 3 follows immediately from the Proposition 2.

4. Cubic and biquadratic fields

We now investigate the question of bounding the least nonsplit prime when K is either cubic or biquadratic. The general philosophy is the same for the two cases, although the technical details are different. There is always a "trivial" bound which arises from considering cancellation in a quadratic character, and our purpose is to show that this bound can be improved. In both cases, we benefit from interaction between a primary multiplicative function of interest and quadratic characters. Simply put, if all the primes split up to the trivial bound, then the quadratic character is extremal and we may predict its behavior far beyond the cancellation point. In this case, the interaction with the primary multiplicative function produces a contradiction. In order to obtain an actual bound, we need to understand what it means for a quadratic character to be close to extremal.

4.1. ***Extremal behavior.*** Let χ denote a quadratic character with modulus q such that $\chi(p) = 1$ for all $p \le y$ whenever $p \nmid q$. We set

$$P(u) = \frac{1}{v(y^u)} \sum_{p \le y^u} \chi(p) \log p,$$

where $v(x) = \sum_{p \le x} \log p$. Also, let $\sigma(u) = \frac{1}{y^u} \sum_{n \le y^u} \chi(n)$. We further define

$$I_j(u) = \int_{\substack{t_1+\cdots+t_j \le u \\ t_i \ge 1 \, \forall 1 \le i \le j}} \prod_{i=1}^{j} \frac{1 - P(t_i)}{t_i} \, dt_1 \cdots dt_j.$$

We remind the reader that

$$\sigma(u) = \sum_{j \ge 0} \frac{(-1)^j I_j(u)}{j!},$$

where $I_0 \equiv 1$. Note that the sum on the right is finite. Moreover, we have

$$\sum_{j=0}^{2m-1} \frac{(-1)^j I_j(u)}{j!} \le \sigma(u) \le \sum_{j=0}^{2m} \frac{(-1)^j I_j(u)}{j!}$$

for any $m \ge 0$. Once again, we refer the reader to [Granville and Soundararajan 2001] for more details.

Let $A > 0$ be such that $y^A = q^{1/4}$, so that $\sigma(u) = o(1)$ for $u > A$. The reader should think of A as being somewhat larger than $\sqrt{e}$. The simple case when $A = \sqrt{e}$ is the extremal case appearing in the bound (1) and the behavior of $P(t)$ here has been studied by other authors. In their study of Beurling primes, Diamond, Montgomery, and Vorhauer reproduce the unpublished analysis of Heath-Brown on this subject in the appendix of [Diamond et al. 2006]. This is also examined in

[Granville and Soundararajan ≥ 2012]. The lemma below quantifies the behavior of $P(t)$ by comparing χ to an extremal character.

Lemma 12. *Suppose that* $\sqrt{e} \le A \le 2$, *and set*[3] $E = 2\log A - 1$.

1. *Say that we have some interval* $(a, b) \subset (1, A)$. *Then*

$$\int_a^b \frac{1-P(t)}{t}\,dt \ge 2\log\frac{b}{a} - E + o(1).$$

2. *For all* $t \in [2, 3]$ *but for a set of measure* 0, *we have*

$$\frac{1-P(t)}{t} = \frac{1}{2}\int_1^{t-1} \frac{1-P(u)}{u}\frac{1-P(t-u)}{t-u}du.$$

Moreover, *for all* $t \in [2, 4]$ *but for a set of measure* 0, *we have*

$$\frac{1-P(t)}{t} \le \frac{1}{2}\int_1^{t-1} \frac{1-P(u)}{u}\frac{1-P(t-u)}{t-u}du.$$

3. *For all* $t \in [2, 1 + A]$ *but for a set of measure* 0, *we have*

$$\frac{4}{t}\log(t-1) - 2E \le \frac{1-P(t)}{t} \le \frac{4}{t}\log(t-1)$$

4. *For all* $t \in [1 + A, 3]$ *but for a set of measure* 0, *we have*

$$\frac{1-P(t)}{t} \ge \frac{4}{t}\log\frac{A}{t-A} - 2E + o(1),$$

and for $t \in [3, 4]$, *we have*

$$\frac{1-P(t)}{t} \ge \frac{4}{t}\log\frac{A}{t-A} - 2E - \frac{2}{3}(t-3)^2 + o(1).$$

Moreover, *for all* $t \in [1 + A, 2A]$ *but for a set of measure* 0, *we have*

$$\frac{1-P(t)}{t} \le \frac{4}{t}\log\frac{A}{t-A} + o(1).$$

Proof. Note that $\sigma(u) = o(1)$ for $u > A$. Thus

$$\int_1^A \frac{1-P(t)}{t}\,dt = 1 + o(1)$$

and the first assertion follows since $1 - P(t) \le 2$.

The second assertion follows from the fact that $P(t)$ is continuous almost everywhere, and when $P(t)$ is continuous,

$$\frac{1-P(t)}{t} = \lim_{\epsilon\to 0}\frac{1}{\epsilon}(I_1(t+\epsilon) - I_1(t)).$$

[3] E measures the deviation of A from $\sqrt{e}$. In particular, $E = 0$ when $A = \sqrt{e}$.

For $t \in [2, 3]$,

$$I_1(t+\epsilon) - I_1(t) = \tfrac{1}{2}(I_2(t+\epsilon) - I_2(t)),$$

and for $t \in [2, 4]$,

$$\begin{aligned} I_1(t+\epsilon) - I_1(t) &= \tfrac{1}{2}(I_2(t+\epsilon) - I_2(t)) - \tfrac{1}{6}(I_3(t+\epsilon) - I_3(t)) \\ &\le \tfrac{1}{2}(I_2(t+\epsilon) - I_2(t)). \end{aligned}$$

Thus, it remains to evaluate

$$\begin{aligned} \lim_{\epsilon\to 0} \frac{1}{2\epsilon}(I_2(t+\epsilon) - I_2(t)) &= \lim_{\epsilon\to 0} \frac{1}{2\epsilon} \int_{\substack{t\le t_1+t_2\le t+\epsilon \\ t_1,t_2\ge 1}} \frac{1-P(t_1)}{t_1}\frac{1-P(t_2)}{t_2}\,dt_1\,dt_2 \\ &= \frac{1}{2}\int_1^{t-1} \frac{1-P(t_1)}{t_1}\frac{1-P(t-t_1)}{t-t_1}\,dt_1, \end{aligned}$$

almost everywhere, as desired.

To prove the upper bound in the third assertion, note that

$$\frac{1}{2}\int_1^{t-1} \frac{1-P(u)}{u}\frac{1-P(t-u)}{t-u}du \le 2\int_1^{t-1} \frac{1}{u}\frac{1}{t-u}du = \frac{4}{t}\log(t-1).$$

To prove the lower bound in the third assertion, we let $f(t) = (1 - P(t))/t$ and $m(t) = 2/t \ge f(t)$ for all t. Then for $t \in [2, 1 + A]$ we have

$$\begin{aligned} &\int_1^{t-1} f(u)f(t-u)\,du \\ &\quad= \int_1^{t-1} (f(u) - m(u))f(t-u)\,du + \int_1^{t-1} m(u)(f(t-u) - m(t-u))\,du \\ &\qquad\qquad + \int_1^{t-1} m(u)m(t-u)\,du \\ &\quad\ge \frac{8}{t}\log(t-1) - 4E. \end{aligned}$$

Here we have bounded both the first two terms from below by $-2E$ using the first assertion and that $f(u) \le m(u) \le 2$ for all $u \in [1, A]$.

The proof of the fourth assertion is similar. The only difference in the proof of the first and last bounds arises from the fact that $\int_A^2 (1 - P(u))/u\,du = o(1)$. Thus for $1 + A \le t = 1 + A + \delta \le 2A$,

$$\int_1^{t-1} \frac{1-P(u)}{u}\frac{1-P(t-u)}{t-u}du = \int_{1+\delta}^{t-1-\delta} \frac{1-P(u)}{u}\frac{1-P(t-u)}{t-u}du + o(1).$$

For the second bound in the fourth assertion, one also needs to use that

$$\begin{aligned} \frac{1-P(t)}{t} &= \lim_{\epsilon\to 0} \frac{1}{\epsilon}\left(\tfrac{1}{2}(I_2(t+\epsilon) - I_2(t)) - \tfrac{1}{6}(I_3(t+\epsilon) - I_3(t))\right) \\ &\ge \tfrac{1}{2}\lim_{\epsilon\to 0} \frac{1}{\epsilon}(I_2(t+\epsilon) - I_2(t)) - \tfrac{2}{3}(t-3)^3. \end{aligned}$$

This follows from the calculation that

$$\lim_{\epsilon\to 0}\frac{1}{\epsilon}(I_3(t+\epsilon)-I_3(t)) = \int_{\substack{t_1+t_2\le t-1\\ t_1,t_2\ge 1}} \frac{1-P(t_1)}{t_1}\frac{1-P(t_2)}{t_2}\frac{1-P(t-t_1-t_2)}{t-t_1-t_2}\,dt_1\,dt_2$$
$$\le 8\int_{\substack{t_1+t_2\le t-1\\ t_1,t_2\ge 1}} \frac{1}{t_1}\frac{1}{t_2}\frac{1}{t-t_1-t_2}\,dt_1\,dt_2 \le 8\frac{(t-3)^2}{2},$$

upon calculating the volume of the region of integration. □

4.2. ***Cubic fields.*** Let K be a cubic field. In this case, it is easy to see that a much better result than $\mathcal{N} \ll d_K^{1/(2(l-1))}$ is possible. In the case where K is Galois, then K must necessarily be abelian, and so $\zeta_K(s) = \zeta(s)L(s,\chi_1)L(s,\chi_2)$ for some Dirichlet characters χ_1 and χ_2 with conductors q_1 and q_2 respectively. Say that $q_1 \le q_2$. Then since χ_1 has order 3, by [Heath-Brown 1992, Lemma 2.4], $\chi_1(n)$ exhibits cancellation by $q^{1/4+\epsilon}$. Thus $\mathcal{N} \ll_\epsilon q_1^{1/4+\epsilon} \ll d_K^{1/8+\epsilon}$. Clearly, a stronger statement should be possible in the abelian case, but we shall be more interested in the general case here.

For the rest of this section, say that K is not Galois. Then

$$\zeta_K(s) = \zeta(s)L(f,s),$$

where f is a holomorphic modular Hecke eigenform of weight k and level N. Also, the L-function associated to f is of the form

$$L(f,s) = \prod_p \Big(1-\frac{\alpha_p}{p^s}\Big)^{-1}\Big(1-\frac{\beta_p}{p^s}\Big)^{-1} = \prod_p \Big(1-\frac{a(p)}{p^s}+\frac{\chi(p)}{p^{2s}}\Big)^{-1},$$

where χ is a quadratic character with modulus $q \le d_K$. Visibly from the Euler product above, p cannot split in K if $\chi(p) = -1$. Thus,

$$\mathcal{N} \ll d_K^{1/4\sqrt{e}} + o(1). \tag{22}$$

This is the starting point for our investigation.

Let $f(n)$ be the completely multiplicative function with $f(p) = a(p)$ for all primes p. Then $f(n)$ exhibits cancellation by $d_K^{1/2+o(1)}$. We now try to improve the bound of $\mathcal{N} \ll d_K^{1/4\sqrt{e}}$ by leveraging information about the two multiplicative functions $f(n)$ and $\chi(n)$.

Remark 5. Our main focus here is to show that improvements over the bound (22) are possible. For simplicity, we will not attempt to completely optimize our calculations. In particular, we do not use the available subconvexity result for $\zeta_K(s)$ which shows that $f(n)$ exhibits cancellation by $d_K^{1/2-\delta}$ for some $\delta > 0$ (see Appendix A of [Einsiedler et al. 2011] for a synopsis of known results).

As in Section 4.1, let $P(t)$ denote the average over primes of $f(p)$ and let $P'(t)$ denote the same average for $\chi(p)$. Let[4] $\sigma(t) = 1/(y^t \log y^t) \sum_{n \le y^t} f(n)$. Also as in Section 4.1, assume that there exists some $y = d_K^A$ such that all primes $p \le y$ split completely, where we may assume that $A > \frac{1}{8}$.

We begin by quantifying the relationship between $f(p)$ and $\chi(p)$.

Lemma 13. *With f and χ as above, we have $f(p) \ge -(\chi(p)+1)/2$ for all unramified primes p. It follows that $P(t) \ge -(P'(t)+1)/2 + o(1)$, where the $o(1)$ is a quantity tending to 0 as $d_K \to \infty$ uniformly for $t \ge 1$.*

Proof. This follows from the fact that $f(p) = \alpha_p + \beta_p$ and $\chi(p) = \alpha_p \beta_p$. First assume that p is unramified. There are three possibilities to check, corresponding to the three possibilities for the local factor at p in $\zeta_K(s)$, which is always of the form $\prod_{\mathfrak{p}|p}\left(1 - 1/N(\mathfrak{p})^s\right)^{-1}$. When p splits completely, the local factor is $\left(1-1/p^s\right)^{-3}$, so $\alpha_p = \beta_p = 1$ whence $f(p) = 2$ and $\chi(p) = 1$. When p is inert, the local factor is of the form $\left(1-1/p^{3s}\right)^{-1}$, so $\alpha_p = 1/\beta_p = e^{\pm 2\pi i/3}$ and $f(p) = -1$ and $\chi(p) = 1$. In the remaining case, p factors as $p = \mathfrak{p}_1\mathfrak{p}_2$, where the norms of the ideals on the right are p and p^2; thus the local factor is of the form

$$\left(1 - \frac{1}{p^s}\right)\left(1 - \frac{1}{p^{2s}}\right).$$

In this case, then, $\alpha_p = -\beta_p = \pm 1$ and $f(p) = 0$ and $\chi(p) = -1$. In all three cases, we have verified that $f(p) \ge -\frac{1}{2}(\chi(p)+1)$. The statement about the averages $P(t)$ and $P'(t)$ follows by definition, and since the number of ramified primes is bounded by $\log d_K$, and hence contribute at most

$$O\left(\frac{\log^2 d_K}{y}\right) = O\left(\frac{\log^2 d_K}{d_K}\right) = o(1). \qquad \square$$

Outline of proof. Our bound for $\mathcal{N}$ will result from a lower bound for the first zero of $\sigma(t)$, which we know must eventually be identically zero by cancellation. The previous lemma, combined with Proposition 1, tells us that we can instead study the first zero of the solution to (11) with $-\frac{1}{2}(P'(t)+1)$ in place of $P(t)$. We then use our estimates for $P'(t)$ from Lemma 8 to finish the proof.

We let

$$I_j(u) = \int_{\substack{t_1+\cdots+t_j \le u \\ t_k \ge 1 \ \forall 1 \le k \le j}} \left(\frac{u - \sum_{k=1}^j t_k}{u}\right) \prod_{k=1}^{j} \frac{(2 - P(t_k))}{t_k}\, dt_1 \cdots dt_j.$$

Then for $u \le 4$,

$$\sigma(u) = 1 - I_1(u) + \frac{I_2(u)}{2} - \frac{I_3(u)}{6}.$$

[4]This definition of $\sigma(t)$ differs from the definition in Section 3 by a factor of t.

Set

$$I_3'(u) = \int_{\substack{t_1+t_2+t_3 \le u \\ t_k \ge 1\ \forall 1 \le k \le 3}} \frac{u-t_1-t_2-t_3}{ut_1t_2t_3}\, dt_1\, dt_2\, dt_3.$$

Note that

$$\frac{I_3(u)}{6} \le \frac{9}{2} I_3'(u),$$

where we have used the trivial bound $2 - P(t) \le 3$. We thus have

$$\sigma(u) \ge 1 - I_1(u) + \frac{I_2(u)}{2} - \frac{9}{2} I_3'(u). \tag{23}$$

By Proposition 1 and Lemma 13, we know that (23) still holds when $P(t)$ is replaced by $-\frac{1}{2}(P'(t)+1)$. Henceforth, assume that $P(t) = -\frac{1}{2}(P'(t)+1)$ for all $t \ge 1$. Now, we calculate an upper bound for $I_1(u)$.

Lemma 14. *For notational convenience, set*

$$g(t,u) = g(t) = \frac{u-t}{tu}.$$

For all $t \in [A,4]$ but for a set of measure zero, we have $-P(t) \le U(t)$, where

$$U(t) = \begin{cases} 1 & \text{if } A < t \le 2, \\ \min(1, 1 - 2\log(t-1) + Et) & \text{if } 2 < t \le 1+A, \\ \min\big(1, 1 - 2\log\frac{A}{t-A} + Et\big) & \text{if } 1+A < t \le 3, \\ \min\big(1, 1 - 2\log\frac{A}{t-A} + Et + \frac{1}{3}t(t-3)^3\big) & \text{if } 3 \le t \le 4. \end{cases}$$

Let $u = 2A \le 4$. Then,

$$\int_1^u (2 - P(t))g(t)\, dt \le 2\int_1^u g(t)\, dt + \int_A^u U(t)g(t)\, dt + \frac{1}{2}\left(\log A - 1 + \frac{1}{u}\Big(1 + A - \frac{2A}{\sqrt{e}}\Big) + \int_1^A g(t)\, dt\right).$$

Proof. Since we assume that $P(t) = -\frac{1}{2}(P'(t)+1)$ and Lemma 12 applies to $P'(t)$, we see that $-P(t) \le U(t)$ for $A \le t \le u$. Hence,

$$\int_1^u (2 - P(t))g(t)\, dt \le 2\int_1^u g(t)\, dt + \int_A^u U(t)g(t)\, dt + \int_1^A \tfrac{1}{2}(1 + P'(t))g(t)\, dt,$$

and moreover,

$$\int_1^A \tfrac{1}{2}(1 + P'(t))g(t)\, dt = \frac{1}{2}\left(\int_1^A g(t)\, dt + \int_1^A \frac{P'(t)}{t} dt - \int_1^A \frac{P'(t)}{u} dt\right).$$

We know that $\int_1^A \frac{1-P'(t)}{t}\,dt = 1$, so $\int_1^A \frac{P'(t)}{t}\,dt = \log A - 1$. We claim that

$$\int_1^A P'(t)\,dt \geq \int_1^{A/\sqrt{e}} 1\,dt - \int_{A/\sqrt{e}}^A 1\,dt = 2A/\sqrt{e} - 1 - A.$$

To see this, let

$$\gamma(t) = \begin{cases} 1 & \text{if } 1 \leq t \leq A/\sqrt{e}, \\ -1 & \text{if } A/\sqrt{e} < t \leq A. \end{cases}$$

Note that $\int_1^A (\gamma(t)/t)\,dt = \log A - 1$. Let $\lambda(t) : [1, A] \to [-1, 1]$ be any function with $\int_1^A (\lambda(t)/t)\,dt = \log A - 1$ and let $h(t) = \lambda(t) - \gamma(t)$. It suffices to show that $\int_1^A h(t)\,dt \geq 0$. We have

$$A/\sqrt{e} \int_1^{A/\sqrt{e}} \frac{h(t)}{t}\,dt + A/\sqrt{e} \int_{A/\sqrt{e}}^A \frac{h(t)}{t}\,dt = 0.$$

Note that $h(t) \leq 0$ for $1 \leq t \leq A/\sqrt{e}$ and $h(t) \geq 0$ for $A/\sqrt{e} < t \leq A$. Thus we have

$$A/\sqrt{e} \int_1^{A/\sqrt{e}} \frac{h(t)}{t}\,dt \leq \int_1^{A/\sqrt{e}} h(t)\,dt$$

and

$$A/\sqrt{e} \int_{A/\sqrt{e}}^A \frac{h(t)}{t}\,dt \leq \int_{A/\sqrt{e}}^A h(t)\,dt.$$

Adding the two inequalities immediately produces the desired result.

From this, we get that

$$\int_1^A \frac{1+P'(t)}{2} g(t)\,dt \leq \frac{1}{2}\left(\log A - 1 + \frac{1}{u}\Big(1 + A - \frac{2A}{\sqrt{e}}\Big) + \int_1^A g(t)\,dt\right). \quad \square$$

We now need a lower bound for $I_2(u)$.

Lemma 15. *Let*

$$L(t) = \begin{cases} 0 & \text{if } 1 \leq t \leq A, \\ 1 & \text{if } A < t \leq 2, \\ \min(1, 1 - 2\log(t-1)) & \text{if } 2 < t \leq 1 + A, \\ \min\big(1, 1 - 2\log \frac{A}{t-A}\big) & \text{if } 1 + A < t \leq 2A. \end{cases}$$

Then for all $t \in [1, 2A]$ but for a set of measure zero we have $-P(t) \geq L(t)$. Thus, for $u = 2A$,

$$I_2(u) \geq \int_{\substack{t_1+t_2 \leq u \\ t_k \geq 1}} \frac{2 + L(t_1)}{t_1} \frac{2 + L(t_2)}{t_2} \frac{u - t_1 - t_2}{u}\,dt_1\,dt_2.$$

Proof. The proof is immediate from Lemma 12, and the fact that we have set $P(t) = -\frac{1}{2}(1 + P'(t))$. □

Proof of Theorem 4. Preserve the notation from the lemma above. Since $\sigma(u) = o(1)$ for $u = 2A$, we have

$$o(1) \geq 1 - 2\int_1^u g(t)\,dt + \int_A^u U(t)g(t)\,dt + \int_1^A \frac{1+P'(t)}{2} g(t)\,dt + \frac{1}{2}\int_{\substack{t_1+t_2\leq u \\ t_k\geq 1}} \frac{(2+L(t_1))}{t_1}\frac{(2+L(t_2))}{t_2}\frac{u-t_1-t_2}{u}\,dt_1\,dt_2 - \frac{9}{2}I_3'(u).$$

Using Maple and the above lemmas, we can check that the right side of the above inequality is positive when $A = 1.6625$. Thus, for the inequality to be true, we must have $A > 1.6625$, so $4A > 6.65$, and since $\mathcal{N} \ll_\epsilon d_K^{1/(4A)+\epsilon}$, we must have

$$\mathcal{N} \ll d_K^{1/6.65}.$$

The number 6.65 should be compared with $4\sqrt{e} = 6.59\ldots$ □

4.3. ***Biquadratic fields.*** We now fix K to be a biquadratic field. Then $\zeta_K(s) = \zeta(s)L(s, \chi_1)L(s, \chi_2)L(s, \chi_1\chi_2)$, where χ_1 and χ_2 are quadratic characters with moduli q_1 and q_2, say. Finding the smallest nonsplit prime is the same as finding the smallest prime which is a quadratic nonresidue for either q_1 or q_2. Clearly, the trivial bound here is of the form $\mathcal{N} \ll_\epsilon \min(q_1, q_2)^{1/(4\sqrt{e})+\epsilon}$ arising immediately from the discussion in the introduction. Our purpose here is to show that more information can be gleaned from considering the behavior of $\chi := \chi_1\chi_2$ in conjunction with that of χ_1 and χ_2. Let $q = \max(q_1, q_2)$; we will only use the fact that both χ_i exhibit cancellation by $q^{1/4} + o(1)$. Note that if q_1 and q_2 are far apart, then we expect to derive little information from the interaction of χ_1 and χ_2. This will be reflected in the discussion at the end of this section.

Assume that all the primes split up to y. (Here the reader may find it helpful to think of y as being a slightly smaller power of q_1q_2 than the trivial bound.) We set

$$P_i(u) = \frac{1}{\nu(y^u)} \sum_{p\leq y^u} \chi_i(p)\log p,$$

for $i = 1, 2$ and where $\nu(x) = \sum_{p\leq x} \log p$. Similarly, we set

$$P(u) = \frac{1}{\nu(y^u)} \sum_{p\leq y^u} \chi(p)\log p.$$

Finally, define $\sigma_i(u)$ for $i \in \{1, 2\}$, and $\sigma(u)$ as in Section 4.1.

We also define

$$I_{i,j}(u) = \int_{\substack{t_1+\cdots+t_j\le u\\ t_k\ge 1\ \forall 1\le k\le j}} \prod_{k=1}^{j} \frac{1-P_i(t_k)}{t_k}\, dt_1\cdots dt_j,$$

and similarly

$$I_j(u) = \int_{\substack{t_1+\cdots+t_j\le u\\ t_k\ge 1\ \forall 1\le k\le j}} \prod_{k=1}^{j} \frac{1-P(t_k)}{t_k}\, dt_1\cdots dt_j.$$

We begin with the following basic observation.

Lemma 16. *Let*

$$S_1 = \frac{1}{\nu(y^u)} \sum_{\substack{p\le y^u\\ \chi_1(p)=\chi_2(p)=1}} \log p, \quad \textit{and} \quad S_{-1} = \frac{1}{\nu(y^u)} \sum_{\substack{p\le y^u\\ \chi_1(p)=\chi_2(p)=-1}} \log p.$$

Then

$$P(u) = 2S_1 + 2S_{-1} - 1 + o(1).$$

Furthermore, if $P_i(t) \ge \alpha > 0$ for all $i \in \{1,2\}$, or if $P_i(t) \le -\alpha < 0$ for all $i \in \{1,2\}$, then

$$P(u) \ge 2\alpha - 1.$$

Proof. Let

$$S_{1,-1}(u) = \frac{1}{\nu(y^u)} \sum_{\substack{p\le y^u\\ \chi_1(p)=-\chi_2(p)=1}} \log p,$$

and similarly define $S_{-1,1}(u)$. Then

$$S_1 + S_{-1} + S_{1,-1} + S_{-1,1} = 1 + o(1),$$

where the $o(1)$ comes from the ramified primes. Since $\chi(p) = \chi_1(p)\chi_2(p)$, we also have

$$P(u) = S_1(u) + S_{-1}(u) - S_{1,-1}(u) - S_{-1,1}(u).$$

Adding the two equations gives the first portion of the lemma. Now say that $P_i(t) \ge \alpha > 0$ for $i \in \{1,2\}$. Then since $\alpha \le P_1(t) = S_1(t) - S_{-1}(t) + S_{1,-1}(t) - S_{-1,1}(t)$ and $\alpha \le P_2(t) = S_1(t) - S_{-1}(t) - S_{1,-1}(t) + S_{-1,1}(t)$, we have $2\alpha \le 2(S_1(t) - S_{-1}(t)) \le P(t) + 1$, as desired. The remaining assertion is proven in the exact same way. □

Outline of proof. As in Section 4.2, our bound for $\mathcal{N}$ will result from a lower bound for the first zero of $\sigma(t)$, which we know must eventually be identically zero by cancellation. The Lemma above relates the behaviour of $P(t)$ with expressions $P_1(t)$ and $P_2(t)$ which may be estimated by Lemma 8.

Lemma 17. *Let A be such that $y^A = q^{1/4}$, and $B \le 2A$ be such that $y^B = (q_1 q_2)^{1/4}$. Then*

$$0 \ge 3 - 4\log A - \int_2^B \frac{1-P(t)}{t}\,dt + o(1).$$

Proof. We have $0 = \sigma_i(u) = 1 - I_{i,1}(u)$ for $A \le u \le 2$. Adding this for $i = 1, 2$, we get

$$\log u - 1 = \int_1^u \frac{P_1(t) + P_2(t)}{2t}\,dt = \int_1^u \frac{S_1(t) - S_{-1}(t)}{t}\,dt.$$

Rearranging, and noting that $S_1(t) \ge 0$, we get that $\int_1^u S_{-1}(t)/t \ge 1 - \log u$. Hence by the previous lemma

$$\int_1^u \frac{P(u)}{u}du \ge \int_1^u \frac{2S_{-1}(t) - 1}{t}\,dt \ge 2 - 3\log u.$$

Thus, rearranging again, and setting $u = A$, we get that

$$1 - \int_1^A \frac{1-P(u)}{u}du \ge 3 - 4\log A + o(1).$$

Observe that $\int_A^2 (1-P_i(u))/u\,du = o(1)$ for each i and so $\int_A^2 (1-P(u))/u\,du = o(1)$ also. We thus have

$$o(1) = \sigma(B) \ge 1 - I_1(B) \ge 3 - 4\log A - \int_2^B \frac{1-P(t)}{t}\,dt. \qquad \square$$

Lemma 16 would give us a nontrivial upper bound[5] for $\int_2^B (1 - P(t))/t\,dt$ provided that we have sufficient information about χ_1 and χ_2. The latter is furnished by Lemma 12. We collect the calculations and prove the theorem below.

Proof. For $2 \le u \le 1 + A$, we have by Lemmas 12 and 16 that $P(t) \ge 1 - 8\log(t-1)$. Hence

$$\int_2^{1+e^{1/4}} \frac{1-P(t)}{t}\,dt \le \int_2^{1+e^{1/4}} \frac{8\log(t-1)}{t}\,dt < 0.13538.$$

In the range $2 \le u \le 1 + A$, we have that $P_i(t) \le 1 - 4\log(t-1) + 2Et$ by Lemma 12. By Lemma 16, we have $1 - P(t) \le 4(1 - 2\log(t-1) + Et)$. This

[5] By nontrivial, we mean that it must be smaller than the trivial bound given by $1 - P(t) \le 2$.

bound is only meaningful when the right hand side is ≤ 2. Thus, let $t_0 < 1+A$ be such that $2(1-2\log(t_0-1)+Et_0)=1$. Then

$$\int_{t_0}^{1+A} \frac{1-P(t)}{t}\,dt \le 4\int_{t_0}^{1+A}\Big(\frac{1-2\log(t-1)}{t}+E\Big)\,dt.$$

Further, in the range $1+A \le u \le 3$, we have by Lemma 12 that $P_i(t) \le 1 - 4\log(A/(t-A)) + 2Et + o(1)$. By Lemma 16, we have

$$\frac{1-P(t)}{t} \le 4\frac{1-2\log(A/(t-A))+Et}{t} + o(1).$$

Let $t_1 > 1+A$ be such that $2(1-2\log(A/(t-A))+Et_1)=1$. Then

$$\int_{1+A}^{t_1} \frac{1-P(t)}{t}\,dt \le 4\int_{1+A}^{t_1}\left(\frac{1-2\log(A/(t-A))}{t}+E\right)dt + o(1).$$

Let $t_2 = A(1+e^{1/4})/e^{1/4}$. In the range, $t_2 \le u \le B \le 2A$, we have by Lemma 12 that $1-P_i(t) \le 4\log(A/(t-A))+o(1)$. Then similarly, we get that

$$\int_{t_2}^{B} \frac{1-P(t)}{t}\,dt \le 8\int_{t_2}^{B}\frac{\log(A/(t-A))}{t}\,dt.$$

We use the trivial bound of $1-P(t)\le 2$ for the range not given above. For any given B, the preceding discussion gives us an upper bound for $\int_2^B (1-P(t))/t\,dt$ and we may derive a lower bound for A by Lemma 17 which states that

$$4\log A \ge 3 - \int_2^B \frac{1-P(t)}{t}\,dt + o(1).$$

Without loss of generality, say that for some $\delta \ge 0$ that $q_1 = q^{1-\delta}$ and $q_2 = q$, and note that $B = (2-\delta)A$. If q_1 is much smaller compared to q_2, then we expect to derive little benefit from the above and then our bound will be $\mathcal{N} \ll q^{(1-\delta)/(4\sqrt{e})}$. The rest is a numerical optimization using Maple over values of δ from which we derive that the worst value for δ occurs when $\delta = 0.061\ldots$ and then

$$\mathcal{N} \ll q^{0.142},$$

or equivalently,

$$\mathcal{N} \ll (q_1q_2)^{0.146/2}.$$

When $q_1 \asymp q_2 = q$, $\delta = 0$ and we have

$$\mathcal{N} \ll (q_1q_2)^{0.141/2}.$$

Remark 6. The reader may be curious about whether this result might be improved if we included the $I_2(u)$ and $I_3(u)$ terms, as we did in the cubic case. While we may improve the result with enough care, the possible improvements here are limited.

The reason is because when $1 \leq t \leq A$, we expect $P_i(t)$ to be close to -1, and when $A < t \leq 2$, we have $P_i(t) = 1$. Thus $P(t)$ is close to 1 for $1 \leq t \leq 2$. Hence for $u \leq 4$, it would be reasonable to expect $I_2(u)$ and $I_3(u)$ to be fairly small. □

Acknowledgements

I would like to express my gratitude to Professor Soundararajan for very generously sharing his time and ideas on various topics in this paper, as well as for his constant encouragement throughout. I also wish to thank Vorrapan Chandee for a careful reading of this paper. Finally, I am grateful to the referee for many helpful editorial remarks.

References

[Bessassi 2003] S. Bessassi, "Bounds for the degrees of CM-fields of class number one", *Acta Arith.* **106**:3 (2003), 213–245. MR 2003m:11183 Zbl 1146.11329

[Burgess 1957] D. A. Burgess, "The distribution of quadratic residues and non-residues", *Mathematika* **4** (1957), 106–112. MR 20 #28 Zbl 0081.27101

[Davenport 2000] H. Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics **74**, Springer, New York, 2000. MR 2001f:11001 Zbl 1002.11001

[Diamond et al. 2006] H. G. Diamond, H. L. Montgomery, and U. Vorhauer, "Beurling primes with large oscillation", *Math. Ann.* **334**:1 (2006), 1–36. MR 2006j:11131 Zbl 1207.11105

[Einsiedler et al. 2011] M. Einsiedler, E. Lindenstrauss, P. Michel, and A. Venkatesh, "The distribution of periodic torus orbits and Duke's theorem for cubic fields", *Ann. of Math.* (2) **173**:2 (2011), 815–885. MR 2776363 (2012h:37006) Zbl pre05960672

[Granville and Soundararajan 2001] A. Granville and K. Soundararajan, "The spectrum of multiplicative functions", *Ann. of Math.* (2) **153**:2 (2001), 407–470. MR 2002g:11127 Zbl 1036.11042

[Granville and Soundararajan ≥ 2012] A. Granville and K. Soundararajan, "Notes on Burgess's theorem", In preparation.

[Halberstam and Richert 1979] H. Halberstam and H.-E. Richert, "On a result of R. R. Hall", *J. Number Theory* **11**:1 (1979), 76–89. MR 80j:10050 Zbl 0395.10048

[Heath-Brown 1992] D. R. Heath-Brown, "Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression", *Proc. London Math. Soc.* (3) **64**:2 (1992), 265–338. MR 93a:11075 Zbl 0739.11033

[Hoffstein 1979] J. Hoffstein, "Some analytic bounds for zeta functions and class numbers", *Invent. Math.* **55**:1 (1979), 37–47. MR 80k:12019 Zbl 0474.12009

[Lagarias et al. 1979] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, "A bound for the least prime ideal in the Chebotarev density theorem", *Invent. Math.* **54**:3 (1979), 271–296. MR 81b:12013 Zbl 0401.12014

[Louboutin 2000] S. Louboutin, "Explicit bounds for residues of Dedekind zeta functions, values of L-functions at $s = 1$, and relative class numbers", *J. Number Theory* **85**:2 (2000), 263–282. MR 2002i:11111 Zbl 0967.11049

[Louboutin 2001] S. Louboutin, "Explicit upper bounds for residues of Dedekind zeta functions and values of L-functions at $s = 1$, and explicit lower bounds for relative class numbers of CM-fields", *Canad. J. Math.* **53**:6 (2001), 1194–1222. MR 2003d:11167 Zbl 0998.11066

[Murty 1994] V. K. Murty, "The least prime which does not split completely", *Forum Math.* **6**:5 (1994), 555–565. MR 95h:11131 Zbl 0834.11045

[Rosser and Schoenfeld 1962] J. B. Rosser and L. Schoenfeld, "Approximate formulas for some functions of prime numbers", *Illinois J. Math.* **6** (1962), 64–94. MR 25 #1139 Zbl 0122.05001

[Stark 1975] H. M. Stark, "The analytic theory of algebraic numbers", *Bull. Amer. Math. Soc.* **81**:6 (1975), 961–972. MR 56 #2961 Zbl 0329.12010

[Stechkin 1970] S. B. Stechkin, "The zeros of the Riemann zeta-function", *Mat. Zametki* **8** (1970), 419–429. In Russian; translated in *Math. Notes* **8**: 4 (1971), 706–711. MR 43 #6168 Zbl 0233.10020

[Tenenbaum 1995] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics **46**, Cambridge University Press, 1995. MR 97e:11005b Zbl 0831.11001

[Vaaler and Voloch 2000] J. D. Vaaler and J. F. Voloch, "The least nonsplit prime in Galois extensions of $\mathbf{Q}$", *J. Number Theory* **85**:2 (2000), 320–335. MR 2002a:11129 Zbl 0963.11066

[Vinogradov 1927] J. M. Vinogradov, "On the bound of the least non-residue of nth powers", *Trans. Amer. Math. Soc.* **29**:1 (1927), 218–226. MR 1501385 JFM 53.0124.04

Communicated by Andrew Granville
Received 2010-06-22 Revised 2011-09-08 Accepted 2011-09-26

xli@math.stanford.edu *Department of Mathematics, Stanford University, Stanford 94305, United States*

ALGEBRA AND NUMBER THEORY 6:6 (2012)
dx.doi.org/10.2140/ant.2012.6.1097

msp

On the geometric realization of the inner product and canonical basis for quantum affine $\mathfrak{sl}_n$

Kevin McGerty

We give a geometric interpretation of the inner product on the modified quantum group of $\widehat{\mathfrak{sl}}_n$. We also give some applications of this interpretation, including a positivity result for the inner product, and a new geometric construction of the canonical basis.

1. Introduction

Let $\mathbf{U}$ be a quantized universal enveloping algebra. The positive part $\mathbf{U}^+$ of $\mathbf{U}$ is well known to possess a canonical basis [Lusztig 1990; Kashiwara 1991; Lusztig 1991]. In contrast, there is no natural basis for the algebra $\mathbf{U}$ itself. However Lusztig [1992] has defined a variant of the quantized enveloping algebra known as the modified quantum group. This algebra has essentially the same representation theory, and can be given a canonical basis $\dot{\mathbf{B}}$ which packages together natural bases of the tensor product of a highest and lowest weight $\mathbf{U}$-module (when such modules exist), in the same way that the canonical basis $\mathbf{B}$ of $\mathbf{U}^+$ packages together natural bases of highest weight representations. Just as for $\mathbf{B}$ (see [Grojnowski and Lusztig 1993; Kashiwara 1991]) it is possible to characterise this basis, up to sign, in terms of an involution and an inner product.

In [Beilinson et al. 1990] the quantized enveloping algebra of $\mathfrak{gl}_n$ was constructed geometrically as a limit of certain convolution algebras. Subsequently Lusztig [1993, Part 4, Notes 1; 1999], and independently Ginzburg and Vasserot [1993], observed that this construction could be extended to the case of quantum affine $\mathfrak{sl}_n$. More precisely, one can define a sequence of algebra $\mathfrak{A}_D$, and maps $\psi_D : \mathfrak{A}_D \to \mathfrak{A}_{D-n}$, along with compatible maps ϕ_D from the modified quantum group $\dot{\mathbf{U}}(\widehat{\mathfrak{sl}}_n)$ such that the resulting map into the inverse limit of the system $(\mathfrak{A}_D, \psi_D)_{D\in\mathbb{N}}$ is injective (in fact we will give a new proof of this injectivity statement in Section 7). One of the main results of the present paper is a construction of the inner product on

MSC2010: primary 20G42; secondary 20G43, 17B37.
Keywords: quantum groups, canonical bases, perverse sheaves.

the modified quantum group $\dot{\mathbf{U}}(\widehat{\mathfrak{sl}}_n)$ as a kind of limit of a natural family of inner products on the algebras $(\mathfrak{A}_D)_{D\in\mathbb{N}}$. We do this both in the context of function on $\mathbb{F}_q$-rational points and perverse sheaves, giving two proofs of the fact that our construction yields the inner product on the modified quantum group — the first is elementary, using explicit formulae for multiplication in $\mathfrak{A}_{D,n,n}$, while the second, although requiring more machinery, gives a more conceptual explanation in terms of equivariant cohomology. As applications of these results we give a new construction of the canonical basis of $\dot{\mathbf{U}}$ in this context (which was already shown in [Schiffmann and Vasserot 2000] using crystal basis techniques), and a prove a positivity property for the inner product of elements of $\dot{\mathbf{B}}$ which is conjectured to hold for arbitrary types.

2. Background

We begin by recalling the setup of [Lusztig 1999]. Fix a positive integer n. Let D be a positive integer, ϵ an indeterminate, $\Bbbk$ a finite field with q elements and v a square root of q. Given a free $\Bbbk[\epsilon,\epsilon^{-1}]$-module V of rank D, a *lattice* in V is a free $\Bbbk[\epsilon]$-submodule of V, of rank D. Let $\mathscr{F}^n$ denote the set of *n-step periodic lattices* in V, that is, $\mathscr{F}^n$ consists of sequences of lattices $\boldsymbol{L}=(L_i)_{i\in\mathbb{Z}}$ where $L_{i-1}\subset L_i$, and $L_{i-n}=\epsilon L_i$ for all $i\in\mathbb{Z}$. We will also write $\mathscr{F}^n_D$ if we wish to emphasise the rank of V. Throughout this paper, if X is a finite set, we will write $|X|$ for the cardinality of X.

The group $G=\mathrm{Aut}(V)$ of automorphisms of V acts on $\mathscr{F}^n$ in the natural way. We shall be interested in functions supported on $\mathscr{F}^n$ and its square which are invariant with respect to the action of G (where G acts diagonally on $\mathscr{F}^n\times\mathscr{F}^n$). Thus we first describe the orbits of G on these spaces. Let $\mathfrak{S}_{D,n}$ be the finite set of all $\boldsymbol{a}=(a_i)_{i\in\mathbb{Z}}$ such that

- $a_i\in\mathbb{N}$;
- $a_i=a_{i+n}$ for all $i\in\mathbb{Z}$;
- $a_i+a_{i+1}+\cdots+a_{i+n-1}=D$ for all $i\in\mathbb{Z}$.

For $\boldsymbol{L}\in\mathscr{F}^n$, let $|\boldsymbol{L}|\in\mathfrak{S}_{D,n}$ be given by $|\boldsymbol{L}|_i=\dim(L_i/L_{i-1})$. The G-orbits on $\mathscr{F}^n$ are indexed by this graded dimension: for $\boldsymbol{a}\in\mathfrak{S}_{D,n}$ set $\mathscr{F}_{\boldsymbol{a}}=\{\boldsymbol{L}\in\mathscr{F}^n : |\boldsymbol{L}|=\boldsymbol{a}\}$; then the $\mathscr{F}_{\boldsymbol{a}}$ are precisely the G-orbits on $\mathscr{F}^n$. The G-orbits on $\mathscr{F}^n\times\mathscr{F}^n$ are indexed, slightly more elaborately, by the set $\mathfrak{S}_{D,n,n}$ of matrices $A=(a_{i,j})_{i,j\in\mathbb{Z}}$ such that

- $a_{i,j}\in\mathbb{N}$;
- $a_{i,j}=a_{i+n,j+n}$ for all $i,j\in\mathbb{Z}$;
- $a_{i,*}+a_{i+1,*}+\cdots+a_{i+n-1,*}=D$ for any $i\in\mathbb{Z}$;
- $a_{*,j}+a_{*,j+1}+\cdots+a_{*,j+n-1}=D$ for any $j\in\mathbb{Z}$.

Here

$$a_{i,*} = \sum_{j \in \mathbb{Z}} a_{i,j} \quad \text{and} \quad a_{*,j} = \sum_{i \in \mathbb{Z}} a_{i,j}.$$

For $A \in \mathfrak{S}_{D,n,n}$ set

$$r(A) = (a_{i,*})_{i \in \mathbb{Z}} \in \mathfrak{S}_{D,n} \quad \text{and} \quad c(A) = (a_{*,j})_{j \in \mathbb{Z}} \in \mathfrak{S}_{D,n}.$$

For $A \in \mathfrak{S}_{D,n,n}$ the corresponding G-orbit $\mathbb{O}_A$ consists of pairs $(\boldsymbol{L}, \boldsymbol{L}')$ such that

$$a_{i,j} = \dim\left(\frac{L_i \cap L'_j}{(L_{i-1} \cap L'_j) + (L_i \cap L'_{j-1})}\right),$$

thus $\boldsymbol{L} \in \mathcal{F}_{r(A)}$ and $\boldsymbol{L}' \in \mathcal{F}_{c(A)}$.

Let $\mathfrak{A}_{D;q}$ be the space of integer-valued G-invariant functions on $\mathcal{F}^n \times \mathcal{F}^n$ supported on a finite number of orbits. If e_A denotes the characteristic function of an orbit $\mathbb{O}_A$, the set $\{e_A : A \in \mathfrak{S}_{D,n,n}\}$ is a basis of $\mathfrak{A}_{D;q}$. The space $\mathfrak{A}_{D;q}$ has a natural convolution product which gives it the structure of an associative algebra. With respect to the basis of characteristic functions the structure constants are given as follows. For $A, B, C \in \mathfrak{S}_{D,n,n}$, let $\eta^C_{A,B;q}$ be the coefficient of e_C in the product $e_A e_B$. Then $\eta^C_{A,B;q}$ is zero unless $c(A) = r(B)$, $r(A) = r(C)$ and $c(B) = c(C)$. Now suppose these conditions are satisfied and fix $(\boldsymbol{L}, \boldsymbol{L}'') \in \mathbb{O}_C$. Then $\eta^C_{A,B;q}$ is the number of points in the set

$$\{\boldsymbol{L}' \in \mathcal{F}_{c(A))} : (\boldsymbol{L}, \boldsymbol{L}') \in \mathbb{O}_A, (\boldsymbol{L}', \boldsymbol{L}'') \in \mathbb{O}_B\}.$$

Clearly this is independent of the choice of $(\boldsymbol{L}, \boldsymbol{L}'')$, and moreover it can be shown that these structure constants are polynomial in q, allowing us to construct an algebra $\mathfrak{A}_{D,\mathbb{Z}[t]}$ over $\mathbb{Z}[t]$, which is a free $\mathbb{Z}[t]$-module on a basis $\{e_A : A \in \mathfrak{S}_{D,n,n}\}$ such that $\mathfrak{A}_{D,\mathbb{Z}[t]|t=q} = \mathfrak{A}_{D,q}$. In fact we will use the algebra $\mathfrak{A}_{D,\mathcal{A}}$ which is obtained from $\mathfrak{A}_{D,\mathbb{Z}[t]}$ by extending scalars to $\mathcal{A} = \mathbb{Z}[v, v^{-1}]$ where $v^2 = t$ and the $\mathbb{Q}(v)$-algebra $\mathfrak{A}_D$ obtained by extending scalars to $\mathbb{Q}(v)$ (we will, by deliberate misuse, treat v as both an indeterminate and a square root of q, depending on the context). The algebra $\mathfrak{A}_D$ is sometimes known as the affine q-Schur algebra. In what follows it will be more convenient to use a rescaled version of the basis $\{e_A\}_{A \in \mathfrak{S}_{D,n,n}}$ of $\mathfrak{A}_{D,\mathcal{A}}$, with elements $[A] = v^{-d_A} e_A$, where

$$d_A = \sum_{\substack{i \geq k \\ j < l \\ 1 \leq i \leq n}} a_{ij} a_{kl}.$$

Note that if we define $\Psi([A]) = [A^t]$, where $(A^t)_{ij} = a_{ji}$, then it is straightforward to check that Ψ is an algebra antiautomorphism (see [Lusztig 1999, Lemma 1.11] for details), which we will sometimes call the transpose antiautomorphism.

Next we introduce quantum groups. In order to do this we recall the notion of a root datum from [Lusztig 1993].

Definition 2.1. A *Cartan datum* is a pair $(I, \cdot)$ consisting of a finite set I and a $\mathbb{Z}$-valued symmetric bilinear pairing on the free abelian group $\mathbb{Z}[I]$, such that

- $i \cdot i \in \{2, 4, 6, \dots\}$ and
- $2\frac{i \cdot j}{i \cdot i} \in \{0, -1, -2, \dots\}$, for $i \neq j$.

A *root datum* of type $(I, \cdot)$ is a pair Y, X of finitely generated free abelian groups and a perfect pairing $\langle \cdot, \cdot \rangle : Y \times X \to \mathbb{Z}$, together with embeddings $I \subset X$ $(i \mapsto i)$ and $I \subset Y$ $(i \mapsto i')$ such that $\langle i', j \rangle = 2(i \cdot j)/(i \cdot i)$.

Given a root datum, we may define an associated quantum group $\mathbf{U}$. Since it is the only case we need, we will assume that our datum is symmetric and simply laced so that $i \cdot i = 2$ for each $i \in I$, and $i \cdot j \in \{0, -1\}$ if $i \neq j$. In this case, $\mathbf{U}$ is generated as an algebra over $\mathbb{Q}(v)$ by symbols E_i, F_i, K_μ, $i \in I$, $\mu \in Y$, subject to the following relations.

(1) $K_0 = 1$, $K_{\mu_1} K_{\mu_2} = K_{\mu_1 + \mu_2}$ for $\mu_1, \mu_2 \in Y$.

(2) $K_\mu E_i K_\mu^{-1} = v^{\langle \mu, i' \rangle} E_i, \quad K_\mu F_i K_\mu^{-1} = v^{-\langle \mu, i' \rangle} F_i$ for all $i \in I$, $\mu \in Y$.

(3) $E_i F_j - F_j E_i = \delta_{i,j}(K_i - K_i^{-1})/(v - v^{-1})$.

(4) $E_i E_j = E_j E_i, \quad F_i F_j = F_j F_i$, for $i, j \in I$ with $i \cdot j = 0$.

(5) $E_i^2 E_j + (v + v^{-1}) E_i E_j E_i + E_j E_i^2 = 0$ for $i, j \in I$ with $i \cdot j = -1$.

(6) $F_i^2 F_j + (v + v^{-1}) F_i F_j F_i + F_j F_i^2 = 0$ for $i, j \in I$ with $i \cdot j = -1$.

Thus $\mathbf{U}$ is naturally X-graded, $\mathbf{U} = \bigoplus_{\nu \in X} \mathbf{U}_\nu$. The subalgebras $\mathbf{U}^+$ and $\mathbf{U}^-$ generated by the E_is and F_is respectively are isomorphic to each other, and indeed are isomorphic to the $\mathbb{Q}(v)$-algebra $\mathbf{f}$ generated by symbols $\{\theta_i : i \in I\}$ subject only to the relation

$$\theta_i \theta_j - \theta_j \theta_i = 0 \text{ for } i, j \in I \text{ with } i \cdot j = 0,$$
$$\theta_i^2 \theta_j + (v + v^{-1}) \theta_i \theta_j \theta_i + \theta_j \theta_i^2 = 0 \text{ for } i, j \in I \text{ with } i \cdot j = -1.$$

Note that the algebra $\mathbf{f}$ depends only on the Cartan datum.

We also need to consider the modified quantum group $\dot{\mathbf{U}}$. This is defined by

$$\dot{\mathbf{U}} = \bigoplus_{\lambda \in X} \mathbf{U} 1_\lambda, \quad \mathbf{U}\, 1_\lambda = \mathbf{U} \Big/ \sum_{\mu \in Y} \mathbf{U}(K_\mu - v^{\langle \mu, \lambda \rangle}),$$

where the multiplicative structure is given in the natural way by the formulae

$$1_\lambda x = x 1_{\lambda - \nu} \quad \text{for } x \in \mathbf{U}_\nu,$$
$$1_\lambda 1_{\lambda'} = \delta_{\lambda, \lambda'} 1_\lambda.$$

Let $\dot{\mathbf{U}}_{\mathscr{A}}$ be the $\mathscr{A}$-subalgebra of $\dot{\mathbf{U}}$ generated by $\{E_i^{(n)}1_\lambda, F_i^{(n)}1_\lambda : n \in \mathbb{Z}_{\geq 0}, \lambda \in X\}$. It is known [Lusztig 1993] that $\dot{\mathbf{U}}_{\mathscr{A}}$ is an $\mathscr{A}$-form of $\dot{\mathbf{U}}$, and moreover it is a free $\mathscr{A}$-module.

To describe the connection between our convolution algebra and quantum groups, we will need the following notation. For $\boldsymbol{a} \in \mathfrak{S}_{D,n}$ let $\boldsymbol{i}_{\boldsymbol{a}} \in \mathfrak{S}_{D,n,n}$ be the diagonal matrix with $(\boldsymbol{i}_{\boldsymbol{a}})_{i,j} = \delta_{i,j}a_i$. Let $E^{i,j} \in \mathfrak{S}_{1,n,n}$ be the matrix with $(E^{i,j})_{k,l}$ equal to 1 if $k = i + sn$ and $l = j + sn$ for some $s \in \mathbb{Z}$, and to 0 otherwise. Let $\mathfrak{S}^n$ be the set of all $\boldsymbol{b} = (b_i)_{i\in\mathbb{Z}}$ such that $b_i = b_{i+n}$ for all $i \in \mathbb{Z}$. Let $\mathfrak{S}^{n,n}$ denote the set of all matrices $A = (a_{i,j})$, $i, j \in \mathbb{Z}$, with entries in $\mathbb{Z}$ such that

- $a_{i,j} \geq 0$ for all $i \neq j$;
- $a_{i,j} = a_{i+n,j+n}$ for all $i, j \in \mathbb{Z}$;
- for any $i \in \mathbb{Z}$ the set $\{j \in \mathbb{Z} : a_{i,j} \neq 0\}$ is finite;
- for any $j \in \mathbb{Z}$ the set $\{i \in \mathbb{Z} : a_{i,j} \neq 0\}$ is finite.

Thus we have $\mathfrak{S}_{D,n,n} \subset \mathfrak{S}^{n,n}$ for all D. For $i \in \mathbb{Z}/n\mathbb{Z}$, let $\boldsymbol{i} \in \mathfrak{S}^n$ be given by $\boldsymbol{i}_k = 1$ if $k = i \bmod n$, $\boldsymbol{i}_k = -1$ if $k = i + 1 \bmod n$, and $\boldsymbol{i}_k = 0$ otherwise. We write $\boldsymbol{a} \cup_i \boldsymbol{a}'$ if $\boldsymbol{a} = \boldsymbol{a}' + \boldsymbol{i}$. For such $\boldsymbol{a}, \boldsymbol{a}'$ set

$$
\begin{aligned}
{}_{\boldsymbol{a}}\boldsymbol{e}_{\boldsymbol{a}'} &= \boldsymbol{i}_{\boldsymbol{a}} - E^{i,i} + E^{i,i+1} \in \mathfrak{S}^{n,n},\\
{}_{\boldsymbol{a}'}\mathbf{f}_{\boldsymbol{a}} &= \boldsymbol{i}_{\boldsymbol{a}'} - E^{i+1,i+1} + E^{i+1,i} \in \mathfrak{S}^{n,n}.
\end{aligned}
$$

Note that if $\boldsymbol{a}, \boldsymbol{a}' \in \mathfrak{S}_{D,n}$ then ${}_{\boldsymbol{a}}\boldsymbol{e}_{\boldsymbol{a}'}$, ${}_{\boldsymbol{a}'}\mathbf{f}_{\boldsymbol{a}} \in \mathfrak{S}_{D,n,n}$. For $i \in \mathbb{Z}/n\mathbb{Z}$ set

$$
E_i(D) = \sum [\,{}_{\boldsymbol{a}}\boldsymbol{e}_{\boldsymbol{a}'}], \qquad F_i(D) = \sum [\,{}_{\boldsymbol{a}'}\mathbf{f}_{\boldsymbol{a}}],
$$

where the sum is taken over all $\boldsymbol{a}, \boldsymbol{a}'$ in $\mathfrak{S}_{D,n}$ such that $\boldsymbol{a} \cup_i \boldsymbol{a}'$. For $\boldsymbol{a} \in \mathfrak{S}^n$ set

$$
K_{\boldsymbol{a}}(D) = \sum_{\boldsymbol{b}\in\mathfrak{S}_{D,n}} v^{\boldsymbol{a}\cdot\boldsymbol{b}}[\boldsymbol{i}_{\boldsymbol{b}}]
$$

where $\boldsymbol{a} \cdot \boldsymbol{b} = \sum_{i=1}^n a_i b_i \in \mathbb{Z}$ for any $\boldsymbol{a}, \boldsymbol{b} \in \mathfrak{S}^n$. If we let $X = Y = \mathfrak{S}^n$, and $I = \mathbb{Z}/n\mathbb{Z}$, with the embedding of $I \subset X = Y$ given by $i \mapsto \boldsymbol{i}$ and pairing as given above, we obtain a symmetric simply laced root datum. We call the quantum group associated to it $\mathbf{U}(\widehat{\mathfrak{gl}}_n)$ (in fact this is the degenerate, or level zero, form of the affine quantum group associated to $\widehat{\mathfrak{gl}}_n$). It can be shown [Lusztig 1999] that the elements $E_i(D)$, $F_i(D)$, $K_{\boldsymbol{a}}(D)$ generate a subalgebra $\mathbf{U}_D$ which is a quotient of the quantum group $\mathbf{U}(\widehat{\mathfrak{gl}}_n)$, via the map that the notation suggests. In particular this gives the algebra $\mathfrak{A}_D$ the structure of a $\mathbf{U}(\widehat{\mathfrak{gl}}_n)$-module. Since $E_i(D)$, $F_i(D)$, $K_{\boldsymbol{a}}(D)$ all lie in $\mathfrak{A}_{D,\mathscr{A}}$ we similarly have an $\mathscr{A}$-subalgebra $\mathbf{U}_{D,\mathscr{A}}$. Note that the idea that one may extend the construction of [Beilinson et al. 1990] to the affine context is mentioned already in [Lusztig 1993, Notes on Part IV] and [Ginzburg and Vasserot 1993], but

note that the surjectivity claimed in Theorem 9.2 of [Ginzburg and Vasserot 1993] is false, as shown in [Lusztig 1999].

Similarly, letting $\boldsymbol{b}_0 = (\ldots, 1, 1, \ldots) \in \mathfrak{S}^n$, we have a root datum given by $X' = \mathfrak{S}^n/\mathbb{Z}\boldsymbol{b}_0$, $Y' = \{\boldsymbol{a} \in \mathfrak{S}^n : \boldsymbol{a} \cdot \boldsymbol{b}_0 = 0\}$ with embeddings $I \subset X', Y'$ induced by the above embeddings into X and Y. This new root datum is associated to (again the degenerate form of) the quantum group $\mathbf{U}(\widehat{\mathfrak{sl}}_n)$. We have an algebra map $\phi_D : \dot{\mathbf{U}}(\widehat{\mathfrak{sl}}_n) \to \mathfrak{A}_D$ given by $E_i^{(n)} 1_\lambda \mapsto E_i(D)^{(n)}[\boldsymbol{i}_{\boldsymbol{a}}]$ where $\boldsymbol{a} \in \mathfrak{S}_{D,n}$ satisfies $\boldsymbol{a} \equiv \lambda \bmod \mathbb{Z}\boldsymbol{b}_0$ if such an $\boldsymbol{a}$ exists, and $E_i^{(n)} 1_\lambda \mapsto 0$ otherwise, and similarly for the $F_i^{(n)} 1_\lambda$. Clearly ϕ_D restricts to a map between the integral forms $\dot{\mathbf{U}}(\widehat{\mathfrak{sl}}_n)_{\mathscr{A}}$ and $\mathfrak{A}_{D,\mathscr{A}}$. It can be readily checked, using a Vandermonde determinant argument, that the image of ϕ_D is exactly $\mathbf{U}_D$ (see [Lusztig 1999, Lemma 2.8]).

3. Inner product on $\mathbf{U}_D$

Definition 3.1. We define a bilinear form

$$(\cdot, \cdot)_D : \mathfrak{A}_{D;q} \times \mathfrak{A}_{D;q} \to \overline{\mathbb{Q}}_l$$

by

$$(f, \tilde{f})_D = \sum_{\boldsymbol{L}, \boldsymbol{L}'} v^{\sum |\boldsymbol{L}|_i^2 - \sum |\boldsymbol{L}'|_i^2} f(\boldsymbol{L}, \boldsymbol{L}') \tilde{f}(\boldsymbol{L}, \boldsymbol{L}'), \tag{3-1}$$

for f and $\tilde{f}$ in $\mathfrak{A}_{D,q}$, where $\boldsymbol{L}$ runs over $\mathscr{F}^n$ and $\boldsymbol{L}'$ runs over a set of representatives for the G-orbits on $\mathscr{F}^n$.

Let $\mathbb{O}_A$ be a G-orbit on $\mathscr{F}^n \times \mathscr{F}^n$, and let

$$X_A^{\boldsymbol{L}} = \{\boldsymbol{L}' \in \mathscr{F}^n : (\boldsymbol{L}, \boldsymbol{L}') \in \mathbb{O}_A\}.$$

It is easy to check that

$$2d_A - 2d_{A^t} = \sum_{i=1}^n a_{i,*}^2 - \sum_{j=1}^n a_{*,j}^2. \tag{3-2}$$

Thus if A, A' are in $\mathfrak{S}_{D,n,n}$ we find that

$$(e_A, e_{A'})_D = \delta_{A,A'} q^{d_A - d_{A^t}} |X_{A^t}^{\boldsymbol{L}'}|,$$

where $\boldsymbol{L}'$ is any lattice in $\mathscr{F}_{c(A)}$. Thus the basis $\{e_A : A \in \mathfrak{S}_{D,n,n}\}$ is orthogonal for our inner product, and hence $(\cdot, \cdot)$ is nondegenerate. If $\{\eta_{A,B;q}^C\}$ are the structure constants of $\mathfrak{A}_{D;q}$ with respect to the basis $\{[A] : A \in \mathfrak{S}_{D,n,n}\}$, then we have

$$([A], [A'])_D = \delta_{A,A'} v^{-d_{A^t}} \eta_{A^t,A;q}^{\boldsymbol{i}_{c(A)}}. \tag{3-3}$$

We therefore obtain an inner product on $\mathfrak{A}_{D,\mathscr{A}}$ taking values in $\mathscr{A}$ by defining

$$([A], [A'])_D = \delta_{A,A'} v^{-d_{A^t}} \eta_{A^t,A}^{\boldsymbol{i}_{c(A)}} \in \mathbb{Z}[v, v^{-1}]. \tag{3-4}$$

By extending scalars, we obtain a $\mathbb{Q}(v)$-valued symmetric bilinear form on $\mathfrak{A}_D$. We now give some basic properties of this inner product:

Proposition 3.2. *Let $A \in \mathfrak{S}_{D,n}$, and let $f, \tilde{f} \in \mathfrak{A}_D$. Then*

$$([A]f, \tilde{f})_D = v^{d_A - d_{A^t}} (f, [A^t]\tilde{f}).$$

Proof. Clearly it suffices to establish this equation in the algebra $\mathfrak{A}_{D;q}$. Since the characteristic functions of G-orbits form a basis of $\mathfrak{A}_{D;q}$, we may assume that $f = e_B$ and $\tilde{f} = e_C$, moreover we may assume that

$$r(A) = r(C), \quad c(A) = r(B), \quad c(B) = c(C). \tag{3-5}$$

as both sides are zero otherwise. It follows immediately that

$$[A] \cdot e_B = v^{-d_A} e_A \cdot e_B, \quad v^{d_A - d_{A^t}} [A^t] \cdot e_C = v^{d_A - 2d_{A^t}} e_{A^t} \cdot e_C.$$

Hence, if $(\tilde{\boldsymbol{L}}, \boldsymbol{L}') \in \mathbb{O}_C$ is fixed,

$$\begin{aligned}([A] \cdot e_B, e_C)_D &= q^{d_C - d_{C^t}} |X_{C^t}^{\boldsymbol{L}'}| \cdot v^{-d_A} \big|\{\boldsymbol{L}'' : (\tilde{\boldsymbol{L}}, \boldsymbol{L}'') \in \mathbb{O}_A, (\boldsymbol{L}'', \boldsymbol{L}') \in \mathbb{O}_B\}\big| \\ &= v^{\alpha} \big|\{\boldsymbol{L}, \boldsymbol{L}'' : (\boldsymbol{L}, \boldsymbol{L}'') \in \mathbb{O}_A, (\boldsymbol{L}'', \boldsymbol{L}') \in \mathbb{O}_B, (\boldsymbol{L}, \boldsymbol{L}') \in \mathbb{O}_C\}\big|, \end{aligned} \tag{3-6}$$

where $\alpha = 2d_C - 2d_{C^t} - d_A$. Similarly, if $(\tilde{\boldsymbol{L}}'', \boldsymbol{L}') \in \mathbb{O}_B$ is fixed,

$$\begin{aligned} &v^{d_A - d_{A^t}} (e_B, [A^t] \cdot e_C)_D \\ &\qquad = q^{d_B - d_{B^t}} |X_{B^t}^{\boldsymbol{L}'}| \cdot v^{d_A - 2d_{A^t}} \big|\{\boldsymbol{L} : (\tilde{\boldsymbol{L}}'', \boldsymbol{L}) \in \mathbb{O}_{A^t}, (\boldsymbol{L}, \boldsymbol{L}') \in \mathbb{O}_C\}\big| \\ &\qquad = v^{\beta} \big|\{\boldsymbol{L}, \boldsymbol{L}'' : (\boldsymbol{L}'', \boldsymbol{L}) \in \mathbb{O}_{A^t}, (\boldsymbol{L}'', \boldsymbol{L}') \in \mathbb{O}_B, (\boldsymbol{L}, \boldsymbol{L}') \in \mathbb{O}_C\}\big|, \end{aligned} \tag{3-7}$$

where $\beta = 2d_B - 2d_{B^t} + d_A - 2d_{A^t}$. But now considering the diagrams

$$\begin{array}{ccc} \boldsymbol{L} & \xrightarrow{A} & \boldsymbol{L}'' \\ & {\scriptstyle C}\searrow & \downarrow{\scriptstyle B} \\ & & \boldsymbol{L}' \end{array} \quad \text{and} \quad \begin{array}{ccc} \boldsymbol{L} & \xleftarrow{A^t} & \boldsymbol{L}'' \\ & {\scriptstyle C}\searrow & \downarrow{\scriptstyle B} \\ & & \boldsymbol{L}' \end{array}$$

it is clear that the last line of (3-6) is the same as the last line of (3-7) if $\alpha = \beta$, that is, if

$$2d_C - 2d_{C^t} - d_A = 2d_B - 2d_{B^t} + d_A - 2d_{A^t} \tag{3-8}$$

But this follows directly from (3-2) and (3-5). □

We have the following easy consequence:

Corollary 3.3. *Let $i \in \mathbb{Z}$, and let $f, \tilde{f} \in \mathfrak{A}_D$ and $\boldsymbol{c} \in \mathfrak{S}^n$. Then*

(1) $(E_i(f), \tilde{f})_D = (f, vK_{\boldsymbol{i}} F_i(\tilde{f}))_D$,

(2) $(F_i(f), \tilde{f})_D = (f, vK_{-\boldsymbol{i}} E_i(\tilde{f}))_D$,

(3) $(K_{\boldsymbol{c}}(f), \tilde{f})_D = (f, K_{\boldsymbol{c}}(\tilde{f}))_D$.

Proof. We may assume that $f = e_A$ and $\tilde{f} = e_B$. The third equation can then be checked immediately from the formulas above. The second equation follows from the symmetry of the inner product and the other two, so it only remains to prove the first. We may assume that $r(A) = r(B) - \boldsymbol{i}$ and $c(A) = c(B)$, as both sides are zero otherwise. Set $\boldsymbol{a} = r(A), \boldsymbol{b} = r(B)$. Now from the definitions we have

$$E_i(e_A) = [{}_{\boldsymbol{b}}\boldsymbol{e}_{\boldsymbol{a}}] \cdot e_A, \quad vK_{\boldsymbol{i}} F_i(e_B) = v^{1+\boldsymbol{i}\cdot\boldsymbol{a}} [{}_{\boldsymbol{a}}\mathbf{f}_{\boldsymbol{b}}] \cdot e_B.$$

Since ${}_{\boldsymbol{b}}\boldsymbol{e}_{\boldsymbol{a}} = {}_{\boldsymbol{a}}\mathbf{f}_{\boldsymbol{b}}^t$ and $d_{{}_{\boldsymbol{b}}\boldsymbol{e}_{\boldsymbol{a}}} - d_{{}_{\boldsymbol{a}}\mathbf{f}_{\boldsymbol{b}}} = 1 + \boldsymbol{i} \cdot \boldsymbol{a}$, the result now follows immediately from the previous proposition. □

Remark 3.4. There is a unique algebra antiautomorphism $\rho : \mathbf{U}(\widehat{\mathfrak{gl}}_n) \to \mathbf{U}(\widehat{\mathfrak{gl}}_n)$ such that

$$\rho(E_i) = vK_{\boldsymbol{i}} F_i, \quad \rho(F_i) = vK_{-\boldsymbol{i}} E_i \quad \rho(K_i) = K_i$$

With this we may state the result of the previous corollary in the form

$$(u(f), \tilde{f})_D = (f, \rho(u)\tilde{f})_D \quad \text{for } u \in \mathbf{U}(\widehat{\mathfrak{gl}}_n) \text{ and } f, \tilde{f} \in \mathfrak{A}_D. \tag{3-9}$$

Note also that another natural choice[1] of definition for an inner product on $\mathfrak{A}_{D,q}$ would be given by taking the sum in (3-1) over a set of representative of the $\mathrm{Aut}(V)$-orbits on $\mathcal{F}$ in the first factor, and all lattices in the second (the opposite of our choice). This inner product, which we denote by $(\,\cdot\,,\,\cdot\,)_D^t$ is obtained from the one we use via the transpose antiautomorphism Ψ, that is,

$$(f, \tilde{f})_D^t = (\Psi(f), \Psi(\tilde{f}))_D,$$

and thus obeys "transposed" versions of the properties established in this section so that

$$(fu, \tilde{f})_D^t = (f, \tilde{f}\bar{\rho}(u))_D^t, \quad u \in \mathbf{U}(\widehat{\mathfrak{gl}}_n), \quad f, \tilde{f} \in \mathfrak{A}_D, \tag{3-10}$$

where $\bar{\rho}$ is given by $\bar{\rho}(x) = \overline{\rho(\bar{x})}$. The precise relation between $(\,\cdot\,,\,\cdot\,)_D$ and $(\,\cdot\,,\,\cdot\,)_D^t$ can be given as follows: if $f, \tilde{f} \in [\boldsymbol{i}_{\boldsymbol{a}}]\mathfrak{A}_D[\boldsymbol{i}_{\boldsymbol{b}}]$ then

$$v^{\sum_{i=1}^n b_i^2} ([\![\boldsymbol{b}]\!]!)^{-1} (f, \tilde{f})_D = v^{\sum_{i=1}^n a_i^2} ([\![\boldsymbol{a}]\!]!)^{-1} (f, \tilde{f})_D^t. \tag{3-11}$$

where we define $[\![\boldsymbol{a}]\!]! = \prod_{i=1}^n \prod_{j=1}^{a_i} (1 - v^{-2j})$. In the finite type case of [Beilinson et al. 1990] this follows easily from considering the orbits on the product of the

[1] It is clear that one needs to restrict one factor to run over representatives of the G-orbits to avoid infinity sums — in the finite type case considered in [Beilinson et al. 1990] this issue doesn't arise.

space of n-step flags with itself, while in the affine case it requires some more care. Since we will not use this fact we do not include the details.

Lemma 3.5. (1) *For $A \in \mathfrak{S}_{D,n,n}$, we have $([A],[A])_D \in 1+v^{-1}\mathbb{Z}[v^{-1}]$.*

(2) *For $A, A' \in \mathfrak{S}_{D,n,n}$ and $A \neq A'$, we have $([A],[A'])_D = 0$.*

Proof. The second part of the statement is obvious. For the first, note that by [Lusztig 1999, 4.3] the set $X_{A^t}^{\boldsymbol{L}'}$ is an irreducible variety of dimension d_{A^t}. Since

$$([A],[A'])_D = \delta_{A,A'} q^{-d_{A^t}} |X_{A^t}^{\boldsymbol{L}'}|,$$

the Lang–Weil estimates [1954] then show that $([A],[A])_D$ lies in $1+v^{-1}\mathbb{Z}[v^{-1}]$, as required. □

Remark 3.6. The results of this section are analogues of the results of [Lusztig 1999, §7]; however our inner product is *not* the same as that of [Lusztig 1999, 7.1], and this makes the proofs somewhat simpler. Lusztig's choice of inner product is compatible with the left and right $\mathbf{U}$-module structure, in the sense that Equations (3-9) and (3-10) both hold. Although this is not quite proved in [Lusztig 1999] it follows from our above discussion using (3-11). However, it does not produce the inner product on $\dot{\mathbf{U}}$ in the way we need.

4. Inner product on $\dot{\mathbf{U}}$

In this section we will write $\dot{\mathbf{U}}$ to denote the modified quantum group $\dot{\mathbf{U}}(\widehat{\mathfrak{sl}}_n)$ associated to the root datum (X', Y') defined in Section 2. We wish to obtain an inner product on $\dot{\mathbf{U}}$ using those on the family of algebras $\{\mathbf{U}_D\}_{D\in\mathbb{N}}$.

We begin with some technical lemmas. Given $A \in \mathfrak{S}^{n,n}$ let $a_{i,\geq s} = \sum_{j\geq s} a_{i,j}$, and $a_{i,>s}$, $a_{i,\leq s}$, etc. similarly.

Lemma 4.1. (a) *Let $A \in \mathfrak{S}_{D,n,n}$ and $\boldsymbol{a}' = r(A)$. If there is an $\boldsymbol{a} \in \mathfrak{S}_{D,n}$ such that $\boldsymbol{a} \cup_i \boldsymbol{a}'$ (i.e., if $a'_{i+1} > 0$), then*

$$[_{\boldsymbol{a}}\boldsymbol{e}_{\boldsymbol{a}'}][A] = \sum_{\substack{s\in\mathbb{Z}\\ a_{i+1,s}\geq 1}} v^{a_{i,\geq s}-a_{i+1,>s}} \left(\frac{1-v^{-2(a_{i,s}+1)}}{1-v^{-2}}\right) [A+E^{i,s}-E^{i+1,s}], \quad (4\text{-}1)$$

where $A = (a_{i,j})$.

(b) *Let $A' \in \mathfrak{S}_{D,n,n}$ and $\boldsymbol{a} = r(A')$. If there is an $\boldsymbol{a}' \in \mathfrak{S}_{D,n}$ such that $\boldsymbol{a} \cup_i \boldsymbol{a}'$ (i.e., if $a_i > 0$), then*

$$[_{\boldsymbol{a}'}\mathbf{f}_{\boldsymbol{a}}][A'] = \sum_{\substack{s\in\mathbb{Z}\\ a'_{i,s}\geq 1}} v^{a'_{i+1,\leq s}-a'_{i,<s}} \left(\frac{1-v^{-2(a'_{i+1,s}+1)}}{1-v^{-2}}\right) [A'-E^{i,s}+E^{i+1,s}], \quad (4\text{-}2)$$

where $A' = (a'_{i,j})$.

Proof. This follows by rescaling the statement of [Lusztig 1999, Proposition 3.5]. □

Let $\mathcal{R}$ be the subring of $\mathbb{Q}(v)[u]$ generated by $\{v^j : j \in \mathbb{Z}\}$ and by the elements

$$\prod_{i=1}^{t} \frac{v^{-2(a-i)}u^2 - 1}{v^{-2i} - 1} \quad \text{for } a \in \mathbb{Z},\ t \geq 1.$$

For $A \in \mathfrak{S}^{n,n}$ let ${}_pA$ be the matrix with $({}_pA)_{i,j} = a_{i,j} + p\delta_{i,j}$. We have the following partial analogue of [Beilinson et al. 1990, 4.2].

Lemma 4.2. *Let $A_1, A_2, \ldots, A_k$ be matrices of the form ${}_{\boldsymbol{a}}\boldsymbol{e}_{\boldsymbol{a}'}$ or ${}_{\boldsymbol{a}}\mathbf{f}_{\boldsymbol{a}'}$, for $\boldsymbol{a}, \boldsymbol{a}' \in \mathfrak{S}^n$, and A any element of $\mathfrak{S}^{n,n}$. Then there exist matrices $Z_1, Z_2, \ldots, Z_m \in \mathfrak{S}^{n,n}$, and $G_1, G_2, \ldots, G_m \in \mathcal{R}$ and an integer $p_0 \in \mathbb{Z}$ such that*

$$[{}_pA_1][{}_pA_2]\ldots[{}_pA_k][{}_pA] = \sum_{i=1}^{m} G_i(v, v^{-p})[{}_pZ_i], \tag{4-3}$$

for all $p \geq p_0$.

Proof. This follows using the same argument as in the proof of Proposition 4.2 in [Beilinson et al. 1990] (where a similar but stronger result is proved for the finite-type case). One uses induction on k. When $k = 1$ the result follows from the previous lemma, once we note that both $a_{i,\geq s} - a_{i+1,>s}$ and $a_{i+1,\leq s} - a_{i,<s}$ are unchanged when A is replaced with $A + pI$. □

Recall from Section 2 that there is a surjective homomorphism $\phi_D : \dot{\mathbf{U}} \to \mathbf{U}_D$ which, for $\lambda \in X$, sends $E_i 1_\lambda \mapsto E_i(D)[\boldsymbol{i}_{\boldsymbol{a}}]$ and $F_i 1_\lambda \mapsto F_i(D)[\boldsymbol{i}_{\boldsymbol{a}}]$ if there is an $\boldsymbol{a}$ in $\mathfrak{S}_{D,n}$ such that $\boldsymbol{a} = \lambda \bmod \mathbb{Z}\boldsymbol{b}_0$, otherwise both $E_i 1_\lambda$, $F_i 1_\lambda$ are sent to zero. Let $\mathbf{f}$ be the algebra defined in Section 2. Pick a monomial basis of $\mathbf{f}$, $\{\zeta_i : i \in J\}$ say. The triangular decomposition for $\dot{\mathbf{U}}$ [Lusztig 1992, 23.2.1] shows that $\mathfrak{B} = \{\zeta_i^+ \zeta_j^- 1_\lambda : i, j \in J, \lambda \in X\}$ is a basis of $\dot{\mathbf{U}}$, where $+ : \mathbf{f} \to \mathbf{U}^+$, and $- : \mathbf{f} \to \mathbf{U}^-$ are the standard isomorphisms defined by $\theta_i \mapsto E_i$ and $\theta_i \mapsto F_i$ respectively. Define a bilinear pairing $\langle \cdot, \cdot \rangle_D$ on $\dot{\mathbf{U}}$ via ϕ_D as follows:

$$\langle x, y \rangle_D = (\phi_D(x), \phi_D(y))_D.$$

Proposition 4.3. *Let $k \in \{0, 1, \ldots, n-1\}$, then if $x, y \in \dot{\mathbf{U}}$*

$$\langle x, y \rangle_{k+pn}$$

converges in $\mathbb{Q}((v^{-1}))$, as $p \to \infty$, to an element of $\mathbb{Q}(v)$.

Proof. We may assume that x, y are elements of $\mathfrak{B}$. Then we need to show that

$$\langle \zeta_{i_1}^+ \zeta_{j_1}^- 1_\lambda, \zeta_{i_2}^+ \zeta_{j_2}^- 1_\mu \rangle_{k+pn}, \quad \text{for } i_1, i_2, j_1, j_2 \in J; \lambda, \mu \in X,$$

converges as $p \to \infty$. Let $\iota : \mathbf{f} \to \mathbf{f}$ be the $\mathbb{Q}(v)$-algebra antiautomorphism fixing the generators θ_i, $1 \le i \le n$. Using Corollary 3.3, it is easy to see that this inner product differs from

$$\langle 1_\lambda, \iota(\zeta_{j_1})^+ \iota(\zeta_{i_1})^- \zeta_{i_2}^+ \zeta_{j_2}^- 1_\mu \rangle_{k+pn} \tag{4-4}$$

by a power of v which is independent of p. But then the definition of the inner product and Lemma 4.2 show that (4-4) may be written as $G(v, v^{-p})$ for some $G \in \mathcal{R}$. The result then follows immediately from the definition of $\mathcal{R}$. □

Remark 4.4. The proof of the last proposition actually allows us to conclude that

$$(\phi_D(\zeta_i^+ \zeta_j^- 1_\lambda), [{}_pA])_{k+pn}$$

converges to an element of $\mathbb{Q}(v)$, as $p \to \infty$, for any $A \in \mathfrak{S}^{n,n}$. We will need this in the next section.

Definition 4.5. We define

$$\langle \cdot, \cdot \rangle : \dot{\mathbf{U}} \times \dot{\mathbf{U}} \to \mathbb{Q}(v),$$

a symmetric bilinear form on $\dot{\mathbf{U}}$ given by

$$\langle x, y \rangle = \sum_{k=0}^{n-1} \lim_{p \to \infty} \langle x, y \rangle_{k+pn}.$$

Remark 4.6. Although the inner products $(\cdot, \cdot)_D$ satisfy only (3-9) and not (3-10), the formula (3-11) which relates $(\cdot, \cdot)_D$ and $(\cdot, \cdot)_D^t$ can be used to show that our limiting inner product $\langle \cdot, \cdot \rangle$ satisfies the analogue of both equations, as indeed Lusztig shows for his inner product on $\dot{\mathbf{U}}$ in [Lusztig 1993, Proposition 26.1.3].

5. Comparison of inner products

Lusztig has shown that the algebra $\dot{\mathbf{U}}$ has a natural inner product which characterised by the following result. (Again, in this section $\dot{\mathbf{U}}$ denotes the modified quantum group attached to the root datum (X', Y').)

Theorem 5.1 (Lusztig). *There exists a unique $\mathbb{Q}(v)$ bilinear pairing*

$$(\cdot, \cdot) : \dot{\mathbf{U}} \times \dot{\mathbf{U}} \to \mathbb{Q}(v)$$

such that

(1) $(1_{\lambda_1} x 1_{\lambda_2}, 1_{\mu_1} y 1_{\mu_2}) = 0$ *for all* $x, y \in \dot{\mathbf{U}}$ *unless* $\lambda_1 = \mu_1, \lambda_2 = \mu_2$;

(2) $(ux, y) = (x, \rho(u)y)$ *for all* $x, y \in \dot{\mathbf{U}}$ *and* $u \in \mathbf{U}$;

(3) $(x^- 1_\lambda, y^- 1_\lambda) = (x, y)$ *for all* $x, y \in \mathbf{f}$ *and* $\lambda \in X$.

Here (x, y) *is the standard inner product on* $\mathbf{f}$ (see [Lusztig 1993, 1.2.5]). *The resulting inner product is automatically symmetric.*

Proof. See [Lusztig 1993, 26.1.2]. □

Theorem 5.2. *The inner products* $\langle \cdot, \cdot \rangle$ *of Section 4 and* $(\cdot, \cdot)$ *of Theorem 5.1 coincide.*

The remainder of this section is devoted to a proof of this theorem. Property (1) in Theorem 5.1 clearly holds for $\langle \cdot, \cdot \rangle$, as the representatives for elements of X in $\mathfrak{S}_{D,n}$ are distinct when they exist. Property (2) follows from Corollary 3.3; thus it only remains to verify (3).

Fix $\lambda \in X$. The algebra $\mathbf{f}$ is naturally graded: $\mathbf{f} = \bigoplus_{\nu \in \mathbb{N}I} \mathbf{f}_\nu$. For $\nu \in \mathbb{Z}[I]$ with $\nu = \sum_{i \in I} \nu_i i$, let $\mathrm{tr}(\nu) = \sum_{i \in I} \nu_i$. If z is homogeneous we set $|z| = \nu$, where $z \in \mathbf{f}_\nu$. Thus for the third property we may assume that $x, y \in \mathbf{f}$ are homogeneous, i.e., $x, y \in \mathbf{f}_\nu$ for some ν, and proceed by induction on $N = \mathrm{tr}(\nu)$. If $N = 0$ then we are reduced to the equation

$$\langle 1_\lambda, 1_\lambda \rangle = 1,$$

which holds trivially. Now suppose that $N > 0$ and the result is known for $x, y \in \mathbf{f}_\nu$ when $\mathrm{tr}(\nu) < N$. If x, y are in $\mathbf{f}_\nu$ and $\mathrm{tr}(\nu) = N$, then we may assume that they are monomials, and $y = \theta_i z$ for some $z \in \mathbf{f}_{\nu - \boldsymbol{i}}$. Thus we have

$$\begin{aligned} \langle x^- 1_\lambda, y^- 1_\lambda \rangle &= \langle x^- 1_\lambda, F_i z^- 1_\lambda \rangle \\ &= \langle v K_{-\boldsymbol{i}} E_i x^- 1_\lambda, z^- 1_\lambda \rangle, \end{aligned}$$

using property (2) of the inner product (which we have already seen holds for both $(\cdot, \cdot)$ and $\langle \cdot, \cdot \rangle$). Now using standard commutation formulas (see [Lusztig 1993, 3.1.6]) this becomes

$$\langle v K_{-\boldsymbol{i}} x^- E_i 1_\lambda, z^- 1_\lambda \rangle + \frac{1}{1 - v^{-2}} \langle ({}_i r(x)^- - v K_{-\boldsymbol{i}} r_i(x)^- K_{-\boldsymbol{i}}) 1_\lambda, z^- 1_\lambda \rangle$$

where ${}_i r$ and r_i are the twisted derivations defined in [Lusztig 1993, 1.2.13]. Tidying this up we get

$$\frac{1}{1 - v^{-2}} \langle {}_i r(x)^- 1_\lambda, z^- 1_\lambda \rangle + \left\langle v^{\boldsymbol{i} \cdot |x| - \boldsymbol{i} \cdot \lambda - 1} \left(x^- E_i - \frac{v^{-\boldsymbol{i} \cdot \lambda}}{v - v^{-1}} r_i(x)^- \right) 1_\lambda, z^- 1_\lambda \right\rangle$$

But ${}_i r(x), z \in \mathbf{f}_{\nu - \boldsymbol{i}}$, hence by induction we have $\langle {}_i r(x) 1_\lambda, z 1_\lambda \rangle = ({}_i r(x)^-, z)$, and by standard properties of the inner product $(\cdot, \cdot)$ on $\mathbf{f}$ we know that

$$\frac{1}{1 - v^{-2}} ({}_i r(x), z) = (x, \theta_i z);$$

thus we are done by induction if we can show that for any $x \in \mathbf{f}_\nu$ the element

$$u(x) = \left(x^- E_i - \frac{v^{-\boldsymbol{i}\cdot\lambda}}{v - v^{-1}} r_i(x)^- \right) 1_\lambda \tag{5-1}$$

annihilates $\mathbf{U}^- 1_\lambda$. To see this we need some (rather technical) lemmas about multiplication in $\mathfrak{A}_D$.

Lemma 5.3. *Let $A \in \mathfrak{S}^{n,n}$ be such that $a_{r,s} = 0$ for $r < s$ unless $r = s-1$ and $r = i$ mod n, when $a_{r,r+1} \in \{0, 1\}$; then the following hold for p sufficiently large.*

(1) *For $j \neq i$ we have*

$$F_j[{}_pA] = \sum_{k=1}^{m} g_k(v)[{}_pZ_k]$$

where $g_k(v) \in \mathscr{A}$ and $Z_k \in \mathfrak{S}^{n,n}$ $(1 \le k \le m)$ and moreover $g_k(v)$ is independent both of p and $\{a_{r,s} : r \le s\}$, and we have $(Z_k)_{r,s} = a_{r,s}$ for $r < s$.

(2) $$F_i[{}_pA] = \sum_{k=1} g_k(v)[{}_pZ_k] + v^{1-\boldsymbol{i}\cdot r(A)} \left(\frac{1 - v^{-2(a_{i+1,i+1}+1+p)}}{1 - v^{-2}} \right) [{}_p(A + E^{i+1,i+1} - E^{i,i+1})],$$

where $g_k(v) \in \mathscr{A}$ is independent of p and $\{a_{r,s} : r \le s\}$, and we have $(Z_k)_{r,s} = a_{r,s}$ for $r < s$, and the final term occurs only if $a_{i,i+1} = 1$.

Proof. By Lemma 4.1, for any $A \in \mathfrak{S}^{n,n}$ and p large enough we have

$$F_j[{}_pA] = \sum_{k:({}_pA)_{j,k} \ge 1} v^{a_{j+1,\le k} - a_{j,<k}} \left(\frac{1 - v^{-2(a_{j+1,k} + p\delta_{j+1,k}+1)}}{1 - v^{-2}} \right) [{}_pA + E^{j+1,k} - E^{j,k}].$$

We claim that in our case the coefficients are independent of p and of $\{a_{r,s} : r \le s\}$, unless $j \equiv i \bmod n$. Indeed then $({}_pA)_{j,k} \ge 1$ implies that $j \ge k$, and hence the coefficient of $[{}_pA + E^{j+1,k} - E^{j,k}]$ in the sum above is

$$v^{a_{j+1,\le k} - a_{j,<k}} \left(\frac{1 - v^{-2(a_{j+1,k}+1)}}{1 - v^{-2}} \right),$$

which evidently involves only entries $a_{r,s}$ of A with $r > s$, thus establishing the first part of the lemma.

For the second part, if $j \equiv i \bmod n$ then we get the same conclusion except when $k = j + 1$, if $a_{j,j+1} = 1$ in which case $a_{j+1,\le j+1} = a_{j+1,*}$ and $a_{j,<j+1} = a_{j,*} - 1$ by our assumptions, so that the term $a_{j+1,\le k} - a_{j,<k} = 1 - \boldsymbol{i} \cdot r(A)$, and this yields the final term in second part, as required. □

Fix $\lambda \in X'$. Then $\sum_{i=1}^n \lambda_i = k \bmod n$ for a well-defined $k \in \{0, 1, \dots n-1\}$. If $D = k + pn$, then there is a unique $\boldsymbol{a} \in X$ which is a representative of $\lambda \in X'$ satisfying $\sum_{i=1}^n a_i = D$ (that is, $\boldsymbol{a} \in \mathfrak{S}_{D,n}$).

Lemma 5.4. *Let $\sum_{j=1}^n \lambda_j = k \bmod n$, where $k \in \{0, 1, \dots, n-1\}$, and suppose that $D = k + pn$ for some p. Then if x is a monomial in the generators $\{\theta_i : i \in I\}$ we have, for sufficiently large p,*

$$\begin{aligned}\phi_D(x^- E_i 1_\lambda) &= \sum_{k=1}^{m_1} a_k(v)[{}_pB_k] + \sum_{k=1}^{m_2}(b_k(v) + v^{-2p}c_k(v))[{}_pH_k],\\ \phi_D(x^- 1_\lambda) &= \sum_{k=1}^{m_1} a_k(v)[{}_pB_k + E^{i+1,i+1} - E^{i,i+1}]\end{aligned} \tag{5-2}$$

for some $B_k, H_k \in \mathfrak{S}^{n,n}$ independent of p, where $(B_k)_{r,s} = (H_k)_{r,s} = 0$ for $r < s$ unless $r = i \bmod n$ when $(B_k)_{i,i+1} = 1$, and the coefficients a_k, b_k, c_k are independent of p, with $a_k \in \mathcal{A}$ and $b_k, c_k \in (v - v^{-1})^{-1}\mathcal{A}$. Moreover, we have

$$\frac{v^{-\boldsymbol{i}\cdot\lambda}}{v - v^{-1}}\phi_D(r_i(x)^- 1_\lambda) = \sum_{k=1}^{m_2} b_k(v)[{}_pH_k]$$

Proof. We use induction on $N = \mathrm{tr}(|x|)$. If $N = 0$ then the result is clear, since we have $\phi_D(E_i 1_\lambda) = [\boldsymbol{i_a} + E^{i,i+1} - E^{i+1,i+1}]$ and $\phi_E(1_\lambda) = [\boldsymbol{i_a}]$ (thus in this case we have $m_1 = 1$ and $m_2 = 0$). Now suppose the result is known for all y with $\mathrm{tr}(|y|) < N$. We may write $x = \theta_j z$ where $\mathrm{tr}(|z|) = N - 1$.

By induction, we have

$$\begin{aligned}\phi_D(xE_i 1_\lambda) &= F_j\phi_D(zE_i 1_\lambda)\\ &= F_j\Big(\sum_{k=1}^{m_1'} a_k'(v)[{}_pB_k'] + \sum_{k=1}^{m_2'}(b_k'(v) + v^{-2p}c_k'(v))[{}_pH_k']\Big),\end{aligned}$$

with a_k', b_k', c_k', B_k', H_k' as in the statement of the lemma (for $x = z$). Now applying Lemma 5.3 to each of these terms, we find that

$$\begin{aligned}&\phi_D(xE_i 1_\lambda) =\\ &\sum_{k=1}^{m_1} a_k(v)[{}_pB_k] + \delta_{i,j}v^{1-\boldsymbol{i}\cdot r(B_k')}\left(\frac{1 - v^{-2((B_k')_{i+1,i+1}+1+p)}}{1 - v^{-2}}\right)a_k'(v)[{}_pB_k' + E^{i+1,i+1} - E^{i,i+1}]\\ &\qquad + \sum_{k=1}^{m_2''}(b_k(v) + v^{-2p}c_k)[{}_pH_k],\end{aligned} \tag{5-3}$$

where $(B_k)_{r,s} = 0$ if $r < s$ unless $r = i \bmod n$ and $s = r+1$, and similarly $(H_k)_{r,s} = 0$ if $r < s$. Thus the first formula of the lemma is established by induction once we

note that when $i \equiv j \bmod n$ we may write

$$\begin{aligned} v^{1-\boldsymbol{i}\cdot r(B'_k)}&\left(\frac{1-v^{-2((B'_k)_{i+1,i+1}+1+p)}}{1-v^{-2}}\right)a'_k(v)[{}_pB'_k + E^{i+1,i+1} - E^{i,i+1}] \\ &= \frac{v^{-\boldsymbol{i}\cdot r(B'_k)}}{v-v^{-1}}\big(1-v^{-2p}v^{-2((B'_k)_{i+1,i+1}+1}\big)a'_k(v)[{}_pB'_k + E^{i+1,i+1} - E^{i,i+1}] \\ &= (b_{m''_2+k} + v^{-2p}c_{m''_2+k})[H_{m''_2+k}], \end{aligned}$$

where the last line defines $b_{m''_2+k}$, $c_{m''_2+k}$ and $H_{m''_2+k}$, and by induction $b_{m''_2+k}$, $c_{m''_2+k}$ lie in $(v-v^{-1})^{-1}\mathscr{A}$, since $a'_k(v) \in \mathscr{A}$. Setting $m_2 = m''_2 + \delta_{i,j}m_1$ the first formula is therefore established.

To show the second formula, we again use induction so that we have

$$\phi_D(x^-1_\lambda) = F_j.\sum_{k=1}^{m'_1} a'_k(v)[{}_pB'_k + E^{i+1,i+1} - E^{i,i+1}]$$

Now by Lemma 5.3 (in particular the independence of the coefficients from the values of $\{a_{r,s} : r \le s\}$ in all but the final term of the second formula) this is equal to

$$\sum_{k=1}^{m_1} a_k(v)[{}_pB_k + E^{i+1,i+1} - E^{i,i+1}],$$

as required. Finally, to see the "moreover" part of the lemma, note that by definition we have

$$\begin{aligned} \left(\frac{v^{-\boldsymbol{i}\cdot\lambda}}{v-v^{-1}}\right)\phi_D(r_i(x)^-1_\lambda) &= \left(\frac{v^{-\boldsymbol{i}\cdot\lambda}}{v-v^{-1}}\right)\phi_D(r_i(\theta_j z)^-1_\lambda) \\ &= \left(\frac{v^{-\boldsymbol{i}\cdot\lambda}}{v-v^{-1}}\right)\big(\delta_{i,j}v^{\boldsymbol{i}\cdot|z|}\phi_D(z^-1_\lambda) + F_j(\phi_D(r_i(z)^-1_\lambda)\big). \end{aligned}$$

Comparing this with (5-3), we note that $r(B'_k) = \boldsymbol{a} + \boldsymbol{i} - |z|$, hence $1 - \boldsymbol{i}\cdot r(B'_k) = \boldsymbol{i}\cdot(|z|-\lambda) - 1$, so that

$$v^{1-\boldsymbol{i}\cdot r(B'_k)}\left(\frac{1-v^{-2((B'_k)_{i+1,i+1}+p+1)}}{1-v^{-2}}\right) = \left(\frac{v^{\boldsymbol{i}\cdot(|z|-\lambda)}}{v-v^{-1}}\right)(1-v^{-2p}v^{-2((B'_k)_{i+1,i+1}+1)}).$$

Hence the result follow once again by induction. □

Having established these technical lemmas, it is now straightforward to complete the proof of Theorem 5.2.

Definition 5.5. Let

$$\mathfrak{A}_D^- = \operatorname{span}\{[A] : a_{r,s} = 0 \text{ for all } r < s\}$$

and let $\pi_D : \mathfrak{A}_D \to \mathfrak{A}_D^-$ be the orthogonal projection; thus its kernel is spanned by the elements $[A]$ such that $a_{r,s} > 0$ for some $r, s \in \mathbb{Z}$ with $r < s$. Note that Lemma 5.3 shows that $\phi_D(x^- 1_\lambda) \in \mathfrak{A}_D^-$ for any $x \in \mathbf{f}$. Let $s_D : \mathbf{f} \to \mathfrak{A}_D^-$ be given by

$$x \mapsto \pi_D(\phi_D(x^- E_i 1_\lambda))$$

and define $r_D : \mathbf{f} \to \mathfrak{A}_D^-$ by setting

$$x \mapsto \frac{v^{-\boldsymbol{i}\cdot\lambda}}{v - v^{-1}} \phi_D(r_i(x)^- 1_\lambda).$$

Corollary 5.6. *Let $x \in \mathbf{f}$.*

$$s_D(x) - r_D(x) = \frac{v^{-2p}}{v - v^{-1}} \left(\sum_{k=1}^{m} c_k(v)[{}_p Z_k] \right)$$

for some $Z_k \in \mathfrak{S}^{n,n}$ and $c_k \in \mathcal{A}$, independent of p. Hence the element $u(x)$ of (5-1) *is orthogonal to $\mathbf{U}^- 1_\lambda$.*

Proof. Let $y \in \mathbf{f}$ be a monomial. Then we have

$$(u, y^- 1_\lambda) = \lim_{p \to \infty} \langle u, y^- 1_\lambda \rangle_{k+pn},$$

and by definition

$$\langle u, y^- 1_\lambda \rangle_{k+pn} = (s_{k+pn}(x) - r_{k+pn}(x), \phi_{k+pn}(y^- 1_\lambda))_{k+pn}. \tag{5-4}$$

By Lemma 5.4.

$$s_{k+pn}(x) - r_{k+pn}(x) = v^{-2p} \left(\sum_{j=1}^{m} c_j(v)[{}_p Z_j] \right), \quad Z_j \in \mathfrak{S}^{n,n},$$

and by Remark 4.4, we know that $([{}_p Z_j], \phi_{k+pn}(y^- 1_\lambda))_{k+pn}$ converges in $\mathbb{Q}((v^{-1}))$ as $p \to \infty$. Thus the right-hand side of (5-4) tends to zero as required. □

6. Geometric interpretation

Recall from [Lusztig 1999, §4] that $\mathfrak{A}_D$ possesses a canonical basis $\mathfrak{B}_D$ consisting of elements $\{A\}$, $A \in \mathfrak{S}_{D,n,n}$. To define these elements we must assume $\Bbbk$ is algebraically closed (either the algebraic closure of $\mathbb{F}_q$, in which case we must use sheaves in the étale topology, or $\mathbb{C}$ in which case we use the analytic topology). Fix $A \in \mathfrak{S}_{D,n}$, and $\boldsymbol{L} \in \mathscr{F}_{r(A)}$.

The space $\mathscr{F}^n$ can be given the structure of an ind-scheme such that each set $X_A^{\boldsymbol{L}}$ (see Section 3) lies naturally in a projective algebraic variety. This follows from the fact that if we fix $i_0, j_0 \in \mathbb{Z}$, then the subsets

$$\mathscr{F}^p_{\boldsymbol{b},\boldsymbol{L}} = \{\boldsymbol{L}' \in \mathscr{F}_{\boldsymbol{b}} : \varepsilon^p L_{i_0} \subset L'_{j_0} \subset \varepsilon^{-p} L_{i_0}\}$$

(for $p = 1, 2, \dots$) are naturally projective algebraic varieties each embedded in the next, and for any fixed $A \in \mathfrak{S}_{D,n,n}$ there is a $p_0 \in \mathbb{Z}$ such that $X_A^{\boldsymbol{L}}$ is a locally closed subset of $\mathscr{F}_{\boldsymbol{b},\boldsymbol{L}}^p$ for all $p \geq p_0$. Thus its closure $\overline{X}_A^{\boldsymbol{L}}$ is naturally a projective algebraic variety. Let $\mathcal{I}_A^{\boldsymbol{L}}$ (or sometimes for convenience just $\mathcal{I}_A$) denote the simple perverse sheaf on $\overline{X}_A^{\boldsymbol{L}}$ whose restriction to $X_A^{\boldsymbol{L}}$ is $\mathbb{C}[d_A]$. Let $\mathscr{H}^s(\mathcal{I}_A^{\boldsymbol{L}})$ be the s-th cohomology sheaf of $\mathcal{I}_A^{\boldsymbol{L}}$. For $A_1 \in \mathfrak{S}_{D,n,n}$ such that $X_{A_1}^{\boldsymbol{L}} \subset \overline{X}_A^{\boldsymbol{L}}$ we write $A_1 \leq A$, and set

$$\Pi_{A_1,A} = \sum_{s \in \mathbb{Z}} \dim(\mathscr{H}_y^{s-d_{A_1}}(\mathcal{I}_A^{\boldsymbol{L}}))v^s \in \mathbb{Z}[v^{-1}],$$

where $\mathscr{H}_y^{s-d_{A_1}}(\mathcal{I}_A^{\boldsymbol{L}})$ is the stalk of $\mathscr{H}^{s-d_{A_1}}(\mathcal{I}_A^{\boldsymbol{L}})$ at a point $y \in \overline{X}_{A_1}^{\boldsymbol{L}}$ (since $\mathcal{A}^{\boldsymbol{L}}$ is constructible with respect to the stratification of $\overline{X}_A^{\boldsymbol{L}}$ given by $\{X_{A_1}^{\boldsymbol{L}} : A_1 < A\}$, this is independent of the choice of y). We let

$$\{A\} = \sum_{A_1; A_1 \leq A} \Pi_{A_1,A}[A_1].$$

The next result is an immediate consequence of the definitions and Lemma 3.5. (It is the analogue for our inner product of [Lusztig 1999, Lemma 7.5]).

Lemma 6.1. *Let $A, A' \in \mathfrak{S}_{D,n,n}$. Then*

$$(\{A\}, \{A'\})_D \in \delta_{A,A'} + v^{-1}\mathbb{Z}[v^{-1}]. \qquad \square$$

The algebra $\mathfrak{A}_D$ may be viewed as a convolution algebra of (equivariant) complexes on $\mathscr{F}^n$. One must be slightly careful here since one cannot (at least straightforwardly) consider convolution on $\mathscr{F}^n \times \mathscr{F}^n$ as the "complexes" one would then have to consider would have infinite-dimensional support. However, [Lusztig 1999, 4.2] gives one way in which this difficulty can be avoided: given $A, B \in \mathfrak{S}_{D,n,n}$ we may consider the set

$$Z = \left\{(\boldsymbol{L}', \boldsymbol{L}'') \in \mathscr{F}_{\boldsymbol{b}} \times \mathscr{F}_{\boldsymbol{c}} : \boldsymbol{L}' \in \overline{X}_A^{\boldsymbol{L}}, \boldsymbol{L}'' \in \overline{X}_B^{\boldsymbol{L}'}\right\}.$$

As with $\overline{X}_A^{\boldsymbol{L}}$ we see that Z is naturally a projective variety and the projection π to the second factor gives a proper map $Z \to \mathscr{F}_{\boldsymbol{c}}$. The group $G_{\boldsymbol{L}} \subset \mathrm{Aut}(V)$ of automorphisms stabilising $\boldsymbol{L}$ acts on $\mathscr{F}_{\boldsymbol{b}}$ through a quotient which is naturally an algebraic group, and thus it makes sense to speak of $G_{\boldsymbol{L}}$-equivariant perverse sheaves on $\mathscr{F}_{\boldsymbol{b}}$ and Z. If $\mathcal{I}$ denotes the middle extension of the constant sheaf on the smooth locus of Z, then $\mathcal{I}$ has a canonical $G_{\boldsymbol{L}}$-equivariant structure, and so by the decomposition theorem its push-forward along π is a direct sum of (shifted) perverse sheaves of the form $\mathcal{I}_C$, ($C \in \mathfrak{S}_{D,n,n}$). We denote this push-forward by $\mathcal{I}_A * \mathcal{I}_B$. If $\mathscr{K}_{D,n,n}$ denotes the free $\mathcal{A}$-module on the set $[\mathcal{I}_A^{\boldsymbol{L}}]$ of isomorphism classes of the sheaves $\mathcal{I}_A^{\boldsymbol{L}}$ (as $\boldsymbol{L}$ runs over a set of $\mathrm{Aut}(V)$-orbit representatives on $\mathscr{F}$) then the convolution $*$ gives $\mathscr{K}_{D,n,n}$ an associative $\mathcal{A}$-algebra structure, which

is shown in [Lusztig 1999, 4.4] to be isomorphic to $\mathfrak{A}_{D,\mathscr{A}}$ via the map Θ given by $\Theta([\mathcal{J}_A]) = \{A\}$. Moreover, Lusztig has shown that the submodule $K_{D,n,n}$ of $\mathcal{K}_{D,n,n}$ spanned by the elements $\{[\mathcal{J}_A] : A \in \mathfrak{S}^{\mathrm{ap}}_{D,n,n}\}$ is precisely the preimage under Θ of the subalgebra $\mathbf{U}_{D,\mathscr{A}}$, where $\mathfrak{S}^{\mathrm{ap}}_{D,n,n}$ is the subset of $\mathfrak{S}_{D,n,n}$ consisting of those matrices $A \in \mathfrak{S}_{D,n,n}$ for which, given any $p \in \mathbb{Z}\backslash\{0\}$, there is a $k \in \mathbb{Z}$ with $a_{k,k+p} = 0$.

Remark 6.2. Note also that this isomorphism yields the existence of an $\mathscr{A}$-antilinear involution on $\mathfrak{A}_{D,\mathscr{A}}$ which fixes the basis elements $\{A\}$, $(A \in \mathfrak{S}_{D,n,n})$, by transporting via Θ the action of the Verdier duality functor. We will write this involution as $x \mapsto \bar{x}$. Since it fixes the generators $E_i(D)$, $F_i(D)$, $K_{\boldsymbol{a}}$ it preserves the subalgebra $\mathbf{U}_{D,\mathscr{A}}$ and is compatible with the bar involution on $\dot{\mathbf{U}}$ (see [Lusztig 1999, 4.13] for more details). Moreover, Lusztig [Lusztig 1999, Proposition 4.12] shows that the antiautomorphism Ψ corresponds to the map on $\mathcal{K}_{D,n,n}$ which sends $[\mathcal{J}_A]$ to $[\mathcal{J}_{A^t}]$.

We wish to give an interpretation of the inner product of Section 3 in the context of the algebra $\mathcal{K}_{D,n,n}$. Suppose that $A, B \in \mathfrak{S}_{D,n,n}$. We want to describe $(\{A\}, \{B\})$. We may assume that $r(A) = r(B) = \boldsymbol{a}$ and $c(A) = c(B) = \boldsymbol{b}$. Let $\boldsymbol{L}' \in \mathcal{F}_{\boldsymbol{b}}$. Let $\mathcal{J}^{\boldsymbol{L}'}_{A^t}$ and $\mathcal{J}^{\boldsymbol{L}'}_{B^t}$ denote the simple perverse sheaves on $\bar{X}^{\boldsymbol{L}'}_{A^t}$ and $\bar{X}^{\boldsymbol{L}'}_{B^t}$ respectively. Then define

$$\langle \mathcal{J}_A, \mathcal{J}_B \rangle^D = \sum_{i \in \mathbb{Z}} \dim(H^i_c(\mathcal{F}_{\boldsymbol{a}}, \mathcal{J}^{\boldsymbol{L}'}_{A^t} \otimes \mathcal{J}^{\boldsymbol{L}'}_{B^t}))v^i. \tag{6-1}$$

(Here as usual $\otimes$ denotes the derived tensor product.) Clearly $\langle \cdot, \cdot \rangle^D$ extends to an inner product on the whole of $\mathfrak{A}_D$ (viewed as an algebra of equivariant complexes on $\mathcal{F}^n$). We want to show that it is the same as the inner product $(\cdot, \cdot)_D$ of Section 3, at least on the subalgebra $\mathbf{U}_D$. We start by showing that $\langle \cdot, \cdot \rangle^D$ satisfies the properties of Corollary 3.3.

Lemma 6.3. *Let $A, B, C \in \mathfrak{S}_{D,n,n}$, and suppose that $\mathbb{O}_A$ is a closed orbit. Then*

$$\langle \mathcal{J}_A * \mathcal{J}_B, \mathcal{J}_C \rangle^D = v^{d_A - d_{A^t}} \langle \mathcal{J}_B, \mathcal{J}_{A^t} * \mathcal{J}_C \rangle^D.$$

Proof. Both sides are obviously zero unless $r(A) = r(C) = \boldsymbol{a}$, $c(A) = r(B) = \boldsymbol{b}$ and $c(B) = c(C) = \boldsymbol{c}$; thus we assume these equalities from now on. Pick $\boldsymbol{L}^0 \in \mathcal{F}_{\boldsymbol{c}}$, and pick a subset $Y = \mathcal{F}^p_{\boldsymbol{b},\boldsymbol{L}^0}$ of $\mathcal{F}_{\boldsymbol{b}}$ large enough that Y is a smooth projective variety containing $X^{\boldsymbol{L}_0}_{B^t}$. Let

$$Z_A = \{(\boldsymbol{L}, \boldsymbol{L}') \in \mathbb{O}_A : \boldsymbol{L}' \in Y\},$$

We have maps $p_1 : Z_A \to \mathcal{F}_{\boldsymbol{a}}$ and $p_2 : Z \to Y$, the first and second projections respectively. The map p_1 is clearly proper (as the fibre is $X^{\boldsymbol{L}}_A \cap Y$) and the map p_2 is smooth with fibre dimension d_{A^t}. It follows that the complex $\mathcal{J}$ used in the definition of $\mathcal{J}_A * \mathcal{J}_B$ is the pull-back $p_2^*(\mathcal{J}_{B^t})[d_{A^t}]$, and hence we have

$$(\mathcal{J}_A * \mathcal{J}_B)^t = (p_1)_! p_2^*(\mathcal{J}_{B^t})[d_{A^t}],$$

and thus in particular

$$\begin{aligned}(\mathcal{J}_A * \mathcal{J}_B)^t \otimes \mathcal{J}_{C^t} &= (p_1)_! p_2^*(\mathcal{J}_{B^t})[d_{A^t}] \otimes \mathcal{J}_{C^t} \\ &= (p_1)_!(p_2^*(\mathcal{J}_{B^t}) \otimes p_1^*(\mathcal{J}_{C^t})[d_{A^t}]),\end{aligned} \tag{6-2}$$

where we use the projection formula in the second equality.

On the other hand, to compute the product $\mathcal{J}_{A^t} * \mathcal{J}_C$ we may similarly pick a smooth projective variety $W \subset \mathcal{F}_{\boldsymbol{a}}$ which contains $X^{\boldsymbol{L}^0}_{C^t}$, and consider the variety

$$Z_{A^t} = \{(\boldsymbol{L}, \boldsymbol{L}') \in \mathbb{O}_A : \boldsymbol{L} \in W\}.$$

As above there are projection maps p_1, p_2, and the product is given by

$$(\mathcal{J}_{A^t} * \mathcal{J}_C)^t = (p_2)_! p_1^*(\mathcal{J}_{C^t})[d_A].$$

so that

$$\begin{aligned}\mathcal{J}_{B^t} \otimes (\mathcal{J}_{A^t} * \mathcal{J}_C)^t &= \mathcal{J}_{B^t} \otimes (p_2)_! p_1^*(\mathcal{J}_{C^t})[d_{A^t}] \\ &= (p_2)_!(p_2^*(\mathcal{J}_{B^t}) \otimes p_1^*(\mathcal{J}_{C^t}))[d_A]\end{aligned}$$

where we again use the projection formula. Now since tensor product is local, we may restrict to $Z_A \cap Z_{A^t}$, and then it is clear that both inner products are given by the compactly supported cohomologies of $p_2^*(\mathcal{J}_{B^t}) \otimes p_1^*(\mathcal{J}_{C^t})$ up to shift, with the difference in shifts being $d_A - d_{A^t}$ as required. □

Lemma 6.4. *Let $A, B \in \mathfrak{S}_{D,n,n}$, and $\boldsymbol{c} \in \mathfrak{S}^n$. Then*

(1) $\langle E_i\{A\}, \{B\}\rangle^D = \langle \{A\}, v K_{\boldsymbol{i}} F_i\{B\}\rangle^D$,

(2) $\langle F_i\{A\}, \{B\}\rangle^D = \langle \{A\}, v K_{-\boldsymbol{i}} E_i\{B\}\rangle^D$,

(3) $\langle K_{\boldsymbol{c}}\{A\}, \{B\}\rangle^D = \langle \{A\}, K_{\boldsymbol{c}}\{B\}\rangle^D$.

Proof. This follows from the previous lemma exactly as in the proof of Corollary 3.3, since the varieties $X^{\boldsymbol{L}}_{\boldsymbol{a}+i\boldsymbol{e}_{\boldsymbol{a}}}$ are closed. □

The algebra $\mathbf{U}_D$ is spanned by elements of the form $T_1 T_2 \dots T_N[\boldsymbol{i}_{\boldsymbol{a}}]$ where T_s is either E_i or F_i for some i. Thus, by Corollary 3.3, in order to show that the inner products $(\,)_D$ and $\langle \cdot, \cdot \rangle^D$ coincide via the isomorphism the previous lemma shows we need only check that

$$\langle T_1 T_2 \dots T_N[\boldsymbol{i}_{\boldsymbol{a}}], [\boldsymbol{i}_{\boldsymbol{a}}]\rangle^D = (T_1 T_2 \dots T_N[\boldsymbol{i}_{\boldsymbol{a}}], [\boldsymbol{i}_{\boldsymbol{a}}])_D$$

But this will follow if we can show that

$$\langle \{A\}, [\boldsymbol{i}_{\boldsymbol{a}}]\rangle^D = (\{A\}, [\boldsymbol{i}_{\boldsymbol{a}}])_D$$

for all $A \in \mathfrak{S}_{D,n,n}$, as $\{\{A\} : A \in \mathfrak{S}_{D,n,n}\}$ is a basis of $\mathfrak{A}_D$. The simple perverse sheaf corresponding to $\{\boldsymbol{i}_{\boldsymbol{a}}\} = [\boldsymbol{i}_{\boldsymbol{a}}]$ is just the skyscraper sheaf at the point $\boldsymbol{L}'$; hence this last equality follows from directly from the definitions. We have therefore shown the following result.

Proposition 6.5. *On the algebra* $\mathbf{U}_D$ *the inner products* $\langle \cdot, \cdot \rangle^D$ *and* $(\cdot, \cdot)_D$ *coincide.* □

Remark 6.6. It can be shown that the algebra $\mathfrak{A}_D$ is generated by the elements $\{A\}$ for which $X_A^{\mathbf{L}}$ is closed, and so the above argument adapts to show that the inner products in fact agree on the whole of $\mathfrak{A}_D$, but we will not need this. Henceforth we will use the notation $(\cdot, \cdot)_D$ when referring to the inner product on $\mathfrak{A}_D$ in either of its incarnations.

We now give a second proof of the agreement of the limit of the inner products on $\mathbf{U}_D$ with Lusztig's inner product on $\dot{\mathbf{U}}$. Recall that Theorem 5.1 characterises the inner product by three properties, the first two of which are evident for our limiting inner product. The difficulty then is establishing the third property, which relates the inner product on $\dot{\mathbf{U}}$ to that on $\mathbf{f}$. We give a proof of this property, which while less elementary than the proof in Section 5 is more conceptual. In the remainder of this section we will assume that our base field $\Bbbk$ is the field of complex numbers $\mathbb{C}$, and work with sheaves in the analytic topology. We thus briefly review some basics of the equivariant derived category, following the approach of [Bernstein and Lunts 1994].

We first need to recall the geometric construction of the algebra $\mathbf{f}$ and its inner product (at least in the case of the cyclic quiver). Let Q be the cyclic quiver $1 \to 2 \to \cdots \to n \to 1$. A representation of Q is a $\mathbb{Z}/n\mathbb{Z}$-graded vector space $W = \bigoplus_{i \in \mathbb{Z}/n\mathbb{Z}} W_i$ equipped with linear maps $y_i : W_i \to W_{i+1}$ (where $i \in \mathbb{Z}/n\mathbb{Z}$). The space of such representations is denoted E_W. Such a representation is *nilpotent* if there is an $N > 0$ such that all compositions of y_is of length greater than N are equal to zero, and we write E_W^{nil} for the subvariety of nilpotent representations. The group $G_W = \prod_{i \in \mathbb{Z}/n\mathbb{Z}} \mathrm{GL}(V_i)$ acts on E_W^{nil} with finitely many orbits. The algebra $\mathbf{f}$ associated to the Cartan datum of affine type $\widehat{\mathfrak{sl}}_n$ is then given as a convolution algebra of semisimple perverse sheaves which are G_W-equivariant and are supported on E_V^{nil}; thus, since the stabiliser of a nilpotent representation is connected, the simple objects are labelled by the G_W-orbits on E_W^{nil}, that is, by the isomorphism classes of nilpotent representations.

Given a pair $(t, m) \in \mathbb{Z} \times \mathbb{Z}_{\geq 0}$ we have a representation $V_{t,m}$ of the cyclic quiver with basis $\{e_j : t \leq j \leq t + p - 1\}$ where e_j has degree $j \bmod n$, and $e_t \to e_{t+1} \to \cdots e_{t+p-1} \to 0$. The representations $V_{t,p}$ are a complete set of representatives for the isomorphism classes of indecomposable nilpotent representations of the cyclic quiver; thus, since any nilpotent representation is a direct sum of indecomposables, we can record the isomorphism class of any such representation by a tableau $(\mu_{t,p})_{t,p \in \mathbb{Z}}$ where the entry $\mu_{t,p}$ records the multiplicity of $V_{t,m}$ in the representation. We therefore have a natural parametrisation of the canonical basis $\mathbf{B}$ by tableaux $(\mu_{t,p})_{t \in \mathbb{Z}, p \in \mathbb{N}}$, where $\mu_{t,p} \in \mathbb{N}$ and $\mu_{t,p} = \mu_{t-n,p}$ for all $t \in \mathbb{Z}$ and for fixed t only finitely many of the $\mu_{t.p}$ are nonzero.

If $\dim(W_i) = \nu_i$, $(i \in \mathbb{Z}/n\mathbb{Z})$, the orbits of G_W on E_W^{nil} correspond to the isomorphism classes of nilpotent representations of dimension ν hence they are labelled by the set Σ_ν consisting of those tableaux $(\mu_{t,p})$ for which

$$\sum_{\substack{t,p \\ t \le k < t+p}} \mu_{t,p} = \nu_k,$$

and so this same set indexes the ν-homogeneous part of $\mathbf{f}$.

The inner product on $\mathbf{f}$ is defined in [Lusztig 1993, §12.2]. Let A_1, A_2 be G_W-equivariant simple perverse sheaves on E_W^{nil}. Note that the definition there is simply an explicit calculation of

$$(A_1, A_2) = \sum_{j \in \mathbb{Z}} \dim(H^j_{G,c}(A_1 \otimes A_2))v^{-j}. \tag{6-3}$$

where $H^*_{G,c}$ denotes equivariant cohomology with compact supports (see below for more details).

Definition 6.7. Let X be a variety with a G-action (or more compactly, a G-variety). A *resolution* of X is a map $p : P \to X$ where P is smooth G-variety on which G acts freely (so that $\bar{P} = P/G$ is a smooth variety also). Let $\pi : P \to \bar{P}$ denote the quotient map. The category $D^b_G(X, P)$ consists of triples $(\mathcal{F}, \mathcal{G}, \phi)$ where $\mathcal{F}$ is an object in $D^b(\bar{P})$ and $\mathcal{G}$ is an object in $D^b(X)$ and $\phi : \pi^*(\mathcal{F}) \to p^*(\mathcal{G})$ is an isomorphism.

We will also need to recall the notion of an n-acyclic map.

Definition 6.8. A map $f : Y \to X$ is said to be n-acyclic if it has the following properties:

(i) For any sheaf F on Y the adjunction morphism $B \to R^0 f_* f^*(B)$ is an isomorphism, and $R^i f_* f^*(F) = 0$ for $0 < i \le n$.

(ii) For any base change $\tilde{X} \to X$ the induced map $\tilde{f} : \tilde{Y} = Y \times_X \tilde{X} \to \tilde{X}$ has property (i).

If we write $\tau_{\le n}$ for the truncation functor on the derived category $D^b(Y)$, the first condition may be rewritten as saying that the adjunction map $F \to \tau_{\le n} R f_* f^*(F)$ in $D^b(Y)$ is an isomorphism for any sheaf F (thought of as an complex in $D^b(Y)$ concentrated in degree 0).

For sufficiently acyclic resolutions P (i.e., resolutions $p : P \to X$ with p an n-acyclic map for n large), the cohomologies of objects in the category $D^b_G(X, P)$ can be used to calculate the cohomologies in $D^b_G(X)$ as indeed Bernstein and Lunts take a limit of resolution of X to obtain their definition of the equivariant derived category. The construction in [Lusztig 1993, §12.2] gives an explicit construction

of a collection of G-resolutions of a variety which can be made arbitrarily highly connected (and hence his definition is the same as that of (6-3)) however for our comparison result we need a more flexible context.

To compare the inner products on $\mathbf{f}$ and $\mathbf{U}_D$ we need to relate the geometry of periodic lattices to the cyclic quiver. The description of the relation we need goes back to [Lusztig 1990, §11], and is also used in [Ginzburg and Vasserot 1993]. Here we follow the presentation of [Lusztig 1999]. Suppose that $\boldsymbol{L}$ is a fixed lattice, and $\boldsymbol{a} \in \mathfrak{S}^n$ is such that $\dim(V_i) = a_i$ (where on the left-hand side of this equality i is understood to be taken modulo n). Consider the following spaces:

- $\mathscr{X}^{\boldsymbol{L}}_{\boldsymbol{a},\nu} = \{\boldsymbol{L}' \in \mathscr{F}_{\boldsymbol{a}} : L'_i \subseteq L_i \text{ and } \dim(L_i/L'_i) = \nu_i \text{ for all } i \in \mathbb{Z}\}$.
- $\tilde{\mathscr{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu} = \{(\boldsymbol{L}', (\phi_i)_{i\in\mathbb{Z}} : \boldsymbol{L}' \in \mathscr{X}^{\boldsymbol{L}}_{\boldsymbol{a},\nu} \text{ and } \phi_i : L_i/L'_i \to V_i \text{ is an isomorphism}\}$.
- $\mathscr{U}_{\boldsymbol{a}} \subset E_W^{\mathrm{nil}}$ consists of those representations with label $(\mu_{t,p})$ such that

$$\mu_{t,1} + \mu_{t,2} + \cdots \leq a_t \quad \text{for all } t \in \mathbb{Z}.$$

Both $\mathscr{X}^{\boldsymbol{L}}_{\boldsymbol{a},\nu}$ and $\tilde{\mathscr{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu}$ can be given a natural structure of algebraic variety (with $\mathscr{X}^{\boldsymbol{L}}_{\boldsymbol{a},\nu}$ projective), in the same fashion as for $\overline{X}^A_{\boldsymbol{L}}$ above, and the variety $\mathscr{U}_{\boldsymbol{a}}$ is an open subset of E_W^{nil} (see [Lusztig 1999, Lemma 5.8]). We then have the correspondence

$$\mathscr{X}^{\boldsymbol{L}}_{\boldsymbol{a},\nu} \xleftarrow{\alpha} \tilde{\mathscr{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu} \xrightarrow{\beta} \mathscr{U}_{\boldsymbol{a}},$$

where the map α is given by $(\boldsymbol{L}, \phi) \mapsto \boldsymbol{L}$, while the map β is given by sending $(\boldsymbol{L}, \phi)$ to the element $(y_i) \in E_V^{\mathrm{nil}}$ where y_i given by the composition

$$V_i \xrightarrow{\phi_i^{-1}} L_i/L'_i \longrightarrow L_{i+1}/L'_{i+1} \xrightarrow{\phi_{i+1}} V_{i+1} \ ,$$

with the middle map induced by the inclusion $L_i \subseteq L_{i+1}$ (the point $(y_i)_{i\in\mathbb{Z}/n\mathbb{Z}}$ is automatically nilpotent as a representation of Q by the periodicity of the flags $\boldsymbol{L}, \boldsymbol{L}'$). The map α is clearly a principal G_W-bundle, while the map β is smooth with connected fibres of dimension $\sum_{1\leq i\leq n} a_i \nu_i$ (see [Lusztig 1999, Lemma 5.11]).

Notice that if $\boldsymbol{a}$ has a_i large enough for all i, then we have $E_W^{\mathrm{nil}} = \mathscr{U}_{\boldsymbol{a}}$. In what follows we will always assume that this is the case. Moreover, the groups $G_{\boldsymbol{L}}$ (that is, the group of automorphisms of V which preserve the lattice $\boldsymbol{L}$) and G_W act naturally on $\tilde{\mathscr{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\boldsymbol{b}}$, making the maps α and β equivariant (for the actions of $G_{\boldsymbol{L}}$ on $\mathscr{X}_{\boldsymbol{a},\boldsymbol{L}}$ and G_W on E_W^{nil}). Thus since $\tilde{\mathscr{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu}$ is free G_W-space (using the map α) it is a resolution of E_W^{nil}.

Now Lusztig has shown in [Lusztig 1999, §5] that if b is an element of the canonical basis which corresponds to the simple perverse sheaf P on E_W^{nil} with associated G_W-orbit corresponding to the tableau $(\mu_{t,p})$ then $\phi_D(b)[\boldsymbol{i}_{\boldsymbol{a}}] \in \mathfrak{A}_{D,n,n}$ is the element $\{B\}$ where $b_{i,i+j} = \mu_{i,j}$ and $b_{ii} = a_i - \sum_{p>0} \mu_{i,p}$, and $b_{ij} = 0$ if

$i > j$. Moreover, we have

$$\alpha^*(\mathcal{I}_B) \cong \beta^*(P)$$

Picking an isomorphism θ (which is unique up to a scalar since A is simple) we therefore obtain an element $\tilde{P} = (\alpha^*(\mathcal{I}_B), P, \theta)$ of $D^b_G(E^{\mathrm{nil}}_W, \tilde{\mathcal{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu})$. Thus if b_1, b_2 are elements of $\mathbf{B}_\nu$ with associated tableau $(\mu_{t,p})$ and $(\rho_{t,p})$, and P_1, P_2 the corresponding perverse sheaves on E^{nil}_W, and B_1 and B_2 are the associated elements of $\mathfrak{S}^-_{D,n,n}$ then we may choose elements $\tilde{P}_k = (\mathcal{I}_{B_k}, P_k, \theta_k)$ (where $k = 1, 2$) in the category $D^b_G(E^{\mathrm{nil}}_W, \tilde{\mathcal{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu})$ such that

$$(\mathcal{I}_A, \mathcal{I}_B)_D = \sum_{j\in\mathbb{Z}} H^j_c(\tilde{P}_1 \otimes \tilde{P}_2)v^{-j},$$

where $H^j_c(\tilde{P}_1 \otimes \tilde{P}_2)$ denotes the cohomology with compact supports of the object $\tilde{P}_1 \otimes \tilde{P}_2$ in the category $D^b_G(E^{\mathrm{nil}}_W, \tilde{\mathcal{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu})$. It follows that if we consider $\boldsymbol{a}' = \boldsymbol{a} + p\boldsymbol{b}_0$ instead of $\boldsymbol{a}$ for larger and larger p, this inner product will converge to (b_1, b_2) provided the resolutions $\tilde{\mathcal{X}}^{\boldsymbol{L}}_{\boldsymbol{a}',\nu}$ become more and more highly connected as the $a'_i \to \infty$. Thus the compatibility of the inner products is reduced to showing that the maps $\beta : \tilde{X}^{\boldsymbol{L}}_{\boldsymbol{a},\nu} \to E^{\mathrm{nil}}_W$ is k-connected where $k \to \infty$ as $\min\{a_i\} \to \infty$. The rest of this section will be devoted to a proof of this result.

We wish to use a general lemma which gives a criterion for a map to be n-acyclic. Since we cannot find a precise reference for what we need, we sketch the result, though it is presumably well-known to the experts. The statement is a version of the Vietoris–Begle theorem proved in [Kashiwara and Schapira 1994, Proposition 2.7.8].

Lemma 6.9. *Suppose we have a map $f : Y \to X$ which has k-connected fibres, and that we may exhaust $Y = \bigcup_n Y_n$, by closed subsets Y_n such that $Y_n \subset \mathrm{Int}(Y_{n+1})$ and the restriction of f to Y_n is proper with k-connected fibres for all n, then $\tau_{\le k} Rf_* \circ f^* \cong \mathrm{id}$.*

Proof. In fact the reference [Kashiwara and Schapira 1994, Proposition 2.7.8] more is proved under the assumption that the fibres of f are contractible, but the weaker statement that we need is precisely what follows from the proof given there. The key point is that in the case where f is proper, one may use proper base change to conclude the vanishing of the functors $Rf^j_* f^*$ in the appropriate range from the k-connectedness of the fibres. The extension to the noncompact case then follows via the Mittag-Leffler condition. □

Since the hypotheses of Lemma 6.9 are preserved by base change, it yields a criterion for a map to be n-acyclic. We now use the above lemma to show that β is a k-acyclic map for $k = \min_{0\le i\le n-1}\{(a_i - \nu_i)\}$.

Lemma 6.10. *The fibres of $\beta : \tilde{\mathcal{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu} \to \mathcal{U}_{\boldsymbol{a}}$ are k-connected for $k = 2 \min\limits_{1\le i\le n} \{(a_i - \nu_i)\}$.*

pt

Proof. First note that we may view $X = \tilde{\mathscr{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu}$ as the set

$$\{(\varphi_i)_{i\in\mathbb{Z}} : \varphi_i : L_i/\ker(\varphi_{i-1}) \to W_i\},$$

where φ_i is surjective, $\ker(\varphi_i)$ is a lattice, and $\varphi_{i-n} = \epsilon\varphi_i\epsilon^{-1}$. The corresponding pair $(\boldsymbol{L}', (\phi_i))$ is given by $\boldsymbol{L}' = (\ker(\varphi_i))_{i\in\mathbb{Z}}$ with the isomorphisms $\phi_i : L_i/L_i' \to W_i$ induced by the surjections φ_i.

Now suppose that $y = (y_i)_{i\in\mathbb{Z}/n\mathbb{Z}} \in E_W^{\mathrm{nil}}$ is a nilpotent representation of the cyclic quiver, and that $(\varphi_i)_{i\in\mathbb{Z}}$ is in the fibre of y. Considering the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker(\varphi_{i+1}) & \longrightarrow & L_{i+1} & \xrightarrow{\varphi_{i+1}} & W_{i+1} & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow{\scriptstyle y_i} & & \\
0 & \longrightarrow & \ker(\varphi_i) & \longrightarrow & L_i & \xrightarrow{\varphi_i} & W_{i+1} & \longrightarrow & 0
\end{array}$$

we see that the restriction of φ_{i+1} is determined on L_i as it is given by $y_i \circ \varphi_i$ there. Thus given φ_i, the collection of φ_{i+1}s which induce y_i is given by choosing a surjection $\pi : L_{i+1}/L_i \to W_{i+1}/\mathrm{im}(y_i)$, and then picking a lift of the pair of maps $(\pi, y_i \circ \varphi_i)$ to a map $\varphi_{i+1} : L_i/\ker(\varphi_i) \to W_{i+1}$ (since any such lift will be a surjective map). Thus the space of such choices is homotopy equivalent to the space of surjections from L_{i+1}/L_i to $W_{i+1}/\mathrm{im}(y_i)$. This is a complex Stiefel manifold, and hence $2(a_i - \nu_i + \mathrm{rank}(y_i))$ connected.

Thus if we set $k = 2\min_{1\le i\le n}\{(a_i - \nu_i)\}$ we may view $\beta^{-1}(y)$ as an iterated sequence of fibre bundles over the space B of surjections $\{\varphi_0 : L_0 \to W_0\}$ where in each case the fibres are at least k-connected. Thus by the standard long exact sequence $\beta^{-1}(y)$ will be k-connected provided we can show that B is. Now B is the space of surjective linear maps from L_0 to W_0 which intertwine the action of ϵ with the composition $\theta = y_n y_{n-1} y_{n-2} \dots y_0 : W_0 \to W_0$ (note that since the action of ϵ is nilpotent, this shows the representation y must be also) and the following lemma shows that in fact B is at least $2(D - \nu_0) \ge 2(a_0 - \nu_0)$ connected, so we are done. □

Lemma 6.11. *Let (U, θ) be a finite-dimensional vector space U equipped with nilpotent endomorphism θ of Jordan type λ, and let L be a free $\mathbb{C}[\epsilon]$-module of rank D. Viewing U as a $\mathbb{C}[\epsilon]$-module via $\epsilon \mapsto \theta$, the space of $\mathbb{C}[\epsilon]$-module surjections $\varphi : L \to U$ is d-connected, where $d = 2(D - \ell(\lambda))$ and $\ell(\lambda)$ is the length of the partition λ.*

Proof. A $\mathsf{k}[\epsilon]$-module map $\varphi : L \to U$ is surjective if and only if the induced k-linear map $\bar{\varphi} : L/\epsilon(L) \to U/\theta(U)$ is surjective. Moreover, since the space of surjections from $L/\epsilon(L)$ to $U/\theta(U)$ is a complex Stiefel manifold of k-frames in a D dimensional space, it is $2(D - \ell(\lambda))$-connected.

Now suppose that ψ is a $\mathbb{C}$-linear map from $L/\epsilon(L) \to U/\theta(U)$. Let K denotes the D-dimensional $\mathbb{C}$-vector space spanned by a set of $\mathbb{C}[\epsilon]$-generators of L, say $\{e_1, \ldots, e_D\}$. A $\mathsf{k}[\epsilon]$-module map $\varphi : L \to U$ with $\bar{\varphi} = \psi$ is completely determined by its restriction to K, and the induced map $\varphi' : K \to U$ is given by a choice of lifts for the vectors $\{\psi(e_i)\}$ in U (where by abuse of notation we denote by ψ the composition of $L \to L/\epsilon(L) \to U/\theta(U)$), and hence the space of such surjections is clearly a vector bundle over the Stiefel manifold of surjections from $L/\epsilon L$ to $U/\theta(U)$ which proves the lemma. □

Proposition 6.12. *The map $\beta : \tilde{\mathscr{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu} \to E^{nil}_W$ is k-connected.*

Proof. To show β is a k-connected map we wish to apply Lemma 6.9. By Lemma 6.10 we know that the fibres of β are k-connected, and hence we must show that we can filter $\tilde{\mathscr{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu}$ by subvarieties $\{Y_i\}_{i\in\mathbb{N}}$ such that $\beta_{|Y_i}$ is proper while ensuring that the fibres remain k-connected. To do this we simply note that the topology of the fibres of β all come from Stiefel manifolds, and these deformation retract on to the compact Stiefel manifolds. Moreover the retraction can be done via the Gram–Schmidt process, once we endow our vector spaces with a Hermitian inner product.

More precisely, we may equip V with an Hermitian inner product (here we will assume that $\mathsf{k} = \mathbb{C}$, as in the rest of this section) so that ϵ is a unitary map (e.g., take a $\mathbb{C}[\epsilon]$-basis $\{e_1, e_2, \ldots e_D\}$ of L_0 and define the Hermitian product $\langle \cdot, \cdot \rangle^D$ by setting

$$\langle \epsilon^l e_j, \epsilon^m e_k \rangle = \delta_{j,k}\delta_{l,m}, \quad (l, m \in \mathbb{Z}, 1 \le j, k \le D),$$

Similarly we may equip the $\{W_i\}$ with Hermitian inner products. Then we have a norm function N on $\tilde{\mathscr{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu}$ given by

$$\mathrm{N}(\boldsymbol{L}, (\phi_i)) = \max_{0\le i\le n-1}\{\sup\{\|\phi_i(u)\| : u \in L_i/L'_i, \|u\| = 1\}.$$

where the norm on L_i/L'_i is induced from that on V via the canonical isomorphism $(L'_i)^\perp \cong L_i/L'_i$. Now we may set $Y_i = \{(\boldsymbol{L}, (\phi_i)) : i^{-1} \le \mathrm{N}(\boldsymbol{L}, (\phi_i)) \le i\}$. Since the map α from $\tilde{\mathscr{X}}^{\boldsymbol{L}}_{\boldsymbol{a},\nu}$ to $\mathscr{X}^{\boldsymbol{L}}_{\boldsymbol{a},\nu}$ is a principal G_W-bundle over a projective variety, and the norm condition defining Y_i clearly cuts out a compact subset of the fibres of α, it follows that Y_i is compact, and so in particular $\beta_{|Y_i}$ is proper. Thus it remains to check that the fibres of $\beta_{|Y_i}$ are still k-connected.

To do this we may use the Gram–Schmidt process to iteratively deform the linear maps in the fibres in the same manner as we checked k-connectedness via a sequence of fibre bundles. In the case of the choice of the surjection $L_0 \to W_0$ which defines L'_0 and ϕ_0, note that we need only apply Gram–Schmidt to the frame defining the map from K to $W_0/\theta(W_0)$, where $K = \mathrm{span}_{\mathbb{C}}\{e_1, \ldots, e_D\}$. □

We can now complete the geometric proof of the equality of our inner product with that in [Lusztig 1993].

Theorem 6.13. *The inner products* $\langle \cdot, \cdot \rangle$ *and* $(\cdot, \cdot)$ *on* $\dot{\mathbf{U}}$ *coincide.*

Proof. As discussed above, it is enough to know that the varieties $\tilde{\mathcal{X}}^{\boldsymbol{L}}_{\boldsymbol{a}+p\boldsymbol{b}_0,\nu}$ become more and more connected as p tends to infinity. Since the value of $k = \min_{0\leq i\leq n-1}\{(a_i + p - \nu_i)\}$ clearly tends to infinity as p does (where $\boldsymbol{a}$ is the representative of $\lambda \in X'$ lying in $\mathfrak{S}_{D,n}$) the equality of the inner products follows. □

7. A construction of the canonical basis of $\dot{\mathbf{U}}(\widehat{\mathfrak{sl}}_n)$

Lusztig [2000] defined homomorphisms

$$\psi_D : \mathfrak{A}_D \to \mathfrak{A}_{D-n},$$

which are characterised, at least on $\mathbf{U}_D$, by the conditions

- $\psi_D(E_i(D)) = E_i(D-n)$,
- $\psi_D(F_i(D)) = F_i(D-n)$,
- $\psi_D(K_{\boldsymbol{a}}(D)) = v^{\boldsymbol{a}\cdot\boldsymbol{b}_0} K_{\boldsymbol{a}}(D-n)$,

where $\boldsymbol{b}_0$ has all entries equal to 1. It follows that if we work with the root datum (X', Y'), i.e., with $\widehat{\mathfrak{sl}}_n$, then the maps ψ_D and $\phi_D : \dot{\mathbf{U}} \to \mathfrak{A}_{D,n,n}$ are compatible, that is $\psi_{D+n} \circ \phi_{D+n} = \phi_D$.

Let $\hat{\mathbf{U}} = \varprojlim_D \mathfrak{A}_D$, where the limit is taken over the projective system given by the maps $(\psi_D)_{D\in\mathbb{N}}$ described above. Since the maps ϕ_D are compatible with this system, there is a unique map $\phi : \dot{\mathbf{U}} \to \hat{\mathbf{U}}$, which factors each of the maps ϕ_D through the canonical map $\hat{\mathbf{U}} \to \mathfrak{A}_D$. Theorem 5.2 allows us to give an alternative proof of the following injectivity result which is due to Lusztig [2000].

Proposition 7.1. *The homomorphism* ϕ *is injective.*

Proof. We first note that the inner product on $\dot{\mathbf{U}}$ is nondegenerate. While this is not explicitly stated in the book [Lusztig 1993], it follows easily from the results there. For example, one may use the results of §26.2 and the nondegeneracy of the inner product defined in §19.1 which is established in Lemma 19.1.4 (all references in this sentence are to sections of [Lusztig 1993]). Now suppose that u is in the kernel of ϕ. Then for every D we have $\phi_D(u) = 0$, and hence by Theorem 5.2 we see that u is in the radical of the inner product on $\dot{\mathbf{U}}$, and hence it follows that $u = 0$. □

The modified quantum group $\dot{\mathbf{U}}$ is equipped with a canonical basis $\dot{\mathbf{B}}$ which generalises the canonical basis of $\mathbf{U}^-$. We now show that the compatibility of the inner products can be used to give an essentially self-contained construction of this basis. Let $\mathbf{A} = \mathbb{Q}(v) \cap \mathbb{Q}[\![v^{-1}]\!]$ and let $\mathbb{B}^{\pm}$ be defined by

$$\mathbb{B}^{\pm} = \{b \in \dot{\mathbf{U}}_{\mathscr{A}} : (b, b) \in 1 + v^{-1}\mathbf{A}, \bar{b} = b\}.$$

We show that this set is a signed basis of $\dot{\mathbf{U}}$. (We will also be able to choose a basis within this set.)

Remark 7.2. Lusztig [1993] showed that $\dot{\mathbf{B}}$ is "almost orthonormal" for the inner product, from which one can also deduce the (weaker) nondegeneracy statement used in the proof of Proposition 7.1. We prefer the argument given above since we wish to give a geometric construction of the canonical basis which does not presuppose its existence.

We begin by showing that $\mathbb{B}^{\pm}$ is closely related to the bases $\mathfrak{B}_D$ of the algebras $\mathfrak{A}_D$.

Proposition 7.3. *Let $b \in \mathbb{B}^{\pm}$. Then there exists λ such that $b \in \dot{\mathbf{U}}1_\lambda$. If k is the residue of $\sum_{i=1}^n \lambda_i \mod n$ then there is a $p_0 > 0$ such that for all $p > p_0$ we have $\phi_{k+pn}(b) \in \pm\mathfrak{B}_D$. Conversely, if $b \in \dot{\mathbf{U}}1_\lambda$ has $\phi_D(b) \in \pm\mathfrak{B}_{k+pn}$ for all $p > p_1$ (some $p_1 \in \mathbb{N}$) then $b \in \mathbb{B}^{\pm}$.*

Proof. Suppose that $b \in \mathbb{B}^{\pm}$. Then since the inner product $\dot{\mathbf{U}}$ is obtained as a limit from the inner products on $\mathfrak{A}_D$, we see that for large p we have (in the notation of Section 4)

$$\sum_{l=0}^{n-1} \langle b, b\rangle_{l+pn} = 1 \bmod v^{-1}\mathbb{Z}[v^{-1}].$$

Now for each l, $(0 \le l \le n-1)$ set $x_{l+pn} = \phi_{l+pn}(b)$. It is clear that x_{l+pn} is bar-invariant (for the bar involution on $\mathfrak{A}_{l+pn}$, see Remark 6.2), and lies in $\mathfrak{A}_{l+pn,\mathscr{A}}$. Thus we may write $x_{l+pn} = \sum_{i\in I} a_i\{A_i\}$ for some $a_i \in \mathscr{A}$ and $A_i \in \mathfrak{S}^{\mathrm{ap}}_{l+pn,n,n}$, where $\bar{a}_i = a_i$. Now suppose that $a_i \in v^m\mathbb{Z}[v^{-1}]$ for all $i \in I$, and m is minimal with this property. Then, using the "almost orthonormality" property that $(\{A_i\}, \{A_j\}) \in \delta_{i,j} + v^{-1}\mathbb{Z}[v^{-1}]$ (see Lemma 6.1), we see that if $J \subset I$ denotes the subset consisting of those i with $a_i = c_i v^m + \cdots$, where $c_i \ne 0$, then

$$(x_{l+pn}, x_{l+pn})_{l+pn} = \left(\sum_{i\in J} c_i^2\right) v^{2m} + \text{ lower order terms.}$$

In particular, since $(x_{l+pn}, x_{l+pn}) \in \mathbb{Z}[v^{-1}]$ we must have $m = 0$. But then since x_{l+pn} is bar-invariant, we must have $a_i \in \mathbb{Z}$ for each $i \in I$. Now since

$$\sum_{k=1}^{n-1} (x_{k+pn}, x_{k+pn}) \in 1 + v^{-1}\mathbb{Z}[v^{-1}],$$

it follows that in fact there is a $k \in \{0, 1, \ldots, n-1\}$ such that $x_{l+pn} = 0$ for $l \ne k$ and $x_{k+pn} = \pm\{A\}$ for some $A \in \mathfrak{S}_{k+pn,n,n}$. Indeed the same argument shows that the signed basis $\pm\mathfrak{B}_D$ is characterised by the properties that its elements are

bar-invariant, integral, and almost orthonormal. Note also that if $\lambda = c(A) \bmod \mathbb{Z}\boldsymbol{b}_0$ it is then easy to see that $b = b1_\lambda$ as claimed in the statement of the lemma.

The converse is easier, since we know that $\dot{\mathbf{U}}$ injects into the inverse limit of the $\mathfrak{A}_D$, so that if $\phi_D(b) \in \mathfrak{A}_{D,\mathscr{A}}$ for all $D \equiv k \bmod n$, then $b \in \dot{\mathbf{U}}_{\mathscr{A}}$, and bar invariance and the condition on (b, b) is also evident. □

To extract a basis from $\mathbb{B}^{\pm}$ we need to recall some results of Lusztig. For this we need some definitions. Let $\mathfrak{S}^-_{D,n,}$ be the set of all $B \in \mathfrak{S}_{D,n,n}$ such that $b_{ij} = 0$ for $i > j$. Let $\mathfrak{S}^+_{D,n,n}$ be the set of all $B \in \mathfrak{S}_{D,n,n}$ such that $b_{ij} = 0$ for all $i < j$. Given $A \in \mathfrak{S}_{D,n,n}$ we may define A^+ and A^- in $\mathfrak{S}^+_{D,n,n}$ and $\mathfrak{S}^-_{D,n,n}$ respectively by

$$a^-_{ij} = a_{ij} \text{ if } i < j, \quad a^-_{ij} = 0 \text{ if } i > j, \quad a^-_{ii} = \sum_{j \in \mathbb{Z}, i \geq j} a_{ij},$$

$$a^+_{ij} = a_{ij} \text{ if } i > j, \quad a^+_{ij} = 0 \text{ if } i > j, \quad a^-_{ii} = \sum_{k \in \mathbb{Z}, k \leq i} a_{ki}.$$

Lemma 7.4. *Let $A \in \mathfrak{S}_{D,n,n}$.*

(1) *If $A \in \mathfrak{S}^{\pm}_{D,n,n}$ then $\psi_D(\{A\}) = \{A - I\}$.*

(2) *For any $A \in \mathfrak{S}_{D,n,n}$ we have*

$$\{A^-\}\{A^+\} = \{A\} + \sum_{A' < A} c_{A,A'}\{A'\},$$

where $c_{A,A'} \in \mathbb{Z}[v, v^{-1}]$.

(3) *For any $A \in \mathfrak{S}_{D,n,n}$ we have*

$$\psi_D(\{A\}) = \{A - I\} + \sum_{A' < A} e_{A,A'}\{A' - I\},$$

where $\{A - I\}$ is interpreted as 0 if $A - I$ does not lie in $\mathfrak{S}_{D,n,n}$, and likewise for $\{A' - I\}$.

Proof. In [Lusztig 2000, §3.7] the elements of $A \in \mathfrak{S}^{\pm}_{D,n,n}$ are related to perverse sheaves on quiver varieties attached to the cyclic quiver, giving a geometric interpretation of part of the map from $\dot{\mathbf{U}}$ to $\mathfrak{A}_{D,n,n}$ (see also Section 6 and [Lusztig 1999, §5] for more details). From this and the compatibility of the maps ϕ_D and ψ_D, part (1) readily follows. Part (2) is [Lusztig 1999, Proposition 4.11]. The last part follows by induction on the partial order $<$ using parts (1) and (2) together with the fact that $(A - I)^{\pm} = A^{\pm} - I$. □

Definition 7.5. Next we note that the partial order $\leq$ has a combinatorial cousin $\preceq$ which we can make more explicit: Given $A, B \in \mathfrak{S}^{n,n}$ say $A \preceq B$ if for all $i < j \in \mathbb{Z}$ we have

$$\sum_{r \leq i; s \geq j} a_{r,s} \leq \sum_{r \leq i; s \geq j} b_{r,s},$$

and for any $i > j$ we have

$$\sum_{r\geq i; s\leq j} a_{r,s} \leq \sum_{r\geq i; s\leq j} b_{r,s}.$$

It is easy to check that if $A, B \in \mathfrak{S}_{D,n,n}$ and $A \leq B$ then $A \preceq B$ (see for example [Beilinson et al. 1990, Lemma 3.6] and [Lusztig 1999, §1.6]). Also, if we write ${}_pA = A + pI$, then it is clear that $A \preceq B$ if and only if ${}_pA \preceq {}_pB$. Moreover, crucially in what follows, given $A \in \mathfrak{S}^{n,n}$ the set

$$\{B \in \mathfrak{S}^{n,n} : B \preceq A,\ r(B) = r(A),\ c(B) = c(A)\}$$

is finite.

We now resolve the ambiguity of signs in the definition of $\mathbb{B}^{\pm}$ and extract a basis from the signed basis $\mathbb{B}^{\pm}$.

Corollary 7.6. *Let*

$$\mathbb{B} = \left\{b \in \mathbb{B}^{\pm} : \phi_D(b) \in \mathfrak{B}_D \cup \{0\} \text{ for all } D \gg 0\right\}.$$

Then $\mathbb{B}^{\pm} = \mathbb{B} \sqcup (-\mathbb{B})$. *Moreover, if* $\phi_{k+pn}(b) = \{A_{k+pn}\}$, *where* $A_{k+pn} \in \mathfrak{S}_{D,n,n}$ *for all* $p > p_0$ *say, then* $A_{k+(p+1)n} = A_{k+pn} + I$.

Proof. It is only necessary to show that $\mathbb{B}$ is well-defined. Suppose $b \in \mathbb{B}^{\pm}$. The previous proposition shows that if $b = b1_\lambda$, and $k = \sum_{i=1}^n \lambda_i$, then for large enough p, say $p \geq p_0$, we have $\phi_{k+pn}(b) \in \pm\mathfrak{B}_{k+pn}$, and moreover $\phi_D(b) = 0$ if D is not congruent to k modulo n. Thus we have $\phi_{k+pn}(b) = \epsilon_{k+pn}\{A_{k+pn}\}$ where $\epsilon_{k+pn} \in \{\pm 1\}$ and $A_{k+pn} \in \mathfrak{S}_{k+pn,n,n}$ for all $p \geq p_0$. But now by part (3) of Lemma 7.4 we have

$$\psi_{k+(p+1)n}(\{A_{k+(p+1)n}\}) = \{A_{k+(p+1)n} - I\} + \sum_{B\preceq A_{k+pn}} e_B\{B\}, \quad (e_B \in \mathcal{A}),$$

whereas $\psi_{k+(p+1)n}(\phi_{k+(p+1)n}(b)) = \phi_{k+pn}(b) = \epsilon_{k+pn}\{A_{k+pn}\}$. Comparing these two expressions we conclude that $\epsilon_{k+(p+1)n} = \epsilon_{k+pn}$ and $\{A_{k+(p+1)n}\} = \{A_{k+pn}\} + I$ as claimed. □

Corollary 7.7. *The set* $\mathbb{B}$ *is almost orthonormal, that is*

$$(b_1, b_2) \in \delta_{b_1,b_2} + v^{-1}\mathbb{Z}[\![v^{-1}]\!].$$

Thus the set $\mathbb{B}$ *is linearly independent.*

Proof. Let $b_1, b_2 \in \mathbb{B}$. Take $\lambda \in X'$ so that $b_1 = b_1 1_\lambda$. Then either $b_2 1_\lambda = 0$, in which case the corollary holds trivially, or $b_2 = b_2 1_\lambda$. In that case, we see from

Corollary 7.6 that we may find a $p_0 \in \mathbb{N}$ and $A, B \in \mathfrak{S}^{n,n}$ so that $\phi_{p_0+pn}(b) = \{{}_pA\}$ and $\phi_{p_0+pn}(b_2) = \{{}_pB\}$ for all $p \geq 0$. But then it follows from Lemma 6.1 that

$$(\{{}_pA\}, \{{}_pB\}) \in \delta_{A,B} + v^{-1}\mathbb{Z}[\![v^{-1}]\!].$$

for all p, and hence taking the limit we obtain the same result for b_1, b_2. To see that this implies the linear independence of the set $\mathbb{B}$, consider a dependence involving the minimal number of elements of $\mathbb{B}$:

$$\sum_{j=1}^{k} p_j b_j = 0,$$

where by clearing denominators if necessary we may assume that $p_k \in \mathbb{Z}[v, v^{-1}]$ (and by minimality they are all nonzero) and $b_k \in \mathbb{B}$. We may moreover assume, multiplying through by an appropriate power of v, that $p_i = n_i + v^{-1}\mathbb{Z}[v^{-1}]$, where $n_i \in \mathbb{Z}$, and, reordering if necessary, that $n_1 \neq 0$. Pick D large enough so that

$$\sum_{l=0}^{n-1} (\phi_D(b_r), \phi_D(b_s))_{D+l} = (b_r, b_s) \mod v^{-1}\mathbb{Z}[\![v^{-1}]\!] \quad \text{for} \quad 1 \leq r, s \leq k.$$

and moreover that for each j we have $\phi_D(b_j) = \{B_j\}$ for some $B_j \in \mathfrak{S}_{D,n,n}$. Then

$$\begin{aligned} 0 = \left(\sum_{r=1}^{k} p_r b_r, \sum_{s=1}^{k} p_s b_s \right) &= \sum_{1 \leq r,s \leq k} p_r p_s (b_r, b_s) \\ &\equiv \sum_{1 \leq r,s \leq k} p_r p_s (\{B_r\}, \{B_s\})_D \mod v^{-1}\mathbb{Z}[v^{-1}] \\ &\equiv \sum_{1 \leq r \leq k} n_r^2 \mod v^{-1}\mathbb{Z}[v^{-1}], \end{aligned}$$

which is a contradiction, since $n_1 \neq 0$. □

We now show that if $A \in \mathfrak{S}^{n,n}$ then for large enough p there is a unique $b \in \mathbb{B}$ such that $\phi_D(b) = \{{}_pA\}$ (where $D = \sum_{i \in [1,n], j \in \mathbb{Z}} a_{ij} + pn$), and hence by Corollary 7.6 it will also follows that for large enough p we have $\psi_D(\{{}_pA\}) = \{{}_{p-1}A\}$. We need to recall the relation between the canonical basis $\mathbf{B}$ of $\mathbf{U}^-$ and $\mathfrak{B}_D$. Recall from Section 6 that the representation theory of the cyclic quiver allows us to parametrise $\mathbf{B}$ by tableaux $(\mu_{t,p})_{t \in \mathbb{Z}, p \in \mathbb{N}}$, where $\mu_{t,p} \in \mathbb{N}$ and $\mu_{t,p} = \mu_{t-n,p}$ for all $t \in \mathbb{Z}$ and for fixed t only finitely many of the $\mu_{t.p}$ are nonzero. The ν-graded part $\mathbf{B}_\nu$ is then indexed by Σ_ν.

The correspondence described in Section 6 gives a bijection between those $(\mu_{t,p})$ in Σ_ν satisfying

$$\mu_{i,1} + \mu_{i,2} + \cdots \leq a_i \quad \text{for all } i,$$

and the orbits in corresponding to matrices $B \in \mathfrak{S}^-_{D,n,n}$ with $r(B) = \boldsymbol{a}$. (Note that if the integers a_i are sufficiently positive, this gives an injection from $\mathbf{B}_\nu$ into $\mathfrak{S}^-_{D,n,n}$.) Using the same correspondence, composed with the transpose map Ψ, we obtain a similar correspondence between (appropriate subsets of) $\mathbf{B}_\nu$ and elements of $\mathfrak{S}^+_{D,n,n}$. These can be combined to give a correspondence between the set of triples $\mathcal{T} = \{(b_1, b_2, \lambda) : b_1, b_2 \in \mathbf{B}, \lambda \in X\}$ and elements of $\mathfrak{S}^{n,n}$ as follows: the elements b_1, b_2 corresponds to tableau $(\mu_{t,p})$ and $(\rho_{t,p})$ say, and we define $A = A(b_1, b_2, \lambda) \in \mathcal{S}^{n,n}$ by setting

$$a_{ij} = \begin{cases} \mu_{i,j-i} & \text{if } i < j, \\ \rho_{j,i-j} & \text{if } i > j, \\ \lambda_i - \sum_{t\geq 1} \mu_{i,t} - \sum_{s\geq 1} \rho_i & \text{if } i = j. \end{cases}$$

We will write b_A for the element $b_1^+ 1_\lambda b_2^- \in \dot{\mathbf{U}}$, and ${}_D b_A$ for its image under ϕ_D. It follows from the [Lusztig 1999, §5] and [Lusztig 1999, Proposition 4.11] that if $\sum_{i=1}^n \lambda_i = D$ and the entries of $A(b_1, b_2, \lambda)$ are all nonnegative, then

$${}_D b_A = \{{}_p A\} + \sum_{B \prec_p A} e_{B,{}_p A}\{B\} \tag{7-1}$$

Proposition 7.8. *Let $A \in \mathfrak{S}^{n,n}$. For large enough p we have*

$$\psi_D(\{{}_p A\}) = \{{}_{p-1} A\}$$

Proof. Via the bijection described above between $\mathcal{T}$ and $\mathfrak{S}^{n,n}$, we may find a subset $\mathcal{T}_{\boldsymbol{a}}$ of $\mathcal{T}$ such that $\{A(b_1, b_2, \boldsymbol{a})\}$ is a basis of $\mathfrak{A}_D[\boldsymbol{i}_{\boldsymbol{a}}]$ as $(b_1, b_2, \boldsymbol{a})$ runs over the set $\mathcal{T}_{\boldsymbol{a}}$. Then the elements ${}_D b_A$ are clearly also a basis of $\mathfrak{A}_D[\boldsymbol{i}_{\boldsymbol{a}}]$ since they are related to the elements $\{A\}$ by an upper triangular matrix, and moreover they satisfy

(1) $\overline{{}_D b_A} = {}_D b_A$,

(2) ${}_D b_A \in \mathbf{U}_{D,\mathcal{A}}$.

As in the proof of Proposition 7.3, the basis $\{\{A\} : A \in \mathfrak{S}_{D,n,n}\}$ is characterised up to sign by the properties of being bar-invariant, integral (that is, contained in $\mathbf{U}_{D,\mathcal{A}}$), and being almost orthonormal, so that

$$(\{A\}, \{B\})_D \in \delta_{A,B} + v^{-1}\mathbb{Z}[v^{-1}].$$

(In fact, Proposition 7.3 shows that less than this characterises $\pm\mathfrak{B}_D$).

We now show that one can obtain $\{A\}$ from ${}_D b_A$ by a Gram–Schmidt style process. Indeed if A is minimal for the ordering $\preceq$, then clearly $\{A\} = b_A$. Thus we consider the following claim:

- For each $A \in \mathfrak{S}^{n,n}$, there is a $p_0 \in \mathbb{Z}$ such that for all $p > p_0$ we have

$$\{{}_pA\} = {}_Db_A + \sum_{A' \prec A} d_{A',A\,D} b_{A'}.$$

where $d_{A',A} \in \mathscr{A}$ do not depend on p, and $D = pn + \sum_{i,j:1\le i\le n} a_{ij}$.

The proof of the proposition now follows immediately since $\psi_D({}_Db_A) =_{D-n} b_A$. We show this by induction on $\preceq$: if A is minimal, then (7-1) implies that $b_A = \{A\}$, and we are done. Thus suppose that the result is known for all $B \prec A$, and let I be the (finite) set

$$\{B \in \mathfrak{S}^{n,n} : B \preceq A, r(A) = r(B), c(A) = c(B)\}.$$

Now for x in the span of $\{\{B\} : B \in I\}$, set $N(x) = \max\{\nu(x, \{B\})_D : B \in I, B \neq A\}$, where for $f \in \mathscr{A}$ we let $\nu(f)$ denote the highest power of v occurring in f. Let $N = N(b_A)$, and suppose that $N \geq 0$. Let J denotes the subset of I for which $\nu(b_A, \{B\}) = N$, so that if $B \in J$ we have

$$(b_A, \{B\})_D = c_B v^N + \text{ lower order terms} \quad (c_B \in \mathbb{Z}).$$

Now $(\{B\}, \{B\})_D \in 1 + v^{-1}\mathbb{Z}[v^{-1}]$, so we may recursively solve for

$$a_B \in v^{-N}\mathbb{Z}[v] \cap \mathbb{Z}[v^{-1}]$$

such that $a_B.(\{B\}, \{B\})_D \in 1 + v^{-N-1}\mathbb{Z}[v^{-1}]$. It follows immediately that we may find $e_B \in \mathscr{A}$ such that $\bar{e}_B = e_B$ and $e_B = c_B v^N a_B \bmod v^{-1}\mathbb{Z}[v^{-1}]$. Then we set

$$b'_A = b_A - \sum_{B \in J} e_B \{B\}.$$

It follows from the almost orthonormality of the $\{B\}$ that $(b'_A, \{B\})_D \in v^{N-1}\mathbb{Z}[v^{-1}]$, and b'_A is again bar-invariant, lies in $\mathbf{U}_{D,\mathscr{A}}$, and satisfies $N(b'_A) < N$. We may thus iterate this construction to obtain an element b''_A which has $N(b''_A) \leq -1$, is bar-invariant, and lies in $\mathbf{U}_{D,\mathscr{A}}$. But then we claim that we must have $b''_A = \{A\}$. Indeed we know from (7-1) that we can write

$$b''_A = \{A\} + \sum_{B \prec A} f_B \{B\}$$

for some $f_B \in \mathscr{A}$ with $\bar{f}_B = f_B$. If it is not the case that $f_B = 0$ for all B, then there is some B with $\nu(f_B) \geq 0$ maximal, whence we see that $\nu(b''_A, \{B\})_D \geq 0$ which is a contradiction. Thus $b''_A = \{A\}$ as required.

Now examining the above process, we see that it uses only the values of $(b_A, \{B\})_D$ down to order to $v^{-N(b_A)}\mathbb{Z}[v^{-1}]$, and by induction we see that these, for large enough p are determined by the values of $(b_A, b_B)_D$, down to some possibly lower order (determined by the coefficients $d_{B,C}$). Since the values of $(b_A, b_B)_D$ converge in $\mathbb{Z}((v^{-1}))$ we see that we may find a large enough p_0 so that $\{{}_pA\}$ is

a linear combination of $\{\phi_D(b_{A'}) : A' \preceq A\}$ with coefficients independent of p as required. □

We can now show that the set $\mathbb{B}$ is a basis of $\dot{\mathbf{U}}$.

Theorem 7.9. *$\mathbb{B}$ is a basis of $\dot{\mathbf{U}}$.*

Proof. Notice first that given any $b \in \mathbb{B}$, Proposition 7.3 implies that $\phi_D(b) \in \mathfrak{B}_D \cup \{0\}$ for large enough D, and is nonzero provided D has a fixed residue modulo n. By Corollary 7.7 we know that the elements of $\mathbb{B}$ are linearly independent, so we need only show that they span $\dot{\mathbf{U}}$. To do this it is enough to show that the element $b_1^+ b_2^- 1_\lambda$ for $b_1, b_2 \in \mathbf{B}$ and $\lambda \in X$ lie in the span of $\mathbb{B}$, since they form a basis for $\dot{\mathbf{U}}$. But the claim in the proof of Proposition 7.8 shows that we may find an element of $\mathbb{B}$ which is a linear combination of such basis elements with leading coefficient 1, so that the matrix relating the two sets is invertible and $\mathbb{B}$ indeed spans $\dot{\mathbf{U}}$. □

Remark 7.10. The results of [Lusztig 1993, §26.3] then show that $\mathbb{B} = \dot{\mathbf{B}}$, and thus the results of this section give a new proof of the conjecture made in [Lusztig 1999, §9.3], which was originally proved by Schiffmann and Vasserot [2000]. Our goal here was to construct the canonical basis purely within the context of the inverse system $\mathbf{U}_D$; thus, unlike Schiffmann and Vasserot, we do not need to assume the existence of $\dot{\mathbf{B}}$, nor use any properties of crystal bases. It should be noted however that by using results of Kashiwara on global crystal bases, those authors have obtained a more precise result (also conjectured in [2000]) saying that the maps ϕ_D are all compatible with the canonical basis; i.e., if $b \in \dot{\mathbf{B}}$ then $\phi_D(b) \in \mathfrak{B}_D \cup \{0\}$, and moreover the kernel of ϕ_D is spanned by a subset of $\dot{\mathbf{B}}$. The results of this section show that this theorem would also follow if we could show that the maps ψ_D are compatible with the bases $\mathbf{B}_D$ and $\mathbf{B}_{D-n}$, a question which can be phrased purely geometrically (in terms of perverse sheaves). Note that it is *not* true that the maps ψ_D send $\mathfrak{B}_D$ to $\mathfrak{B}_{D-n} \cup \{0\}$, as was pointed out already in [Lusztig 2000, 1.12]. It is possible to give a construction of the maps ψ_D in the context of perverse sheaves on the ind-varieties $\mathscr{F}_{\boldsymbol{a}}$, (i.e., to show that there exists a functor on the derived category that preserves perverse sheaves (up to shift) and induces ψ_D on the Grothendieck group which moreover is compatible with the "convolution" on $\mathscr{K}_{D,n,n}$), but it is not immediately clear why this functor preserves simple objects.

8. A positivity result

We may combine Theorem 5.2 and Proposition 6.5 to prove a positivity result for the inner product of two elements of $\dot{\mathbf{B}}$. This has been conjectured by Lusztig for all types.

Theorem 8.1. *Let $b_1, b_2 \in \dot{\mathbf{B}}$. Then*

$$(b_1, b_2) \in \mathbb{N}[\![v^{-1}]\!] \cap \mathbb{Q}(v).$$

Proof. We may assume that there is a $\lambda \in X$ such that $b_1 1_\lambda = b_1$, and $b_2 1_\lambda = b_2$. Let $k \in \{0, 1, \ldots, n-1\}$ be such that $\sum_{j=1}^{n} \lambda_j = k \bmod n$. Then

$$(b_1, b_2) = \lim_{p \to \infty} (\phi_{k+pn}(b_1), \phi_{k+pn}(b_2))_{k+pn}$$

By Proposition 7.3 we know that for all large enough D we have $\phi_D(b_1), \phi_D(b_2)$ are in $\mathfrak{B}_D$, hence it is clear from (6-1) that

$$(\phi_{k+pn}(b_1), \phi_{k+pn}(b_2))_{k+pn} \in \mathbb{N}[v, v^{-1}].$$

However, it follows also from Lemma 6.1 that the left-hand side is in fact in $\mathbb{N}[v^{-1}]$ (this can also be seen directly, using the definition of intersection cohomology sheaves). Hence (b_1, b_2) is the limit of elements of $\mathbb{N}[v^{-1}]$, and the statement follows. □

Remark 8.2. All the results of this paper have analogues for the nonaffine case, which can be proved in exactly the same way. The module V is replaced by a D-dimensional vector space over $\Bbbk$, and the space $\mathscr{F}^n$ of n-step periodic lattices should be replaced by the space of n-step flags in that vector space. In this case the algebra corresponding to $\mathbf{U}_D$ is actually equal to the algebra analogous to $\mathfrak{A}_D$, hence the results are sometimes more straightforward.

Acknowledgements

This paper is based on a chapter of my thesis, written under the direction of George Lusztig. I would like to thank him both for posing the problem that led to this paper and for our many conversations about the contents of this paper and much else besides. I would also like to thank Jared Tanner for a useful conversation.

References

[Beilinson et al. 1990] A. A. Beilinson, G. Lusztig, and R. MacPherson, "A geometric setting for the quantum deformation of GL_n", *Duke Math. J.* **61**:2 (1990), 655–677. MR 1074310 (91m:17012) Zbl 0713.17012

[Bernstein and Lunts 1994] J. Bernstein and V. Lunts, *Equivariant sheaves and functors*, Lecture Notes in Mathematics **1578**, Springer, Berlin, 1994. MR 95k:55012 Zbl 0808.14038

[Ginzburg and Vasserot 1993] V. Ginzburg and É. Vasserot, "Langlands reciprocity for affine quantum groups of type A_n", *Internat. Math. Res. Notices* **1993**:3 (1993), 67–85. MR 1208827 (94j:17011 Zbl 0785.17014

[Grojnowski and Lusztig 1993] I. Grojnowski and G. Lusztig, "A comparison of bases of quantized enveloping algebras", pp. 11–19 in *Linear algebraic groups and their representations* (Los Angeles, CA, 1992), edited by R. S. Elman et al., Contemp. Math. **153**, Amer. Math. Soc., Providence, RI, 1993. MR 1247495 (94m:17012) Zbl 1009.17502

[Kashiwara 1991] M. Kashiwara, "On crystal bases of the Q-analogue of universal enveloping algebras", *Duke Math. J.* **63**:2 (1991), 465–516. MR 93b:17045 Zbl 0739.17005

[Kashiwara and Schapira 1994] M. Kashiwara and P. Schapira, *Sheaves on manifolds*, Grundlehren Math. Wiss. **292**, Springer, Berlin, 1994. MR 95g:58222

[Lang and Weil 1954] S. Lang and A. Weil, "Number of points of varieties in finite fields", *Amer. J. Math.* **76** (1954), 819–827. MR 16,398d Zbl 0058.27202

[Lusztig 1990] G. Lusztig, "Canonical bases arising from quantized enveloping algebras", *J. Amer. Math. Soc.* **3**:2 (1990), 447–498. MR 90m:17023 Zbl 0703.17008

[Lusztig 1991] G. Lusztig, "Quivers, perverse sheaves, and quantized enveloping algebras", *J. Amer. Math. Soc.* **4**:2 (1991), 365–421. MR 1088333 (91m:17018) Zbl 0738.17011

[Lusztig 1992] G. Lusztig, "Canonical bases in tensor products", *Proc. Nat. Acad. Sci. U.S.A.* **89**:17 (1992), 8177–8179. MR 93j:17033 Zbl 0760.17011

[Lusztig 1993] G. Lusztig, *Introduction to quantum groups*, vol. 110, Progress in Mathematics, Birkhäuser Boston Inc., Boston, MA, 1993. MR 1227098 (94m:17016)

[Lusztig 1999] G. Lusztig, "Aperiodicity in quantum affine $\mathfrak{gl}_n$", *Asian J. Math.* **3**:1 (1999), 147–177. MR 1701926 (2000i:17027)

[Lusztig 2000] G. Lusztig, "Transfer maps for quantum affine $\mathfrak{sl}_n$", pp. 341–356 in *Representations and quantizations* (Shanghai, 1998), edited by Z. L. Jian-pan Wang, China High. Educ. Press, Beijing, 2000. MR 1802182 (2002f:17026)

[Schiffmann and Vasserot 2000] O. Schiffmann and E. Vasserot, "Geometric construction of the global base of the quantum modified algebra of $\widehat{\mathfrak{gl}}_n$", *Transform. Groups* **5**:4 (2000), 351–360. MR 1800532 (2001k:17029) Zbl 0978.17007

Communicated by Edward Frenkel
Received 2010-10-03 Revised 2011-05-08 Accepted 2011-06-30

mcgerty@maths.ox.ac.uk *Mathematical Institute, University of Oxford, 24-29 St Giles', Oxford, OX1 3LB, United Kingdom*

msp

ALGEBRA AND NUMBER THEORY 6:6 (2012)
dx.doi.org/10.2140/ant.2012.6.1133

Combinatorics of the tropical Torelli map

Melody Chan

This paper is a combinatorial and computational study of the moduli space M_g^{tr} of tropical curves of genus g, the moduli space A_g^{tr} of principally polarized tropical abelian varieties, and the tropical Torelli map. These objects were studied recently by Brannetti, Melo, and Viviani. Here, we give a new definition of the category of stacky fans, of which M_g^{tr} and A_g^{tr} are objects and the Torelli map is a morphism. We compute the poset of cells of M_g^{tr} and of the tropical Schottky locus for genus at most 5. We show that A_g^{tr} is Hausdorff, and we also construct a finite-index cover for the space A_3^{tr} which satisfies a tropical-type balancing condition. Many different combinatorial objects, including regular matroids, positive-semidefinite forms, and metric graphs, play a role.

1. Introduction

This paper is a combinatorial and computational study of the tropical moduli spaces M_g^{tr} and A_g^{tr} and the tropical Torelli map.

There is, of course, a vast (to say the least) literature on the subjects of algebraic curves and moduli spaces in algebraic geometry. For example, two well-studied objects are the moduli space $\mathcal{M}_g$ of smooth projective complex curves of genus g and the moduli space $\mathcal{A}_g$ of g-dimensional principally polarized complex abelian

MSC2010: primary 14T05; secondary 14H10, 05C30.

Keywords: tropical geometry, tropical curves, metric graphs, Torelli map, moduli of curves, abelian varieties.

varieties. The Torelli map

$$t_g : \mathcal{M}_g \to \mathcal{A}_g$$

sends a genus-g algebraic curve to its Jacobian, which is a certain g-dimensional complex torus. The image of t_g is called the Torelli locus or the Schottky locus. The problem of how to characterize the Schottky locus inside $\mathcal{A}_g$ is already very deep. See, for example, [Grushevsky 2010].

The perspective we take in this paper is the perspective of tropical geometry [Maclagan and Sturmfels 2009]. From this viewpoint, one replaces algebraic varieties with piecewise-linear or polyhedral objects. These latter objects are amenable to combinatorial techniques, but they still carry information about the former ones. Roughly speaking, the information they carry has to do with what is happening "at the boundary" or "at the missing points" of the algebraic object.

For example, the tropical analogue of $\mathcal{M}_g$, denoted M_g^{tr}, parametrizes certain weighted metric graphs, and has a poset of cells corresponding to the boundary strata of the Deligne–Mumford compactification $\overline{\mathcal{M}}_g$ of $\mathcal{M}_g$. Under this correspondence, a stable curve C in $\overline{\mathcal{M}}_g$ is sent to its so-called dual graph. The irreducible components of C, weighted by their geometric genus, are the vertices of this graph, and each node in the intersection of two components is recorded with an edge. The correspondence in genus 2 is shown in Figure 1. A rigorous proof of this correspondence was given in [Caporaso 2012, Section 5.3].

We remark that the correspondence above yields dual graphs that are just graphs, not metric graphs. One can refine the correspondence using Berkovich analytification, whereby an algebraic curve over a complete nonarchimedean valued field is associated to its Berkovich skeleton, which is intrinsically a metric graph. In this way, one obtains a map between classical and tropical moduli spaces. This very interesting perspective is developed by Baker, Payne, and Rabinoff in [Baker et al. 2011]; see Section 5 in particular.

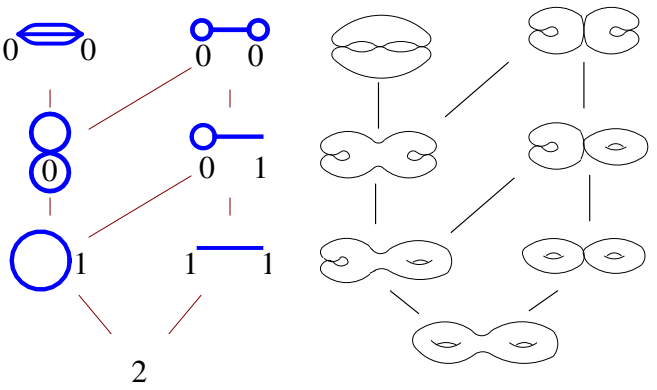


Figure 1. Posets of cells of M_2^{tr} (left) and of $\overline{\mathcal{M}}_2$ (right).

The starting point of this paper is the article [BMV 2011], by Brannetti, Melo, and Viviani, where the authors rigorously define a plausible category for tropical moduli spaces called stacky fans. (The term "stacky fan" originates there, and is unrelated, as far as we know, to the construction of [Borisov et al. 2005]). Those authors further define the tropical versions M_g^{tr} and A_g^{tr} of $\mathcal{M}_g$ and $\mathcal{A}_g$ and a tropical Torelli map between them, and prove many results about these objects, some of which we will review here.

Preceding [BMV 2011] are the foundational papers [Mikhalkin 2006; Mikhalkin and Zharkov 2008], in which tropical curves and Jacobians were first introduced and studied in detail. The notion of tropical curves in [BMV 2011] is slightly different from the original definition, in that curves now come equipped with vertex weights. We should also mention the work of Caporaso [2012], who proves geometric results on M_g^{tr} considered just as a topological space, and Caporaso and Viviani [2010], who prove a tropical Torelli theorem stating that the tropical Torelli map is "mostly" injective, as originally conjectured in [Mikhalkin and Zharkov 2008].

In laying the groundwork for the results we will present here, we ran into some inconsistencies in [BMV 2011]. It seems that the definition of a stacky fan there is inadvertently restrictive. In fact, it excludes M_g^{tr} and A_g^{tr} themselves from being stacky fans. Also, there is a topological subtlety in defining A_g^{tr}, which we will address in Section 4D. Thus, we find ourselves doing some foundational work here too.

We begin in Section 2 by recalling the definition in [BMV 2011] of the tropical moduli space M_g^{tr} and presenting computations, summarized in Theorem 2.13, for $g \leq 5$. With M_g^{tr} as a motivating example, we attempt a better definition of stacky fans in Section 3. In Section 4, we define the space A_g^{tr}, recalling the beautiful combinatorics of Voronoi decompositions along the way, and prove that it is Hausdorff. Note that our definition of this space, Definition 4.10, is different from the one in [BMV 2011, §4.2], and corrects a minor error there. In Section 5, we study the combinatorics of the zonotopal subfan. We review the tropical Torelli map in Section 6; Theorem 6.4 presents computations on the tropical Schottky locus for $g \leq 5$. Tables 1 and 2 compare the number of cells in the stacky fans M_g^{tr}, the Schottky locus, and A_g^{tr} for $g \leq 5$. In Section 7, we partially answer a question suggested by Diane Maclagan: we give finite-index covers of A_2^{tr} and A_3^{tr} that satisfy a tropical-type balancing condition.

2. The moduli space of tropical curves

In this section, we review the construction in [BMV 2011] of the moduli space of tropical curves of a fixed genus g (see also [Mikhalkin 2006]). This space is

denoted M_g^{tr}. Then, we present explicit computations of these spaces in genus up to 5.

We will see that the moduli space M_g^{tr} is not itself a tropical variety, in that it does not have the structure of a balanced polyhedral fan [Maclagan and Sturmfels 2009, Definition 3.3.1]. That would be too much to expect, as it has automorphisms built into its structure that precisely give rise to "stackiness." Contrast this with the situation of moduli space $M_{0,n}$ of tropical rational curves with n marked points, constructed and studied in [Speyer and Sturmfels 2004; Mikhalkin 2007; Gathmann et al. 2009]. As expected by analogy with the classical situation, this latter space is well known to have the structure of a tropical variety that comes from the tropical Grassmannian $Gr(2, n)$.

2A. ***Definition of tropical curves.*** Before constructing the moduli space of tropical curves, let us review the definition of a tropical curve.

First, recall that a *metric graph* is a pair (G, l), where G is a finite connected graph, loops and parallel edges allowed, and l is a function

$$l : E(G) \to \mathbb{R}_{>0}$$

on the edges of G. We view l as recording lengths of the edges of G. The *genus* of a graph G is the rank of its first homology group:

$$g(G) = |E| - |V| + 1.$$

Definition 2.1. A *tropical curve* C is a triple (G, l, w), where (G, l) is a metric graph (so G is connected), and w is a weight function

$$w : V(G) \to \mathbb{Z}_{\geq 0}$$

on the vertices of G, with the property that every weight-zero vertex has degree at least 3.

Definition 2.2. Two tropical curves (G, l, w) and (G', l', w') are isomorphic if there is an isomorphism of graphs $G \xrightarrow{\cong} G'$ that preserves edge lengths and preserves vertex weights.

We are interested in tropical curves only up to isomorphism. When we speak of a tropical curve, we will really mean its isomorphism class.

Definition 2.3. Given a tropical curve $C = (G, l, w)$, write

$$|w| := \sum_{v \in V(G)} w(v).$$

Then the *genus* of C is defined to be

$$g(C) = g(G) + |w|.$$

In this paper, we will restrict our attention to tropical curves of genus at least 2.

The *combinatorial type* of C is the pair (G, w), in other words, all of the data of C except for the edge lengths.

Remark 2.4. Informally, we view a weight of k at a vertex v as k loops, based at v, of infinitesimally small length. Each infinitesimal loop contributes once to the genus of C. Furthermore, the property that only vertices with positive weight may have degree 1 or 2 amounts to requiring that, were the infinitesimal loops really to exist, every vertex would have degree at least 3.

Permitting vertex weights will ensure that the moduli space M_g^{tr}, once it is constructed, is complete. That is, a sequence of genus-g tropical curves obtained by sending the length of a loop to zero will still converge to a genus-g curve. Furthermore, permitting vertex weights allows the combinatorial types of genus-g tropical curves to correspond precisely to dual graphs of stable curves in $\overline{\mathcal{M}}_g$, as discussed in the introduction and in [Caporaso 2012, §5.3]. See Figure 1.

Figure 2 shows an example of a tropical curve C of genus 3. Note that if we allow the edge lengths l to vary over all positive real numbers, we obtain all tropical curves of the same combinatorial type as C. This motivates our construction of the moduli space of tropical curves below. We will first group together curves of the same combinatorial type, obtaining one cell for each combinatorial type. Then, we will glue our cells together to obtain the moduli space.

2B. ***Definition of the moduli space of tropical curves.*** Fix $g \geq 2$. Our goal now is to construct a moduli space for genus-g tropical curves, that is, a space whose points correspond to tropical curves of genus g and whose geometry reflects the geometry of the tropical curves in a sensible way. The following construction is due to [BMV 2011].

First, fix a combinatorial type (G, w) of genus g. What is a parameter space for all tropical curves of this type? Our first guess might be a positive orthant $\mathbb{R}_{>0}^{|E(G)|}$, that is, a choice of positive length for each edge of G. But we have overcounted by symmetries of the combinatorial type (G, w). For example, in Figure 2, $(a, b, c) = (1, 2, 3)$ and $(a, b, c) = (1, 3, 2)$ give the same tropical curve.

Furthermore, with foresight, we will allow lengths of zero on our edges as well, with the understanding that a curve with some zero-length edges will soon be

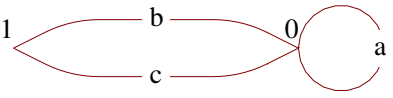


Figure 2. A tropical curve of genus 3. Here, a, b, and c are fixed positive real numbers.

identified with the curve obtained by contracting those edges. This suggests the following definition.

Definition 2.5. Given a combinatorial type (G, w), let the *automorphism group* $\mathrm{Aut}(G, w)$ be the set of all permutations $\varphi : E(G) \to E(G)$ that arise from weight-preserving automorphisms of G. That is, $\mathrm{Aut}(G, w)$ is the set of permutations $\varphi : E(G) \to E(G)$ that admit a permutation $\pi : V(G) \to V(G)$ which preserves the weight function w, and such that if an edge $e \in E(G)$ has endpoints v and w, then $\varphi(e)$ has endpoints $\pi(v)$ and $\pi(w)$.

Now, the group $\mathrm{Aut}(G, w)$ acts naturally on the set $E(G)$, and hence on the orthant $\mathbb{R}^{E(G)}_{\geq 0}$, with the latter action given by permuting coordinates. We define $\overline{C(G, w)}$ to be the topological quotient space

$$\overline{C(G, w)} = \frac{\mathbb{R}^{E(G)}_{\geq 0}}{\mathrm{Aut}(G, w)}.$$

Next, we define an equivalence relation on the points in the union

$$\coprod \overline{C(G, w)},$$

as (G, w) ranges over all combinatorial types of genus g. Regard a point $x \in \overline{C(G, w)}$ as an assignment of lengths to the edges of G. Now, given two points $x \in \overline{C(G, w)}$ and $x' \in \overline{C(G', w')}$, let $x \sim x'$ if the two tropical curves obtained from them by contracting all edges of length zero are isomorphic. Note that contracting a loop, say at vertex v, means deleting that loop and adding 1 to the weight of v. Contracting a nonloop edge, say with endpoints v_1 and v_2, means deleting that edge and identifying v_1 and v_2 to obtain a new vertex whose weight is $w(v_1) + w(v_2)$.

Now we glue the cells $\overline{C(G, w)}$ along $\sim$ to obtain our moduli space:

Definition 2.6. The *moduli space* M_g^{tr} is the topological space

$$M_g^{\mathrm{tr}} := \coprod \overline{C(G, w)} \,/\sim,$$

where the disjoint union ranges over all combinatorial types of genus g, and $\sim$ is the equivalence relation defined above.

In fact, the space M_g^{tr} carries additional structure: it is an example of a stacky fan. We will define the category of stacky fans in Section 3.

Example 2.7. Figure 3 is a picture of M_2^{tr}. Its cells are quotients of polyhedral cones; the dotted lines represent symmetries, and faces labeled by the same combinatorial type are in fact identified. The poset of cells, which we will investigate next for higher g, is shown in Figure 1. It has two vertices, two edges and two 2-cells.

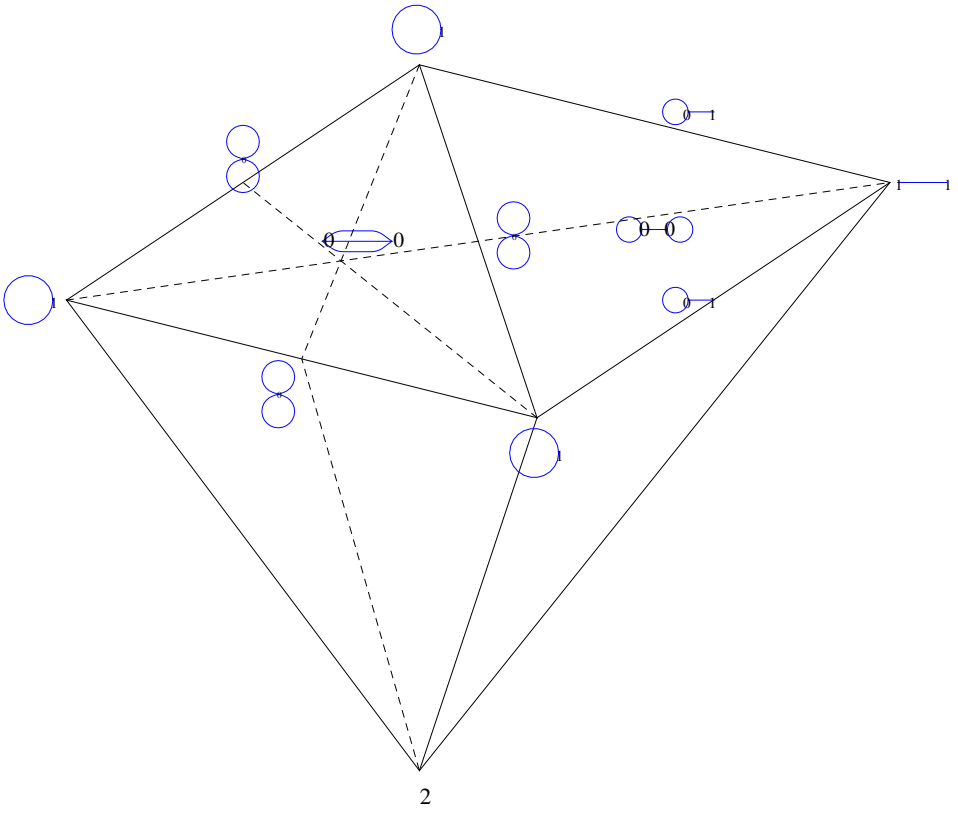


Figure 3. The stacky fan M_2^{tr}.

Remark 2.8. One can also construct the moduli space of genus-g tropical curves with n marked points using the same methods, as done, for example, in [Caporaso 2011].

2C. ***Explicit computations of*** M_g^{tr}**.** Our next goal will be to compute the space M_g^{tr} for g at most 5. The computations were done in Mathematica, and the code is available in the Electronic Supplement and at the author's website.

What we compute, to be precise, is the partially ordered set P_g on the cells of M_g^{tr}. This poset is defined in Lemma 2.10. Our results, summarized in Theorem 2.13, provide independent verification of the first six terms of the sequence A174224 in [Sloane 2011], which counts the number of tropical curves of genus g:

$$0, 0, 7, 42, 379, 4555, 69808, 1281678, \ldots.$$

This sequence, along with much more data along these lines, was first obtained by an algorithm described in [Maggiolo and Pagani 2011].

Definition 2.9. Given two combinatorial types (G, w) and (G', w') of genus g, we say that (G', w') is a *specialization*, or *contraction*, of (G, w) if it can be obtained from (G, w) by a sequence of edge contractions. Here, contracting a loop means deleting it and adding 1 to the weight of its base vertex; contracting a nonloop edge, say with endpoints v_1 and v_2, means deleting the edge and identifying v_1 and v_2 to obtain a new vertex whose weight we set to $w(v_1) + w(v_2)$.

Lemma 2.10. *The relation of specialization on genus-g combinatorial types yields a graded partially ordered set P_g on the cells of M_g^{tr}. The rank of a combinatorial type (G, w) is $|E(G)|$.*

Proof. It is clear that we obtain a poset; furthermore, (G', w') is covered by (G, w) precisely if (G', w') is obtained from (G, w) by contracting a single edge. The formula for the rank then follows. □

For example, P_2 is shown in Figure 1; it also appeared in [BMV 2011, Figure 1]. The poset P_3 is shown in Figure 4. It is color-coded according to the Torelli map, as explained in Section 6.

Our goal is to compute P_g. We do so by first listing its maximal elements, and then computing all possible specializations of those combinatorial types. For the first step, we use [BMV 2011, Proposition 3.2.4(i)], which characterizes the maximal cells of M_g^{tr}: they correspond precisely to combinatorial types $(G, \bar{0})$, where G is a connected 3-regular graph of genus g, and $\bar{0}$ is the zero-weight function on $V(G)$. Connected, 3-regular graphs of genus g are equivalently characterized as connected, 3-regular graphs on $2g - 2$ vertices. These have been enumerated:

Proposition 2.11. *The number of maximal cells of M_g^{tr} is equal to the $(g-1)$-st term in the sequence*

$$2, 5, 17, 71, 388, 2592, 21096, 204638, 2317172, 30024276, 437469859, \ldots.$$

Proof. This is sequence A005967 in [Sloane 2011], whose g-th term is the number of connected 3-regular graphs on $2g$ vertices. □

In fact, the connected, 3-regular graphs of genus g have been conveniently written down for g at most 6. This work was done in the 1970s by Balaban, a chemist whose interests along these lines were in molecular applications of graph theory. The graphs for $g \leq 5$ appear in [Balaban 1976], and the 388 genus-6 graphs appear in [Balaban 1970].

Given the maximal cells of M_g^{tr}, we can compute the rest of them:

Algorithm 2.12. Input: Maximal cells of M_g^{tr}.
Output: Poset of all cells of M_g^{tr}.

1. Initialize P_g to be the set of all maximal cells of M_g^{tr}, with no relations. Let L be a list of elements of P_g.

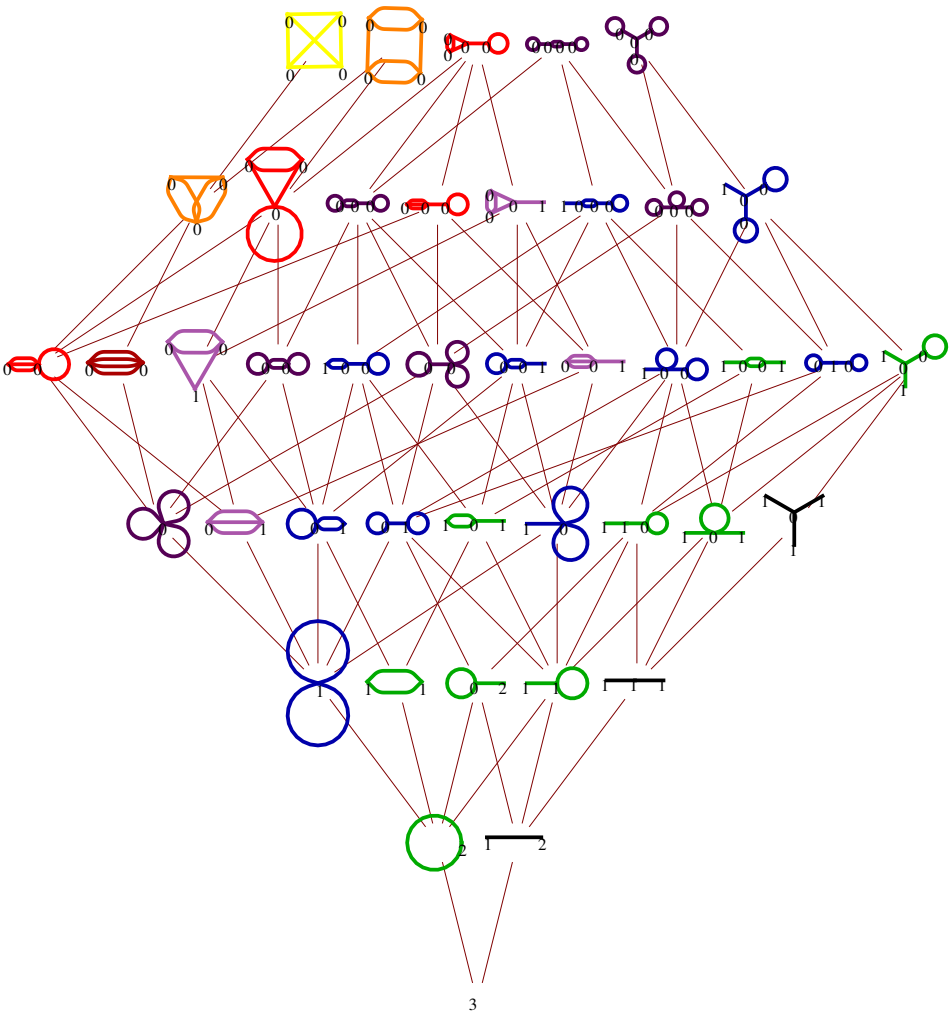


Figure 4. Poset of cells of M_3^{tr}, color-coded according to their images in A_3^{tr} via the tropical Torelli map.

2. While L is nonempty:

   Let (G, w) be the first element of L. Remove (G, w) from L. Compute all one-edge contractions of (G, w).

   For each such contraction (G', w'):

   If (G', w') is isomorphic to an element (G'', w'') already in the poset P_g, add a cover relation $(G'', w'') \leq (G, w)$.

   Else, add (G', w') to P_g and add a cover relation $(G', w') \leq (G, w)$.

   Add (G', w') to the list L.

3. Return P_g.

We implemented this algorithm in Mathematica. The most costly step is computing graph isomorphisms in Step 2. Our results are summarized in the following theorem. By an f-vector of a poset, we mean the vector whose i-th entry is the number of elements of rank $i-1$. (The term "f-vector" originates from counting faces of polytopes).

Theorem 2.13. *We obtained the following computational results*:

(i) *The moduli space* M_3^{tr} *has* 42 *cells and* f*-vector*

$$(1, 2, 5, 9, 12, 8, 5).$$

Its poset of cells P_3 *is shown in Figure 4.*

(ii) *The moduli space* M_4^{tr} *has* 379 *cells and* f*-vector*

$$(1, 3, 7, 21, 43, 75, 89, 81, 42, 17).$$

(iii) *The moduli space* M_5^{tr} *has* 4555 *cells and* f*-vector*

$$(1, 3, 11, 34, 100, 239, 492, 784, 1002, 926, 632, 260, 71).$$

The posets P_4 and P_5 are much too large to display here, but are available in the Electronic Supplement and at the author's website.

Remark 2.14. The data of P_3, illustrated in Figure 4, is related to, but not the same as, the enumeration by T. Brady [1993, Appendix A] of the cells of the deformation retract K_3 of Outer space [Culler and Vogtmann 1986] modulo the action of the group $\mathrm{Out}(F_3)$. In that setting, one only needs to consider bridgeless graphs with all vertices of weight zero, thus throwing out all but eight cells of the poset P_3. In turn, the cells of $K_3/\mathrm{Out}(F_n)$ correspond to chains in the poset on those eight cells. It is these chains that are listed by Brady.

Note that the pure part of $M_g^{\mathrm{tr}'}$, that is, those tropical curves in $M_g^{\mathrm{tr}'}$ with all vertex weights zero, is a quotient of rank-g Outer space by the action of the outer automorphism group $\mathrm{Out}(F_g)$. We believe that further exploration of the connection between Outer space and M_g^{tr} would be interesting to researchers in both tropical geometry and geometric group theory.

Remark 2.15. What is the topology of M_g^{tr}? Of course, M_g^{tr} is always contractible: there is a deformation retract onto the unique 0-dimensional cell. So to make this question interesting, we restrict our attention to the subspace $M_g^{\mathrm{tr}'}$ of M_g^{tr} consisting of graphs with total edge length 1, say. For example, by looking at Figure 3, we can see that $M_2^{\mathrm{tr}'}$ is still contractible. We would like to know if the space $M_g^{\mathrm{tr}'}$ is also contractible for larger g.

3. Stacky fans

In Section 2, we defined the space M_g^{tr}. In Sections 4 and 6, we will define the space A_g^{tr} and the Torelli map $t_g^{\mathrm{tr}} : M_g^{\mathrm{tr}} \to A_g^{\mathrm{tr}}$. For now, however, let us pause and define the category of stacky fans, of which M_g^{tr} and A_g^{tr} are objects and t_g^{tr} is a morphism. The reader is invited to keep M_g^{tr} in mind as a running example of a stacky fan.

The purpose of this section is to offer a new definition of stacky fans, Definition 3.2, which we hope fixes an inconsistency in [BMV 2011, Definition 2.1.1]. We believe that their condition for integral-linear gluing maps is too restrictive and fails for M_g^{tr} and A_g^{tr}. See Remark 3.6. However, we do think that their definition of a stacky fan morphism is correct, so we repeat it in Definition 3.5. We also prove that M_g^{tr} is a stacky fan according to our new definition. The proof for A_g^{tr} is deferred to Section 4C.

Definition 3.1. A *rational open polyhedral cone* in $\mathbb{R}^n$ is a subset of $\mathbb{R}^n$ of the form $\{a_1x_1 + \cdots + a_tx_t : a_i \in \mathbb{R}_{>0}\}$, for some fixed vectors $x_1, \ldots, x_t \in \mathbb{Z}^n$. By convention, we also allow the trivial cone $\{0\}$.

Definition 3.2. Let $X_1 \subseteq \mathbb{R}^{m_1}, \ldots, X_k \subseteq \mathbb{R}^{m_k}$ be full-dimensional rational open polyhedral cones. For each $i = 1, \ldots, k$, let G_i be a subgroup of $\mathrm{GL}_{m_i}(\mathbb{Z})$ that fixes the cone X_i setwise, and let X_i/G_i denote the topological quotient thus obtained. The action of G_i on X_i extends naturally to an action of G_i on the Euclidean closure $\overline{X}_i$, and we let $\overline{X}_i/G_i$ denote the quotient.

Suppose that we have a topological space X and, for each $i = 1, \ldots, k$, a continuous map

$$\alpha_i : \overline{X}_i/G_i \to X.$$

Write $C_i = \alpha_i(X_i/G_i)$ and $\overline{C}_i = \alpha_i(\overline{X}_i/G_i)$ for each i. Given $Y \subseteq X_i$, we will abuse notation by writing $\alpha_i(Y)$ for α_i applied to the image of Y under the map $\overline{X}_i \twoheadrightarrow \overline{X}_i/G_i$.

Suppose that the following properties hold for each index i:

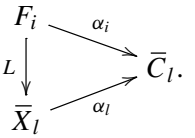
(i) The restriction of α_i to $\dfrac{X_i}{G_i}$ is a homeomorphism onto C_i.

(ii) We have an equality of sets $X = \coprod C_i$.

(iii) For each cone $\overline{X}_i$ and for each face F_i of $\overline{X}_i$, $\alpha_i(F_i) = \overline{C}_l$ for some l. Furthermore, $\dim F_i = \dim \overline{X}_l = m_l$, and there is an $\mathbb{R}$-invertible linear map $L : \mathrm{span}\langle F_i\rangle \cong \mathbb{R}^{m_l} \to \mathbb{R}^{m_l}$ such that

- $L(F_i) = \overline{X}_l$,
- $L(\mathbb{Z}^{m_i} \cap \mathrm{span}(F_i)) = \mathbb{Z}^{m_l}$, and

- the following diagram commutes:



We say that $\overline{C}_l$ is a *stacky face* of $\overline{C}_i$ in this situation.

(iv) For each pair i, j,

$$\overline{C}_i \cap \overline{C}_j = C_{l_1} \cup \cdots \cup C_{l_t},$$

where $C_{l_1}, \ldots, C_{l_t}$ are the common stacky faces of $\overline{C}_i$ and $\overline{C}_j$.

Then we say that X is a *stacky fan*, with cells $\{X_i/G_i\}$.

Remark 3.3. Condition (iii) essentially says that $\overline{X}_i$ has a face F_i that looks "exactly like" $\overline{X}_l$, even taking into account where the lattice points are. It plays the role of the usual condition on polyhedral fans that the set of cones is closed under taking faces. Condition (iv) replaces the usual condition on polyhedral fans that the intersection of two cones is a face of each. Here, we instead allow unions of common faces.

Theorem 3.4. *The moduli space M_g^{tr} is a stacky fan with cells*

$$C(G, w) = \frac{\mathbb{R}_{>0}^{E(G)}}{\mathrm{Aut}(G, w)}$$

as (G, w) ranges over genus-g combinatorial types. Its points are in bijection with tropical curves of genus g.

Proof. Recall that

$$M_g^{\mathrm{tr}} = \frac{\coprod \overline{C(G, w)}}{\sim},$$

where $\sim$ is the relation generated by contracting zero-length edges. Thus, each equivalence class has a unique representative (G_0, w, l) corresponding to an honest metric graph: one with all edge lengths positive. This gives the desired bijection.

Now we prove that M_g^{tr} is a stacky fan. For each (G, w), let

$$\alpha_{G,w} : \overline{C(G, w)} \to \frac{\coprod \overline{C(G', w')}}{\sim}$$

be the natural map. Now we check each of the requirements to be a stacky fan, in the order (ii), (iii), (iv), and (i).

For (ii), the fact that

$$M_g^{\mathrm{tr}} = \coprod C(G, w)$$

follows immediately from the observation above.

Let us prove (iii). Given a combinatorial type (G, w), the corresponding closed cone is $\mathbb{R}^{E(G)}_{\geq 0}$. A face F of $\mathbb{R}^{E(G)}_{\geq 0}$ corresponds to setting edge lengths of some subset S of the edges to zero. Let (G', w') be the resulting combinatorial type, and let $\pi : E(G) \setminus S \to E(G')$ be the natural bijection (it is well-defined up to (G', w')-automorphisms, but this is enough). Then π induces an invertible linear map,

$$L_\pi : \mathbb{R}^{E(G)\setminus S} \longrightarrow \mathbb{R}^{E(G')},$$

with the desired properties. Note also that the stacky faces of $\overline{C(G, w)}$ are thus all possible specializations $\overline{C(G', w')}$.

For (iv), given two combinatorial types (G, w) and (G', w'), then

$$\overline{C(G, w)} \cap \overline{C(G', w')}$$

consists of the union of all cells corresponding to common specializations of (G, w) and (G', w'). As noted above, these are precisely the common stacky faces of $\overline{C(G, w)}$ and $\overline{C(G', w')}$.

For (i), we show that $\alpha_{G,w}$ restricted to $C(G, w) = \mathbb{R}^{E(G)}_{>0}/\operatorname{Aut}(G, w)$ is a homeomorphism onto its image. It is continuous by definition of $\alpha_{G,w}$ and injective by definition of $\sim$. Let V be closed in $C(G, w)$, say $V = W \cap C(G, w)$ where W is closed in $\overline{C(G, w)}$. To show that $\alpha_{G,w}(V)$ is closed in $\alpha_{G,w}(C(G, w))$, it suffices to show that $\alpha_{G,w}(W)$ is closed in M^{tr}_g. Indeed, the fact that the cells $C(G, w)$ are pairwise disjoint in M^{tr}_g implies that

$$\alpha_{G,w}(V) = \alpha_{G,w}(W) \cap \alpha_{G,w}(C(G, w)).$$

Now, note that M^{tr}_g can equivalently be given as the quotient of the space

$$\coprod_{(G,w)} \mathbb{R}^{E(G)}_{\geq 0}$$

by all possible linear maps L_π arising as in the proof of (iii). All of the maps L_π identify faces of cones with other cones. Now let $\tilde{W}$ denote the lift of W to $\mathbb{R}^{E(G)}_{\geq 0}$; then for any other type (G', w'), we see that the set of points in $\mathbb{R}^{E(G')}_{\geq 0}$ that are identified with some point in $\tilde{W}$ is both closed and $\operatorname{Aut}(G', w')$-invariant, and passing to the quotient $\mathbb{R}^{E(G')}_{\geq 0}/\operatorname{Aut}(G', w')$ gives the claim. □

We close this section with the definition of a morphism of stacky fans. The tropical Torelli map, which we will define in Section 6, will be an example.

Definition 3.5 [BMV 2011, Definition 2.1.2]. Let

$$X_1 \subseteq \mathbb{R}^{m_1}, \ldots, X_k \subseteq \mathbb{R}^{m_k}, \quad Y_1 \subseteq \mathbb{R}^{n_1}, \ldots, Y_l \subseteq \mathbb{R}^{n_l}$$

be full-dimensional rational open polyhedral cones. Let $G_1 \subseteq \mathrm{GL}_{m_1}(\mathbb{Z}), \ldots, G_k \subseteq \mathrm{GL}_{m_k}(\mathbb{Z})$, $H_1 \subseteq \mathrm{GL}_{n_1}(\mathbb{Z}), \ldots, H_l \subseteq \mathrm{GL}_{n_l}(\mathbb{Z})$ be groups stabilizing $X_1, \ldots, X_k$,

$Y_1, \ldots, Y_l$, respectively. Let X and Y be stacky fans with cells

$$\left\{\frac{X_i}{G_i}\right\}_{i=1}^{k} \quad \text{and} \quad \left\{\frac{Y_j}{H_j}\right\}_{j=1}^{l}.$$

Denote by α_i and β_j the maps $\overline{X}_i/G_i \to X$ and $\overline{Y}_j/H_j \to Y$ that are part of the stacky fan data of X and Y.

A *morphism of stacky fans* from X to Y is a continuous map $\pi : X \to Y$ such that for each cell X_i/G_i there exists a cell Y_j/H_j such that

(i) $\pi\big(\alpha_i\big(X_i/G_i\big)\big) \subseteq \beta_j\big(Y_j/H_j\big)$, and

(ii) there exists an integral-linear map

$$L : \mathbb{R}^{m_i} \to \mathbb{R}^{n_j},$$

that is, a linear map defined by a matrix with integer entries, restricting to a map

$$L : X_i \to Y_j,$$

such that the following diagram commutes:

$$\begin{array}{ccc} X_i & \longrightarrow & \alpha_i(X_i/G_i) \\ {\scriptstyle L}\downarrow & & \downarrow{\scriptstyle \pi} \\ Y_j & \longrightarrow & \beta_j(Y_j/H_j). \end{array}$$

Remark 3.6. Here is why we believe the original definition of a stacky fan, [BMV 2011, Definition 2.1.1], is too restrictive. The original definition requires that for every pair of cones $\overline{X}_i$ and $\overline{X}_j$, there exists a linear map $L : \overline{X}_i \to \overline{X}_j$ that induces the inclusion

$$\alpha_i\left(\frac{\overline{X}_i}{G_i}\right) \cap \alpha_j\left(\frac{\overline{X}_j}{G_j}\right) \hookrightarrow \alpha_j\left(\frac{\overline{X}_j}{G_j}\right).$$

We claim that such a map does not always exist in the cases of M_g^{tr} and A_g^{tr}. For example, let $\overline{X}_i$ be the maximal cone of M_2^{tr} drawn on the left in Figure 3, and let $\overline{X}_j$ be the maximal cone drawn on the right. There is no map from $\overline{X}_i$ to $\overline{X}_j$ that takes each of the three facets of $\overline{X}_i$ isomorphically to a single facet of $\overline{X}_j$, as would be required. There is a similar problem for A_g^{tr}.

4. Principally polarized tropical abelian varieties

The purpose of this section is to construct the moduli space of principally polarized tropical abelian varieties, denoted A_g^{tr}. Our construction is different from the one in [BMV 2011], though it is still very much inspired by the ideas in that paper. The reason for presenting a new construction here is that a topological subtlety in the

construction there prevents their space from being a stacky fan as claimed in [BMV 2011, Theorem 4.2.4].

We begin in Section 4A by recalling the definition of a principally polarized tropical abelian variety. In Section 4B, we review the theory of Delone subdivisions and the main theorem of Voronoi reduction theory. We construct A_g^{tr} in Section 4C and prove that it is a stacky fan and that it is Hausdorff. We remark on the difference between our construction and the one in [BMV 2011] in Section 4D.

4A. ***Definition of principally polarized tropical abelian variety.*** Fix $g \geq 1$. Following [Mikhalkin and Zharkov 2008; BMV 2011], we define a *principally polarized tropical abelian variety* (*pptav*) to be a pair

$$(\mathbb{R}^g/\Lambda, Q),$$

where Λ is a lattice of rank g in $\mathbb{R}^g$ (that is, a discrete subgroup of $\mathbb{R}^g$ that is isomorphic to $\mathbb{Z}^g$), and Q is a positive-semidefinite quadratic form on $\mathbb{R}^g$ whose nullspace is rational with respect to Λ. We say that the nullspace of Q is *rational* with respect to Λ if the subspace $\ker(Q) \subseteq \mathbb{R}^g$ has a vector space basis whose elements are each of the form

$$a_1\lambda_1 + \cdots + a_k\lambda_k, \quad a_i \in \mathbb{Q}, \quad \lambda_i \in \Lambda.$$

We say that Q has *rational nullspace* if its nullspace is rational with respect to $\mathbb{Z}^g$.

We say that two pptavs $(\mathbb{R}^g/\Lambda, Q)$ and $(\mathbb{R}^g/\Lambda', Q')$ are isomorphic if there exists a matrix $X \in \mathrm{GL}_g(\mathbb{R})$ such that

- left multiplication by X^{-1} sends Λ isomorphically to Λ', that is, the map $X^{-1}: \mathbb{R}^g \to \mathbb{R}^g$ sending a column vector v to $X^{-1}v$ restricts to an isomorphism of lattices Λ and Λ', and
- $Q' = X^T Q X$.

Note that any pptav $(\mathbb{R}^g/\Lambda, Q)$ is isomorphic to one of the form $(\mathbb{R}^g/\mathbb{Z}^g, Q')$, namely by taking X to be any matrix sending $\mathbb{Z}^g$ to Λ and setting $Q' = X^T Q X$. Furthermore, $(\mathbb{R}^g/\mathbb{Z}^g, Q)$ and $(\mathbb{R}^g/\mathbb{Z}^g, Q')$ are isomorphic if and only if there exists $X \in \mathrm{GL}_g(\mathbb{Z})$ with $X^T Q X = Q'$.

Remark 4.1. Since we are interested in pptavs only up to isomorphism, we might be tempted to define the moduli space of pptavs to be the quotient of the topological space $\tilde{S}^g_{\geq 0}$, the space of positive-semidefinite matrices with rational nullspace, by the action of $\mathrm{GL}_g(\mathbb{Z})$. That is what is done in [BMV 2011]. That quotient space is the correct moduli space of pptavs set-theoretically. But it has an undesirable topology: as we will see in Section 4D, it is not even Hausdorff!

We will fix this problem by putting a different topology on the set of pptavs. We will first group matrices together into cells according to their Delone subdivisions,

and then glue the cells together to obtain the full moduli space. We review the theory of Delone subdivisions next.

4B. ***Voronoi reduction theory.*** Recall that a matrix has rational nullspace if its kernel has a basis consisting of vectors with entries in $\mathbb{Q}$.

Definition 4.2. Let $\tilde{S}^g_{\geq 0}$ denote the set of $g \times g$ positive-semidefinite matrices with rational nullspace. By regarding a $g \times g$ symmetric real matrix as a vector in $\mathbb{R}^{\binom{g+1}{2}}$, with one coordinate for each diagonal and above-diagonal entry of the matrix, we view $\tilde{S}^g_{\geq 0}$ as a subset of $\mathbb{R}^{\binom{g+1}{2}}$.

The group $\mathrm{GL}_g(\mathbb{Z})$ acts on $\tilde{S}^g_{\geq 0}$ on the right by changing basis:

$$Q \cdot X = X^T Q X, \quad \text{for all} \quad X \in \mathrm{GL}_g(\mathbb{Z}), \quad Q \in \tilde{S}^g_{\geq 0}.$$

Definition 4.3. Given $Q \in \tilde{S}^g_{\geq 0}$, define $\mathrm{Del}(Q)$ as follows. Consider the map $l : \mathbb{Z}^g \to \mathbb{Z}^g \times \mathbb{R}$ sending $x \in \mathbb{Z}^g$ to $(x, x^T Q x)$. View the image of l as an infinite set of points in $\mathbb{R}^{g+1}$, one above each point in $\mathbb{Z}^g$, and consider the convex hull of these points. The lower faces of the convex hull (the faces that are visible from $(0, -\infty)$) can now be projected to $\mathbb{R}^g$ by the map $\pi : \mathbb{R}^{g+1} \to \mathbb{R}^g$ that forgets the last coordinate. This produces an infinite periodic polyhedral subdivision of $\mathbb{R}^g$, called the *Delone subdivision* of Q and denoted $\mathrm{Del}(Q)$.

Now, we group together matrices in $\tilde{S}^g_{\geq 0}$ according to the Delone subdivisions to which they correspond.

Definition 4.4. Given a Delone subdivision D, let

$$\sigma_D = \{Q \in \tilde{S}^g_{\geq 0} : \mathrm{Del}(Q) = D\}.$$

Proposition 4.5 [Voronoï 1908; 1909]. *The set σ_D is an open rational polyhedral cone in $\tilde{S}^g_{\geq 0}$.*

Let $\bar{\sigma}_D$ denote the Euclidean closure of σ_D in $\mathbb{R}^{\binom{g+1}{2}}$, so $\bar{\sigma}_D$ is a closed rational polyhedral cone. We call it the *secondary cone* of D.

Example 4.6. Figure 5 shows the decomposition of $\tilde{S}^2_{\geq 0}$ into secondary cones. Here is how to interpret the picture. First, points in $\tilde{S}^2_{\geq 0}$ are 2×2 real symmetric matrices, so we regard them as points in $\mathbb{R}^3$. Then $\tilde{S}^2_{\geq 0}$ is a cone in $\mathbb{R}^3$. Instead of drawing the cone in $\mathbb{R}^3$, however, we only draw a hyperplane slice of it. Since it was a cone, our drawing does not lose information. For example, what looks like a point in the picture, labeled by the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, really is the ray in $\mathbb{R}^3$ passing through the point $(1, 0, 0)$.

Now, the action of the group $\mathrm{GL}_g(\mathbb{Z})$ on $\tilde{S}^g_{\geq 0}$ extends naturally to an action (say, on the right) on subsets of $\tilde{S}^g_{\geq 0}$. In fact, given $X \in \mathrm{GL}_g(\mathbb{Z})$ and D a Delone

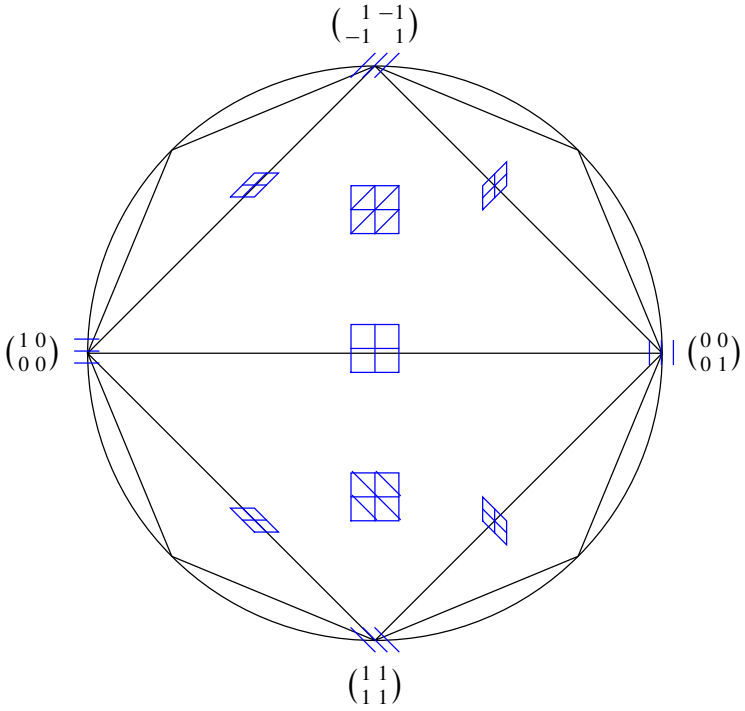


Figure 5. Infinite decomposition of $\tilde{S}^2_{\geq 0}$ into secondary cones.

subdivision,

$$\sigma_D \cdot X = \sigma_{X^{-1}D} \quad \text{and} \quad \overline{\sigma}_D \cdot X = \overline{\sigma}_{X^{-1}D}.$$

So $\mathrm{GL}_g(\mathbb{Z})$ acts on the set

$$\{\overline{\sigma}_D : D \text{ is a Delone subdivision of } \mathbb{R}^g\}.$$

Furthermore, $\mathrm{GL}_g(\mathbb{Z})$ acts on the set of Delone subdivisions, with action induced by the action of $\mathrm{GL}_g(\mathbb{Z})$ on $\mathbb{R}^g$. Two cones σ_D and $\sigma_{D'}$ are $\mathrm{GL}_g(\mathbb{Z})$-equivalent if and only if D and D' are.

Theorem 4.7 (Main theorem of Voronoi reduction theory [Voronoï 1908; 1909]). *The set of secondary cones*

$$\{\overline{\sigma}_D : D \textit{ is a Delone subdivision of } \mathbb{R}^g\}$$

yields an infinite polyhedral fan whose support is $\tilde{S}^g_{\geq 0}$, *known as the* second Voronoi decomposition. *There are only finitely many* $\mathrm{GL}_g(\mathbb{Z})$*-orbits of this set.*

4C. *Construction of A_g^{tr}.* Equipped with Theorem 4.7, we will now construct our tropical moduli space A_g^{tr}. We will show that its points are in bijection with the points of $\tilde{S}^g_{\geq 0}/\operatorname{GL}_g(\mathbb{Z})$, and that it is a stacky fan whose cells correspond to $\operatorname{GL}_g(\mathbb{Z})$-equivalence classes of Delone subdivisions of $\mathbb{R}^g$.

Definition 4.8. Given a Delone subdivision D of $\mathbb{R}^g$, let

$$\operatorname{Stab}(\sigma_D) = \{X \in \operatorname{GL}_g(\mathbb{Z}) : \sigma_D \cdot X = \sigma_D\}$$

be the setwise stabilizer of σ_D.

Now, the subgroup $\operatorname{Stab}(\sigma_D) \subseteq \operatorname{GL}_g(\mathbb{Z})$ acts on the open cone σ_D, and we may extend this action to an action on its closure $\overline{\sigma}_D$.

Definition 4.9. Given a Delone subdivision D of $\mathbb{R}^g$, let

$$C(D) = \overline{\sigma}_D/\operatorname{Stab}(\sigma_D).$$

Thus, $C(D)$ is the topological space obtained as a quotient of the rational polyhedral cone $\overline{\sigma}_D$ by a group action.

Now, by Theorem 4.7, there are only finitely many $\operatorname{GL}_g(\mathbb{Z})$-orbits of secondary cones $\overline{\sigma}_D$. Thus, we may choose $D_1, \ldots, D_k$ Delone subdivisions of $\mathbb{R}^g$ such that $\overline{\sigma}_{D_1}, \ldots, \overline{\sigma}_{D_k}$ are representatives for $\operatorname{GL}_g(\mathbb{Z})$-equivalence classes of secondary cones. (Note that we do not need anything like the axiom of choice to select these representatives. Rather, we can use [Vallentin 2003, Algorithm 1]. We start with a particular Delone triangulation and then walk across codimension-1 faces to all of the other ones; then we compute the faces of these maximal cones to obtain the nonmaximal ones. The key idea that allows the algorithm to terminate is that all maximal cones are related to each other by finite sequences of "bistellar flips" as described in [Vallentin 2003, §2.4]).

Definition 4.10. Let $D_1, \ldots, D_k$ be Delone subdivisions such that $\overline{\sigma}_{D_1}, \ldots, \overline{\sigma}_{D_k}$ are representatives for $\operatorname{GL}_g(\mathbb{Z})$-equivalence classes of secondary cones in $\mathbb{R}^g$. Consider the disjoint union

$$C(D_1) \sqcup \cdots \sqcup C(D_k),$$

and define an equivalence relation $\sim$ on it as follows. Given $Q_i \in \overline{\sigma}_{D_i}$ and $Q_j \in \overline{\sigma}_{D_j}$, let $[Q_i]$ and $[Q_j]$ be the corresponding elements in $C(D_i)$ and $C(D_j)$, respectively. Now let

$$[Q_i] \sim [Q_j]$$

if and only if Q_i and Q_j are $\operatorname{GL}_g(\mathbb{Z})$-equivalent matrices in $\tilde{S}^g_{\geq 0}$. Since $\operatorname{Stab}(\sigma_{D_i})$ and $\operatorname{Stab}(\sigma_{D_j})$ are subgroups of $\operatorname{GL}_g(\mathbb{Z})$, the relation $\sim$ is defined independently of the choice of representatives Q_i and Q_j, and is clearly an equivalence relation.

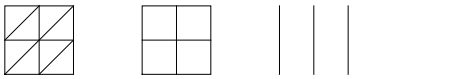


Figure 6. Cells of A_2^{tr}. Note that D_4 is the trivial subdivision of $\mathbb{R}^2$, consisting of $\mathbb{R}^2$ itself.

We now define the *moduli space of principally polarized tropical abelian varieties*, denoted A_g^{tr}, to be the topological space

$$A_g^{\mathrm{tr}} = \coprod_{i=1}^{k} C(D_k)/\sim .$$

Example 4.11. Let us compute A_2^{tr}. Combining the taxonomies in [Vallentin 2003, §4.1 and §4.2], we may choose four representatives D_1, D_2, D_3, and D_4 for orbits of secondary cones as in Figure 6.

We can describe the corresponding secondary cones as follows: Let

$$R_{12} = \left(\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix}\right), \quad R_{13} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), \quad R_{23} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

Then

$$\overline{\sigma}_{D_1} = \mathbb{R}_{\geq 0}\langle R_{12}, R_{13}, R_{23}\rangle, \quad \overline{\sigma}_{D_2} = \mathbb{R}_{\geq 0}\langle R_{13}, R_{23}\rangle,$$
$$\overline{\sigma}_{D_3} = \mathbb{R}_{\geq 0}\langle R_{13}\rangle, \qquad\qquad \overline{\sigma}_{D_4} = \{0\}.$$

Note that each closed cone $\overline{\sigma}_{D_2}$, $\overline{\sigma}_{D_3}$, and $\overline{\sigma}_{D_4}$ is just a face of $\overline{\sigma}_{D_1}$. One may check — and we will, in Section 5 — that for each $j = 2, 3, 4$, two matrices Q and Q' in $\overline{\sigma}_{D_j}$ are $\mathrm{Stab}(\sigma_{D_j})$-equivalent if and only if they are $\mathrm{Stab}(\sigma_{D_1})$-equivalent. Thus, gluing the cones $C(D_2)$, $C(D_3)$, and $C(D_4)$ to $C(D_1)$ does not change $C(D_1)$. We will see in Theorem 5.10 that the action of $\mathrm{Stab}(\sigma_{D_1})$ on $\overline{\sigma}_{D_1}$ is an S_3-action that permutes the three rays of $\overline{\sigma}_{D_1}$. So we may pick a fundamental domain, say the closed cone

$$C = \mathbb{R}_{\geq 0}\left\langle \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & -1 \\ -1 & 2 \end{smallmatrix}\right)\right\rangle,$$

and conclude that $C(D_1)$, and hence A_2^{tr}, is homeomorphic to C. See Figure 7 on the next page for a picture of A_2^{tr}. Of course, A_2^{tr} has further structure, as the next theorem shows.

Theorem 4.12. *The space A_g^{tr} constructed in Definition 4.10 is a stacky fan with cells $\sigma_{D_i}/\mathrm{Stab}(\sigma_{D_i})$ for $i = 1, \ldots, k$.*

Proof. For each $i = 1, \ldots, k$, let α_i be the composition

$$\frac{\overline{\sigma}_{D_i}}{\mathrm{Stab}(\sigma_{D_i})} \xhookrightarrow{\gamma_i} \coprod_{j=1}^{k} C(D_j) \xrightarrow{q} \Big(\coprod_{j=1}^{k} C(D_j)\Big)\Big/\sim,$$

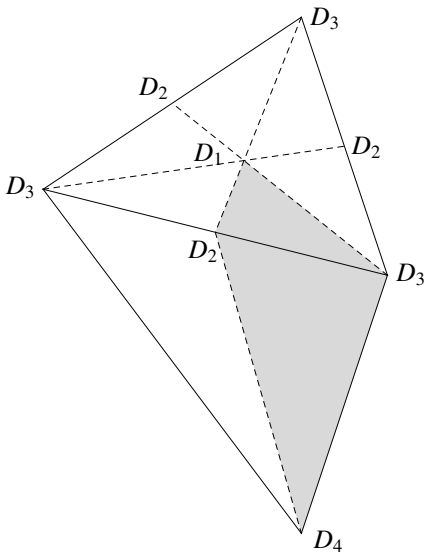


Figure 7. The stacky fan A_2^{tr}. The shaded area represents a choice of fundamental domain.

where γ_i is the inclusion of $C(D_i) = \overline{\sigma}_{D_i}/\mathrm{Stab}(\sigma_{D_i})$ into $\coprod_{j=1}^{k} C(D_j)$ and q is the quotient map. Now we check the four conditions listed in Definition 3.2 for A_g^{tr} to be a stacky fan.

First, we prove that the restriction of α_i to $\sigma_{D_i}/\mathrm{Stab}(\sigma_{D_i})$ is a homeomorphism onto its image. Now, α_i is continuous since both γ_i and q are. To show that $\alpha_i|_{\sigma_{D_i}/\mathrm{Stab}(\sigma_{D_i})}$ is one-to-one onto its image, let Q, $Q' \in \sigma_{D_i}$ such that

$$\alpha_i([Q]) = \alpha_i([Q']).$$

Then $[Q] \sim [Q']$, so there exists $A \in \mathrm{GL}_g(\mathbb{Z})$ such that $Q' = A^T Q A$. Hence $Q' \in A^T \sigma_{D_i} A = \sigma_{A^{-1}D_i}$. Thus $\sigma_{A^{-1}D_i}$ and σ_{D_i} intersect, hence $\sigma_{A^{-1}D_i} = \sigma_{D_i}$ and $A \in \mathrm{Stab}(\sigma_{D_i})$. So $[Q] = [Q']$.

Thus, $\alpha_i|_{\sigma_{D_i}/\mathrm{Stab}(\sigma_{D_i})}$ has a well-defined inverse map, and we wish to show that this inverse map is continuous. Let $X \subseteq \sigma_{D_i}/\mathrm{Stab}\,\sigma_{D_i}$ be closed; we wish to show that $\alpha_i(X)$ is closed in $\alpha_i(\sigma_{D_i}/\mathrm{Stab}\,\sigma_{D_i})$. Write $X = Y \cap \sigma_{D_i}/\mathrm{Stab}\,\sigma_{D_i}$ where $Y \subseteq \overline{\sigma}_{D_i}/\mathrm{Stab}\,\sigma_{D_i}$ is closed. Then

$$\alpha_i(X) = \alpha_i(Y) \cap \alpha_i\left(\frac{\sigma_{D_i}}{\mathrm{Stab}\,\sigma_{D_i}}\right);$$

this follows from the fact that $\mathrm{GL}_g(\mathbb{Z})$-equivalence never identifies a point on the boundary of a closed cone with a point in the relative interior. So we need only show that $\alpha_i(Y)$ is closed in A_g^{tr}. To be clear: we want to show that given any closed $Y \subseteq \overline{\sigma}_{D_i}/\mathrm{Stab}\,\sigma_{D_i}$, the image $\alpha_i(Y) \subseteq A_g^{\mathrm{tr}}$ is closed.

Let $\tilde{Y} \subseteq \overline{\sigma}_{D_i}$ be the preimage of Y under the quotient map

$$\overline{\sigma}_{D_i} \twoheadrightarrow \frac{\overline{\sigma}_{D_i}}{\operatorname{Stab}\sigma_{D_i}}.$$

Then, for each $j = 1, \ldots, k$, let

$$\tilde{Y}_j = \{Q \in \overline{\sigma}_{D_j} : Q \equiv_{\mathrm{GL}_g(\mathbb{Z})} Q' \text{ for some } Q' \in \tilde{Y}\} \subseteq \overline{\sigma}_{D_j}.$$

We claim each $\tilde{Y}_j$ is closed in $\overline{\sigma}_{D_j}$. First, notice that for any $A \in \mathrm{GL}_g(\mathbb{Z})$, the cone $A^T \overline{\sigma}_{D_i} A$ intersects $\overline{\sigma}_{D_j}$ in a (closed) face of $\overline{\sigma}_{D_j}$ (after all, the cones form a polyhedral subdivision). In other words, A defines an integral-linear isomorphism $L_A : F_{A,i} \to F_{A,j}$ sending $X \mapsto A^T X A$, where $F_{A,i}$ is a face of $\overline{\sigma}_{D_i}$ and $F_{A,j}$ is a face of $\overline{\sigma}_{D_j}$. Moreover, the map L_A is entirely determined by three choices: the choice of $F_{A,i}$, the choice of $F_{A,j}$, and the choice of a bijection between the rays of $F_{A,i}$ and $F_{A,j}$. Thus there exist only finitely many distinct such maps. Therefore

$$\tilde{Y}_j = \bigcup_{A \in \mathrm{GL}_g(\mathbb{Z})} L_A(\tilde{Y} \cap F_{A,i}) = \bigcup_{k=1}^{s} L_{A_k}(\tilde{Y} \cap F_{A_k,i})$$

for some choice of finitely many matrices $A_1, \ldots, A_s \in \mathrm{GL}_g(\mathbb{Z})$. Now, each L_A is a homeomorphism, so each $L_A(\tilde{Y} \cap F_{A,i})$ is closed in $F_{A,j}$ and hence in $\overline{\sigma}_{D_j}$. So $\tilde{Y}_j$ is closed.

Finally, let Y_j be the image of $\tilde{Y}_j \subseteq \overline{\sigma}_{D_j}$ under the quotient map

$$\overline{\sigma}_{D_j} \xrightarrow{\pi_i} \frac{\overline{\sigma}_{D_j}}{\operatorname{Stab}\sigma_{D_j}}.$$

Since $\pi_j^{-1}(Y_j) = \tilde{Y}_j$, we have that Y_j is closed. Then the inverse image of $\alpha_i(Y)$ under the quotient map

$$\coprod_{j=1}^{k} C(D_j) \longrightarrow \Big(\coprod_{j=1}^{k} C(D_j) \Big) \Big/ \sim$$

is precisely $Y_1 \sqcup \cdots \sqcup Y_k$, which is closed. Hence $\alpha_i(Y)$ is closed. This finishes the proof that $\alpha_i|_{\sigma_{D_i}/\mathrm{Stab}(\sigma_{D_i})}$ is a homeomorphism onto its image.

Property (ii) of being a stacky fan follows from the fact that any matrix $Q \in \tilde{S}^g_{\geq 0}$ is $\mathrm{GL}_g(\mathbb{Z})$-equivalent only to some matrices in a single chosen cone, say σ_{D_i}, and no others. Here, $\mathrm{Del}(Q)$ and D_i are $\mathrm{GL}_g(\mathbb{Z})$-equivalent. Thus, given a point in A_g^{tr} represented by $Q \in \tilde{S}^g_{\geq 0}$, Q lies in $\alpha_i(\sigma_{D_i}/\operatorname{Stab}\sigma_{D_i})$ and no other $\alpha_j(\sigma_{D_j}/\operatorname{Stab}\sigma_{D_j})$, and is the image of a single point in $\sigma_{D_i}/\operatorname{Stab}\sigma_{D_i}$ since α_i was shown to be bijective on $\sigma_{D_i}/\operatorname{Stab}\sigma_{D_i}$. This shows that

$$A_g^{\mathrm{tr}} = \coprod_{i=1}^{k} \alpha_i\left(\frac{\sigma_{D_i}}{\operatorname{Stab}\sigma_{D_i}}\right)$$

as a set.

Third, a face F of some cone $\overline{\sigma}_{D_i}$ is $\overline{\sigma}_{D(F)}$, where $D(F)$ is a Delone subdivision that is a coarsening of D_i [Vallentin 2003, Proposition 2.6.1]. Then there exists D_j and $A \in \mathrm{GL}_g(\mathbb{Z})$ with $\overline{\sigma}_{D(F)} \cdot A = \overline{\sigma}_{D_j}$ (recall that A acts on a point $p \in \tilde{S}^g_{\geq 0}$ by $p \mapsto A^T pA$). Restricting A to the linear span of $\overline{\sigma}_{D(F)}$ gives a linear map

$$L_A : \mathrm{span}(\overline{\sigma}_{D(F)}) \longrightarrow \mathrm{span}(\overline{\sigma}_{D_j})$$

with the desired properties. Note, therefore, that $\overline{\sigma}_{D_k}$ is a stacky face of $\overline{\sigma}_{D_i}$ precisely if D_k is $\mathrm{GL}_g(\mathbb{Z})$-equivalent to a coarsening of D_i.

The fourth property then follows: the intersection

$$\alpha_i(\overline{\sigma}_{D_i}) \cap \alpha_j(\overline{\sigma}_{D_j}) = \bigcup \alpha_k(\sigma_{D_k}),$$

where σ_{D_k} ranges over all common stacky faces. □

Proposition 4.13. *The construction of A^{tr}_g in Definition 4.10 does not depend on our choice of $D_1, \ldots, D_k$. More precisely, suppose $D'_1, \ldots, D'_k$ are another choice of representatives such that D'_i and D_i are $\mathrm{GL}_g(\mathbb{Z})$-equivalent for each i. Let $A^{\mathrm{tr}'}_g$ be the corresponding stacky fan. Then there is an isomorphism of stacky fans between A^{tr}_g and $A^{\mathrm{tr}'}_g$.*

Proof. For each i, choose $A_i \in \mathrm{GL}_g(\mathbb{Z})$ with

$$\sigma_{D_i} \cdot A_i = \sigma_{D'_i}.$$

Then we obtain a map

$$C(D_1) \amalg \cdots \amalg C(D_k) \xrightarrow{(A_1,\ldots,A_k)} C(D'_1) \amalg \cdots \amalg C(D'_k)$$

descending to a map

$$A^{\mathrm{tr}}_g \longrightarrow A^{\mathrm{tr}'}_g,$$

and this map is an isomorphism of stacky fans, as evidenced by the inverse map $A^{\mathrm{tr}'}_g \to A^{\mathrm{tr}}_g$ constructed from the matrices $A_1^{-1}, \ldots, A_k^{-1}$. □

Theorem 4.14. *The moduli space A^{tr}_g is Hausdorff.*

Remark 4.15. Theorem 4.14 complements the theorem of Caporaso that M^{tr}_g is Hausdorff [Caporaso 2012, Theorem 5.2].

Proof. Let $\overline{\sigma}_{D_1}, \ldots, \overline{\sigma}_{D_k}$ be representatives for $\mathrm{GL}_g(\mathbb{Z})$-classes of secondary cones. Let us regard A^{tr}_g as a quotient of the cones themselves, rather than the cones modulo their stabilizers; thus

$$A^{\mathrm{tr}}_g = \Big(\coprod_{i=1}^{k} \overline{\sigma}_{D_k} \Big) / \sim,$$

where $\sim$ denotes $\mathrm{GL}_g(\mathbb{Z})$-equivalence as usual. Denote by β_i the natural maps

$$\beta_i : \overline{\sigma}_{D_i} \to A_g^{\mathrm{tr}}.$$

Now suppose $p \neq q \in A_g^{\mathrm{tr}}$. For each $i = 1, \ldots, k$, pick disjoint open sets U_i and V_i in $\overline{\sigma}_{D_i}$ such that $\beta_i^{-1}(p) \subseteq U_i$ and $\beta_i^{-1}(q) \subseteq V_i$. Let

$$U := \{x \in A_g^{\mathrm{tr}} : \beta_i^{-1}(x) \subseteq U_i \text{ for all } i\},$$
$$V := \{x \in A_g^{\mathrm{tr}} : \beta_i^{-1}(x) \subseteq V_i \text{ for all } i\}.$$

By construction, we have $p \in U$ and $q \in V$. We claim that U and V are disjoint open sets in A_g^{tr}.

Suppose $x \in U \cap V$. Now $\beta_i^{-1}(x)$ is nonempty for some i, hence $U_i \cap V_i$ is nonempty, which is a contradiction. Hence U and V are disjoint. So we just need to prove that U is open (similarly, V is open). It suffices to show that for each $j = 1, \ldots, k$, the set $\beta_j^{-1}(U)$ is open. Now,

$$\begin{aligned}\beta_j^{-1}(U) &= \{y \in \overline{\sigma}_{D_j} : \beta_i^{-1}\beta_j(y) \subseteq U_i \text{ for all } i\} \\ &= \bigcap_i \{y \in \overline{\sigma}_{D_j} : \beta_i^{-1}\beta_j(y) \subseteq U_i\}.\end{aligned}$$

Write U_{ij} for the sets in the intersection above, so that $\beta_j^{-1}(U) = \bigcap_i U_{ij}$, and let $Z_i = \overline{\sigma}_{D_i} \setminus U_i$. Note that U_{ij} consists of those points in $\overline{\sigma}_{D_j}$ that are not $\mathrm{GL}_g(\mathbb{Z})$-equivalent to any point in Z_i. Then, just as in the proof of Theorem 4.12, there exist finitely many matrices $A_1, \ldots, A_s \in \mathrm{GL}_g(\mathbb{Z})$ such that

$$\overline{\sigma}_{D_j} \setminus U_{ij} = \{y \in \overline{\sigma}_{D_j} : y \sim z \text{ for some } z \in Z_i\} = \bigcup_{l=1}^{s} (A_l^T Z_i A_l \cap \overline{\sigma}_{D_j}),$$

which shows that $\overline{\sigma}_{D_j} \setminus U_{ij}$ is closed. Thus the U_{ij} are open and so $\beta_j^{-1}(U)$ is open for each j. Hence U is open; similarly, V is open. □

Remark 4.16. Actually, we could have done a much more general construction of A_g^{tr}. We made a choice of decomposition of $\tilde{S}_{\geq 0}^g$: we chose the second Voronoi decomposition, whose cones are secondary cones of Delone subdivisions. This decomposition has the advantage that it interacts nicely with the Torelli map, as we will see. But, as rightly pointed out in [BMV 2011], we could use any decomposition of $\tilde{S}_{\geq 0}^g$ that is "$\mathrm{GL}_g(\mathbb{Z})$-admissible." This means that it is an infinite polyhedral subdivision of $\tilde{S}_{\geq 0}^g$ such that $\mathrm{GL}_g(\mathbb{Z})$ permutes its open cones in a finite number of orbits. See [Ash et al. 1975, §II] for the formal definition. Every result in this section can be restated for a general $\mathrm{GL}_g(\mathbb{Z})$-admissible decomposition: each such decomposition produces a moduli space which is a stacky fan, which is independent of any choice of representatives, and which is Hausdorff. The proofs are all the same. In this paper, though, we chose to fix a specific decomposition purely for the

sake of concreteness and readability, invoking only what we needed to build up to the definition of the Torelli map.

4D. ***The quotient space*** $\tilde{S}^g_{\geq 0}/\operatorname{GL}_g(\mathbb{Z})$**.** We briefly remark on the construction of A_g^{tr} originally proposed in [BMV 2011]. There, the strategy is to try to equip the quotient space $\tilde{S}^g_{\geq 0}/\operatorname{GL}_g(\mathbb{Z})$ directly with a stacky fan structure. To do this, one maps a set of representative cones σ_D, modulo their stabilizers $\operatorname{Stab}(\sigma_D)$, into the space $\tilde{S}^g_{\geq 0}/\operatorname{GL}_g(\mathbb{Z})$, via the map

$$i_D : \sigma_D/\operatorname{Stab}(\sigma_D) \to \tilde{S}^g_{\geq 0}/\operatorname{GL}_g(\mathbb{Z})$$

induced by the inclusion $\sigma_D \hookrightarrow \tilde{S}^g_{\geq 0}$.

The problem is that the map i_D above may not be a homeomorphism onto its image. In fact, the image of $\sigma_D/\operatorname{Stab}(\sigma_D)$ in $\tilde{S}^g_{\geq 0}/\operatorname{GL}_g(\mathbb{Z})$ may not even be Hausdorff, even though $\sigma_D/\operatorname{Stab}(\sigma_D)$ certainly is. The following example shows that the cone σ_{D_3}, using the notation of Example 4.11, exhibits such behavior. Note that $\operatorname{Stab}(\sigma_{D_3})$ happens to be trivial in this case.

Example 4.17. Let $\{X_n\}_{n\geq 1}$ and $\{Y_n\}_{n\geq 1}$ be the sequences of matrices

$$X_n = \begin{pmatrix} 1 & 1/n \\ 1/n & 1/n^2 \end{pmatrix}, \quad Y_n = \begin{pmatrix} 1/n^2 & 0 \\ 0 & 0 \end{pmatrix},$$

in $\tilde{S}^2_{\geq 0}$. Then we have

$$\{X_n\} \to \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \{Y_n\} \to \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

On the other hand, for each n, $X_n \equiv_{\mathrm{GL}_2(\mathbb{Z})} Y_n$ even while $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \not\equiv_{\mathrm{GL}_2(\mathbb{Z})} \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. This example then descends to non-Hausdorffness in the topological quotient. It can easily be generalized to $g > 2$.

Thus, we disagree with the claim in the proof of [BMV 2011, Theorem 4.2.4] that the open cones σ_D, modulo their stabilizers, map homeomorphically onto their image in $\tilde{S}^g_{\geq 0}/\operatorname{GL}_g(\mathbb{Z})$. However, we emphasize that our construction in Section 4C is just a minor modification of the ideas already present in [BMV 2011].

5. Regular matroids and the zonotopal subfan

In the previous section, we defined the moduli space A_g^{tr} of principally polarized tropical abelian varieties. In this section, we describe a particular stacky subfan of A_g^{tr} whose cells are in correspondence with simple regular matroids of rank at most g. This subfan is called the zonotopal subfan and denoted A_g^{zon} because its cells correspond to those classes of Delone triangulations which are dual to zonotopes; see [BMV 2011, §4.4]. The zonotopal subfan A_g^{zon} is important because, as we

shall see in Section 6, it contains the image of the Torelli map. For $g \geq 4$, this containment is proper. Our main contribution in this section is to characterize the stabilizing subgroups of all zonotopal cells.

We begin by recalling some basic facts about matroids. A good reference is [Oxley 1992]. The connection between matroids and the Torelli map seems to have been first observed by Gerritzen [1982], and our approach here can be seen as an continuation of his work in the late 1970s.

Definition 5.1. A matroid is said to be *simple* if it has no loops and no parallel elements.

Definition 5.2. A matroid M is *regular* if it is representable over every field; equivalently, M is regular if it is representable over $\mathbb{R}$ by a totally unimodular matrix. (A totally unimodular matrix is a matrix such that every square submatrix has determinant in $\{0, 1, -1\}$.)

Next, we review the correspondence between simple regular matroids and zonotopal cells.

Construction 5.3. *Let M be a simple regular matroid of rank at most g, and let A be a $g \times n$ totally unimodular matrix that represents M. Let $v_1, \ldots, v_n$ be the columns of A. Then let $\sigma_A \subseteq \mathbb{R}^{\binom{g+1}{2}}$ be the rational open polyhedral cone*

$$\mathbb{R}_{>0}\langle v_1 v_1^T, \ldots, v_n v_n^T \rangle.$$

Example 5.4. Here is an example of Construction 5.3 at work. Let M be the uniform matroid $U_{2,3}$; equivalently M is the graphic matroid $M(K_3)$. Then M is represented by the 2×3 totally unimodular matrix $A = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \end{smallmatrix}\right)$, and σ_A is the open cone generated by the matrices $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix}\right)$. It is the cone σ_{D_1} in Example 4.11 and is shown in Figure 7.

Proposition 5.5 [BMV 2011, Lemma 4.4.3, Theorem 4.4.4]. *Let M be a simple regular matroid of rank at most g, and let A be a $g \times n$ totally unimodular matrix that represents M. Then the cone σ_A, defined in Construction 5.3, is a secondary cone in $\tilde{S}^g_{\geq 0}$. Choosing a different totally unimodular matrix A' to represent M produces a cone $\sigma_{A'}$ that is $\mathrm{GL}_g(\mathbb{Z})$-equivalent to σ_A. Thus, we may associate to M a unique cell of A_g^{tr}, denoted $C(M)$.*

Definition 5.6. The *zonotopal subfan* A_g^{zon} is the union of cells in A_g^{tr}

$$A_g^{\mathrm{zon}} = \bigcup_{\substack{M \text{ a simple regular} \\ \text{matroid of rank} \leq g}} C(M).$$

We briefly recall the definition of the Voronoi polytope of a quadratic form in $\tilde{S}^g_{\geq 0}$, just in order to explain the relationship with zonotopes.

Definition 5.7. Let $Q \in \tilde{S}^g_{\geq 0}$, and let $H = (\ker Q)^\perp \subseteq \mathbb{R}^g$. Then

$$\mathrm{Vor}(Q) = \{x \in H : x^T Q x \leq (x-\lambda)^T Q (x-\lambda)\ \forall \lambda \in \mathbb{Z}^g\}$$

is a polytope in $H \subseteq \mathbb{R}^g$, called the *Voronoi polytope* of Q.

Theorem 5.8 [BMV 2011, Theorem 4.4.4, Definition 4.4.5]. *The zonotopal subfan A_g^{zon} is a stacky subfan of A_g^{tr}. It consists of those points of the tropical moduli space A_g^{tr} whose Voronoi polytope is a zonotope.*

Remark 5.9. Suppose σ is an open rational polyhedral cone in $\mathbb{R}^n$. Then any $A \in \mathrm{GL}_n(\mathbb{Z})$ such that $A\sigma = \sigma$ must permute the rays of $\overline{\sigma}$, since the action of A on $\overline{\sigma}$ is linear. Furthermore, it sends a first lattice point on a ray to another first lattice point; that is, it preserves lattice lengths. Thus, the subgroup $\mathrm{Stab}(\sigma) \subseteq \mathrm{GL}_n(\mathbb{Z})$ realizes some subgroup of the permutation group on the rays of $\overline{\sigma}$ (although if σ is not full-dimensional then the action of $\mathrm{Stab}(\sigma)$ on its rays may not be faithful).

Now, given a simple regular matroid M of rank $\leq g$, we have almost computed the cell of A_g^{tr} to which it corresponds. Specifically, we have computed the cone $\overline{\sigma}_A$ for A a matrix representing M, in Construction 5.3. The remaining task is to compute the action of the stabilizer $\mathrm{Stab}(\sigma_A)$.

Note that $\overline{\sigma}_A$ has rays corresponding to the columns of A: a column vector v_i corresponds to the ray generated by the symmetric rank-1 matrix $v_i v_i^T$. In light of Remark 5.9, we might conjecture that the permutations of rays of $\overline{\sigma}_A$ coming from the stabilizer are the ones that respect the matroid M, that is, come from matroid automorphisms. That is precisely the case and provides valuable local information about A_g^{tr}.

Theorem 5.10. *Let A be a $g \times n$ totally unimodular matrix representing the simple regular matroid M. Let H denote the group of permutations of the rays of σ_A which are realized by the action of* $\mathrm{Stab}(\sigma_A)$. *Then*

$$H \cong \mathrm{Aut}(M).$$

Remark 5.11. This seems to have been known in [Gerritzen 1982], but we present a new proof here, one which might be easier to read. Our main tool is the combinatorics of unimodular matrices.

Here is a nice fact about totally unimodular matrices: they are essentially determined by the placement of their zeroes.

Lemma 5.12 [Truemper 1992, Lemma 9.2.6]. *Suppose A and B are $g \times n$ totally unimodular matrices with the same support, that is, $a_{ij} \neq 0$ if and only if $b_{ij} \neq 0$ for all i and j. Then A can be transformed into B by negating rows and negating columns.*

Lemma 5.13. *Let A and B be $g \times n$ totally unimodular matrices, with column vectors $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$, respectively. Suppose that the map $v_i \mapsto w_i$ induces an isomorphism of matroids*

$$M[A] \xrightarrow{\cong} M[B];$$

that is, it takes independent sets to independent sets and dependent sets to dependent sets. Then there exists $X \in \mathrm{GL}_g(\mathbb{Z})$ such that

$$Xv_i = \pm w_i \quad \text{for each } i = 1, \ldots, n.$$

Proof. First, let $r = \mathrm{rank}(A) = \mathrm{rank}(B)$, noting that the ranks are equal since the matroids are isomorphic. Since the statement of Lemma 5.13 does not depend on the ordering of the columns, we may simultaneously reorder the columns of A and the columns of B and so assume that the first r rows of A (respectively B) form a basis of $M[A]$ (respectively $M[B]$). Furthermore, we may replace A by ΣA and B by $\Sigma' B$, where Σ, $\Sigma' \in \mathrm{GL}_g(\mathbb{Z})$ are appropriate permutation matrices, and assume that the upper-left-most $r \times r$ submatrices of both A and B are nonsingular; in fact, they have determinant ± 1. Then, we can act further on A and B by elements of $\mathrm{GL}_g(\mathbb{Z})$ so that, without loss of generality, both A and B have the form

$$\left[\begin{array}{c|c} \mathrm{Id}_{r\times r} & * \\ \hline 0 & 0 \end{array}\right].$$

Note that after these operations, A and B are still totally unimodular; this follows from the fact that totally unimodular matrices are closed under multiplication and taking inverses. But then A and B are totally unimodular matrices with the same support. Indeed, the support of a column v_i of A, for each $i = r+1, \ldots, n$, is determined by the fundamental circuit of v_i with respect to the basis $\{v_1, \ldots, v_r\}$ in $M[A]$, and since $M[A] \cong M[B]$, each v_i and w_i have the same support.

Thus, by Lemma 5.12, there exists a diagonal matrix $X \in \mathrm{GL}_g(\mathbb{Z})$, whose diagonal entries are ± 1, such that XA can be transformed into B by a sequence of column negations. This is what we claimed. □

Proof of Theorem 5.10. Let $v_1, \ldots, v_n$ be the columns of A. Let $X \in \mathrm{Stab}\,\sigma_A$. Then X acts on the rays of $\overline{\sigma}_A$ via

$$(v_i v_i^T) \cdot X = X^T v_i v_i^T X = v_j v_j^T$$

for some column v_j. So $v_j = \pm X^T v_i$. But X^T is invertible, so a set of vectors $\{v_{i_1}, \ldots, v_{i_k}\}$ is linearly independent if and only if $\{X^T v_{i_1}, \ldots, X^T v_{i_k}\}$ is, so X induces a permutation that is in $\mathrm{Aut}(M)$.

Conversely, suppose we are given $\pi \in \mathrm{Aut}(M)$. Let B be the matrix

$$B = \begin{bmatrix} | & & | \\ v_{\pi(1)} & \cdots & v_{\pi(n)} \\ | & & | \end{bmatrix}.$$

Then $M[A] = M[B]$, so, by Lemma 5.13, there exists $X \in \mathrm{GL}_g(\mathbb{Z})$ such that $X^T \cdot v_i = \pm v_{\pi(i)}$ for each i. Then

$$X^T v_i v_i^T X = (\pm v_{\pi(i)})(\pm v_{\pi(i)}^T) = v_{\pi(i)} v_{\pi(i)}^T$$

so X realizes π as a permutation of the rays of $\overline{\sigma}_A$. □

6. The tropical Torelli map

The classical Torelli map $t_g : \mathcal{M}_g \to \mathcal{A}_g$ sends a curve to its Jacobian. Jacobians were developed thoroughly in the tropical setting in [Mikhalkin and Zharkov 2008; Zharkov 2010]. Here, we define the tropical Torelli map following [BMV 2011], and recall the characterization of its image, the so-called Schottky locus, in terms of cographic matroids. We then present a comparison of the number of cells in M_g^{tr}, in the Schottky locus, and in A_g^{tr}, for small g.

Definition 6.1. The tropical Torelli map

$$t_g^{\mathrm{tr}} : M_g^{\mathrm{tr}} \to A_g^{\mathrm{tr}}$$

is defined as follows. Consider the first homology group $H_1(G, \mathbb{R})$ of the graph G, whose elements are formal sums of edges with coefficients in $\mathbb{R}$ lying in the kernel of the boundary map. Given a genus-g tropical curve $C = (G, l, w)$, we define a positive-semidefinite form Q_C on $H_1(G, \mathbb{R}) \oplus \mathbb{R}^{|w|}$, where

$$|w| := \sum w(v).$$

The form is 0 whenever the second summand $\mathbb{R}^{|w|}$ is involved, and on $H_1(G, \mathbb{R})$ it is

$$Q_C\Big(\sum_{e \in E(G)} \alpha_e \cdot e\Big) = \sum_{e \in E(G)} \alpha_e^2 \cdot l(e).$$

Here, the edges of G are oriented for reference, and the α_e are real numbers such that $\sum \alpha_e \cdot e \in H_1(G, \mathbb{R})$.

Now, pick a basis of $H_1(G, \mathbb{Z})$; this identifies $H_1(G, \mathbb{Z}) \oplus \mathbb{Z}^{|w|}$ with the lattice $\mathbb{Z}^g$, and hence $H_1(G, \mathbb{R}) \oplus \mathbb{R}^{|w|}$ with $\mathbb{R}^g = \mathbb{Z}^g \otimes_{\mathbb{Z}} \mathbb{R}$. Thus Q_C is identified with an element of $\tilde{S}^g_{\geq 0}$. Choosing a different basis gives another element of $\tilde{S}^g_{\geq 0}$ only up to a $\mathrm{GL}_g(\mathbb{Z})$-action, so we have produced a well-defined element of A_g^{tr}, called the *tropical Jacobian* of C.

Theorem 6.2 [BMV 2011, Theorem 5.1.5]. *The map*

$$t_g^{\mathrm{tr}} : M_g^{\mathrm{tr}} \to A_g^{\mathrm{tr}}$$

is a morphism of stacky fans.

Note that the proof by Brannetti, Melo, and Viviani of Theorem 6.2 is correct under the new definitions. In particular, the definition of a morphism of stacky fans has not changed.

The next theorem tells us how the tropical Torelli map behaves, at least on the level of stacky cells. Given a graph G, its cographic matroid is denoted $M^*(G)$, and

$$\widetilde{M^*(G)}$$

is then the matroid obtained by removing loops and replacing each parallel class with a single element. See [BMV 2011, Definition 2.3.8].

Theorem 6.3 [BMV 2011, Theorem 5.1.5]. *The map t_g^{tr} sends the cell $C(G, w)$ of M_g^{tr} surjectively to the cell $C(\widetilde{M^*(G)})$.*

We denote by A_g^{cogr} the stacky subfan of A_g^{tr} consisting of those cells

$$\{C(M) : M \text{ a simple cographic matroid of rank} \leq g\}.$$

The cell $C(M)$ was defined in Construction 5.3. Note that A_g^{cogr} sits inside the zonotopal subfan of Section 5:

$$A_g^{\mathrm{cogr}} \subseteq A_g^{\mathrm{zon}} \subseteq A_g^{\mathrm{tr}}.$$

Also, $A_g^{\mathrm{cogr}} = A_g^{\mathrm{tr}}$ when $g \leq 3$, but not when $g \geq 4$ [BMV 2011, Remark 5.2.5]. The previous theorem says that the image of t_g^{tr} is precisely $A_g^{\mathrm{cogr}} \subseteq A_g^{\mathrm{tr}}$. So, in analogy with the classical situation, we call A_g^{cogr} the *tropical Schottky locus*.

Figures 4 and 8 illustrate the tropical Torelli map in genus 3. The cells of M_3^{tr} in Figure 4 are color-coded according to the color of the cells of A_3^{tr} in Figure 8 to which they are sent. These figures serve to illustrate the correspondence in Theorem 6.3.

Our contribution in this section is to compute the poset of cells of A_g^{cogr}, for $g \leq 5$, using Mathematica. First, we computed the cographic matroid of each graph of genus $\leq g$, and discarded the ones that were not simple. Then we checked whether any two matroids obtained in this way were in fact isomorphic. Part of this computation was done by hand in the genus-5 case, because it became intractable to check whether two 12-element matroids were isomorphic. Instead, we used some heuristic tests and then checked by hand that, for the few pairs of matroids passing the tests, the original pair of graphs were related by a sequence of vertex cleavings and Whitney flips. This condition ensures that they have the same cographic matroid; see [Oxley 1992].

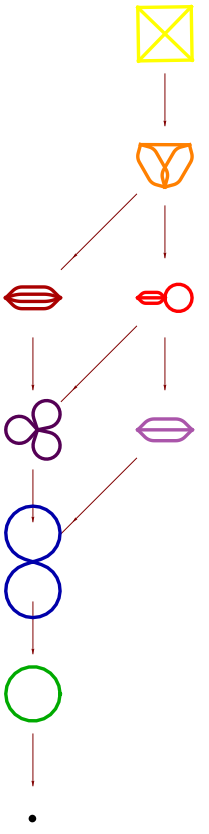


Figure 8. Poset of cells of $A_3^{\mathrm{tr}} = A_3^{\mathrm{cogr}}$. Each cell corresponds to a cographic matroid, and, for convenience, we draw a graph G in order to represent its cographic matroid $M^*(G)$.

We obtained the following computational results:

Theorem 6.4. (i) *The tropical Schottky locus A_3^{cogr} has nine cells and f-vector*

$$(1, 1, 1, 2, 2, 1, 1).$$

(Its poset of cells is shown in Figure 8.)

(ii) *The tropical Schottky locus A_4^{cogr} has 25 cells and f-vector*

$$(1, 1, 1, 2, 3, 4, 5, 4, 2, 2).$$

(iii) *The tropical Schottky locus A_5^{cogr} has 92 cells and f-vector*

$$(1, 1, 1, 2, 3, 5, 9, 12, 15, 17, 15, 7, 4).$$

g	M_g^{tr}	A_g^{cogr}	A_g^{tr}
2	2	1	1
3	5	1	1
4	17	2	3
5	71	4	222

Table 1. Number of maximal cells in the stacky fans M_g^{tr}, A_g^{cogr}, and A_g^{tr}.

g	M_g^{tr}	A_g^{cogr}	A_g^{tr}
2	7	4	4
3	42	9	9
4	379	25	61
5	4555	92	179433

Table 2. Total number of cells in the stacky fans M_g^{tr}, A_g^{cogr}, and A_g^{tr}.

Remark 6.5. Actually, since $A_3^{\mathrm{cogr}} = A_3^{\mathrm{tr}}$, the results of part (i) of Theorem 6.4 were already known, say in [Vallentin 2003].

Tables 1 and 2 show a comparison of the number of maximal cells and the number of total cells, respectively, of M_g^{tr}, A_g^{cogr}, and A_g^{tr}. The numbers in the first column of Table 2 were obtained in [Maggiolo and Pagani 2011] and in Theorem 2.13. The first column of Table 1 is from [Balaban 1976]. The results in the second column are our contribution in Theorem 6.4. The third columns are due to [Engel 2000] and [Engel and Grishukhin 2002]; computations for $g > 5$ were done in [Vallentin 2003].

It would be desirable to extend our computations of A_g^{cogr} to $g \geq 6$, but this would require some new ideas on effectively testing matroid isomorphisms.

7. Tropical covers via level structure

All tropical varieties are stacky fans: at least in the "constant coefficient" case (see [Maclagan and Sturmfels 2009]), tropical varieties are polyhedral fans, and all polyhedral fans are stacky fans in which every cone has only trivial symmetries. On the other hand, stacky fans are not always tropical varieties. Indeed, one problem with the spaces M_g^{tr} and A_g^{tr} is that although they are tropical moduli spaces, they do not "look" very tropical: they do not satisfy a tropical balancing condition (see [Maclagan and Sturmfels 2009]).

But what if we allow ourselves to consider finite-index covers of our spaces — can we then produce a more tropical object? In what follows, we answer this

question for the spaces A_2^{tr} and A_3^{tr}. The uniform matroid U_4^2 and the Fano matroid F_7 play a role. We are grateful to Diane Maclagan for suggesting this question and the approach presented here.

Given $n \geq 1$, let $\mathbb{FP}^n$ denote the complete polyhedral fan in $\mathbb{R}^n$ associated to projective space $\mathbb{P}^n$, regarded as a toric variety. Concretely, we fix the rays of $\mathbb{FP}^n$ to be generated by

$$e_1, \ldots, e_n, \quad e_{n+1} := -e_1 - \cdots - e_n,$$

and each subset of at most n rays spans a cone in $\mathbb{FP}^n$. So $\mathbb{FP}^n$ has $n+1$ top-dimensional cones. Given $S \subseteq \{1, \ldots, n+1\}$, let $\mathrm{cone}(S)$ denote the open cone $\mathbb{R}_{>0}\{e_i : i \in S\}$ in $\mathbb{FP}^n$, let $\mathrm{cone}(\hat{\imath}) := \mathrm{cone}(\{1, \ldots, \hat{\imath}, \ldots, n+1\})$, and let $\overline{\mathrm{cone}}(S)$ be the closed cone corresponding to S. Note that the polyhedral fan $\mathbb{FP}^n$ is also a stacky fan: each open cone can be equipped with trivial symmetries. Its support is the tropical variety corresponding to all of $\mathbb{T}^n$.

By a *generic point* of A_g^{tr}, we mean a point x lying in a cell of A_g^{tr} of maximal dimension such that any positive-semidefinite matrix X representing x is fixed only by the identity element in $\mathrm{GL}_g(\mathbb{Z})$.

7A. ***A tropical cover for*** $\boldsymbol{A_3^{\mathrm{tr}}}$**.** By the classification in [Vallentin 2003, §4.1–4.3], we note that

$$A_3^{\mathrm{tr}} = \Big(\coprod_{M \subseteq MK_4} C(M) \Big) \Big/ \sim .$$

In the disjoint union above, the symbol MK_4 denotes the graphic (equivalently, in this case, cographic) matroid of the graph K_4, and $M \subseteq M'$ means that M is a submatroid of M', that is, obtained by deleting elements. The cell $C(M)$ of a regular matroid M was defined in Construction 5.3. There is a single maximal cell $C(MK_4)$ in A_3^{tr}, and the other cells are stacky faces of it. The cells are also listed in Figure 8.

Now define a continuous map

$$\pi : \mathbb{FP}^6 \to A_3^{\mathrm{tr}}$$

as follows. Let A be a 3×6 unimodular matrix representing MK_4, for example,

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1 & -1 \end{pmatrix},$$

and let $\bar{\sigma}_A$ be the cone in $\tilde{S}^3_{\geq 0}$ with rays $\{v_i v_i^T\}$, where the v_i are the columns of A, as in Construction 5.3. Fix, once and for all, a Fano matroid structure on the set $\{1, \ldots, 7\}$. For example, we could take F_7 to have circuits $\{124, 235, 346, 457, 156, 267, 137\}$.

Now, for each $i = 1, \ldots, 7$, the deletion $F_7 \setminus \{i\}$ is isomorphic to MK_4, so let

$$\pi_{\hat{\imath}} : [7] \setminus \{i\} \to E(MK_4)$$

be any bijection inducing such an isomorphism. Now define

$$\alpha_{\hat{\imath}} : \overline{\mathrm{cone}}(\hat{\imath}) \to A_3^{\mathrm{tr}}$$

as the composition

$$\overline{\mathrm{cone}}(\hat{\imath}) \xrightarrow{L_{\hat{\imath}}} \overline{\sigma}_A \twoheadrightarrow \frac{\overline{\sigma}_A}{\mathrm{Stab}\,\sigma_A} = C(MK_4) \longrightarrow A_3^{\mathrm{tr}},$$

where $L_{\hat{\imath}}$ is the integral-linear map arising from $\pi_{\hat{\imath}}$.

Now, each $\alpha_{\hat{\imath}}$ is clearly continuous, and to paste them together into a map on all of $\mathbb{FP}^6$, we need to show that they agree on intersections. Thus, fix $i \neq j$ and let $S \subseteq \{1, \ldots, 7\} \setminus \{i, j\}$. We want to show that

$$\alpha_{\hat{\imath}} = \alpha_{\hat{\jmath}} \text{ on } \overline{\mathrm{cone}}(S).$$

Indeed, the map $L_{\hat{\imath}}$ sends $\overline{\mathrm{cone}}(S)$ isomorphically to $\overline{\sigma}_{A|_{\pi_{\hat{\imath}}(S)}}$, where $A|_{\pi_{\hat{\imath}}(S)}$ denotes the submatrix of A gotten by taking the columns indexed by $\pi_{\hat{\imath}}(S)$. Furthermore, the bijection on the rays of the cones agrees with the isomorphism of matroids

$$F_7|_S \xrightarrow{\cong} MK_4|_{\pi_{\hat{\imath}}(S)}.$$

Similarly, $L_{\hat{\jmath}}$ sends $\overline{\mathrm{cone}}(S)$ isomorphically to $\overline{\sigma}_{A|_{\pi_{\hat{\jmath}}(S)}}$, and the map on rays agrees with the matroid isomorphism

$$F_7|_S \xrightarrow{\cong} MK_4|_{\pi_{\hat{\jmath}}(S)}.$$

Hence $MK_4|_{\pi_{\hat{\imath}}(S)} \cong MK_4|_{\pi_{\hat{\jmath}}(S)}$ and by Theorem 5.10, there exists $X \in \mathrm{GL}_3(\mathbb{Z})$ such that this diagram commutes:

$$\begin{array}{ccc} & \xrightarrow{L_{\hat{\imath}}} & \overline{\sigma}_{A|_{\pi_{\hat{\imath}}(S)}} \\ \overline{\mathrm{cone}}(S) & & \downarrow X \\ & \xrightarrow{L_{\hat{\jmath}}} & \overline{\sigma}_{A|_{\pi_{\hat{\jmath}}(S)}}. \end{array}$$

We conclude that $\alpha_{\hat{\imath}}$ and $\alpha_{\hat{\jmath}}$ agree on $\overline{\mathrm{cone}}(S)$, since $L_{\hat{\imath}}$ and $L_{\hat{\jmath}}$ differ only by a $\mathrm{GL}_3(\mathbb{Z})$-action.

Therefore, we can glue the seven maps $\alpha_{\hat{\imath}}$ together to obtain a continuous map $\alpha : \mathbb{FP}^6 \to A_3^{\mathrm{tr}}$.

Theorem 7.1. *The map $\alpha : \mathbb{FP}^6 \to A_3^{\mathrm{tr}}$ is a surjective morphism of stacky fans. Each of the seven maximal cells of $\mathbb{FP}^6$ is mapped surjectively onto the maximal cell of*

A_3^{tr}. *Furthermore, the map α has finite fibers, and if $x \in A_3^{\mathrm{tr}}$ is a generic point, then* $|\alpha^{-1}(x)| = 168$.

Proof. By construction, α sends each cell $\mathrm{cone}(S)$ of $\mathbb{FP}^6$ surjectively onto the cell of A_3^{tr} corresponding to the matroid $F_7|_S$, and each of these maps is induced by some integral-linear map $L_{\hat{\imath}}$. That α is surjective then follows from the fact that every submatroid of MK_4 is a proper submatroid of F_7. Also, by construction, α maps each maximal cell $\mathrm{cone}(\hat{\imath})$ of $\mathbb{FP}^6$ surjectively to the cell $C(MK_4)$ of A_3^{tr}.

By definition of the map α_i, each $x \in A_3^{\mathrm{tr}}$ has only finitely many preimages $\alpha_i^{-1}(x)$ in $\overline{\mathrm{cone}}(\hat{\imath})$, so α has finite fibers. If $x \in A_3^{\mathrm{tr}}$ is a generic point, then x has $24 = |\mathrm{Aut}(MK_4)|$ preimages in each of the seven maximal open cones $\mathrm{cone}(\hat{\imath})$, so $|\alpha^{-1}(x)| = 168$. □

7B. ***A tropical cover for A_2^{tr}.*** Our strategy in Theorem 7.1 for constructing a covering map $\mathbb{FP}^6 \to A_3^{\mathrm{tr}}$ was to use the combinatorics of the Fano matroid to paste together seven copies of MK_4 in a coherent way. In fact, an analogous, and easier, argument yields a covering map $\mathbb{FP}^3 \to A_2^{\mathrm{tr}}$. We will use U_4^2 to paste together four copies of U_3^2. Here, U_n^d denotes the uniform rank-d matroid on n elements.

The space A_2^{tr} can be given by

$$A_2^{\mathrm{tr}} = \Big(\coprod_{M \subseteq U_3^2} C(M) \Big) \Big/ \sim .$$

It has a single maximal cell $C(U_3^2)$, and the three other cells are stacky faces of it of dimensions 0, 1, and 2. See Figure 7.

Analogously to Section 7A, let

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix},$$

say, and for each $i = 1, \ldots, 4$, define

$$\beta_{\hat{\imath}} : \overline{\mathrm{cone}}(\hat{\imath}) \to A_2^{\mathrm{tr}}$$

by sending $\overline{\mathrm{cone}}(\hat{\imath})$ to $\overline{\sigma}_A$ by a bijective linear map preserving lattice points. Here, any of the 3! possible maps will do, because the matroid U_3^2 has full automorphisms.

Just as in Section 7A, we may check that the four maps $\alpha_{\hat{\imath}}$ agree on their overlaps, so we obtain a continuous map

$$\beta : \mathbb{FP}^3 \to A_2^{\mathrm{tr}}.$$

Proposition 7.2. *The map $\beta : \mathbb{FP}^3 \to A_2^{\mathrm{tr}}$ is a surjective morphism of stacky fans. Each of the four maximal cells of $\mathbb{FP}^3$ maps surjectively onto the maximal cell of A_2^{tr}. Furthermore, the map β has finite fibers, and if $x \in A_2^{\mathrm{tr}}$ is a generic point, then* $|\beta^{-1}(x)| = 24$.

Proof. The proof is exactly analogous to the proof of Theorem 7.1. Instead of noting that every one-element deletion of F_7 is isomorphic to MK_4, we make the easy observation that every one-element deletion of U_4^2 is isomorphic to U_3^2. If $x \in A_2^{\mathrm{tr}}$ is a generic point, then x has $6 = |\mathrm{Aut}(U_3^2)|$ preimages in each of the four maximal open cones of $\mathbb{FP}^3$. □

Remark 7.3. We do not know a more general construction for $g \geq 4$. We seem to be relying on the fact that all cells of A_g^{tr} are cographic when $g = 2, 3$, but this is not true when $g \geq 4$: the Schottky locus is proper.

Remark 7.4. Although our constructions look purely matroidal, they come from level structures on A_2^{tr} and A_3^{tr} with respect to the primes $p = 3$ and $p = 2$, respectively. More precisely, in the genus-2 case, consider the decomposition of $\tilde{S}^2_{\geq 0}$ into secondary cones as in Theorem 4.7, and identify rays vv^T and ww^T if $v \equiv \pm w \pmod 3$. Then we obtain $\mathbb{FP}^3$. The analogous statement holds, replacing the prime 3 with 2, in genus 3.

Acknowledgments

The author thanks B. Sturmfels, D. Maclagan, and F. Vallentin for helpful discussions, M. Melo and F. Viviani for comments on an earlier draft, F. Vallentin for many useful references, K. Vogtmann for the reference to [Brady 1993], F. Shokrieh for insight on Delone subdivisions, and R. Masuda for much help with typesetting. The author is supported by a Graduate Research Fellowship from the National Science Foundation.

References

[Ash et al. 1975] A. Ash, D. Mumford, M. Rapoport, and Y. Tai, *Smooth compactification of locally symmetric varieties*, Lie Groups: History, Frontiers and Applications **4**, Math. Sci. Press, Brookline, MA, 1975. MR 56 #15642 Zbl 0334.14007

[Baker et al. 2011] M. Baker, S. Payne, and J. Rabinoff, "Nonarchimedean geometry, tropicalization, and metrics on curves", preprint, 2011. arXiv 1104.0320v1

[Balaban 1970] A. T. Balaban, "Chemical graphs VIII: Valence isomerism and general cubic graphs", *Rev. Roum. Chim.* **15**:3 (1970), 463–486.

[Balaban 1976] A. T. Balaban, "Enumeration of cyclic graphs", pp. 63–105 in *Chemical applications of graphs theory*, edited by A. T. Balaban, Academic Press, New York, 1976.

[BMV 2011] S. Brannetti, M. Melo, and F. Viviani, "On the tropical Torelli map", *Adv. Math.* **226**:3 (2011), 2546–2586. MR 2012e:14121 Zbl 1218.14056

[Borisov et al. 2005] L. A. Borisov, L. Chen, and G. G. Smith, "The orbifold Chow ring of toric Deligne–Mumford stacks", *J. Amer. Math. Soc.* **18**:1 (2005), 193–215. MR 2006a:14091 Zbl 1178.14057

[Brady 1993] T. Brady, "The integral cohomology of $\mathrm{Out}_+(F_3)$", *J. Pure Appl. Algebra* **87**:2 (1993), 123–167. MR 94d:20057 Zbl 0798.20042

[Caporaso 2011] L. Caporaso, "Algebraic and tropical curves: comparing their moduli spaces", preprint, 2011. arXiv 1101.4821v3

[Caporaso 2012] L. Caporaso, "Geometry of tropical moduli spaces and linkage of graphs", *J. Combin. Theory Ser. A* **119**:3 (2012), 579–598. MR 2871751 Zbl 1234.14043

[Caporaso and Viviani 2010] L. Caporaso and F. Viviani, "Torelli theorem for graphs and tropical curves", *Duke Math. J.* **153**:1 (2010), 129–171. MR 2011j:14013 Zbl 1200.14025

[Culler and Vogtmann 1986] M. Culler and K. Vogtmann, "Moduli of graphs and automorphisms of free groups", *Invent. Math.* **84**:1 (1986), 91–119. MR 87f:20048 Zbl 0589.20022

[Engel 2000] P. Engel, "The contraction types of parallelohedra in E^5", *Acta Cryst. Sect. A* **56**:5 (2000), 491–496. MR 2001f:52046 Zbl 1188.52021

[Engel and Grishukhin 2002] P. Engel and V. Grishukhin, "There are exactly 222 L-types of primitive five-dimensional lattices", *European J. Combin.* **23**:3 (2002), 275–279. MR 2003i:11090 Zbl 1017.52006

[Gathmann et al. 2009] A. Gathmann, M. Kerber, and H. Markwig, "Tropical fans and the moduli spaces of tropical curves", *Compos. Math.* **145**:1 (2009), 173–195. MR 2009m:14085 Zbl 1169.51021

[Gerritzen 1982] L. Gerritzen, "Die Jacobi–Abbildung über dem Raum der Mumfordkurven", *Math. Ann.* **261**:1 (1982), 81–100. MR 84f:14021

[Grushevsky 2010] S. Grushevsky, "The Schottky problem", preprint, 2010. arXiv 1009.0369v2

[Maclagan and Sturmfels 2009] D. Maclagan and B. Sturmfels, "Introduction to tropical geometry", preprint, 2009, Available at http://www.warwick.ac.uk/staff/D.Maclagan/papers/TropicalBook.pdf.

[Maggiolo and Pagani 2011] S. Maggiolo and N. Pagani, "Generating stable modular graphs", *J. Symbolic Comput.* **46**:10 (2011), 1087–1097. MR 2012h:05084 Zbl 1238.14018

[Mikhalkin 2006] G. Mikhalkin, "Tropical geometry and its applications", pp. 827–852 in *International Congress of Mathematicians*, vol. 2, edited by M. Sanz-Solé et al., Eur. Math. Soc., Zürich, 2006. MR 2008c:14077 Zbl 1103.14034

[Mikhalkin 2007] G. Mikhalkin, "Moduli spaces of rational tropical curves", pp. 39–51 in *Proceedings of Gökova Geometry–Topology Conference 2006* (Gökova, 2006), edited by S. Akbulut et al., Gökova Geometry/Topology Conference (GGT), Gökova, 2007. MR 2009i:14014 Zbl 1203.14027

[Mikhalkin and Zharkov 2008] G. Mikhalkin and I. Zharkov, "Tropical curves, their Jacobians and theta functions", pp. 203–230 in *Curves and abelian varieties*, edited by V. Alexeev et al., Contemp. Math. **465**, Amer. Math. Soc., Providence, RI, 2008. MR 2011c:14163 Zbl 1152.14028

[Oxley 1992] J. G. Oxley, *Matroid theory*, Oxford University Press, New York, 1992. MR 94d:05033 Zbl 0784.05002

[Sloane 2011] N. Sloane, "The on-line encyclopedia of integer sequences", 2011, Available at http://oeis.org.

[Speyer and Sturmfels 2004] D. Speyer and B. Sturmfels, "The tropical Grassmannian", *Adv. Geom.* **4**:3 (2004), 389–411. MR 2005d:14089 Zbl 1065.14071

[Truemper 1992] K. Truemper, *Matroid decomposition*, Academic Press, Boston, MA, 1992. MR 93h:05046 Zbl 0760.05001

[Vallentin 2003] F. Vallentin, *Sphere coverings, lattices, and tilings (in low dimensions)*, thesis, Technische Universität München, 2003, Available at http://www.cwi.nl/~vallenti/PAPERS/D3.pdf.

[Voronoï 1908] G. Voronoï, "Nouvelles applications des paramètres continus à la théorie des formes quadratiques, Deuxième mémoire: Recherches sur les parallélloedres primitifs", *J. Reine Angew. Math.* **134** (1908), 198–287. JFM 39.0274.01

[Voronoï 1909] G. Voronoï, "Nouvelles applications des paramètres continus à la théorie des formes quadratiques, Deuxième mémoire: Recherches sur les parallélloedres primitifs", *J. Reine Angew. Math.* **136** (1909), 67–178. JFM 40.0267.17

[Zharkov 2010] I. Zharkov, "Tropical theta characteristics", pp. 165–168 in *Mirror symmetry and tropical geometry*, edited by R. Castaño-Bernard et al., Contemp. Math. **527**, Amer. Math. Soc., Providence, RI, 2010. MR 2012a:14139 Zbl 1213.14120

Communicated by Ravi Vakil
Received 2011-02-23 Revised 2011-07-11 Accepted 2011-08-13

mtchan@math.berkeley.edu *Department of Mathematics, University of California Berkeley, 970 Evans Hall #3840, Berkeley, CA 94720-3840, United States*
http://math.berkeley.edu/~mtchan/

ALGEBRA AND NUMBER THEORY 6:6 (2012)
dx.doi.org/10.2140/ant.2012.6.1171

msp

On fusion categories with few irreducible degrees

Sonia Natale and Julia Yael Plavnik

We prove some results on the structure of certain classes of integral fusion categories and semisimple Hopf algebras under restrictions on the set of their irreducible degrees.

1. Introduction

Let k be an algebraically closed field of characteristic zero. Let $\mathcal{C}$ be a fusion category over k. That is, $\mathcal{C}$ is a k-linear semisimple rigid tensor category with finitely many isomorphism classes of simple objects, finite-dimensional spaces of morphisms, and such that the unit object $\mathbf{1}$ of $\mathcal{C}$ is simple.

For example, if G is a finite group, then the categories $\operatorname{Rep} G$ of its finite-dimensional representations and the category $\mathcal{C}(G, \omega)$ of G-graded vector spaces with associativity determined by the 3-cocycle ω are fusion categories over k. More generally, if H is a finite-dimensional semisimple quasi-Hopf algebra over k, then the category $\operatorname{Rep} H$ of its finite-dimensional representations is a fusion category.

Let $\operatorname{Irr}(\mathcal{C})$ denote the set of isomorphism classes of simple objects in the fusion category $\mathcal{C}$. In analogy with the case of finite groups [Isaacs 1976], we shall use the notation $\operatorname{c.d.}(\mathcal{C})$ to indicate the set

$$\operatorname{c.d.}(\mathcal{C}) = \{\operatorname{FPdim} x \mid x \in \operatorname{Irr}(\mathcal{C})\}.$$

Here, $\operatorname{FPdim} x$ denotes the *Frobenius–Perron dimension* of $x \in \operatorname{Irr}(\mathcal{C})$. Notice that, when $\mathcal{C}$ is the representation category of a quasi-Hopf algebra, Frobenius–Perron dimensions coincide with the dimensions of the underlying vector spaces. In this case, we shall use the notation $\operatorname{c.d.}(\mathcal{C}) = \operatorname{c.d.}(H)$.

The positive real numbers $\operatorname{FPdim} x$, $x \in \operatorname{Irr}(\mathcal{C})$, will be called the *irreducible degrees* of $\mathcal{C}$.

The fusion categories that we shall consider in this paper are all *integral*, that is, the Frobenius–Perron dimensions of objects of $\mathcal{C}$ are (natural) integers. By [Etingof

This work was partially supported by CONICET, ANPCyT, and Secyt (UNC).
MSC2010: primary 16T05; secondary 18D10.
Keywords: fusion category, semisimple Hopf algebra, irreducible degree.

et al. 2005, Theorem 8.33], $\mathcal{C}$ is equivalent to the category of representations of some finite-dimensional semisimple quasi-Hopf algebra.

For a finite group G, the knowledge of the set $\mathrm{c.d.}(G) = \mathrm{c.d.}(kG)$ gives in some cases substantial information about the structure of G. It is known, for instance, that if $|\mathrm{c.d.}(G)| \leq 3$, then G is solvable.

On the other hand, if $|\mathrm{c.d.}(G)| = 2$, say $\mathrm{c.d.}(G) = \{1, m\}$, $m \geq 1$, then either G has an abelian normal subgroup of index m or else G is nilpotent of class ≤ 3. Furthermore, if G is nonabelian, then $\mathrm{c.d.}(G) = \{1, p\}$ for some prime number p, if and only if G contains an abelian normal subgroup of index p or the center $Z(G)$ has index p^3; see [Isaacs 1976, Theorems 12.11, 12.14, and 12.15].

In the context of semisimple Hopf algebras, some results in the same spirit are known. A basic one is that of [Zhu 1993], which asserts that if $|\mathrm{c.d.}(H)| \leq 3$, then $G(H^*)$ is not trivial; in other words, H has nontrivial characters of degree 1. A similar result appears in [Natale 1999, Theorem 2.2.3].

Further results, leading to classification theorems in some specific cases, appear in [Izumi and Kosaki 2002] for Kac algebras, that is, Hopf C^*-algebras.

In this paper we consider the general problem of understanding the structure of a fusion category $\mathcal{C}$ from a knowledge of $\mathrm{c.d.}(\mathcal{C})$. For instance, it is well known that $\mathrm{c.d.}(\mathcal{C}) = \{1\}$ if and only if $\mathcal{C}$ is pointed, if and only if $\mathcal{C} \simeq \mathcal{C}(G, \omega)$, for some 3-cocycle ω on the group $G = G(\mathcal{C})$ of isomorphism classes of invertible objects of $\mathcal{C}$.

More specifically, we address the following question:

Question 1.1. *Suppose* $\mathrm{c.d.}(\mathcal{C}) = \{1, p\}$, *with* p *a prime number. What can be said about the structure of* $\mathcal{C}$?

We treat mostly structural questions regarding nilpotency and solvability, in the sense introduced in [Gelaki and Nikshych 2008] and [Etingof et al. 2011]. (A related question for semisimple Hopf algebras, that we shall not discuss in the present paper, was posed in [Natale 2011, Question 7.2].)

The notions of nilpotency and solvability of a fusion category are related to the corresponding notions for finite groups as follows: if G is a finite group, then the category $\mathrm{Rep}\, G$ is nilpotent or solvable if and only if G is nilpotent or solvable, respectively. On the dual side, a pointed fusion category $\mathcal{C}(G, \omega)$ is always nilpotent, while it is solvable if and only if the group G is solvable.

An important class of fusion categories, called *weakly group-theoretical* fusion categories, was introduced and studied in [Etingof et al. 2011]. This generalized in turn the notion of a group-theoretical fusion category of [Etingof et al. 2005]. By definition, $\mathcal{C}$ is group-theoretical if it is Morita equivalent to a pointed fusion category, and it is weakly group-theoretical if it is Morita equivalent to a nilpotent fusion category. Every nilpotent or solvable fusion category is weakly group-theoretical.

With regard to Question 1.1, consider, for instance, the case where $\mathcal{C} = \operatorname{Rep} H$, for a semisimple Hopf algebra H. A result in this direction is known in the case $p = 2$. It is shown in [Bichon and Natale 2011, Corollary 6.6] that if H is a semisimple Hopf algebra such that $\text{c.d.}(H) \subseteq \{1, 2\}$, then H is upper semisolvable. Moreover, H is necessarily cocommutative if $G(H^*)$ is of order 2. The proof of these results relies on a refinement of [Nichols and Richmond 1996, Theorem 11] given in [Bichon and Natale 2011, Theorem 1.1].

In the context of Kac algebras, it is shown in [Izumi and Kosaki 2002, Theorem IX.8(iii)] that if $\text{c.d.}(H^*) = \{1, p\}$ and, in addition, $|G(H)| = p$, then H is a central abelian extension associated to an action of the cyclic group of order p on a nilpotent group. In the recent terminology introduced in [Gelaki and Nikshych 2008], this result implies that such a Kac algebra is *nilpotent*. See Remark 4.5.

The main results of this paper are summarized in the following theorem.

Theorem 1.2. *Let $\mathcal{C}$ be a fusion category over k.*

(i) (Proposition 7.1) *Suppose $\mathcal{C}$ is weakly group-theoretical and has odd dimension. Then $\mathcal{C}$ is solvable.*

Let p be a prime number.

(ii) (Theorem 7.3) *Suppose that $\mathcal{C}$ is braided odd-dimensional and that* $\text{c.d.}(\mathcal{C}) \subseteq \{p^m : m \geq 0\}$. *Then $\mathcal{C}$ is solvable.*

(iii) *Suppose* $\text{c.d.}(\mathcal{C}) \subseteq \{1, p\}$. *Then $\mathcal{C}$ is solvable in any of the following cases*:

- (Corollary 5.4) *$\mathcal{C}$ is of the form $\mathcal{C}(G, \omega, \mathbb{Z}_p, \alpha)$, that is, a group-theoretical fusion category* [Etingof et al. 2005], *and $G(\mathcal{C})$ is of order p.*
- (Theorem 6.2) *$\mathcal{C}$ is a near-group category* [Siehler 2003].
- (Theorem 6.12) *$\mathcal{C} = \operatorname{Rep} H$, where H is a semisimple quasitriangular Hopf algebra and $p = 2$.*

(iv) *Let H be a semisimple Hopf algebra such that* $\text{c.d.}(H) \subseteq \{1, p\}$. *Then H^* is nilpotent in any of the following cases*:

- (Proposition 4.8) *$|G(H^*)| = p$ and p divides $|G(H)|$.*
- (Proposition 4.9) *$|G(H^*)| = p$ and H is quasitriangular.*
- (Proposition 4.12) *H is of type $(1, p; p, 1)$ as an algebra.*

(v) *Let H be a semisimple Hopf algebra such that* $\text{c.d.}(H) \subseteq \{1, 2\}$. *Then*:

- (Theorem 6.4) *H is weakly group-theoretical, and, furthermore, it is group-theoretical if $H = H_{\text{ad}}$.*
- (Corollary 6.9) *The group $G(H)$ is solvable.*

(vi) (Theorem 4.13) *Let H be a semisimple Hopf algebra of type* $(1, p; p, 1)$ *as an algebra. Then H is isomorphic to a twisting of the group algebra kN, where either* $p = 2$ *and* $N = \mathbb{S}_3$ *or* $p = 2^{\alpha-1}$, $\alpha > 1$, *and N is the affine group of the field* $\mathbb{F}_{2^\alpha}$.

The proof of part (i) is a consequence of the Feit–Thompson theorem [1963], which asserts that every finite group of odd order is solvable.

By [Natale 2011, Corollary 4.5], the semisimple Hopf algebras H in part (iv) are *lower semisolvable* in the sense of [Montgomery and Witherspoon 1998].

The results on semisimple Hopf algebras H with $\text{c.d.}(H) \subseteq \{1, 2\}$ rely on the results of [Bichon and Natale 2011]. We also make strong use of several results of [Gelaki and Nikshych 2008; Gelaki and Naidu 2009; Etingof et al. 2011] on weakly group-theoretical, solvable, and nilpotent fusion categories.

Organization of the paper. In Section 2 we recall the main notions and results relevant to the problem we consider. In particular, several properties of group-theoretical fusion categories and Hopf algebra extensions are discussed here. The results on nilpotency are contained in Sections 3 and 4. The strategy in these sections consists in reducing the problem to considering Hopf algebra extensions. Sections 5, 6, and 7 are devoted to the solvability question in different situations.

2. Preliminaries

2A. ***Fusion categories.*** A *fusion category* over k is a k-linear semisimple rigid tensor category $\mathcal{C}$ with finitely many isomorphism classes of simple objects, finite-dimensional spaces of morphisms, and such that the unit object $\mathbf{1}$ of $\mathcal{C}$ is simple. We refer the reader to [Bakalov and Kirillov 2001; Etingof et al. 2005] for basic definitions and facts concerning fusion categories. In particular, if H is a semisimple (quasi-)Hopf algebra over k, then $\text{Rep}\, H$ is a fusion category.

A *fusion subcategory* of a fusion category $\mathcal{C}$ is a full tensor subcategory $\mathcal{C}' \subseteq \mathcal{C}$ such that if $X \in \mathcal{C}$ is isomorphic to a direct summand of an object of $\mathcal{C}'$, then $X \in \mathcal{C}'$. A fusion subcategory is necessarily rigid, so it is indeed a fusion category [Drinfeld et al. 2010, Corollary F.7(i)].

A *pointed fusion category* is a fusion category where all simple objects are invertible. A pointed fusion category is equivalent to the category $\mathcal{C}(G, \omega)$, of finite-dimensional G-graded vector spaces with associativity constraint determined by a cohomology class $\omega \in H^3(G, k^\times)$, for some finite group G. In other words, $\mathcal{C}(G, \omega)$ is the category of representations of the quasi-Hopf algebra k^G, with associator $\omega \in (k^G)^{\otimes 3}$.

The fusion subcategory *generated* by a collection $\mathcal{X}$ of objects of $\mathcal{C}$ is the smallest fusion subcategory containing $\mathcal{X}$.

If $\mathcal{C}$ is a fusion category, then the set of isomorphism classes of invertible objects of $\mathcal{C}$ forms a group, denoted $G(\mathcal{C})$. The fusion subcategory generated by the

invertible objects of $\mathcal{C}$ is a fusion subcategory, denoted $\mathcal{C}_{\mathrm{pt}}$; it is the maximal pointed subcategory of $\mathcal{C}$.

Let $\mathrm{Irr}(\mathcal{C})$ denote the set of isomorphism classes of simple objects in the fusion category $\mathcal{C}$. The set $\mathrm{Irr}(\mathcal{C})$ is a basis over $\mathbb{Z}$ of the Grothendieck ring $\mathcal{G}(\mathcal{C})$.

2B. ***Irreducible degrees.*** For $x \in \mathrm{Irr}(\mathcal{C})$, let $\mathrm{FPdim}\, x$ be its Frobenius–Perron dimension. The positive real numbers $\mathrm{FPdim}\, x$, $x \in \mathrm{Irr}(\mathcal{C})$, will be called the *irreducible degrees* of $\mathcal{C}$. These extend to a ring homomorphism $\mathrm{FPdim} : \mathcal{G}(\mathcal{C}) \to \mathbb{R}$. When $\mathcal{C}$ is the representation category of a quasi-Hopf algebra, Frobenius–Perron dimensions coincide with the dimensions of the underlying vector spaces.

The set of *irreducible degrees* of $\mathcal{C}$ is defined as

$$\mathrm{c.d.}(\mathcal{C}) = \{\mathrm{FPdim}\, x \mid x \in \mathrm{Irr}(\mathcal{C})\}.$$

The category $\mathcal{C}$ is called *integral* if $\mathrm{c.d.}(\mathcal{C}) \subseteq \mathbb{N}$.

If X is any object of $\mathcal{C}$, then its class x in $\mathcal{G}(\mathcal{C})$ decomposes as

$$x = \sum_{y \in \mathrm{Irr}(\mathcal{C})} m(y, x)y,$$

where $m(y, x) = \dim \mathrm{Hom}(Y, X)$ is the multiplicity of Y in X, if Y is an object representing the class $y \in \mathrm{Irr}(\mathcal{C})$.

For all $x, y, z \in \mathcal{G}(\mathcal{C})$, we have:

$$m(x, yz) = m(y^*, zx^*) = m(y, xz^*). \tag{2-1}$$

Let $x \in \mathrm{Irr}(\mathcal{C})$. The stabilizer of x under left multiplication by elements of $G(\mathcal{C})$ in the Grothendieck ring will be denoted by $G[x]$. So, an invertible element $g \in G(\mathcal{C})$ belongs to $G[x]$ if and only if $gx = x$.

In view of (2-1), for all $x \in \mathrm{Irr}(\mathcal{C})$, we have

$$G[x] = \{g \in G(\mathcal{C}) \colon m(g, xx^*) > 0\} = \{g \in G(\mathcal{C}) \colon m(g, xx^*) = 1\}.$$

In particular, we have the following relation in $\mathcal{G}(\mathcal{C})$:

$$xx^* = \sum_{g \in G[x]} g + \sum_{\substack{y \in \mathrm{Irr}(\mathcal{C}) \\ \mathrm{FPdim}\, y > 1}} m(y, xx^*)y.$$

Remark 2.1. An object $g \in \mathcal{C}$ is invertible if and only if $\mathrm{FPdim}\, g = 1$.

Suppose that $\mathcal{C}$ is an integral fusion category with $|\mathrm{c.d.}(\mathcal{C})| = 2$. That is, $\mathrm{c.d.}(\mathcal{C}) = \{1, d\}$ for some integer $d > 1$. We claim that d divides the order of $G[x]$ for all $x \in \mathrm{Irr}(\mathcal{C})$ with $\mathrm{FPdim}\, x > 1$; in particular, d divides the order of $G(\mathcal{C})$, and thus $G(\mathcal{C}) \neq 1$.

Indeed, if $x \in \mathrm{Irr}(\mathcal{C})$ with $\mathrm{FPdim}\, x = d$, we have the relation

$$xx^* = \sum_{g \in G[x]} g + \sum_{\substack{y \in \mathrm{Irr}(\mathcal{C}) \\ \mathrm{FPdim}\, y = d}} m(y, xx^*)y.$$

The claim follows by taking Frobenius–Perron dimensions.

2C. ***Semisimple Hopf algebras.*** Let H be a semisimple Hopf algebra over k. We next recall some of the terminology and conventions from [Natale 2007b] that will be used throughout this paper.

As an algebra, H is isomorphic to a direct sum of full matrix algebras

$$H \simeq k^{(n)} \oplus \bigoplus_{i=1}^{r} M_{d_i}(k)^{(n_i)}, \tag{2-2}$$

where $n = |G(H^*)|$. The Nichols–Zoeller theorem [Nichols and Zoeller 1989] implies that n divides both $\dim H$ and $n_i d_i^2$, for all $i = 1, \ldots, r$.

If we have an isomorphism as in (2-2), we shall say that H is *of type* $(1, n; d_1, n_1; \ldots; d_r, n_r)$ *as an algebra*. If H^* is of type $(1, n; d_1, n_1; \ldots; d_r, n_r)$ as an algebra, we shall say that H is *of type* $(1, n; d_1, n_1; \ldots; d_r, n_r)$ *as a coalgebra*.

Let V be an H-module. The *character* of V is the element $\chi = \chi_V \in H^*$ defined by $\chi(h) = \mathrm{Tr}_V(h)$, for all $h \in H$. For a character χ, its *degree* is the integer $\deg \chi = \chi(1) = \dim V$. The character χ_V is called irreducible if V is irreducible.

The set $\mathrm{Irr}(H)$ of irreducible characters of H spans a semisimple subalgebra $R(H)$ of H^*, called the character algebra of H. It is isomorphic, under the map $V \to \chi_V$, to the extension of scalars $k \otimes_{\mathbb{Z}} \mathcal{G}(\mathrm{Rep}\, H)$ of the Grothendieck ring of the category $\mathrm{Rep}\, H$. In particular, there is an identification $\mathrm{Irr}(H) \simeq \mathrm{Irr}(\mathrm{Rep}\, H)$.

Under this identification, all properties listed in Section 2B hold true for characters.

In this context, we have $G(\mathrm{Rep}\, H) = G(H^*)$. The stabilizer of χ under left multiplication by elements in $G(H^*)$ will be denoted by $G[\chi]$. By the Nichols–Zoeller theorem [Nichols and Zoeller 1989], we have that $|G[\chi]|$ divides $(\deg \chi)^2$.

Following [Isaacs 1976, Chapter 12], we use the notation $\mathrm{c.d.}(H) = \mathrm{c.d.}(\mathrm{Rep}\, H)$. Hence,

$$\mathrm{c.d.}(H) = \{\deg \chi \mid \chi \in \mathrm{Irr}(H)\}.$$

In particular, if H is of type $(1, n; d_1, n_1; \ldots; d_r, n_r)$ as an algebra, then $\mathrm{c.d.}(H) = \{1, d_1, \ldots, d_r\}$.

There is a bijective correspondence between Hopf algebra quotients of H and standard subalgebras of $R(H)$, that is, subalgebras spanned by irreducible characters of H. This correspondence assigns to the Hopf algebra quotient $H \to \overline{H}$ its character algebra $R(\overline{H}) \subseteq R(H)$. See [Nichols and Richmond 1996].

2D. ***Group-theoretical categories.*** A group-theoretical fusion category is a fusion category Morita equivalent to a pointed fusion category $\mathcal{C}(G, \omega)$. Such a fusion category is equivalent to the category $\mathcal{C}(G, \omega, F, \alpha)$ of $k_\alpha F$-bimodules in $\mathcal{C}(G, \omega)$, where G is a finite group, ω is a 3-cocycle on G, $F \subseteq G$ is a subgroup, and $\alpha \in C^2(F, k^\times)$ is a 2-cochain on F such that $\omega|_F = d\alpha$. A semisimple Hopf algebra H is called group-theoretical if the category $\operatorname{Rep} H$ is group-theoretical.

Let $\mathcal{C} = \mathcal{C}(G, \omega, F, \alpha)$ be a group-theoretical fusion category. Let also Γ be a subgroup of G, endowed with a 2-cocycle $\beta \in Z^2(\Gamma, k^\times)$, such that:

- The class $\omega|_\Gamma$ is trivial.
- $G = F\Gamma$.
- The class $\alpha|_{F\cap\Gamma}\beta^{-1}|_{F\cap\Gamma}$ is nondegenerate.

Then there is an associated semisimple Hopf algebra H, such that the category $\operatorname{Rep} H$ is equivalent to $\mathcal{C}$. By [Ostrik 2003], equivalence classes of subgroups Γ of G satisfying the conditions above classify fiber functors $\mathcal{C} \mapsto \mathrm{Vec}$; these correspond to the distinct Hopf algebras H.

Let $\mathcal{C} = \mathcal{C}(G, \omega, F, \alpha)$ be a group-theoretical fusion category. The simple objects of $\mathcal{C}$ are classified by pairs (s, U_s), where s runs over a set of representatives of the double cosets of F in G, that is, orbits of the action of F in the space $F\backslash G$ of left cosets of F in G, $F_s = F \cap sFs^{-1}$ is the stabilizer of $s \in F\backslash G$, and U_s is an irreducible representation of the twisted group algebra $k_{\sigma_s} F_s$, that is, an irreducible projective representation of F_s with respect to a certain 2-cocycle σ_s determined by ω; see [Gelaki and Naidu 2009, Theorem 5.1].

The irreducible representation $W_{(s,U_s)}$ corresponding to such a pair (s, U_s) has dimension

$$\dim W_{(s,U_s)} = [F : F_s] \dim U_s. \tag{2-3}$$

Corollary 2.2. *The irreducible degrees of $\mathcal{C}(G, \omega, F, \alpha)$ divide the order of F.*

Remark 2.3. A group-theoretical category $\mathcal{C} = \mathcal{C}(G, \omega, F, \alpha)$ is an integral fusion category. An explicit construction of a quasi-Hopf algebra H such that $\operatorname{Rep} H \simeq \mathcal{C}$ was given in [Natale 2005].

As an algebra, H is a crossed product $k^{F\backslash G} \#_\sigma kF$, where $F\backslash G$ is the space of left cosets of F in G with the natural action of F, and σ is a certain 2-cocycle determined by ω.

Irreducible representations of H, that is, simple objects of $\mathcal{C}$, can therefore be described using the results for group crossed products in [Montgomery and Witherspoon 1998]: this is done in [Natale 2005, Proposition 5.5].

By [Gelaki and Naidu 2009, Theorem 5.2], the group $G(\mathcal{C})$ of invertible objects of $\mathcal{C}$ fits into an exact sequence

$$1 \to \widehat{F} \to G(\mathcal{C}) \to K \to 1, \tag{2-4}$$

where $K = \{x \in N_G(F) \colon [\sigma_x] = 1\}$.

2E. ***Abelian extensions.*** Suppose that $G = F\Gamma$ is an exact factorization of the finite group G, where Γ and F are subgroups of G. Equivalently, F and Γ form a *matched pair* of groups with the actions $\triangleleft\colon \Gamma \times F \to \Gamma$ and $\triangleright\colon \Gamma \times F \to F$, defined by $sx = (x \triangleleft s)(x \triangleright s)$, $x \in F$, $s \in \Gamma$. In this case, G is isomorphic to the group $F \bowtie \Gamma$ defined as follows: $F \bowtie \Gamma = F \times \Gamma$, with multiplication $(x, s)(t, y) = (x(s \triangleright y), (s \triangleleft y)t)$, for all $x, y \in F$, $s, t \in \Gamma$.

Let $\sigma \in Z^2(F, (k^\Gamma)^\times)$ and $\tau \in Z^2(\Gamma, (k^F)^\times)$ be normalized 2-cocycles with respect to the actions afforded, respectively, by $\triangleleft$ and $\triangleright$, subject to appropriate compatibility conditions [Masuoka 1999].

The bicrossed product $H = k^{\Gamma\,\tau}\#_\sigma kF$ associated to this data is a semisimple Hopf algebra. There is an *abelian* exact sequence

$$k \to k^\Gamma \to H \to kF \to k. \tag{2-5}$$

Moreover, every Hopf algebra H fitting into such an exact sequence can be described in this way. This gives a bijective correspondence between the equivalence classes of Hopf algebra extensions (2-5) associated to the matched pair (F, Γ) and a certain abelian group $\mathrm{Opext}(k^\Gamma, kF)$.

Remark 2.4. The Hopf algebra H is group theoretical. In fact, by [Natale 2003, Section 4.2], we have an equivalence of fusion categories $\mathrm{Rep}\, H \simeq \mathcal{C}(G, \omega, F, 1)$, where ω is the 3-cocycle on G coming from the so-called *Kac exact sequence*.

Irreducible representations of H are classified by pairs (s, U_s), where s runs over a set of representatives of the orbits of the action of F in Γ, $F_s = F \cap sFs^{-1}$ is the stabilizer of $s \in \Gamma$, and U_s is an irreducible representation of the twisted group algebra $k_{\sigma_s}F_s$, that is, an irreducible projective representation of F_s with cocycle σ_s, where $\sigma_s(x, y) = \sigma(x, y)(s)$, $x, y \in F$, $s \in \Gamma$; see [Kashina et al. 2002].

Note that, for all $s \in \Gamma$, the restriction of $\sigma_s : F \times F \to k^\times$ to the stabilizer F_s indeed defines a 2-cocycle on F_s.

The irreducible representation corresponding to such a pair (s, U_s) is in this case of the form

$$W_{(s,U_s)} := \mathrm{Ind}_{k^\Gamma \otimes kF_s}^H s \otimes U_s. \tag{2-6}$$

2F. ***Quasitriangular Hopf algebras.*** Let H be a finite-dimensional Hopf algebra. Recall that H is called *quasitriangular* if there exists an invertible element $R \in H \otimes H$, called an *R-matrix*, such that

$$\begin{aligned}
&(\Delta \otimes \mathrm{id})(R) = R_{13}R_{23}, \quad && (\epsilon \otimes \mathrm{id})(R) = 1,\\
&(\mathrm{id} \otimes \Delta)(R) = R_{13}R_{12}, \quad && (\mathrm{id} \otimes \epsilon)(R) = 1,\\
&\Delta^{\mathrm{cop}}(h) = R\Delta(h)R^{-1} \quad && \text{for all } h \in H.
\end{aligned}$$

The existence of an R-matrix (also called a *quasitriangular structure* in what follows) amounts to the category $\operatorname{Rep} H$ being a braided tensor category; see [Bakalov and Kirillov 2001].

For instance, the group algebra kG of a finite group G is a quasitriangular Hopf algebra with $R = 1 \otimes 1$. On the other hand, the dual Hopf algebra k^G admits a quasitriangular structure if and only if G is abelian.

If it exists, a quasitriangular structure in a Hopf algebra H need not be unique.

Another example of a quasitriangular Hopf algebra is the *Drinfeld double* $D(H)$ of H, where H is any finite-dimensional Hopf algebra. We have $D(H) = H^{*\,\mathrm{cop}} \otimes H$ as coalgebras, with a canonical R-matrix $\mathcal{R} = \sum_i h^i \otimes h_i$, where $(h_i)_i$ is a basis of H and $(h^i)_i$ is the dual basis.

As braided tensor categories, $\operatorname{Rep} D(H) = \mathcal{Z}(\operatorname{Rep} H)$ is equivalent to the center of the tensor category $\operatorname{Rep} H$.

Suppose (H, R) is a quasitriangular Hopf algebra. There are Hopf algebra maps $f_R : H^{*\mathrm{cop}} \to H$ and $f_{R_{21}} : H^* \to H^{\mathrm{op}}$ defined by

$$f_R(p) = p(R^{(1)})R^{(2)}, \quad f_{R_{21}}(p) = p(R^{(2)})R^{(1)},$$

for all $p \in H^*$, where $R = R^{(1)} \otimes R^{(2)} \in H \otimes H$.

We shall denote $f_R(H^*) = H_+$ and $f_{R_{21}}(H^*) = H_-$, respectively. Hence H_+ and H_- are Hopf subalgebras of H and we have $H_+ \simeq (H_-^*)^{\mathrm{cop}}$.

We shall also denote by $H_R = H_- H_+ = H_+ H_-$ the minimal quasitriangular Hopf subalgebra of H; see [Radford 1993].

By [Radford 1993, Theorem 2], the multiplication of H determines a surjective Hopf algebra map $D(H_-) \to H_R$.

A quasitriangular Hopf algebra (H, R) is called *factorizable* if the map $\Phi_R : H^* \to H$ is an isomorphism, where

$$\Phi_R(p) = p(Q^{(1)})Q^{(2)}, \quad p \in H^*; \tag{2-7}$$

here, $Q = Q^{(1)} \otimes Q^{(2)} = R_{21}R \in H \otimes H$ [Reshetikhin and Semenov-Tian-Shansky 1988].

If on the other hand $\Phi_R = \epsilon 1$ (or equivalently, $R_{21}R = 1 \otimes 1$), then (H, R) is called *triangular*. Finite-dimensional triangular Hopf algebras were completely classified in [Etingof and Gelaki 2003]. In particular, if (H, R) is a semisimple quasitriangular Hopf algebra, then H is isomorphic, as a Hopf algebra, to a twisting $(kG)^J$ of some finite group G.

It is well known that the Drinfeld double $(D(H), \mathcal{R})$ is indeed a *factorizable* quasitriangular Hopf algebra. We have $D(H)_+ = H$ and $D(H)_- = H^{*\mathrm{cop}}$.

We shall use later on in this paper the following result about factorizable Hopf algebras. A categorical version is established in [Gelaki and Nikshych 2008].

Theorem 2.5 [Schneider 2001, Theorem 2.3]. *Let (H, R) be a factorizable Hopf algebra. Then the map Φ_R induces an isomorphism of groups $G(H^*) \to G(H) \cap Z(H)$.*

Note that we may identify $G(D(H)) = G(H^*) \times G(H)$. Under this identification, Theorem 2.5 gives us a group isomorphism

$$G(D(H)^*) \to G(D(H)) \cap Z(D(H)),$$

such that $g\#f \mapsto f\#g$. See also [Radford 1993].

In particular, if $f = \epsilon$, then $g \in G(H) \cap Z(H)$, and also if $g = 1$, then $f \in G(H^*) \cap Z(H^*)$.

Suppose (H, R) is a finite-dimensional quasitriangular Hopf algebra, and let $D(H)$ be the Drinfeld double of H. Then there is a surjective Hopf algebra map $f : D(H) \to H$, such that $(f \otimes f)\mathcal{R} = R$. The map f is determined by $f(p \otimes h) = f_R(p)h$, for all $p \in H^*$, $h \in H$.

This corresponds to the canonical inclusion of the braided tensor category Rep H (with braiding determined by the action of the R-matrix) into its center.

In particular, in the case where H is quasitriangular, the group $G(H^*)$ can be identified with a subgroup of $G(D(H)^*)$.

3. Nilpotency

Let G be a finite group. A *G-grading* of a fusion category $\mathcal{C}$ is a decomposition of $\mathcal{C}$ as a direct sum of full abelian subcategories $\mathcal{C} = \bigoplus_{g \in G} \mathcal{C}_g$, such that $\mathcal{C}_g^* = \mathcal{C}_{g^{-1}}$ and the tensor product $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ maps $\mathcal{C}_g \times \mathcal{C}_h$ to $\mathcal{C}_{gh}$. The neutral component $\mathcal{C}_e$ is thus a fusion subcategory of $\mathcal{C}$.

The grading is called *faithful* if $\mathcal{C}_g \neq 0$, for all $g \in G$. In this case, $\mathcal{C}$ is called a *G-extension* of $\mathcal{C}_e$ [Etingof et al. 2011].

The following proposition is a consequence of [Gelaki and Nikshych 2008, Theorem 3.8].

Proposition 3.1. *Let $\mathcal{C} =$* Rep H*, where H is a semisimple Hopf algebra. Then a faithful G-grading on $\mathcal{C}$ corresponds to a* central *exact sequence of Hopf algebras $k \to k^G \to H \to \overline{H} \to k$, such that* Rep $\overline{H} = \mathcal{C}_e$.

Let $\mathcal{C}$ be a fusion category and let $\mathcal{C}_{\mathrm{ad}}$ be the adjoint subcategory of $\mathcal{C}$. That is, $\mathcal{C}_{\mathrm{ad}}$ is the fusion subcategory of $\mathcal{C}$ generated by $X \otimes X^*$, where X runs through the simple objects of $\mathcal{C}$.

It is shown in [Gelaki and Nikshych 2008] that there is a canonical faithful grading on $\mathcal{C}$: $\mathcal{C} = \bigoplus_{g \in U(\mathcal{C})} \mathcal{C}_g$, called the *universal grading*, such that $\mathcal{C}_e = \mathcal{C}_{\mathrm{ad}}$. The group $U(\mathcal{C})$ is called the *universal grading group* of $\mathcal{C}$.

In the case where $\mathcal{C} = \operatorname{Rep} H$, for a semisimple Hopf algebra H, $K = k^{U(\mathcal{C})}$ is the maximal central Hopf subalgebra of H and $\mathcal{C}_{\mathrm{ad}} = \operatorname{Rep} H/HK^+$ [Gelaki and Nikshych 2008, Theorem 3.8].

Recall from [Gelaki and Nikshych 2008; Etingof et al. 2011] that a fusion category $\mathcal{C}$ is called (cyclically) *nilpotent* if there is a sequence of fusion categories

$$\mathcal{C}_0 = \mathrm{Vec},\ \mathcal{C}_1,\ \ldots,\ \mathcal{C}_n = \mathcal{C}$$

and a sequence $G_1, \ldots, G_n$ of finite (cyclic) groups such that $\mathcal{C}_i$ is faithfully graded by G_i with trivial component $\mathcal{C}_{i-1}$.

The semisimple Hopf algebra H is called nilpotent if the fusion category $\operatorname{Rep} H$ is nilpotent [Gelaki and Nikshych 2008, Definition 4.4].

For instance, if G is a finite group, then the dual group algebra k^G is always nilpotent. However, the group algebra kG is nilpotent if and only if the group G is nilpotent [Gelaki and Nikshych 2008, Remark 4.7(1)].

3A. ***Nilpotency of an abelian extension.*** It is shown in [Gelaki and Naidu 2009, Corollary 4.3] that a group-theoretical fusion category $\mathcal{C}(G, \omega, F, \alpha)$ is nilpotent if and only if the normal closure of F in G is nilpotent. On the other hand, this happens if and only if F is nilpotent and subnormal in G, if and only if $F \subseteq \operatorname{Fit}(G)$, where $\operatorname{Fit}(G)$ is the Fitting subgroup of G, that is, the unique largest normal nilpotent subgroup of G [Gelaki and Naidu 2009, §2.3].

Combined with Remark 2.4, this implies:

Proposition 3.2. *Let $k \to k^\Gamma \to H \to kF \to k$ be an abelian exact sequence and let $G = F \bowtie \Gamma$ be the associated factorizable group. Then H is nilpotent if and only if $F \subseteq \operatorname{Fit}(G)$.*

An abelian exact sequence (2-5) is called *central* if the image of k^Γ is a central Hopf subalgebra of H. It is called cocentral if the dual exact sequence is central.

The following facts are well known:

Lemma 3.3. *Consider an abelian exact sequence* (2-5).

(i) *The sequence is central if and only if the action $\triangleleft\colon \Gamma \times F \to \Gamma$ is trivial. In this case, the group $G = F \bowtie \Gamma$ is a semidirect product $G \simeq F \rtimes \Gamma$ with respect to the action $\triangleright\colon \Gamma \times F \to F$.*

(ii) *The sequence is cocentral if and only if the action $\triangleright\colon \Gamma \times F \to F$ is trivial. In this case, the group $G = F \bowtie \Gamma$ is a semidirect product $G \simeq F \ltimes \Gamma$ with respect to the action $\triangleleft\colon \Gamma \times F \to \Gamma$.* □

Remark 3.4. Assume the exact sequence (2-5) is central. Then F is a normal subgroup of G. It follows from Proposition 3.2 that H is nilpotent if and only if F is nilpotent.

4. On the nilpotency of a class of semisimple Hopf algebras

Let p be a prime number. We shall consider in this subsection a nontrivial semisimple Hopf algebra H fitting into an abelian exact sequence

$$k \to k^{\mathbb{Z}_p} \to H \to kF \to k. \tag{4-1}$$

The main result of this subsection is Proposition 4.3 below.

Suppose that $\mathcal{C}$ is any group-theoretical fusion category of the form $\mathcal{C} = \mathcal{C}(G, \omega, \mathbb{Z}_p, \alpha)$ (note that we may assume that $\alpha = 1$). In particular, p divides the order of $G(\mathcal{C})$. We also have c.d.$(\mathcal{C}) \subseteq \{1, p\}$, by Corollary 2.2.

Lemma 4.1. *Let $\mathcal{C} = \mathcal{C}(G, \omega, \mathbb{Z}_p, \alpha)$. Assume that $|G(\mathcal{C})| = p$. Then G is a Frobenius group with Frobenius complement $\mathbb{Z}_p$.*

Proof. The description of the irreducible representations of $\mathcal{C}$ in Section 2D, combined with the assumption that $|G(\mathcal{C})| = p$, implies that $g\mathbb{Z}_p g^{-1} \cap \mathbb{Z}_p = \{e\}$, for all $g \in G \backslash \mathbb{Z}_p$. (In particular, the action of $\mathbb{Z}_p$ on $\mathbb{Z}_p \backslash G$ has no fixed points $s \neq e$.)

This condition says that G is a Frobenius group with Frobenius complement $\mathbb{Z}_p$, as claimed. □

Remark 4.2. Let G be a Frobenius group with Frobenius complement $\mathbb{Z}_p$, as in Lemma 4.1. By the Frobenius theorem we have that the Frobenius kernel N is a normal subgroup of G, such that G is a semidirect product $G = N \rtimes \mathbb{Z}_p$. Moreover, N is a nilpotent group, by a theorem of Thompson. See [Isaacs 1976, Theorem 7.2; Robinson 1982, Theorem 10.5.6]. In fact, the Frobenius kernel N is equal to Fit(G), the Fitting subgroup of G [Robinson 1982, Exercise 10.5.8].

As a consequence we get the following:

Proposition 4.3. *Consider the abelian exact sequence* (4-1) *and assume that $|G(H)| = p$.*

(i) *The sequence is central, that is, $G(H) \subseteq Z(H)$.*

(ii) *$G = F \bowtie \mathbb{Z}_p$ is a Frobenius group with kernel F. In particular, F is nilpotent.*

Proof. We follow the lines of the proof of [Izumi and Kosaki 2002, Proposition X.7(i)]. Consider the matched pair $(F, \mathbb{Z}_p)$ associated to (4-1), as in Section 2E. Let $G = F \bowtie \mathbb{Z}_p$ be the corresponding factorizable group.

We have an equivalence of fusion categories $\mathrm{Rep}\, H^* \simeq \mathcal{C}(G, \omega, \mathbb{Z}_p, 1)$; see Remark 2.4. Then $\mathrm{Rep}\, H^*$ is group-theoretical and, by assumption, $G(\mathrm{Rep}\, H^*)$ is of order p. By Lemma 4.1, G is a Frobenius group with Frobenius complement $\mathbb{Z}_p$. Therefore G is a semidirect product $G = N \rtimes \mathbb{Z}_p$, where $N = \mathrm{Fit}(G)$ is a nilpotent subgroup (see Remark 4.2).

Since $|G(H)| = p$, then the action of $\mathbb{Z}_p$ on F has no fixed points. It follows, after decomposing F as a disjoint union of $\mathbb{Z}_p$-orbits, that $|F| = 1 \pmod p$. In particular, $|F|$ is not divisible by p. Then F must map trivially under the canonical projection $G \to G/N$, that is, $F \subseteq N$. Hence $F = N$, because they have the same order. This shows (ii). Since F is normal in G, we get (i) in view of Lemma 3.3. □

Corollary 4.4. *Let $k \to k^{\mathbb{Z}_p} \to H \to kF \to k$ be an abelian exact sequence such that $|G(H)| = p$. Then H is nilpotent.*

Proof. It follows from Proposition 4.3, in view of Remark 3.4. □

Remark 4.5. In view of [Izumi and Kosaki 2002, Theorem IX.8(iii)], if H is a Kac algebra with $\text{c.d.}(H^*) = \{1, p\}$ and $|G(H)| = p$, then H is a central abelian extension associated to an action of the cyclic group of order p on a nilpotent group. It follows from Corollary 4.4 that H is a nilpotent Hopf algebra.

Remark 4.6. Note that the (dual) assumption that $\text{c.d.}(H) = \{1, p\}$ does not imply that H is nilpotent in general. For example, take H to be the group algebra of a nonabelian semidirect product $F \rtimes \mathbb{Z}_p$, where F is an abelian group such that $(|F|, p) = 1$.

On the other hand, the assumption on $|G(H)|$ in Corollary 4.4 and Proposition 4.3 is essential. Namely, for all prime number p, there exist semisimple Hopf algebras H with $\text{c.d.}(H^*) = \{1, p\}$ and such that H is *not* nilpotent.

To see an example, consider a group F with an automorphism of order p and suppose F is not nilpotent (take, for instance, $F = \mathbb{S}_n$, a symmetric group, such that $n > 6$ is sufficiently large). Consider the corresponding action of $\mathbb{Z}_p$ on F by group automorphisms and let $G = F \rtimes \mathbb{Z}_p$ be the semidirect product.

Then there is an associated (split) abelian exact sequence $k \to k^{\mathbb{Z}_p} \to H \to kF \to k$, such that H is not commutative and not cocommutative. Moreover, in view of Corollary 2.2, $\text{c.d.}(H^*) = \{1, p\}$. But, by Remark 3.4, H is not nilpotent, because F is not nilpotent by assumption.

4A. ***Reduction to abelian extensions from character degrees.*** In this subsection we consider the case where $\text{c.d.}(H) = \{1, p\}$ for some prime p and $|G(H^*)| = p$. We treat the problem of deducing an abelian extension like (4-1) from this assumption.

It is known, for instance, that if $p = 2$, then the assumption implies that H is cocommutative [Izumi and Kosaki 2002, Corollary IX.9; Bichon and Natale 2011, Proposition 6.8].

Lemma 4.7. *If $\text{c.d.}(H^*) = \{1, p\}$ for some prime p, then $H/(kG(H))^+H$ is a cocommutative coalgebra.*

Proof. Let χ be an irreducible character of degree p. We have that

$$\chi\chi^* = \sum_{g \in G[\chi]} g + \sum_{\deg \lambda = p} \lambda.$$

So $p \,|\, |G[\chi]|$. Therefore $|G[\chi]|$ is either $p = \deg \chi$ or p^2, because it divides $(\deg \chi)^2$.

Moreover, since $\chi = g\chi$ for all $g \in G[\chi]$, we have $G[\chi]C = C$, where C is the simple subcoalgebra of H containing χ. Then it follows from [Natale 2007b, Remark 3.2.7] that $C/(kG[\chi])^+C$ is a cocommutative coalgebra (indeed, $|G[\chi]|$ is either $p = \deg \chi$ or p^2, but in the last case, $C/(kG[\chi])^+C$ is one-dimensional, hence also cocommutative). Then $H/(kG(H))^+H$ is a cocommutative coalgebra, by [Natale 2007b, Corollary 3.3.2]. □

4B. ***Results for the type*** **(1, *p*; *p*, *n*).** Let p be a prime number. In this subsection H will be a semisimple Hopf algebra such that c.d.$(H) = \{1, p\}$ and $|G(H^*)| = p$. Hence H is of type $(1, p; p, n)$ as an algebra.

Proposition 4.8. *Suppose that p divides $|G(H)|$. Then $G(H^*) \subseteq Z(H^*)$ and H^* is nilpotent.*

Proof. By assumption, there is a subgroup G of $G(H)$ with $|G| = p$ (that is, $G \simeq \mathbb{Z}_p$) and the Hopf algebra inclusion $kG \to H$ induces the following sequence:

$$kG(H^*) \xrightarrow{i} H^* \xrightarrow{\pi} kG,$$

with π surjective. Set $A = kG(H^*)$ and $B = kG$. By [Natale 2007b, Lemma 4.1.9], $\pi \circ i : kG(H^*) \to kG$ is an isomorphism and $H^* \simeq R\#kG(H^*) \simeq R\#\mathbb{Z}_p$ is a biproduct, where $R \doteq (H^*)^{\mathrm{co}\,\pi}$ is a semisimple braided Hopf algebra over $\mathbb{Z}_p$. The coalgebra R is cocommutative, by Lemma 4.7, because $R \simeq H^*/H^*kG(H^*)^+$ as coalgebras. Since $p \nmid 1 + np = \dim R$ then by [Sommerhäuser 2002, Proposition 7.2], R is trivial. Therefore, by [Natale 2007b, Proposition 4.6.1], H^* fits into an abelian *central* exact sequence

$$k \to k\mathbb{Z}_p \to H^* \to R \to k.$$

Now, since the extension is abelian, there is a group F such that $R \simeq kF$. It follows from Corollary 4.4 that H^* is nilpotent. □

Proposition 4.9. *Suppose H is quasitriangular. Then $G(H^*) \subseteq Z(H^*)$ and H^* is nilpotent.*

Proof. Consider the Drinfeld double $D(H)$. Since H is quasitriangular, $G(H^*) \simeq \mathbb{Z}_p$ is isomorphic to a subgroup of $G(D(H)^*)$. Then $G(D(H)^*)$ has an element $g\#f$ of order p. We have

$$G(D(H)^*) \simeq G(D(H)) \cap Z(D(H)) \subseteq G(D(H)) = G(H^*) \times G(H);$$

see Section 2F.

In particular, the element $f\#g \in G(D(H)) \cap Z(D(H))$ is of order p. If g is of order p, then the proposition follows from Proposition 4.8. Thus we may assume that $g = 1$. Then $f \in G(H^*) \cap Z(H^*)$ is of order p, implying that $G(H^*) \subseteq Z(H^*)$.

Therefore H^* fits into an abelian central exact sequence

$$k \to k^{\mathbb{Z}_p} \to H^* \to kF \to k,$$

where F is a finite group such that $kF \simeq H^*/H^*(k^{\mathbb{Z}_p})^+$, by Lemma 4.7. In view of the assumption on the algebra structure of H, Corollary 4.4 implies that H^* is nilpotent, as claimed. □

4C. ***Results for the type*** **(1, *p*; *p*, 1).** We next discuss the case where H is of type $(1, p; p, 1)$ as an algebra (not necessarily quasitriangular). In particular, $\dim H = p(p+1)$ is even.

Notice that under this assumption, the category Rep H is a *near-group category* with fusion rule given by the group $G = G(H^*) \simeq \mathbb{Z}_p$ and the integer κ [Siehler 2003].

Let χ be the irreducible character of degree p. It follows that $\chi = \chi^*$ and $\chi g = \chi = g\chi$. Then

$$\chi^2 = \sum_{g \in G(H^*)} g + \kappa\chi.$$

Taking degrees in the equation above we obtain $p^2 = p + \kappa p$, which means that $\kappa = p - 1$.

We shall use the following proposition. A more general statement will be proved in Theorem 6.2.

Proposition 4.10. *Suppose H is of type $(1, p; p, 1)$ as an algebra. Then either*

(i) $p = 2$ *and* $H \simeq k\mathbb{S}_3$, *or*

(ii) $p = 2^\alpha - 1$[1] *and* $\dim H = 2^\alpha p$.

In particular, H is solvable.

Proof. By [Siehler 2003, Theorem 1.2], it follows that $G(H^*) \simeq \mathbb{Z}_{q^\alpha - 1}$, for some prime q and $\alpha \geq 1$. Therefore $p = q^\alpha - 1$. If $q > 2$, then $p = 2$, which implies $H \simeq k\mathbb{S}_3$ is cocommutative. If $q = 2$, then p has the particular expression $p = 2^\alpha - 1$.

Hence $\dim H$ equals 6 or $p(p+1) = 2^\alpha p$. By Burnside's theorem for fusion categories [Etingof et al. 2011, Theorem 1.6], H is solvable. □

Remark 4.11. Let p be a prime number such that $p = 2^\alpha - 1$, as in Proposition 4.10. Consider the affine group N of the field $\mathbb{F}_{2^\alpha}$, that is, N is the semidirect product $\mathbb{F}_{2^\alpha} \rtimes \mathbb{F}_{2^\alpha}^\times$ with respect to the natural action of $\mathbb{F}_{2^\alpha}^\times$ on $\mathbb{F}_{2^\alpha}$. Then the group N has the prescribed algebra type (see [Siehler 2003, §4.1]).

[1] Such a prime number is called a *Mersenne prime*; in particular α must be prime.

Furthermore, suppose p is (any) prime number, and N is a group whose group algebra has algebra type $(1, p; p, 1)$. Then N has order $p(p+1)$ and it follows from the main result of [Seitz 1968] that either $p = 2$ and $N \simeq \mathbb{S}_3$ or $p = 2^\alpha - 1$, $\alpha > 1$, and $N \simeq \mathbb{F}_{2^\alpha} \rtimes \mathbb{F}_{2^\alpha}^\times$.

Proposition 4.12. *Let H be a semisimple Hopf algebra of type $(1, p; p, 1)$ as an algebra. Then $G(H^*) \subseteq Z(H^*)$ and H^* is nilpotent.*

Proof. We have just proved in Proposition 4.10 that under this hypothesis H is solvable. Since $\operatorname{Rep} D(H) \simeq Z(\operatorname{Rep} H)$, then $D(H)$ is also solvable [Etingof et al. 2011, Proposition 4.5(i)].

By [Etingof et al. 2011, Proposition 4.5(iv)], $D(H)$ has nontrivial representations of dimension 1, that is, $|G(D(H)^*)| \neq 1$. We have

$$G(D(H)^*) \simeq G(D(H)) \cap Z(D(H)) \subseteq G(D(H)) = G(H^*) \times G(H);$$

see Section 2F.

We next argue as in the proof of Proposition 4.9. Consider an element $1 \neq f\#g \in G(D(H)) \cap Z(D(H))$. If $f = 1$, then $1 \neq g \in Z(H) \cap G(H)$. Therefore, H^* fits into a cocentral extension $k \to K \to H^* \to k^{\langle g \rangle} \to k$, where K is a *proper* normal Hopf subalgebra. The assumption on the algebra structure of H implies that $K = kG(H^*)$. Thus $kG(H^*)$ is normal in H^*, and the extension is abelian, by Lemma 4.7. The proposition follows in this case from Proposition 4.3(i) and Corollary 4.4.

Thus we may assume that $f \neq 1$. In particular, f has order p.

If $|f| = |g| = p = |G(H^*)|$, we have that $p \,|\, |G(H)|$. Then $G(H^*) \subseteq Z(H^*)$ and H^* is nilpotent, by Proposition 4.8.

Otherwise, take $|g| = n$, with $p \neq n$. If $f^n = 1$, then p divides n and thus p divides $|G(H)|$. As before, we are done by Proposition 4.8.

If $f^n \neq 1$, then $f^n\#1 = (f^n\#g^n) = (f\#g)^n \in Z(D(H))$, which implies that $f^n \neq 1$ is central in H^* and thus $G(H^*) \subseteq Z(H^*)$.

Therefore H^* fits into an abelian central exact sequence

$$k \to k^{\mathbb{Z}_p} \to H^* \to kF \to k,$$

where F is a finite group such that $kF \simeq H^*/H^*(k^{\mathbb{Z}_p})^+$, by Lemma 4.7. In view of the assumption on the algebra structure of H, Corollary 4.4 implies that H^* is nilpotent, as claimed. □

Theorem 4.13. *Let H be a semisimple Hopf algebra of type $(1, p, p, 1)$ as an algebra. Then either $p = 2$ and $H \simeq k\mathbb{S}_3$, or H is isomorphic to a twisting of the group algebra kN, where $p = 2^\alpha - 1$, $\alpha > 1$, and N is the affine group of the field $\mathbb{F}_{2^\alpha}$.*

Proof. If $p = 2$, then $\dim H = 6$ and the result follows from [Masuoka 1995]. So suppose that p is odd. By Propositions 4.12 and 4.10, H^* fits into an abelian central exact sequence $k \to k^{\mathbb{Z}_p} \to H^* \to kF \to k$, where F is a finite group of order $p + 1 = 2^\alpha$. Then the action $\triangleleft\colon \mathbb{Z}_p \times F \to \mathbb{Z}_p$ is trivial, while the action $\triangleright\colon \mathbb{Z}_p \times F \to F$ is determined by an automorphism $\varphi \in \operatorname{Aut} F$ of order $p = 2^\alpha - 1$.

We first claim that the group F must be abelian. By a result of P. Hall [Robinson 1982, (5.3.3)], since F is a 2-group, the order of $\operatorname{Aut} F$ divides the number $n2^{(\alpha-r)r}$, where $n = |\mathrm{GL}(r, 2)|$ and 2^r equals the index in F of the Frattini subgroup $\operatorname{Frat}(F)$ (which is defined as the intersection of all the maximal subgroups of F [Robinson 1982, p. 135]). In particular, we have $r \le \alpha$.

Since the order of φ divides the order of $\operatorname{Aut} F$ and $|\mathrm{GL}(r, 2)| = (2^r - 1)(2^r - 2) \ldots (2^r - 2^{r-1})$, it follows that the prime $p = 2^\alpha - 1$ divides $2^r - 1$, which means that $r = \alpha$ and, therefore, $\operatorname{Frat}(F) = 1$.

Since F is nilpotent (because it is a 2-group), a result of Wielandt [Robinson 1982, (5.2.16)] implies that $[F, F]$, the commutator subgroup of F, is a subgroup of the Frattini subgroup $\operatorname{Frat}(F)$. As we have just shown, we have $\operatorname{Frat}(F) = 1$ in this case. Thus $[F, F] = 1$ and therefore F is abelian, as claimed.

Consider the split extension $B_0 = k^{\mathbb{Z}_p} \# kF$ associated to the matched pair $(\mathbb{Z}_p, F)$. Since F is abelian, B_0 (being a central extension) is commutative. This means that B_0 is isomorphic to k^N, where $N = F \rtimes \mathbb{Z}_p$.

Notice that $|F| = 2^\alpha$ is relatively prime to p. It follows from [Natale 2007a, Proposition 5.22] and [Masuoka 2002, Proposition 3.1] that H^* is obtained from the split extension $B_0 = k^{\mathbb{Z}_p} \# kF \simeq k^N$ by twisting the multiplication. Indeed, the element representing the class of H^* in the group $\operatorname{Opext}(kF, k^{\mathbb{Z}_p})$ is the image of an element of $H^2(F, k^\times)$ under the map $H^2(F, k^\times) \oplus H^2(\mathbb{Z}_p, k^\times) \simeq H^2(F, k^\times) \to \operatorname{Opext}(kF, k^{\mathbb{Z}_p})$ in the Kac exact sequence [Masuoka 2002, Theorem 1.10]. Then the claim follows from [Masuoka 2002, Proposition 3.1]. Dualizing, we get that H is a twisting of the group algebra of the group N.

Finally, the assumption on the algebra structure of H implies that N is one of the claimed groups. See Remark 4.11. □

Corollary 4.14. *Let H be a semisimple Hopf algebra of type $(1, p, p, 1)$ as an algebra. Then* $\operatorname{Rep} H \simeq \operatorname{Rep} N$, *where $N = \mathbb{S}_3$ or N is the affine group of the field $\mathbb{F}_{2^\alpha}$, for some $\alpha > 1$.*

5. Solvability

Recall from [Etingof et al. 2011] that a fusion category $\mathcal{C}$ is called *weakly group-theoretical* if it is Morita equivalent to a nilpotent fusion category. If, furthermore, $\mathcal{C}$ is Morita equivalent to a cyclically nilpotent fusion category, then $\mathcal{C}$ is called *solvable*.

In other words, $\mathcal{C}$ is weakly group-theoretical (solvable) if there exists an indecomposable algebra A in $\mathcal{C}$ such that the category ${}_A\mathcal{C}_A$ of A-bimodules in $\mathcal{C}$ is a (cyclically) nilpotent fusion category.

Note that a group-theoretical fusion category is weakly group-theoretical.

On the other hand, the condition on $\mathcal{C}$ being solvable is equivalent to the existence of a sequence of fusion categories

$$\mathcal{C}_0 = \mathrm{Vec}_k,\ \mathcal{C}_1,\ \ldots,\ \mathcal{C}_n = \mathcal{C},$$

such that $\mathcal{C}_i$ is obtained from $\mathcal{C}_{i-1}$ either by a G_i-equivariantization or as a G_i-extension, where $G_1, \ldots, G_n$ are cyclic groups of prime order. See [Etingof et al. 2011, Proposition 4.4].

If G is a finite group and $\omega \in H^3(G, k^\times)$, we have that the categories $\mathcal{C}(G, \omega)$ and $\mathrm{Rep}\, G$ are solvable if and only if G is solvable.

Let us call a semisimple Hopf algebra H *weakly group-theoretical* or *solvable* if the category $\mathrm{Rep}\, H$ is weakly group-theoretical or solvable, respectively.

5A. ***Solvability of an abelian extension.*** By [Etingof et al. 2011, Proposition 4.5(i)], solvability of a fusion category is preserved under Morita equivalence. Therefore, a group-theoretical fusion category $\mathcal{C}(G, \omega, F, \alpha)$ is solvable if and only if the group G is solvable.

Remark 5.1. As a consequence of the Feit–Thompson theorem [1963], we get that if the order of G is odd, then $\mathcal{C}(G, \omega, F, \alpha)$ is solvable. This fact generalizes to weakly group-theoretical fusion categories; see Proposition 7.1 below.

This implies the following characterization of the solvability of an abelian extension:

Corollary 5.2. *Let H be a semisimple Hopf algebra fitting into an abelian exact sequence* (2-5); *then H is solvable if and only if $G = F \bowtie \Gamma$ is solvable.*

In particular, if H is solvable, then F and Γ are solvable.

A result of Wielandt [1958] implies that if the groups Γ and F are nilpotent, then G is solvable. As a consequence, we get the following:

Corollary 5.3. *Suppose Γ and F are nilpotent. Then H is solvable.*

Then, for instance, the abelian extensions in Proposition 4.3 are solvable.

Combining Corollary 5.3 with Lemma 4.1 and Remark 4.2, we get:

Corollary 5.4. *Let*

$$\mathcal{C} = \mathcal{C}(G, \omega, \mathbb{Z}_p, \alpha).$$

Assume that $|G(\mathcal{C})| = p$. Then $\mathcal{C}$ is solvable.

6. Solvability from character degrees

Let p be a prime number. We study in this section fusion categories $\mathcal{C}$ such that $\text{c.d.}(\mathcal{C}) = \{1, p\}$.

It is known that if G is a finite group, then this assumption implies that the group G, and thus the category $\text{Rep}\, G$, are solvable [Isaacs 1976].

Remark 6.1. If H is any semisimple Hopf algebra such that $\text{c.d.}(H) = \{1, p\}$ and G is any finite group, then the tensor product Hopf algebra $A = H \otimes k^G$ also satisfies that $\text{c.d.}(A) = \{1, p\}$ (since the irreducible modules of A are tensor products of irreducible modules of H and k^G).

But A is not solvable unless G is solvable; indeed, k^G is a Hopf subalgebra as well as a quotient Hopf algebra of A.

Our aim in this section is to prove some structural results on $\mathcal{C}$, regarding solvability, under additional restrictions.

The following theorem generalizes Proposition 4.10.

Theorem 6.2. *Let $\mathcal{C}$ be a near-group fusion category such that* $\text{c.d.}(\mathcal{C}) = \{1, p\}$. *Then $\mathcal{C}$ is solvable.*

Proof. In the notation of [Siehler 2003], let the fusion rules of $\mathcal{C}$ be given by the pair (G, κ), where G is the group of invertible objects of $\mathcal{C}$ and κ is a nonnegative integer. Then $\text{Irr}(\mathcal{C}) = G \cup \{m\}$, with the relation

$$m^2 = \sum_{g \in G} g + \kappa m. \tag{6-1}$$

The assumption on $\text{c.d.}(\mathcal{C})$ implies that $\text{FPdim}\, m = p$. Hence $\text{FPdim}\, \mathcal{C} = |G| + p^2$, and since $|G| = |G(\mathcal{C})|$ divides $\text{FPdim}\, \mathcal{C}$, we get that $|G| = p$ or p^2. (Note that, taking Frobenius–Perron dimensions in (6-1), we get that $G \neq 1$.)

If $|G| = p^2$, then $\kappa = 0$ and $\mathcal{C}$ is a Tambara–Yamagami category [Tambara and Yamagami 1998]. Furthermore, $\mathcal{C}$ is a $\mathbb{Z}_2$-extension of a pointed category $\mathcal{C}(G, \omega)$. Then $\mathcal{C}$ is solvable in this case, by [Etingof et al. 2011, Proposition 4.5(i)].

Suppose that $|G| = p$. Then $\kappa = p - 1$. As in the proof of Proposition 4.10, using [Siehler 2003, Theorem 1.2], we get that $\text{FPdim}\, \mathcal{C} = p(p+1)$ equals 6 or $p2^\alpha$. Then $\mathcal{C}$ is solvable, by [Etingof et al. 2011, Theorem 1.6]. □

Our next result is the following theorem, for $\mathcal{C} = \text{Rep}\, H$, which is a consequence of Proposition 4.9. A stronger version of this result will be given in Section 7B, under additional dimension restrictions.

Theorem 6.3. *Suppose H is of type $(1, p; p, n)$ as an algebra. Assume in addition that H is quasitriangular. Then H is solvable.*

Proof. We have shown in Proposition 4.9 that H^* is nilpotent. Moreover, by Lemma 4.7, H fits into an abelian cocentral exact sequence

$$k \to k^F \to H \to k\mathbb{Z}_p \to k,$$

where F is a nilpotent group. Therefore, H is solvable, by Corollary 5.3. □

In the remainder of this section, we restrict ourselves to the case where $\mathcal{C} = \operatorname{Rep} H$ for a semisimple Hopf algebra H.

6A. ***The case p = 2.*** Let H be a semisimple Hopf algebra such that $\text{c.d.}(H) \subseteq \{1, 2\}$. By [Bichon and Natale 2011, Theorem 6.4], one of the following possibilities holds:

(i) there is a cocentral abelian exact sequence $k \to k^F \to H \to k\Gamma \to k$, where F is a finite group and $\Gamma \simeq \mathbb{Z}_2{}^n$, $n \geq 1$, or

(ii) there is a central exact sequence $k \to k^U \to H \to B \to k$, where $B = H_{\text{ad}}$ is a proper Hopf algebra quotient, and $U = U(\operatorname{Rep} H)$ is the universal grading group of the category of finite-dimensional H-modules.

In particular, if $H = H_{\text{ad}}$, then H satisfies (i).

As a consequence of this result we have:

Theorem 6.4. *Let H be a semisimple Hopf algebra such that* $\text{c.d.}(H) \subseteq \{1, 2\}$. *Then H is weakly group-theoretical.*

Moreover, if $H = H_{\text{ad}}$, then H is group-theoretical.

Proof. The assumption implies that H satisfies (i) or (ii) above. If H satisfies (i), then H is group-theoretical, by Remark 2.4.

Otherwise, H satisfies (ii), and then the category $\operatorname{Rep} H$ is a U-extension of $\operatorname{Rep} B$, in view of Proposition 3.1. By an inductive argument, we may assume that B is weakly group-theoretical (note that $\text{c.d.}(B) \subseteq \{1, 2\}$). Therefore so is H, by [Etingof et al. 2011, Proposition 4.1]. □

We next discuss conditions that guarantee the solvability of H. The following result is proved in [Bichon and Natale 2011].

Proposition 6.5 [Bichon and Natale 2011, Proposition 6.8]. *Suppose H is of type $(1, 2; 2, n)$ as an algebra. Then H is cocommutative.*

The proposition implies that such a Hopf algebra H is isomorphic to a group algebra kG for some finite group G. By the assumption on the algebra structure of H, the group G, and then also H, are solvable.

The next lemma gives a sufficient condition for H to be solvable.

Lemma 6.6. *Suppose* $\text{c.d.}(H) \subseteq \{1, 2\}$ *and $H = H_{\text{ad}}$. Then H is solvable if and only if the group F in (i) is solvable.*

Proof. Since $H = H_{\mathrm{ad}}$, then H satisfies (i). Therefore H is solvable if and only if the relevant factorizable group $G = F \bowtie \Gamma$ is solvable, by Corollary 5.2. Also, since the sequence (i) is cocentral, then G is a semidirect product: $G = F \rtimes \Gamma$. This proves the lemma. □

Remark 6.7. Suppose that H has a faithful irreducible character χ of degree 2, such that $\chi\chi^* = \chi^*\chi$. Then it follows from [Bichon and Natale 2011, Theorem 3.5] that H fits into a central abelian exact sequence $k \to k^{\mathbb{Z}_m} \to H \to kT \to k$, for some polyhedral group T of even order and some $m \geq 1$. In particular, since $\mathrm{c.d.}(H) = \{1, 2\}$, then T is necessarily cyclic or dihedral (see, for instance, [Bichon and Natale 2011, p. 10] for a description of the polyhedral groups and their character degrees). Therefore H is solvable in this case.

The assumption on χ is satisfied in the case where H is quasitriangular; hence the conclusion holds in this case. We shall show in the next subsection that every quasitriangular semisimple Hopf algebra with $\mathrm{c.d.}(H) \subseteq \{1, 2\}$ is also solvable.

We next prove some lemmas that will be useful in the next subsection.

Lemma 6.8. *Suppose* $\mathrm{c.d.}(H) \subseteq \{1, 2\}$ *and let* K *be a Hopf subalgebra or quotient Hopf algebra of* H. *Then* $\mathrm{c.d.}(K) \subseteq \{1, 2\}$.

Proof. We only need to show the claim when $K \subseteq H$ is a Hopf subalgebra. In this case, the statement follows from surjectivity of the restriction functor $\mathrm{Rep}\, H \to \mathrm{Rep}\, K$. □

The lemma has the following immediate consequence:

Corollary 6.9. *If* $\mathrm{c.d.}(H) \subseteq \{1, 2\}$, *then the group* $G(H)$ *is solvable.*

Lemma 6.10. *Suppose* $\mathrm{c.d.}(H), \mathrm{c.d.}(H^*) \subseteq \{1, 2\}$. *Then* H *is solvable.*

Proof. By induction on the dimension of H.

Consider the universal grading group U of the category $\mathrm{Rep}\, H$. Then $H^* \to kU$ is a quotient Hopf algebra and therefore $\mathrm{c.d.}(U) \subseteq \{1, 2\}$, by Lemma 6.8. This implies that the group U is solvable.

Suppose first $H_{\mathrm{ad}} \neq H$. In view of Lemma 6.8, we also have $\mathrm{c.d.}(H_{\mathrm{ad}}), \mathrm{c.d.}(H^*_{\mathrm{ad}}) \subseteq \{1, 2\}$. By the inductive assumption H_{ad} is solvable. By [Etingof et al. 2011, Proposition 4.5(i)], H is solvable, since $\mathrm{Rep}\, H$ is a U-extension of $\mathrm{Rep}\, H_{\mathrm{ad}}$.

It remains to consider the case where $H_{\mathrm{ad}} = H$. As pointed out at the beginning of this subsection, it follows from [Bichon and Natale 2011, Theorem 6.4] that in this case H satisfies condition (i), that is, H fits into a cocentral abelian exact sequence $k \to k^F \to H \to k\Gamma \to k$, with $|\Gamma| > 1$ and Γ abelian.

In particular, $k^\Gamma \subseteq H^*$ is a nontrivial central Hopf subalgebra, implying that $H^* \neq H^*_{\mathrm{ad}}$. The inductive assumption implies, as before, that H^*_{ad} and thus also H^* is solvable. Then H is too. □

6B. ***The quasitriangular case.*** We shall assume in this subsection that H is quasitriangular. Let $R \in H \otimes H$ be an R-matrix. We keep the notation of Section 2F.

Remark 6.11. Since the category $\operatorname{Rep} H$ is braided, then the universal grading group $U = U(\operatorname{Rep} H)$ is abelian (and, in particular, solvable).

The following is the main result of this subsection.

Theorem 6.12. *Let H be a quasitriangular semisimple Hopf algebra such that* $\operatorname{c.d.}(H) \subseteq \{1, 2\}$. *Then H is solvable.*

Proof. If $\operatorname{c.d.}(H) = \{1\}$, then H is commutative and, because it is quasitriangular, isomorphic to the group algebra of an abelian group. Hence we may assume that $\operatorname{c.d.}(H) = \{1, 2\}$.

Consider the Hopf subalgebras H_+, $H_- \subseteq H$. By Lemma 6.8, we have $\operatorname{c.d.}(H_+)$, $\operatorname{c.d.}(H_-) \subseteq \{1, 2\}$. Then $\operatorname{c.d.}(H_-)$, $\operatorname{c.d.}(H_-^*) \subseteq \{1, 2\}$, since $(H_-^*)^{\mathrm{cop}} \simeq H_+$.

By Lemma 6.10, H_- is solvable. Therefore the Drinfeld double $D(H_-)$ and its homomorphic image H_R are also solvable.

We may thus assume that $H_R \subsetneq H$.

Observe that, being a quotient of H, H_{ad} is also quasitriangular and satisfies $\operatorname{c.d.}(H_{\mathrm{ad}}) \subseteq \{1, 2\}$. Hence, by induction, we may also assume that $H = H_{\mathrm{ad}}$, and, in particular, $G(H) \cap Z(H) = 1$. Indeed, $\operatorname{Rep} H$ is a U-extension of $\operatorname{Rep} H_{\mathrm{ad}}$ and the group U is abelian, as pointed out before.

Therefore H fits into a cocentral abelian exact sequence $k \to k^F \to H \to k\Gamma \to k$, where $1 \neq \Gamma$ is elementary abelian of exponent 2.

In view of Lemma 6.6, it will be enough to show that the group F is solvable.

We have $\widehat{\Gamma} \subseteq G(H^*) \cap Z(H^*)$. By [Radford 1992, Proposition 3],

$$f_{R_{21}}(G(H^*) \cap Z(H^*)) \subseteq G(H) \cap Z(H).$$

Hence we may assume that $f_{R_{21}}|_{\widehat{\Gamma}} = 1$ and similarly $f_R|_{\widehat{\Gamma}} = 1$. Thus f_R and $f_{R_{21}}$ factorize through the quotient $H^*/H^*(k\widehat{\Gamma})^+ \simeq kF$.

Therefore $H_+ = f_R(H^*)$ and $H_- = f_{R_{21}}(H^*)$ are cocommutative. (Then they are also commutative, since $H_+ \simeq H_-^{*\,\mathrm{cop}}$.) In particular, $H_R = H_+H_-$ is cocommutative. Hence $\Phi_R(H^*) \subseteq H_R \subseteq kG(H)$.

By [Natale 2006, Theorem 4.11], $K = \Phi_R(H^*)$ is a commutative (and cocommutative) normal Hopf subalgebra, which is necessarily solvable, since H_R is. In addition, $\Phi_R(H^*) \simeq kT$, where $T \subseteq G(H)$ is an abelian subgroup [Natale 2006, Example 2.1], and there is an exact sequence of Hopf algebras

$$k \to kT \to H \xrightarrow{\pi} \overline{H} \to k,$$

where $\overline{H}$ is a certain (canonical) triangular Hopf algebra.

Since $\overline{H}$ is triangular, $\overline{H} \simeq (kL)^J$ is a twisting of the group algebra of some

finite group L. Because $\mathrm{c.d.}(L) = \mathrm{c.d.}(\overline{H}) \subseteq \{1, 2\}$, L must be solvable. Hence $\overline{H}$ is solvable, since $\mathrm{Rep}\,\overline{H} \simeq \mathrm{Rep}\,L$.

The map $\pi : H \to \overline{H}$ induces, by restriction to the Hopf subalgebra $k^F \subseteq H$, an exact sequence

$$k \to kT \cap k^F \to k^F \overset{\pi|_{k^F}}{\to} \pi(k^F) \to k.$$

We have $kT \cap k^F = k^{\overline{F}}$ and $\pi(k^F) = k^S$, where $\overline{F}$ and S are a quotient and a subgroup of F, respectively, in such a way that the exact sequence above corresponds to an exact sequence of groups

$$1 \to S \to F \to \overline{F} \to 1.$$

Now, $\overline{F}$ is abelian, because $k^{\overline{F}} = kT \cap k^F$ is cocommutative, and S is solvable, because k^S is a Hopf subalgebra of $\overline{H}$. Therefore F is solvable. This implies that H is solvable and finishes the proof of the theorem. □

7. Odd-dimensional fusion categories

In this section, p will be a prime number. Let $\mathcal{C}$ be a fusion category over k. Recall that the set of irreducible degrees of $\mathcal{C}$ was defined as

$$\mathrm{c.d.}(\mathcal{C}) = \{\mathrm{FPdim}\, x \mid x \in \mathrm{Irr}\,\mathcal{C}\}.$$

The fusion categories that we shall consider in this section are all *integral*, that is, the Frobenius–Perron dimensions of objects of $\mathcal{C}$ are (natural) integers. By [Etingof et al. 2005, Theorem 8.33], $\mathcal{C}$ is isomorphic to the category of representations of some finite-dimensional semisimple quasi-Hopf algebra.

7A. ***Odd-dimensional weakly group-theoretical fusion categories.*** The following result is a consequence of the Feit–Thompson theorem [1963].

Proposition 7.1. *Let $\mathcal{C}$ be a weakly group-theoretical fusion category and assume that* $\mathrm{FPdim}\,\mathcal{C}$ *is an odd integer. Then $\mathcal{C}$ is solvable.*

Note that since $\mathrm{FPdim}\,\mathcal{C}$ is an odd integer, the fusion category $\mathcal{C}$ is integral. See [Drinfeld et al. 2010, Corollary 2.22].

Proof. By definition, $\mathcal{C}$ is Morita equivalent to a nilpotent fusion category. Then, by [Etingof et al. 2011, Proposition 4.5(i)], it will be enough to show that a *nilpotent* fusion category of odd Frobenius–Perron dimension is solvable. So, assume that $\mathcal{C}$ is nilpotent, so that $\mathcal{C}$ is a G-extension of a fusion subcategory $\widetilde{C}$, with $|G| > 1$. In particular, $\mathrm{FPdim}\,\mathcal{C} = |G|\,\mathrm{FPdim}\,\widetilde{\mathcal{C}}$. Hence $\mathrm{FPdim}\,\widetilde{\mathcal{C}}$ and the order of G are both odd, and $\mathrm{FPdim}\,\widetilde{\mathcal{C}} < \mathrm{FPdim}\,\mathcal{C}$. The proposition follows by induction, since G is solvable by the Feit–Thompson theorem; see [Etingof et al. 2011, Proposition 4.5(i)]. □

7B. ***Braided fusion categories.*** We shall need the following lemma whose proof is contained in the proof of [Etingof et al. 2011, Proposition 6.2(i)]. We include a sketch of the argument for the sake of completeness.

Lemma 7.2. *Let $\mathcal{C}$ be a fusion category and let G be a finite group acting on $\mathcal{C}$ by tensor autoequivalences. Assume* c.d.$(\mathcal{C}^G) \subseteq \{p^m : m \geq 0\}$, *where p is a prime number. Then* c.d.$(\mathcal{C}) \subseteq \{p^m : m \geq 0\}$.

Proof. Regard $\mathcal{C}$ as an indecomposable module category over itself via tensor product, and similarly for $\mathcal{C}^G$. Let Y be a simple object of $\mathcal{C}$. Since the forgetful functor $F : \mathcal{C}^G \to \mathcal{C}$ is surjective, Y is a simple constituent of $F(X)$, for some simple object X of $\mathcal{C}^G$.

Since F is a tensor functor, we have FPdim $X =$ FPdim $F(X)$. By formula (7) in [Etingof et al. 2011, Proof of Proposition 6.2],

$$\text{FPdim}(X) = \deg(\pi)[G : G_Y] \,\text{FPdim}\, Y, \tag{7-1}$$

where $G_Y \subseteq G$ is the stabilizer of Y and π is an irreducible representation of G_Y associated to X. Therefore FPdim Y divides FPdim X.

The assumption on $\mathcal{C}^G$ implies that FPdim X is a power of p. Then so is FPdim Y. This proves the lemma. □

Theorem 7.3. *Let $\mathcal{C}$ be a braided fusion category such that* c.d.$(\mathcal{C}) \subseteq \{p^m : m \geq 0\}$, *where p is a prime number. Assume that* FPdim $\mathcal{C}$ *is odd. Then $\mathcal{C}$ is solvable.*

Proof. By induction on FPdim $\mathcal{C}$. (The Frobenius–Perron dimension of a fusion subcategory of $\mathcal{C}$ divides the dimension of $\mathcal{C}$ [Etingof et al. 2005, Proposition 8.15], and the same is true for the Frobenius–Perron dimension of a fusion category $\mathcal{D}$ such that there exists a surjective tensor functor $\mathcal{C} \to \mathcal{D}$ [Etingof et al. 2005, Corollary 8.11]. Thus these fusion categories are odd-dimensional as well.) If c.d.$(\mathcal{C}) = \{1\}$, then $\mathcal{C}$ is pointed. Then $\mathcal{C} \simeq \mathcal{C}(G, \omega)$ for some abelian group G and some 3-cocycle ω on G. Then $\mathcal{C}$ is solvable, by [Etingof et al. 2011, Proposition 4.5(ii)].

Suppose next that $\mathcal{C}$ is not pointed. Then all noninvertible objects in $\mathcal{C}$ have Frobenius–Perron dimension p^m, for some $m \geq 1$. Consider the group $G(\mathcal{C})$ of invertible objects of $\mathcal{C}$. Then $G(\mathcal{C})$ is abelian and $G(\mathcal{C}) \neq 1$, as follows by taking Frobenius–Perron dimensions in a decomposition of the tensor product $X \otimes X^*$, for some simple noninvertible object X.

Let us regard $\mathcal{C}$ as a premodular fusion category with respect to its canonical spherical structure (as FPdim $\mathcal{C}$ is an integer). Then $\mathcal{C}$ is modularizable, in view of [Bruguières and Natale 2011, Lemma 7.2].

Let $\widetilde{\mathcal{C}}$ be its modularization, which is a modular category over k. Then $\mathcal{C}$ is an equivariantization $\mathcal{C} \simeq \widetilde{\mathcal{C}}^G$ with respect to the action of a certain group G on $\widetilde{\mathcal{C}}$ [Bruguières 2000]. (Indeed, the modularization functor $\mathcal{C} \to \widetilde{\mathcal{C}}$ gives rise to

an exact sequence of fusion categories $\operatorname{Rep} G \to \mathcal{C} \to \widetilde{\mathcal{C}}$, which comes from an equivariantization; see [Bruguières and Natale 2011, Example 5.33].)

By construction of G, the category $\operatorname{Rep} G$ is the (tannakian) fusion subcategory of transparent objects in $\mathcal{C}$. Therefore there is an embedding of braided fusion categories $\operatorname{Rep} G \subseteq \mathcal{C}$. In particular, the order of G is odd, implying that G is solvable.

By Lemma 7.2, $\text{c.d.}(\widetilde{\mathcal{C}}) \subseteq \{p^m : m \geq 0\}$. Then, by induction, and since an equivariantization of a solvable fusion category under the action of a solvable group is again solvable, we may and shall assume in what follows that $\mathcal{C} = \widetilde{\mathcal{C}}$ is modular.

It is shown in [Gelaki and Nikshych 2008, Theorem 6.2] that the universal grading group $U(\mathcal{C})$ is (abelian and) isomorphic to the group $\widehat{G(\mathcal{C})}$ of characters of $G(\mathcal{C})$. In particular, $U(\mathcal{C}) \neq 1$. On the other hand, $\mathcal{C}$ is a $U(\mathcal{C})$-extension of its fusion subcategory $\mathcal{C}_{\text{ad}}$. Since also $\text{c.d.}(\mathcal{C}_{\text{ad}}) \subseteq \{p^m : m \geq 0\}$, then $\mathcal{C}_{\text{ad}}$ is solvable, by induction. Therefore $\mathcal{C}$ is solvable, as claimed. □

References

[Bakalov and Kirillov 2001] B. Bakalov and A. Kirillov, Jr., *Lectures on tensor categories and modular functors*, University Lecture Series **21**, American Mathematical Society, Providence, RI, 2001. MR 2002d:18003 Zbl 0965.18002

[Bichon and Natale 2011] J. Bichon and S. Natale, "Hopf algebra deformations of binary polyhedral groups", *Transform. Groups* **16**:2 (2011), 339–374. MR 2012g:16066 Zbl 1238.16024

[Bruguières 2000] A. Bruguières, "Catégories prémodulaires, modularisations et invariants des variétés de dimension 3", *Math. Ann.* **316**:2 (2000), 215–236. MR 2001d:18009 Zbl 0943.18004

[Bruguières and Natale 2011] A. Bruguières and S. Natale, "Exact sequences of tensor categories", *Int. Math. Res. Not.* **2011** (2011), 5644–5705. MR 2863377 Zbl 05994502

[Drinfeld et al. 2010] V. Drinfeld, S. Gelaki, D. Nikshych, and V. Ostrik, "On braided fusion categories, I", *Selecta Math.* (*N.S.*) **16**:1 (2010), 1–119. MR 2011e:18015 Zbl 1201.18005

[Etingof and Gelaki 2003] P. Etingof and S. Gelaki, "The classification of finite-dimensional triangular Hopf algebras over an algebraically closed field of characteristic 0", *Mosc. Math. J.* **3**:1 (2003), 37–43, 258. MR 2004i:16052 Zbl 1062.16043

[Etingof et al. 2005] P. Etingof, D. Nikshych, and V. Ostrik, "On fusion categories", *Ann. of Math.* (2) **162**:2 (2005), 581–642. MR 2006m:16051 Zbl 1125.16025

[Etingof et al. 2011] P. Etingof, D. Nikshych, and V. Ostrik, "Weakly group-theoretical and solvable fusion categories", *Adv. Math.* **226**:1 (2011), 176–205. MR 2012g:18010 Zbl 1210.18009

[Feit and Thompson 1963] W. Feit and J. G. Thompson, "Solvability of groups of odd order", *Pacific J. Math.* **13** (1963), 775–1029. MR 29 #3538 Zbl 0124.26402

[Gelaki and Naidu 2009] S. Gelaki and D. Naidu, "Some properties of group-theoretical categories", *J. Algebra* **322**:8 (2009), 2631–2641. MR 2011d:20099 Zbl 1209.18007

[Gelaki and Nikshych 2008] S. Gelaki and D. Nikshych, "Nilpotent fusion categories", *Adv. Math.* **217**:3 (2008), 1053–1071. MR 2009b:18015 Zbl 1168.18004

[Isaacs 1976] I. M. Isaacs, *Character theory of finite groups*, Pure and Applied Mathematics **69**, Academic, New York, 1976. MR 57 #417 Zbl 0337.20005

[Izumi and Kosaki 2002] M. Izumi and H. Kosaki, *Kac algebras arising from composition of subfactors: general theory and classification*, Mem. Amer. Math. Soc. **158**, 2002. MR 2004b:46090 Zbl 1001.46040

[Kashina et al. 2002] Y. Kashina, G. Mason, and S. Montgomery, "Computing the Frobenius–Schur indicator for abelian extensions of Hopf algebras", *J. Algebra* **251**:2 (2002), 888–913. MR 2003f: 16061 Zbl 1012.16040

[Masuoka 1995] A. Masuoka, "Semisimple Hopf algebras of dimension 6, 8", *Israel J. Math.* **92**:1-3 (1995), 361–373. MR 96j:16045 Zbl 0839.16036

[Masuoka 1999] A. Masuoka, "Extensions and cohomology of Hopf algebras, Lie bialgebras", pp. 131–149 in *Proceedings of the 31st symposium on ring theory and representation theory and Japan–Korea ring theory and representation theory seminar* (Osaka, 1998), edited by K. Nishida and M. Sato, Shinshu University, Matsumoto, 1999. MR 1812913 Zbl 1222.16022

[Masuoka 2002] A. Masuoka, "Hopf algebra extensions and cohomology", pp. 167–209 in *New directions in Hopf algebras*, edited by S. Montgomery and H.-J. Schneider, Math. Sci. Res. Inst. Publ. **43**, Cambridge University Press, 2002. MR 2003d:16050 Zbl 1011.16024

[Montgomery and Witherspoon 1998] S. Montgomery and S. J. Witherspoon, "Irreducible representations of crossed products", *J. Pure Appl. Algebra* **129**:3 (1998), 315–326. MR 99d:16030 Zbl 0932.16039

[Natale 1999] S. Natale, "On semisimple Hopf algebras of dimension pq^2", *J. Algebra* **221**:1 (1999), 242–278. MR 2000k:16050 Zbl 0942.16045

[Natale 2003] S. Natale, "On group theoretical Hopf algebras and exact factorizations of finite groups", *J. Algebra* **270**:1 (2003), 199–211. MR 2004k:16102 Zbl 1040.16027

[Natale 2005] S. Natale, "Frobenius–Schur indicators for a class of fusion categories", *Pacific J. Math.* **221**:2 (2005), 353–377. MR 2007j:16070 Zbl 1108.16035

[Natale 2006] S. Natale, "R-matrices and Hopf algebra quotients", *Int. Math. Res. Not.* **2006**:18 (2006), Art. ID 47182. MR 2007g:16056 Zbl 1113.16043

[Natale 2007a] S. Natale, "On the exponent of tensor categories coming from finite groups", *Israel J. Math.* **162** (2007), 253–273. MR 2008k:16003 Zbl 1152.16029

[Natale 2007b] S. Natale, *Semisolvability of semisimple Hopf algebras of low dimension*, Mem. Amer. Math. Soc. **186**, 2007. MR 2008b:16066 Zbl 1185.16033

[Natale 2011] S. Natale, "Semisimple Hopf algebras and their representations", *Publ. Mat. Uruguay* **12** (2011), 123–167.

[Nichols and Richmond 1996] W. D. Nichols and M. B. Richmond, "The Grothendieck group of a Hopf algebra", *J. Pure Appl. Algebra* **106**:3 (1996), 297–306. MR 97a:16075 Zbl 0848.16034

[Nichols and Zoeller 1989] W. D. Nichols and M. B. Zoeller, "A Hopf algebra freeness theorem", *Amer. J. Math.* **111**:2 (1989), 381–385. MR 90c:16008 Zbl 0672.16006

[Ostrik 2003] V. Ostrik, "Module categories over the Drinfeld double of a finite group", *Int. Math. Res. Not.* **2003**:27 (2003), 1507–1520. MR 2004h:18005 Zbl 1044.18005

[Radford 1992] D. E. Radford, "On the antipode of a quasitriangular Hopf algebra", *J. Algebra* **151**:1 (1992), 1–11. MR 93i:16053 Zbl 0767.16016

[Radford 1993] D. E. Radford, "Minimal quasitriangular Hopf algebras", *J. Algebra* **157**:2 (1993), 285–315. MR 94c:16052 Zbl 0787.16028

[Reshetikhin and Semenov-Tian-Shansky 1988] N. Reshetikhin and M. Semenov-Tian-Shansky, "Quantum R-matrices and factorization problems", *J. Geom. Phys.* **5**:4 (1988), 533–550. MR 92g: 17019 Zbl 0711.17008

[Robinson 1982] D. J. S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics **80**, Springer, New York, 1982. MR 84k:20001 Zbl 0483.20001

[Schneider 2001] H.-J. Schneider, "Some properties of factorizable Hopf algebras", *Proc. Amer. Math. Soc.* **129**:7 (2001), 1891–1898. MR 2002a:16047 Zbl 0982.16031

[Seitz 1968] G. Seitz, "Finite groups having only one irreducible representation of degree greater than one", *Proc. Amer. Math. Soc.* **19** (1968), 459–461. MR 36 #5212 Zbl 0244.20010

[Siehler 2003] J. Siehler, "Near-group categories", *Algebr. Geom. Topol.* **3** (2003), 719–775. MR 2005a:18013 Zbl 1033.18004

[Sommerhäuser 2002] Y. Sommerhäuser, *Yetter–Drinfel'd Hopf algebras over groups of prime order*, Lecture Notes in Mathematics **1789**, Springer, Berlin, 2002. MR 2003m:16054 Zbl 1006.16055

[Tambara and Yamagami 1998] D. Tambara and S. Yamagami, "Tensor categories with fusion rules of self-duality for finite abelian groups", *J. Algebra* **209**:2 (1998), 692–707. MR 2000b:18013 Zbl 0923.46052

[Wielandt 1958] H. Wielandt, "Über Produkte von nilpotenten Gruppen", *Illinois J. Math.* **2** (1958), 611–618. MR 25 #121 Zbl 0084.02904

[Zhu 1993] S. L. Zhu, "On finite-dimensional semisimple Hopf algebras", *Comm. Algebra* **21**:11 (1993), 3871–3885. MR 95d:16057 Zbl 0802.16037

Communicated by Susan Montgomery
Received 2011-03-11 Revised 2011-04-01 Accepted 2011-10-28

natale@famaf.unc.edu.ar *Facultad de Matemática, Astronomía y Física, Universidad Nacional de Córdoba, Medina Allende s/n, Ciudad Universitaria, 5000 Córdoba, Argentina*
http://www.famaf.unc.edu.ar/~natale

plavnik@famaf.unc.edu.ar *Facultad de Matemática, Astronomía y Física, Universidad Nacional de Córdoba, Medina Allende s/n, Ciudad Universitaria, 5000 Córdoba, Argentina*

ALGEBRA AND NUMBER THEORY 6:6 (2012)
dx.doi.org/10.2140/ant.2012.6.1199

Cusp form motives and admissible G-covers

Dan Petersen

There is a natural $\mathbb{S}_n$-action on the moduli space $\overline{\mathcal{M}}_{1,n}(B(\mathbb{Z}/m\mathbb{Z})^2)$ of twisted stable maps into the stack $B(\mathbb{Z}/m\mathbb{Z})^2$, and so its cohomology may be decomposed into irreducible $\mathbb{S}_n$-representations. Working over $\operatorname{Spec}\mathbb{Z}[1/m]$ we show that the alternating part of the cohomology of one of its connected components is exactly the cohomology associated to cusp forms for $\Gamma(m)$. In particular this offers an alternative to Scholl's construction of the Chow motive associated to such cusp forms. This answers in the affirmative a question of Manin on whether one can replace the Kuga–Sato varieties used by Scholl with some moduli space of pointed stable curves.

1. Introduction

Deligne [1971] showed how one can associate a compatible system of ℓ-adic Galois representations for almost all ℓ to elliptic modular forms. Taking these ideas further, one may wish to find a motive associated to modular forms, in the sense that the different ℓ-adic realizations of the motive are exactly the associated Galois representations. This idea was carried out for elliptic modular forms by [Scholl 1990]. See also [Blasius and Rogawski 1993] where Chow motives are associated to Hilbert modular forms.

The Galois representations associated to modular forms can often be realized as subquotients of the cohomology of a smooth projective variety X. To show that these subquotients are actually realizations of a motive, one needs to construct a suitable idempotent correspondence in

$$A^{\dim X}(X \times X)$$

that "cuts out" these pieces of the cohomology. The standard conjectures [Kleiman 1994] would imply that such correspondences exist in great generality. However,

The author is supported by the Göran Gustafsson Foundation for Research in Natural Sciences and Medicine.
MSC2010: primary 11G18; secondary 14H10.
Keywords: Chow motive, cusp form, admissible cover, twisted curve, level structure.

assuming that the standard conjectures will not be proven in the near future, it is still interesting to construct such correspondences by ad hoc methods in cases of interest.

Consider classical elliptic modular forms. Let $\Gamma(m)$ denote the level-m principal congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$. The space of modular forms for $\Gamma(m)$ of weight $n+2$ can be found as a subquotient of the cohomology of the n-th fibered power of the universal elliptic curve (a Kuga–Sato variety) over the modular curve $Y(m)$. Specifically, one can find in the Betti cohomology the direct sum of the space of holomorphic cusp forms and its complex conjugate, the space of antiholomorphic cusp forms. The corresponding parts of the ℓ-adic cohomology of the variety are the Galois representations associated to the modular forms.

To assemble these realizations into a Chow motive, one would need first to find a smooth compactification of the n-th fibered power of the universal curve. To compactify, one can take fibered powers of the universal generalized elliptic curve (in the sense of [Deligne and Rapoport 1973]) over $X(m)$; this compactification is however singular at the boundary. A desingularization of the boundary was constructed by Deligne [1971], and Scholl [1990] showed that the projector given by the "alternating" representation of the hyperoctahedral group

$$\mathbb{S}_2 \wr \mathbb{S}_n = (\underbrace{\mathbb{S}_2 \times \cdots \times \mathbb{S}_2}_{n \text{ times}}) \rtimes \mathbb{S}_n$$

(which canonically acts on the n-th fibered power and its desingularization) cuts out exactly the cohomology coming from cusp forms. Thus there exists a Chow motive associated to cusp forms of given weight for $\Gamma(m)$.

From the point of view of moduli theory, the best possible way to construct a smooth compactification of a moduli problem is to change the definition of the moduli problem to allow also some appropriate degenerations of the objects one is parametrizing. In this sense Deligne's desingularization is not so natural. Taking the n-th fibered power gives you a moduli space of elliptic curves equipped with some level structure, with $n+1$ marked points which are allowed to coincide. This suggests the possibility of constructing a smooth compactification by considering pointed stable curves of genus one with some kind of level structure. This suggestion was put forth by Manin [2005; 2006]. Not only would one then have a modular interpretation of the points on the boundary, but also a space with far more structure: for instance, stable curves have a well understood deformation theory, and they form an operad. (The operadic point of view of stable curves also gets used in this article when computing the contribution from the boundary.)

In level 1 this compactification would just be $\overline{\mathcal{M}}_{1,n+1}$. This space is a smooth and proper stack over $\mathbb{Z}$ and its cohomology defines a Chow motive. In [Consani and Faber 2006] it is shown, independently of Manin's question, that the projector

given by the alternating representation of $\mathbb{S}_{n+1}$ acting on $\overline{\mathcal{M}}_{1,n+1}$ cuts out exactly the space of cusp forms for $\mathrm{SL}(2,\mathbb{Z})$ of weight $n+2$. Thus an alternative to Scholl's construction is found, which however is only valid for modular forms of level 1 due to a lack of an analogue of the space $\overline{\mathcal{M}}_{1,n+1}$ for curves with level structure.

Fix a positive integer m, always assumed to be invertible on our base scheme. By a level-m structure on a smooth curve C, we mean the choice of an isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^{2g(C)} \cong \mathrm{Pic}^0(C)[m].$$

To extend Consani and Faber's construction to higher levels, one would need a smooth and projective moduli space of pointed stable curves with level structure. The problem of constructing such a compactification has a long history. A moduli space $\mathcal{M}_{g,n}(m)$ of pointed *smooth* curves with level structure is easy to construct, in particular as it is a scheme for $m \geq 3$. On the boundary, one runs into problems when trying to define a good notion of a level structure on curves not of compact type, that is, curves whose Jacobian is an extension of an abelian variety by a torus. The problem is roughly that these curves have "too little" m-torsion: for a torus T, the m-torsion group $T[m]$ has order $m^{\dim T}$, while for an abelian variety A the m-torsion group has order $m^{2\dim A}$.

When $g = 1$ and $n = 1$, a good modular compactification is described in [Deligne and Rapoport 1973]. In [Abramovich et al. 2003] a smooth proper stack compactifying $\mathcal{M}_{g,n}(m)$ for any g and n was constructed, seemingly as a byproduct of the work of Abramovich, Vistoli and others on constructing a smooth and projective moduli space of stable maps into a stack. In Section 3 we construct an explicit isomorphism between the stack defined by Deligne and Rapoport and the one defined by Abramovich, Corti and Vistoli when $g = 1$ and $n = 1$. Although this is perhaps not so surprising, the author has not seen this observed anywhere in the literature, and the isomorphism is a bit striking.

Once we are armed with a smooth and proper moduli space $\overline{\mathcal{M}}_{g,n}(m)$ of pointed stable curves with level-m structure, we show in Sections 4 and 5 of this paper that Consani and Faber's construction carries over to this setting as well: the pair of $\overline{\mathcal{M}}_{1,n}(m)$ and the projector given by the alternating representation of $\mathbb{S}_n$ defines the Chow motive of cusp forms of weight $n+1$ for $\Gamma(m)$. The alternating part of the cohomology of the open part $\mathcal{M}_{1,n}(m)$ is exactly the cohomology coming from *all* modular forms, that is, both Eisenstein series and cusp forms. The alternating part of the cohomology of the boundary is isomorphic to the space of Eisenstein series only, and when one computes the cohomology of the total space $\overline{\mathcal{M}}_{1,n}(m)$ the Eisenstein series "cancel" exactly, leaving only the contribution from cusp forms.

Finally in Section 6 of the paper we show that in this set-up, the Hecke correspondences can be given a modular interpretation over the boundary as well.

2. Background

Twisted stable maps, admissible covers and level structures. Abramovich and Vistoli [2002] introduced a stack generalizing the Kontsevich space $\overline{\mathcal{M}}_{g,n}(X)$ of stable maps to a projective variety, namely the stack $\overline{\mathcal{M}}_{g,n}(\mathscr{X})$ of so called *twisted* stable maps, into a tame Deligne–Mumford stack $\mathscr{X}$ with projective coarse moduli space. To this end Abramovich and Vistoli first define the notion of a pointed twisted curve: this is a DM-stack $\mathscr{C}$ whose coarse moduli space C is a pointed nodal curve with the property that $\mathscr{C} \to C$ is an isomorphism away from the nodes and the marked points, with specific restrictions on the type of "stacky" structure $\mathscr{C}$ may have. Roughly speaking, the fibers of $\mathscr{C} \to C$ should all be cyclotomic gerbes. See [Abramovich and Vistoli 2002] for a precise definition. With this definition in place, there is a proper moduli stack $\overline{\mathcal{M}}_{g,n}(\mathscr{X})$ parametrizing flat families of twisted curves equipped with a representable map to $\mathscr{X}$, such that the induced map of coarse moduli spaces $C \to X$ is stable in the sense of Kontsevich.

There is an important open and closed substack $\overline{\mathcal{M}}^{\mathrm{bal}}_{g,n}(\mathscr{X})$ of $\overline{\mathcal{M}}_{g,n}(\mathscr{X})$ which parametrizes twisted stable maps where the source curve is *balanced*. These are exactly the twisted curves that are smoothable, that is, which can be written as stable limits of smooth curves.

Let G be a finite group. We assume that $|G|$ is invertible on our base scheme, so the classifying stack BG is tame. The specific stack $\overline{\mathcal{M}}^{\mathrm{bal}}_{g,n}(BG)$ has an alternative description in terms of admissible covers, as explained in [Abramovich et al. 2003].

Definition 2.1. Let C be a pointed nodal curve and G a finite group. An *admissible torsor* for G over C consists of a morphism of curves $P \to C$ and an action of G on P, such that

(1) the curve C is identified with the scheme quotient P/G,

(2) the map $P \to C$ is an admissible cover,

(3) the restriction of $P \to C$ away from the nodes and markings of C, with the given G-action, is a torsor for the group G.

Then [Abramovich et al. 2003] shows that giving a representable morphism from a balanced twisted curve $\mathscr{C}$ to BG is canonically the same as giving an admissible G-torsor over the coarse moduli space of $\mathscr{C}$: given $\mathscr{C} \to BG$ one gets a G-torsor over $\mathscr{C}$ whose total space P is a nodal curve, and the composition $P \to \mathscr{C} \to C$ is an admissible torsor; conversely, given an admissible torsor $P \to C$, the stack quotient $[P/G]$ is a balanced twisted curve.

Since perhaps most readers are more comfortable with admissible covers than with twisted curves, we shall stick to the language of admissible covers as far as possible in this article.

As mentioned in the introduction, the existence of the stack $\overline{\mathcal{M}}_{g,n}(BG)$ allows one to give a modular compactification of the space $\mathcal{M}_{g,n}(m)$ of smooth pointed curves with level structure. Let $G = (\mathbb{Z}/m\mathbb{Z})^{2g}$. In particular, we assume m is invertible. Suppose we are given a smooth curve C and a level-m structure on C, that is, a not necessarily symplectic isomorphism $\mathrm{Pic}^0(C)[m] \cong G$. Let $\pi_1(C)$ denote the étale fundamental group of C. Since the points of $\mathrm{Pic}^0(C)[m]$ correspond to cyclic étale covers of degree m of C, one gets an isomorphism

$$\mathrm{Pic}^0(C)[m] \cong \pi_1(C)/m\pi_1(C),$$

and hence a bijection between isomorphisms $\mathrm{Pic}^0(C)[m] \cong G$ and surjective morphisms $\pi_1(C) \to G$, that is, connected G-torsors over C. See [Grothendieck 1971, XIII, 2.12]. So the level structure induces a representable map $C \to BG$, and when $2-2g-n<0$ we find a morphism

$$\mathcal{M}_{g,n}(m) \to \overline{\mathcal{M}}_{g,n}(BG).$$

This morphism is not an open immersion. The problem is that every point of $\overline{\mathcal{M}}_{g,n}(BG)$ has G in its automorphism group, coming from the automorphisms of the admissible torsors, while a level structure should generally have no automorphisms. This defect is fixed by composing with the rigidification map

$$\overline{\mathcal{M}}_{g,n}(BG) \to \overline{\mathcal{M}}_{g,n}(BG)/\!\!/G,$$

(where we follow the notation of [Romagny 2005]) in the sense that the composed map is an isomorphism onto an open substack. The closure of $\mathcal{M}_{g,n}(m)$ in $\overline{\mathcal{M}}_{g,n}(BG)/\!\!/G$ is the desired compactification.

The stacks $\overline{\mathcal{M}}_{g,n}(BG)$ and $\overline{\mathcal{M}}_{g,n}(BG)/\!\!/G$ share the same coarse moduli space [Abramovich et al. 2003, Theorem 5.1.5], and in particular they have the same rational and ℓ-adic cohomology. Since in this article we shall only be interested in their cohomology, we propose to *ignore the process of rigidification* (except in Section 3) as it would mostly be a small nuisance.

Thus we define $\overline{\mathcal{M}}_{g,n}(m)$ to be the closure of the image of $\mathcal{M}_{g,n}(m)$ already in $\overline{\mathcal{M}}_{g,n}(BG)$. One can describe this closure explicitly: it is the open and closed substack of $\overline{\mathcal{M}}_{g,n}(BG)$ consisting of connected admissible G-torsors which are unramified over each marked point. Then $\overline{\mathcal{M}}_{g,n}(m)$ is a smooth [Abramovich et al. 2003, Theorem 3.0.2] and proper DM-stack over $\mathrm{Spec}\,\mathbb{Z}[1/m]$.

The stack $\overline{\mathcal{M}}_{g,n}(m)$ has $\phi(m) = |U(\mathbb{Z}/m\mathbb{Z})|$ components, each of which is defined over $\mathrm{Spec}\,\mathbb{Z}[1/m, \zeta_m]$ and which are permuted by $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, where ζ_m is a primitive m-th root of unity. Any one of these components may be taken as the moduli space of curves with *symplectic* level-m structure.

3. Comparison of DR and ACV moduli stacks

Fix an integer m. Deligne and Rapoport [1973] defined a moduli stack parametrizing generalized elliptic curves with full level-m structure over $\operatorname{Spec}\mathbb{Z}[1/m]$. We denote it by $\overline{\mathcal{M}}_{\mathrm{DR}}(m)$ in this section. Just as in the case of $\overline{\mathcal{M}}_{g,n}(m)$, it consists of $\phi(m)$ open and closed substacks, all of which are individually defined over $\operatorname{Spec}\mathbb{Z}[1/m, \zeta_m]$. A choice of a primitive root ζ_m lets us identify one of these components with the modular curve $X(m)$ parametrizing elliptic curves with symplectic level-m structure.

In this section we show that the stack $\overline{\mathcal{M}}_{1,1}(m)$ is isomorphic to $\overline{\mathcal{M}}_{\mathrm{DR}}(m)$, provided that one includes the rigidification procedure as in [Abramovich et al. 2003]. The isomorphism is quite simple: one finds that when $P \to C$ is an admissible G-torsor, the curve P is in a canonical way a generalized elliptic curve in the sense of [Deligne and Rapoport 1973], and this construction provides the isomorphism.

Recall that $\overline{\mathcal{M}}_{\mathrm{DR}}(m)(T)$ is the groupoid of flat families of semistable (that is, each rational component has at least two markings) curves of genus one $E \to T$, such that the singular fibers are Néron m-gons, together with a group scheme structure on $E^{\mathrm{sm}} \to T$ making the singular fibers isomorphic to $\mathbb{G}_m \times \mathbb{Z}/m\mathbb{Z}$, and an isomorphism $E^{\mathrm{sm}}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$.

There is a canonical map $\overline{\mathcal{M}}_{1,1}(m) \to B(\mathbb{Z}/m\mathbb{Z})^2$: pulling back the $(\mathbb{Z}/m\mathbb{Z})^2$-torsor over E^{sm} along the identity section $T \to E^{\mathrm{sm}}$ we get a torsor on T, and this is clearly functorial. This tells us how to interpret the 2-fiber product

$$\overline{\mathcal{M}}_{1,1}(m) \times_{B(\mathbb{Z}/m\mathbb{Z})^2} \operatorname{Spec}\mathbb{Z}[1/m],$$

which (after writing out the definition) is the stack parametrizing elliptic curves with a torsor, together with the added data of a trivialization of the torsor over the identity section.

Proposition 3.1. *There is an isomorphism*

$$\overline{\mathcal{M}}_{\mathrm{DR}}(m) \cong \overline{\mathcal{M}}_{1,1}(m) \times_{B(\mathbb{Z}/m\mathbb{Z})^2} \operatorname{Spec}\mathbb{Z}[1/m].$$

Proof. We define mutually inverse functors from both stacks to each other. Start with an object of $\overline{\mathcal{M}}_{\mathrm{DR}}(m)(T)$, so we have a generalized elliptic curve $E \to T$ and a $(\mathbb{Z}/m\mathbb{Z})^2$-action on E coming from the action of E^{sm} on E. Let E' denote the scheme quotient under this action. The image of the given section of E gives us a section of E'.

We claim that $E' \to T$ is a stable curve of genus one, and $E \to E'$ an admissible cover. On a geometric fiber where E is smooth, E' is also smooth, and $E \to E'$ is étale. When E is a Néron m-gon, E' is a nodal rational curve with ramification index m at the node. Since E^{sm}, hence also $(\mathbb{Z}/m\mathbb{Z})^2$, acts freely on the smooth locus, the restriction of $E \to E'$ to the smooth locus is a $(\mathbb{Z}/m\mathbb{Z})^2$-torsor. Thus we

have an object of $\overline{\mathcal{M}}_{1,1}(m)(T)$. Moreover, by construction we also have a lifting of the section $T \to E'$ to a section $T \to E$, which gives us a trivialization of the torsor on T obtained by pulling back $E \to E'$ along $T \to E'$. Clearly this is functorial.

Conversely, an object of $(\overline{\mathcal{M}}_{1,1}(m) \times_{B(\mathbb{Z}/m\mathbb{Z})^2} \operatorname{Spec} \mathbb{Z}[1/m])(T)$ is an elliptic curve $E \to T$, an admissible torsor $P \to E$, and a trivialization of the torsor over the identity section. We claim that $P \to T$ is a semistable curve of genus one whose geometric fibers are either smooth elliptic curves or Néron m-gons. On the smooth locus this is clear. Over a geometric fiber where $E \to T$ is nodal, we know that the ramification index of $P \to E$ at the node is necessarily m by [Abramovich et al. 2003, 6.1.2]. Since P is a nodal curve of arithmetic genus one, and $(\mathbb{Z}/m\mathbb{Z})^2$ necessarily acts transitively on the dual graph of the fiber, the only possibility then is that it is a Néron m-gon. Also, the trivialization of the torsor gives us a section $T \to P$, contained in the smooth locus of P.

We claim that there is a unique structure of generalized elliptic curve on $P \to T$ such that the given section is the identity section, and the action of $(\mathbb{Z}/m\mathbb{Z})^2$ is given by an isomorphism $(\mathbb{Z}/m\mathbb{Z})^2 \cong P^{\mathrm{sm}}[m]$. By [Deligne and Rapoport 1973, II.3.2] it suffices to show that $(\mathbb{Z}/m\mathbb{Z})^2$ acts trivially on $\operatorname{Pic}^0_{P/T}$, and by [ibid., II.1.7] it suffices to show that $(\mathbb{Z}/m\mathbb{Z})^2$ preserves the cyclic ordering of the vertices of the dual graph of P. Suppose not: then there is a nonidentity $g \in (\mathbb{Z}/m\mathbb{Z})^2$ which maps an irreducible component C of P to itself and interchanges the two nodes of C. But then since no automorphism of $\mathbb{P}^1$ is fixed-point free, there is a fixed point in the smooth locus, contradicting that $P^{\mathrm{sm}} \to E$ is a torsor. □

Proposition 3.2. *There is an isomorphism*

$$\overline{\mathcal{M}}_{1,1}(m) \times_{B(\mathbb{Z}/m\mathbb{Z})^2} \operatorname{Spec} \mathbb{Z}[1/m] \to \overline{\mathcal{M}}_{1,1}(m)/\!\!/(\mathbb{Z}/m\mathbb{Z})^2.$$

That is, trivializing the torsor over the identity is the same as rigidifying the stack.

Proof. The forgetful map $\overline{\mathcal{M}}_{1,1}(m) \times_{B(\mathbb{Z}/m\mathbb{Z})^2} \operatorname{Spec} \mathbb{Z}[1/m] \to \overline{\mathcal{M}}_{1,1}(m)$ composed with the quotient map $\overline{\mathcal{M}}_{1,1}(m) \to \overline{\mathcal{M}}_{1,1}(m)/\!\!/(\mathbb{Z}/m\mathbb{Z})^2$ provides us with the morphism stated in the proposition. To show that it is an isomorphism, it suffices to show that it is a monomorphism and essentially surjective, and the former may be checked on geometric points. Over an algebraically closed field, the automorphism group of a point of the rigidified stack is exactly the quotient of the automorphism group of the original point by the group we are rigidifying along [Abramovich et al. 2003, Theorem 5.1.5]. Thus it is clear that the map is a monomorphism. To show it is essentially surjective, we need to prove that for an admissible torsor $P \to C$ over a base scheme S, there is locally on S a trivialization of the torsor over the identity. But this is the same thing as trivializing the pullback of $P \to C$ along the identity section $S \to C$, so it comes down to the fact that a torsor on S admits a local trivialization. □

Remark 3.3. One reason to be interested in this kind of result is that it may help in understanding the reduction of $\overline{\mathcal{M}}_{g,n}(BG)$ at primes dividing the order of G. Recall that we work over $\operatorname{Spec}\mathbb{Z}[1/m]$ throughout this article, since in [Abramovich et al. 2003] the stack $\overline{\mathcal{M}}_{g,n}(BG)$ is only shown to have any nice properties at all when $|G|$ is invertible on the base. After the publication of that article, the reduction of $\overline{\mathcal{M}}_{g,n}(BG)$ at bad primes has been tentatively studied, for instance in [Abramovich et al. 2011, Section 6] for the case $G = \mu_2$. However, the reduction of $X(m)$ at primes dividing m is much better understood: the appropriate analogue of level structures that should be used to give a modular interpretation over $\operatorname{Spec}\mathbb{Z}$ on the open part $Y(m)$ was worked out in detail in [Katz and Mazur 1985]. In [Conrad 2007] the boundary is given a modular interpretation as well, and it is shown that $X(m)$ is then a flat proper Deligne–Mumford stack over $\operatorname{Spec}\mathbb{Z}$. A natural first step for studying the reduction of $\overline{\mathcal{M}}_{g,n}(BG)$ may then be to see what the appropriate analogues of the theorems and methods for modular curves are in this particular case. Recent progress on the questions raised in this paragraph can be found in [Niles 2012], which in particular proves a generalization of the results of this section over $\operatorname{Spec}\mathbb{Z}$.

Remark 3.4. As a sanity check, let us study the boundary of $\overline{\mathcal{M}}_{1,1}(m)$. We already know from the results of this section that the boundary should consist of a finite set of points, namely $\phi(m)$ times the number of cusps of the curve $X(m)$. Recall from [Diamond and Shurman 2005, Section 3.8] that the number of cusps of $X(m)$ is

$$\frac{1}{2}m^2\prod_{p|m}\Big(1-\frac{1}{p^2}\Big)$$

if $m \geq 3$, and 3 if $m = 2$. Moreover, following their derivation of this formula, the factor

$$m^2\prod_{p|m}\Big(1-\frac{1}{p^2}\Big)$$

arises as the number of order m elements of $(\mathbb{Z}/m\mathbb{Z})^2$.

Let us see how one may compute this number of cusps also by considering admissible G-torsors over a rational curve with a node, where $G = (\mathbb{Z}/m\mathbb{Z})^2$. We work over a separably closed field. Let us first consider admissible torsors over the normalization of the curve. Such torsors correspond to tame covers of $\mathbb{P}^1 \setminus \{x, y\}$, where x and y are two points. Fix an isomorphism

$$\pi_1^{\text{tame}}(\mathbb{P}^1 \setminus \{x, y\}) \cong \widehat{\mathbb{Z}}$$

and a choice σ of generator of tame inertia around x. Tame G-coverings correspond bijectively to homomorphisms $\pi_1^{\text{tame}} \to G$ by [Grothendieck 1971, XIII, 2.12]. By [Abramovich et al. 2003, 6.1.2], σ should map to an element of order m, of which

there are

$$m^2 \prod_{p|m} \Big(1 - \frac{1}{p^2}\Big).$$

Note that all of the resulting G-covers are disconnected since the homomorphism surely is not surjective. Extend the covering to a branched cover of $\mathbb{P}^1$ using Abhyankar's lemma [Grothendieck 1971, appendice 1, 5.2]. The condition that we should obtain a connected admissible torsor over the nodal curve imposes restrictions on how to identify the fibers over the two branch points. Both branch points are torsors for the group G/H, where H is the stabilizer, so there are $|G/H| = m$ possible isomorphisms (as torsors) between the fibers. If we choose a global section of the admissible torsor over $\mathbb{P}^1$ and thus get compatible trivializations of the torsors over both branch points, the condition that we should get a connected cover can be expressed by saying that the identity on one fiber should be glued to a generator on the other. There are thus $\phi(m)$ such gluings, and all of them produce nonisomorphic admissible torsors. However, after gluing the branch points together, we can no longer tell the points x and y apart and hence neither σ and σ^{-1}. So we no longer have an element of order m in G, only a distinguished *unordered pair* $\{g, g^{-1}\}$. When $m \leq 2$ this makes no difference as $g = g^{-1}$ for all $g \in G$, but for $m \geq 3$ we must divide the number of points on the boundary by two. Thus we obtain exactly the right number of cusps.

4. The alternating part of cohomology

Remark 4.1. Throughout this section, $H_c^\bullet$ denotes compactly supported cohomology taking values in either the category of mixed Hodge structures or ℓ-adic Galois representations. We occasionally write out $\mathbb{Q}$-coefficients or mention the phrase "Hodge structure" for notational convenience, but this should not be interpreted as a preference for either cohomology theory.

Let us split the space $\overline{\mathcal{M}}_{1,n}(m)$ into three pieces according to the dual graph of the base curve C:

(1) the interior $\mathcal{M}_{1,n}(m)$ where the dual graph has a single vertex of genus one;

(2) the subspace $\mathcal{M}^{\circlearrowright}_{1,n}(m)$ where the dual graph is a *necklace*, that is, an N-cycle of genus zero vertices for some positive integer N;

(3) the union of all remaining strata. Explicitly, these are all graphs where a nonempty forest of genus zero vertices has been attached to one of the dual graphs appearing in case (1) or (2).

We write $\mathcal{M}^{\circlearrowright}_{1,n}$ for $\mathcal{M}^{\circlearrowright}_{1,n}(1)$. We begin by computing the alternating part of the cohomology of each of these pieces separately.

If M is any $\mathbb{S}_n$-module, let $M[\mathrm{sgn}]$ denote the subspace where $\mathbb{S}_n$ acts by the alternating representation.

Contribution from the interior. The arguments in the next proposition are similar to those in [Consani and Faber 2006], and we omit some details.

Proposition 4.2. *Let $\pi : \mathscr{E} \to \mathcal{M}_{1,1}(m)$ denote the universal elliptic curve. Let $n > 1$. Then*

$$H_c^i(\mathcal{M}_{1,n}(m), \mathbb{Q})[\mathrm{sgn}] \cong \begin{cases} H_c^1(\mathcal{M}_{1,1}(m), \mathrm{Sym}^{n-1} R^1\pi_*\mathbb{Q}) & \text{if } i = n, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We first show that the natural $\mathbb{S}_n$-equivariant open embedding

$$\mathcal{M}_{1,n}(m) \hookrightarrow \mathscr{E}^{n-1}$$

into the $(n-1)$-st fibered power of the universal curve induces an isomorphism $H_c^\bullet(\mathcal{M}_{1,n}(m))[\mathrm{sgn}] \cong H_c^\bullet(\mathscr{E}^{n-1})[\mathrm{sgn}]$. From the long exact sequence

$$H_c^\bullet(\mathcal{M}_{1,n}(m)) \to H_c^\bullet(\mathscr{E}^{n-1}) \to H_c^\bullet(T) \to H_c^{\bullet+1}(\mathcal{M}_{1,n}(m))$$

(see [Peters and Steenbrink 2008, Corollary 5.51]), where T denotes the complement, it suffices to show that the alternating representation does not occur in the cohomology of T. This in turn reduces, by the same exact sequence and inclusion-exclusion, to showing this fact for a subspace of $\mathscr{E}^{n-1}$ defined by two or more points coinciding. But on any such subspace there is a transposition acting trivially, showing that the alternating representation cannot occur in its cohomology.

Next, consider the projection map $\sigma : \mathscr{E}^{n-1} \to \mathcal{M}_{1,1}(m)$. The first observation is that the action of $\mathbb{S}_n$ maps each fiber to itself: this is clear for the subgroup of the last $n-1$ points, and for the first point one also needs to compose with a translation on the elliptic curve. Hence it makes sense to study the $\mathbb{S}_n$-action on the complex $R^\bullet\sigma_!\mathbb{Q} = R^\bullet\sigma_*\mathbb{Q}$. By computing fiberwise it is seen [Consani and Faber 2006, Proposition 1] that the alternating part is concentrated in degree $n-1$ and forms a subspace isomorphic to $\mathrm{Sym}^{n-1} R^1\pi_*\mathbb{Q}$. Moreover, it is known that the local system $\mathrm{Sym}^{n-1} R^1\pi_*\mathbb{Q}$ (respectively the smooth ℓ-adic sheaf $\mathrm{Sym}^{n-1} R^1\pi_*\mathbb{Q}_\ell$) has nonvanishing cohomology only in degree 1. The Leray spectral sequence with compact support for σ degenerates at the E_2 level: since $\mathcal{M}_{1,1}(m)$ is a non-compact curve, there can be at most two nonzero columns. Thus one finds that the alternating part of the cohomology is concentrated in degree n and isomorphic to $H_c^1(\mathcal{M}_{1,1}(m), \mathrm{Sym}^{n-1} R^1\pi_*\mathbb{Q})$, as claimed. □

Contribution from necklaces. In this section we study the alternating part of the cohomology of $\mathcal{M}_{1,n}^{\circlearrowleft}(m)$ and show that $\chi_c\big(\mathcal{M}_{1,n}^{\circlearrowleft}(m)\big)[\mathrm{sgn}]$ has weight zero.

A first observation is that there is a surjection

$$\mathcal{M}_{1,n}^{\circlearrowleft}(m) \to \mathcal{M}_{1,1}^{\circlearrowleft}(m) = \partial\mathcal{M}_{1,1}(m)$$

given by forgetting points, with the property that each fiber is mapped to itself under the $\mathbb{S}_n$-action, and the fibers are permuted transitively by the action of $\mathrm{SL}(2, \mathbb{Z}/m\mathbb{Z})$ on $\overline{\mathcal{M}}_{1,n}(m)$. Hence it is sufficient to consider the cohomology of a single fiber over a cusp of $\partial\mathcal{M}_{1,1}(m)$. Let $\mathscr{X}$ be such a fiber.

Consider a geometric point ξ of $\mathscr{X}$ corresponding to an admissible torsor $P \to C$. Suppose we forget all but one of the marked points of C. Then we may stabilize C to a nodal rational curve C', and as in [Abramovich and Vistoli 2002, Proposition 9.1.1] we get a unique admissible torsor $P' \to C'$ over the stabilized curve. (The previous sentence just describes the forgetting points-morphism.) Then the admissible torsor $P \to C$ is determined up to isomorphism by the admissible torsor $P' \to C'$ — that is, which cusp of $\overline{\mathcal{M}}_{1,1}(m)$ the point ξ maps to — and the stabilization map $C \to C'$. This fact is easiest to see using twisted curves, where the corresponding torsor $P \to \mathscr{C}$ is simply the pullback of $P' \to \mathscr{C}'$.

One is tempted to conclude that the admissible torsor $P \to C$ is determined up to isomorphism by C and the point in $\partial\mathcal{M}_{1,1}(m)$ it maps to under stabilization, and hence that the fiber $\mathscr{X}$ has the same coarse moduli space as $\mathcal{M}^{\circlearrowleft}_{1,n}$. This is however not true, since in the previous paragraph the map $C \to C'$ had to be included in the data.

Definition 4.3. Let $\mathcal{M}^{\circlearrowleft}_{1,n}$ denote the moduli space of stable n-pointed curves of genus 1 whose dual graph forms a necklace, equipped with an orientation on the edges of the dual graph inducing a cyclic ordering of the vertices.

Proposition 4.4. *If $m \leq 2$, then the coarse moduli space of $\mathscr{X}$ is the coarse moduli space of $\mathcal{M}^{\circlearrowleft}_{1,n}$. If $m \geq 3$, $\mathscr{X}$ has coarse moduli space $\mathcal{M}^{\circlearrowleft}_{1,n}$.*

Proof. As before, let $P \to C$ be a geometric point of $\mathscr{X}$, and $P' \to C'$ the point of $\partial\mathcal{M}_{1,1}(m)$ it maps to under the forgetting points-morphism.

The nodal rational curve C' has a unique nontrivial automorphism, so given the pointed curve C, the map $C \to C'$ is determined up to this involution. Let x be the node of C'. Under the isomorphism

$$\pi_1^{\mathrm{tame}}(C' \setminus \{x\}) \cong \widehat{\mathbb{Z}},$$

this involution induces multiplication by -1. In general an automorphism of C induces the identity on C' or this involution, according to whether the automorphism preserves or reverses the cyclic ordering of the vertices in the necklace. Thus the admissible torsor $P \to C$ is uniquely determined by C precisely if the class of P' in the group

$$\mathrm{Hom}(\pi_1^{\mathrm{tame}}(C' \setminus \{x\}), (\mathbb{Z}/m\mathbb{Z})^2)$$

is invariant under multiplication by -1; otherwise, P is uniquely determined by C once we fix a cyclic ordering of its dual graph. By [Abramovich et al. 2003, 6.1.2] the class of P' has order m in the group, so it is invariant under -1 if and only if $m \leq 2$.

There is clearly a forgetful morphism from $\mathscr{X}$ to $\mathcal{M}_{1,n}^{\circlearrowright}$ when $m \leq 2$, and to $\mathcal{M}_{1,n}^{\circlearrowleft}$ when $m \geq 3$. The discussion above shows that this forgetful morphism is bijective on isomorphism classes. □

Remark 4.5. While we have an isomorphism of coarse moduli spaces in the previous proposition, the fiber $\mathscr{X}$ is far from being isomorphic to $\mathcal{M}_{1,n}^{\circlearrowright}$ or $\mathcal{M}_{1,n}^{\circlearrowleft}$, respectively. First of all there is the issue of rigidification, but even taking that into account one also has so-called "ghost automorphisms" [Abramovich et al. 2003, Section 7]. In fact the forgetting points-morphisms are never representable when one works with the spaces $\overline{\mathcal{M}}_{g,n}(BG)$.

Remark 4.6. An alternative proof of the preceding proposition uses the evaluation maps $\overline{\mathcal{M}}_{g,n}(\mathscr{X}) \to \overline{\mathcal{I}}(\mathscr{X})$ [Abramovich 2008]. When $\mathscr{X} = BG$ and G is abelian, the points of $\overline{\mathcal{I}}(BG)$ correspond (after a choice of a primitive root) to the elements of G, and we can describe the evaluation maps as associating to each marked point the monodromy around the marking of the corresponding admissible torsor. This clarifies the relationship with the computations in π_1^{tame} above. One can define evaluation maps not just for markings but also for each branch of a node, and so for every half-edge of the dual graph one gets a decoration by an element of G. For instance, Jarvis and Kimura remark that *"the moduli spaces $\overline{\mathcal{M}}_{g,n}(BG)$ have boundary strata indexed by stable graphs whose tails and half-edges are decorated by elements of G (up to conjugation)"* [2002].

It is not hard to show that specifying the decoration of a single half-edge on a necklace determines all of the other decorations, since the product of both elements along an edge should always be the identity in G (otherwise the cover is not admissible), and the product of all elements incident to a genus zero component should also be the identity (by a computation in the [étale] fundamental group). By [Abramovich et al. 2003, 6.1.2] all half-edges of a stratum in $\mathcal{M}_{1,n}^{\circlearrowright}(m)$ are decorated by an element of order m, so this decoration is invariant under the dihedral symmetry if and only if $m \leq 2$.

We now study the two generating series

$$\sum_{n=1}^{\infty} \chi_c\big(\mathcal{M}_{1,n}^{\circlearrowright}\big)[\mathrm{sgn}]t^n \in K_0(\mathrm{MHS}_{\mathbb{Q}}) \otimes \mathbb{Q}[\![t]\!]$$

and

$$\sum_{n=1}^{\infty} \chi_c\big(\mathcal{M}_{1,n}^{\circlearrowleft}\big)[\mathrm{sgn}]t^n \in K_0(\mathrm{MHS}_{\mathbb{Q}}) \otimes \mathbb{Q}[\![t]\!]$$

of compactly supported Euler characteristics, taken in the Grothendieck ring of rational mixed Hodge structures. The reason for passing to Euler characteristics is that we want to compute with each stratum separately, and this is possible since the compactly supported Euler characteristic satisfies the scissor relation

$$\chi_c(X \setminus Y) = \chi_c(X) - \chi_c(Y)$$

for $Y \subseteq X$ constructible, as well as the usual Künneth formula.

Remark 4.7. Given a dual graph Γ corresponding to a stratum in $\overline{\mathcal{M}}_{g,n}$, the cohomology of the stratum is given by

$$\bigotimes_{v \in \mathrm{Vert}\Gamma} H^\bullet(\mathcal{M}_{g(v),n(v)})_{\mathrm{Aut}\,\Gamma} \tag{1}$$

where the subscript denotes coinvariants with respect to the group action. In the case of $\mathcal{M}^{\circlearrowleft}_{1,n}$ we must replace $\mathrm{Aut}\,\Gamma$ with the cyclic subgroup of index two that preserves the cyclic ordering.

The following is proven in [Consani and Faber 2006]:

Proposition 4.8. *The Euler characteristic* $\chi_c\big(\mathcal{M}^{\circlearrowleft}_{1,n}\big)[\mathrm{sgn}]$ *is pure of weight zero.*

We outline their proof, which uses the theory of modular operads. Let $\Lambda = \bigoplus_n \Lambda^n$ be the ring of symmetric functions. We identify Λ^n with the representation ring of $\mathbb{S}_n$, and we identify virtual representations of $\mathbb{S}_n$ in the category of mixed Hodge structures with elements of $\Lambda^n \otimes K_0(\mathrm{MHS}_{\mathbb{Q}})$, as in [Getzler 1995]. First the generating function

$$\sum_{n=1}^{\infty} \chi_c\big(\mathcal{M}^{\circlearrowleft}_{1,n}\big) \in \Lambda \widehat{\otimes} K_0(\mathrm{MHS}_{\mathbb{Q}})$$

is studied. This sum is naturally interpreted as a sum over graphs, and the so-called semiclassical approximation provides an explicit expression for it. Let $\mathcal{M}$ be the generating function

$$\sum_{n=3}^{\infty} \chi_c(\mathcal{M}_{0,n}) \in \Lambda \widehat{\otimes} K_0(\mathrm{MHS}_{\mathbb{Q}}).$$

It follows from the main theorem of [Getzler 1998] (the semiclassical approximation) that

$$\sum_{n=1}^{\infty} \chi_c\big(\mathcal{M}^{\circlearrowleft}_{1,n}\big) = \left(-\frac{1}{2}\sum_{n=1}^{\infty} \frac{\phi(n)}{n} \log(1-p_n)\right) \circ \frac{\partial^2 \mathcal{M}}{\partial p_1^2} + \frac{\frac{\partial \mathcal{M}}{\partial p_2}\left(2 + \frac{\partial \mathcal{M}}{\partial p_2}\right) + \frac{\partial^2 \mathcal{M}}{\partial p_1^2}}{4\left(1 - p_2 \circ \frac{\partial^2 \mathcal{M}}{\partial p_1^2}\right)},$$

where $\circ$ denotes plethysm of symmetric functions. Consani and Faber proceed to use results of Getzler on the structure of $H^\bullet(\mathcal{M}_{0,n})$ as an $\mathbb{S}_n$-representation to show that only the top-degree cohomology $H_c^{n-3}(\mathcal{M}_{0,n})$, which is pure of weight zero, can contribute nontrivially to the alternating part.

Remark 4.9. In their proof of, Consani and Faber compute an exact expression for $\chi_c\big(\mathcal{M}^{\circlearrowleft}_{1,n}\big)[\mathrm{sgn}]$. However, we prefer to deduce this from Theorem 5.1.

We claim that similarly

$$\sum_{n=1}^{\infty} \chi_c\big(\mathcal{M}_{1,n}^{\circlearrowleft}\big) = \left(-\sum_{n=1}^{\infty} \frac{\phi(n)}{n} \log(1-p_n)\right) \circ \frac{\partial^2 \mathcal{M}}{\partial p_1^2}. \tag{2}$$

A combinatorial proof of Getzler's semiclassical approximation, using wreath product symmetric functions to directly sum over necklaces up to dihedral symmetry, is given in [Petersen 2012]. In that proof, the first term of Getzler's formula corresponds to symmetries under rotation, and the second term corresponds to symmetries under reflections. Then the above formulas show that going from dihedral to cyclic symmetry corresponds to discarding all reflection terms (and multiplying by two). However, as we shall see now, formula (2) can be proved directly using little more than the definition of a plethysm of $\mathbb{S}$-modules.

Definition 4.10. A (virtual) $\mathbb{S}$-module $\mathcal{V}$ is the data of a (virtual) $\mathbb{S}_n$-representation $\mathcal{V}(n)$ for each positive integer n.

We consider only $\mathbb{S}$-modules in the ring category of mixed Hodge structures.

Definition 4.11. Let $\mathcal{V}$ and $\mathcal{W}$ be $\mathbb{S}$-modules. We define their direct sum $\mathcal{V} \oplus \mathcal{W}$ componentwise. We define their tensor product by

$$(\mathcal{V} \otimes \mathcal{W})(n) = \bigoplus_{k+l=n} \mathrm{Ind}_{\mathbb{S}_k \times \mathbb{S}_l}^{\mathbb{S}_n} \mathcal{V}(k) \otimes \mathcal{W}(l).$$

This makes the category of $\mathbb{S}$-modules a symmetric monoidal category.

Definition 4.12. Let $\mathcal{V}$ and $\mathcal{W}$ be $\mathbb{S}$-modules. The plethysm $\mathcal{V} \circ \mathcal{W}$ is defined by

$$(\mathcal{V} \circ \mathcal{W})(n) = \bigoplus_{k=1}^{\infty} \mathcal{V}(k) \otimes_{A[\mathbb{S}_k]} (\mathcal{W}^{\otimes k})(n), \tag{3}$$

where $(\mathcal{W}^{\otimes k})(n)$ is considered as an $\mathbb{S}_k$-module by permuting the factors.

As in the usual theory of symmetric functions, the definitions of product and plethysm extend to virtual $\mathbb{S}$-modules. Let $\mathcal{M}$ be the virtual $\mathbb{S}$-module defined by

$$\mathcal{M}(n) = \begin{cases} \chi_c(\mathcal{M}_{0,n}) & \text{if } n \geq 3, \\ 0 & \text{otherwise.} \end{cases}$$

Note that

$$\left(\frac{\partial^2 \mathcal{M}}{\partial p_1^2}\right)(n) = \mathrm{Res}_{\mathbb{S}_n}^{\mathbb{S}_{n+2}} \chi_c(\mathcal{M}_{0,n+2})$$

for $n \geq 1$. Let moreover $\mathcal{A}ss$ denote the $\mathbb{S}$-module defined by

$$\mathcal{A}ss(n) = \mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{\mathbb{S}_n} \mathbf{1}.$$

Proposition 4.13. $$\left(\mathscr{A}ss \circ \frac{\partial^2 \mathcal{M}}{\partial p_1^2}\right)(n) = \chi_c\big(\mathcal{M}_{1,n}^{\circlearrowleft}\big).$$

Proof. For any $\mathbb{S}_n$-module M and any subgroup H of $\mathbb{S}_n$,

$$\mathrm{Ind}_H^{\mathbb{S}_n} \mathbf{1} \otimes_{A[\mathbb{S}_n]} M = \mathbf{1} \otimes_{A[H]} M = M_H,$$

the coinvariants under H. Also,

$$\left(\frac{\partial^2 \mathcal{M}}{\partial p_1^2}\right)^{\otimes k}(n) = \bigoplus_{n_1+\cdots+n_k=n} \bigotimes_{i=1}^{k} \chi_c(\mathcal{M}_{0,n_i+2})$$

by the additivity and multiplicativity of the Euler characteristic. Hence we are done by comparing equations (1) and (3). □

Proposition 4.14. *There is an equality of generating series*

$$\sum_{n=1}^{\infty} \mathscr{A}ss(n) = -\sum_{n=1}^{\infty} \frac{\phi(n)}{n} \log(1 - p_n).$$

Proof. Use the results of [Macdonald 1995, Chapter 1, Section 7, Example 4]. See also [Getzler and Kapranov 1998, Example 7.6.2]. □

Proposition 4.15. *The alternating part of $\chi_c\big(\mathcal{M}_{1,n}^{\circlearrowleft}\big)$ is pure of weight zero.*

Proof. The alternating part of the right hand side of (2) is shown to have weight zero in [Consani and Faber 2006, Lemma 7 and 8]. □

Remark 4.16. The notions of $\mathbb{S}$-modules and plethysm arise naturally when studying operads, an operad being exactly a monoid in the category of $\mathbb{S}$-modules with respect to plethysm. In this context the definition of plethysm can be understood graphically. Namely, if $\mathscr{V}$ is an operad, one often thinks of $\mathscr{V}(n)$ as spanned by graphs with one output leg and n input legs, with the $\mathbb{S}_n$-action corresponding to permutation of the inputs. Then $\mathscr{V} \circ \mathscr{W}$ corresponds to attaching the output legs of the graphs corresponding to $\mathscr{W}$ to the input legs of the graphs corresponding to $\mathscr{V}$ in all possible ways.

This way of thinking also makes the previous propositions more or less trivial. By our definition of $\mathscr{A}ss(n)$, we can think of it as the $\mathbb{S}_n$-module spanned by necklaces considered up to cyclic symmetry. To make this picture more operadic, we can replace necklaces by corollas (single vertices with several input legs) by placing a vertex in the middle of the necklace and drawing an input leg from each node of the necklace to the vertex in the middle. Then $\mathscr{A}ss(n)$ is spanned by corollas with n cyclically ordered input legs, or equivalently, by corollas equipped with an

embedding in the plane up to ambient isotopy. (In terms of operads, $\mathcal{A}ss$ is the underlying $\mathbb{S}$-module of the cyclic associative operad shifted by one.)

Also, $\mathcal{M}(n)$ is given by marking $n+2$ points on $\mathbb{P}^1$ and then fixing two of them, so in terms of dual graphs there are two fixed legs and the remaining are permuted by the $\mathbb{S}_n$-action. To attach n legs at a node of a necklace we need to have $n+2$ marked points on $\mathbb{P}^1$, where the last two vertices are those which we glue to the incident components. Note that the last two vertices are naturally ordered as one is attached to the edge incident in the clockwise direction of the dual graph, and the other is attached counterclockwise.

So $\mathcal{A}ss \circ \mathcal{M}$ is the result of attaching extra legs to a single cyclically oriented corolla, or equivalently a necklace, which is exactly what we want.

The remaining strata.

Proposition 4.17. *The alternating representation does not occur in the cohomology of any stratum where a nonempty forest of genus zero vertices has been attached to a stable dual graph.*

Proof. Let Γ be the dual graph of such a stratum of $\overline{\mathcal{M}}_{1,n}(m)$. Let v be an extremal vertex of one of the attached trees, say with N incident half-edges. Let Γ' be the dual graph given by deleting v and these half-edges. The graph Γ' defines a stratum of $\overline{\mathcal{M}}_{1,n-N+1}(m)$. If we let $\mathcal{M}(\Gamma)$ and $\mathcal{M}(\Gamma')$ denote the corresponding strata, then there is an isomorphism

$$\mathcal{M}(\Gamma) \to \mathcal{M}(\Gamma') \times \mathcal{M}_{0,N}.$$

The morphism $\mathcal{M}(\Gamma) \to \mathcal{M}(\Gamma')$ is the morphism that forgets all the points on the component v, and the morphism to $\mathcal{M}_{0,N}$ remembers only the markings on the component. This is well-defined since there is at least one marked point on v, so no automorphism of the dual graph could interchange the component with any other. To define an inverse, use that any admissible torsor over the component v is necessarily étale, and since $\mathbb{P}^1$ is simply connected the torsor is necessarily trivial. Hence given an admissible torsor corresponding to an object of $\mathcal{M}(\Gamma')$ there is a unique extension to an admissible torsor over the attached component v (corresponding to an object of $\mathcal{M}_{0,N}$).

It follows in particular that

$$H^\bullet(\overline{\mathcal{M}}(\Gamma)) = H^\bullet(\overline{\mathcal{M}}(\Gamma')) \otimes H^\bullet(\mathcal{M}_{0,N}).$$

Now [Consani and Faber 2006, Lemma 5] describes which $\mathbb{S}_N$-representations may occur in the cohomology of $\mathcal{M}_{0,N}$, and the fact that the alternating representation cannot occur in the left hand side follows by the same Frobenius reciprocity argument as in [ibid., Lemma 6]. □

5. Cusp form motives

Let $\mathbb{V}_n$ denote the local system $\mathrm{Sym}^n R^1\pi_*\mathbb{Q}$ on $\mathcal{M}_{1,1}(m)$, where π is the projection from the universal elliptic curve. Consider for all n the natural morphisms

$$H^1_c(\mathcal{M}_{1,1}(m), \mathbb{V}_n) \to H^1(\mathcal{M}_{1,1}(m), \mathbb{V}_n).$$

We define the *parabolic cohomology* to be the image of this morphism, and the *Eisenstein cohomology* to be the kernel. The parabolic cohomology is denoted $H^1_!(\mathcal{M}_{1,1}(m), \mathbb{V}_n)$. The weight filtration on $H^1_c(\mathcal{M}_{1,1}(m), \mathbb{V}_n)$ has only two steps,

$$0 \subset W_0 \subset W_{n+1} = H^1_c(\mathcal{M}_{1,1}(m), \mathbb{V}_n),$$

where W_0 is the Eisenstein cohomology and W_{n+1}/W_0 is isomorphic to the parabolic cohomology. See for instance [Faltings 1987, §4].

Theorem 5.1. *The alternating part of the cohomology of $\overline{\mathcal{M}}_{1,n}(m)$ is pure of weight n and coincides with the parabolic cohomology groups*

$$H^1_!(\mathcal{M}_{1,1}(m), \mathrm{Sym}^{n-1} R^1\pi_*\mathbb{Q})$$

and $H^1_!(\overline{\mathcal{M}}_{1,1}(m), \mathrm{Sym}^{n-1} R^1\pi_*\mathbb{Q}_\ell)$ in Betti and ℓ-adic cohomology, respectively.

Proof. The proof is similar to [Scholl 1990, Section 1]. Consider the long exact sequence [Peters and Steenbrink 2008, Corollary 5.51]

$$H^\bullet_c(\mathcal{M}_{1,n}(m)) \to H^\bullet_c(\overline{\mathcal{M}}_{1,n}(m)) \to H^\bullet_c(\partial\mathcal{M}_{1,n}(m)) \to H^{\bullet+1}_c(\mathcal{M}_{1,n}(m)).$$

Take the alternating part of the sequence. $H^\bullet_c(\mathcal{M}_{1,n}(m))[\mathrm{sgn}]$ is concentrated in homological degree n by Proposition 4.2, so there is an isomorphism

$$H^i_c(\overline{\mathcal{M}}_{1,n}(m))[\mathrm{sgn}] \to H^i_c(\partial\mathcal{M}_{1,n}(m))[\mathrm{sgn}]$$

for all i except $n-1$ and n, and a surjection

$$H^n_c(\overline{\mathcal{M}}_{1,n}(m))[\mathrm{sgn}] \to H^n_c(\partial\mathcal{M}_{1,n}(m)[\mathrm{sgn}].$$

Since $\overline{\mathcal{M}}_{1,n}(m)$ is a smooth and proper DM-stack, $H^i_c(\partial\mathcal{M}_{1,n}(m))[\mathrm{sgn}]$ is therefore pure of weight i for all i except possibly $i = n-1$.

Since we know that $\chi_c(\partial\mathcal{M}_{1,n}(m))[\mathrm{sgn}]$ has weight zero, this means that any nonvanishing cohomology in $H^i_c(\partial\mathcal{M}_{1,n}(m))[\mathrm{sgn}]$ for $i \notin \{0, n-1\}$ must cancel against some cohomology in $H^{n-1}_c(\partial\mathcal{M}_{1,n}(m))[\mathrm{sgn}]$. But $H^i_c(-)$ has weight at most i for all i, so

$$H^i_c(\partial\mathcal{M}_{1,n}(m))[\mathrm{sgn}] = 0 \text{ for all } i \geq n.$$

Moreover, since $H^i_c(\partial\mathcal{M}_{1,n}(m))[\mathrm{sgn}] \cong H^i_c(\overline{\mathcal{M}}_{1,n}(m))[\mathrm{sgn}]$ for $i \notin \{n-1, n\}$, Poincaré duality for $\overline{\mathcal{M}}_{1,n}(m)$ shows that $H^i_c(\partial\mathcal{M}_{1,n}(m))[\mathrm{sgn}]$ vanishes also for $i < n-1$.

Thus the alternating part of the above long exact sequence is concentrated in the short exact sequence

$$0 \to H_c^{n-1}(\partial \mathcal{M}_{1,n}(m))[\mathrm{sgn}] \to H_c^n(\mathcal{M}_{1,n}(m))[\mathrm{sgn}] \to H_c^n(\overline{\mathcal{M}}_{1,n}(m))[\mathrm{sgn}] \to 0.$$

Now $H_c^n(\mathcal{M}_{1,n}(m))[\mathrm{sgn}] \cong H_c^1(\mathcal{M}_{1,1}(m), \mathbb{V}_{n-1})$ by Proposition 4.2 and we know the weight filtration on this cohomology group by the remarks preceding this proposition. Since we also know the weights on the other two spaces in the sequence, the only possibility is that the first map is the inclusion of the Eisenstein cohomology and the second map is the projection to the parabolic cohomology. □

As first observed by Toën [2000], any smooth and projective DM-stack $\mathcal{X}$ of finite type over a field k defines a Chow motive over k. In the special case of $\mathcal{X} = \overline{\mathcal{M}}_{g,n}(BG)$, where G is a finite group, one can also argue as follows: Combining the results of [Abramovich et al. 2007, Section 4] and [Kresch and Vistoli 2004, Theorem 2.1], we get a finite morphism $f\colon X \to \mathcal{X}$ of degree m where X is a smooth and projective variety over k. We may then define $h(\mathcal{X})$ to be the Chow motive defined by X and the projector $\frac{1}{m}[f^*] \circ [f_*]$.

The stack $\overline{\mathcal{M}}_{1,n}(m)$ is the disjoint union of $\phi(m)$ open and closed substacks, each of which corresponds to symplectic level-m structure. Let $\overline{\mathcal{M}}^s_{1,n}(m)$ be one of these open and closed substacks.

Theorem 5.2. *The Chow motive defined by $\overline{\mathcal{M}}^s_{1,n}(m)$ and the projector onto the alternating representation is the motive associated to cusp forms of weight $n+1$ for $\Gamma(m)$.*

Proof. The results of Section 3 of this paper identifies the modular curve $X(m)$ with the rigidification of $\overline{\mathcal{M}}^s_{1,1}(m)$, and similarly for $Y(m)$ and $\mathcal{M}^s_{1,1}(m)$. The ℓ-adic Galois representations classically associated to cusp forms of level m and weight $n+1$ are the parabolic cohomology groups

$$H^1_!(Y(m), \mathrm{Sym}^{n-1} R^1\pi_* \mathbb{Q}_\ell).$$

It remains to identify the parabolic cohomology groups on $\mathcal{M}^s_{1,1}(m)$ and $Y(m)$ with each other. Let $\rho : \mathcal{M}^s_{1,1}(m) \to \mathcal{M}^s_{1,1}(m)/\!\!/(\mathbb{Z}/m\mathbb{Z})^2 \cong Y(m)$ be the rigidification. The group $(\mathbb{Z}/m\mathbb{Z})^2$ acts trivially on the universal elliptic curve over $\mathcal{M}^s_{1,1}(m)$ and hence also on $\mathrm{Sym}^{n-1} R^1\pi_* \mathbb{Q}_\ell$, so $R^0\rho_*$ is fiberwise an isomorphism of local systems while all higher direct images vanish. Hence by the Leray spectral sequence the two cohomology groups coincide. □

Remark 5.3. By assuming that $n > 1$ in the definition of the Chow motive M we have ruled out cusp forms of weight 2. These motives are instead well understood in terms of Jacobians of modular curves.

6. Hecke operators

Let p and m be positive coprime integers. Throughout this section, we denote by G the group $(\mathbb{Z}/m\mathbb{Z})^2$, and by H the group $\mathbb{Z}/p\mathbb{Z}$.

Definition 6.1. Let $\overline{\mathcal{M}}_{1,n}(m;\, p)$ be the open and closed substack of

$$\overline{\mathcal{M}}_{1,n}(BG \times BH) \times_{BH} \operatorname{Spec} \mathbb{Z}[1/pm]$$

where the admissible G-torsor and H-torsor are connected and unramified at the marked points. The fiber product is taken over the evaluation map at the first marked point, that is, the H-torsor is trivialized over that marking.

This stack will be used to define an $\mathbb{S}_n$-equivariant correspondence from $\overline{\mathcal{M}}_{1,n}(m)$ to itself, such that when p is a prime, the induced endomorphism of the realization of the cusp form motive is exactly the Hecke operator T_p.

We define two maps

$$\phi,\, \psi : \overline{\mathcal{M}}_{1,n}(m;\, p) \to \overline{\mathcal{M}}_{1,n}(m).$$

The map ϕ is induced from the obvious map $BG \times BH \to BG$. Concretely, we just forget the admissible H-torsor.

To define the map ψ, consider an object of $\overline{\mathcal{M}}_{1,n}(m;\, p)(S)$. Let $P_G \to C$ and $\pi : P_H \to C$ be the two admissible torsors. Since there is a distinguished lifting of the identity section to P_H it has a canonical structure of a generalized elliptic curve (see the arguments of Section 3) and $P_H^{\mathrm{sm}} \to C^{\mathrm{sm}}$ is a morphism of group schemes over S. One gets a dual isogeny

$$\pi^\vee : C^{\mathrm{sm}} \to P_H^{\mathrm{sm}}$$

defined by the property that $\pi^\vee \circ \pi = [p]$. Thus the remaining sections $S \to C$ also get canonical lifts to P_H.

Moreover, we may pull back $P_G \to C$ to an admissible cover $\pi^* P_G \to P_H$, unramified away from the nodes. To see this, it is most convenient to work instead with the associated *twisted* curves $\mathcal{P}_G$, $\mathcal{P}_H$ and $\mathcal{C}$. Then $\mathcal{P}_G$ and $\mathcal{P}_H$ are genuine torsors over $\mathcal{C}$ and the pullback $\pi^* P_G$ is just the ordinary fibered product $\mathcal{P}_H \times_{\mathcal{C}} \mathcal{P}_G$. By the argument of [Abramovich et al. 2003, Lemma 2.2.1], $\pi^* P_G$ is untwisted. Moreover, $\pi^* P_G$ is a connected curve: since the groups H and G have coprime exponents by assumption, the surjectivity of the maps

$$\pi_1(\mathcal{C}) \to H \quad \text{and} \quad \pi_1(\mathcal{C}) \to G$$

implies the surjectivity of the product map to $H \times G$.

Hence $\pi^* P_G \to P_H$ is an n-pointed, in general only prestable, curve with a connected admissible G-torsor, and by stabilization [Abramovich and Vistoli 2002, Proposition 9.1.1] we get an object of $\overline{\mathcal{M}}_{1,n}(m)(S)$. This defines the map ψ.

The argument above also shows how to define an $\mathbb{S}_n$-action on $\overline{\mathcal{M}}_{1,n}(m;\, p)$. It is clear how the subgroup permuting the last $n-1$ points acts. For a permutation switching the first and i-th point, we use the dual isogeny induced by the trivialization of the H-torsor over the identity section to get a trivialization over the i-th section as well. With this definition, both ϕ and ψ are $\mathbb{S}_n$-equivariant.

Theorem 6.2. *Let p be a prime. The composition $[\phi_*] \circ [\psi^*]$ defines an endomorphism of the Chow motive M. The induced endomorphism of the Betti realization coincides with the direct sum of the classical Hecke operator T_p acting on holomorphic cusp forms and its conjugate acting on antiholomorphic cusp forms, and the induced endomorphism of the ℓ-adic realizations is the ℓ-adic analogue of the Hecke operator, satisfying the Eichler–Shimura relation.*

Proof. Like [Scholl 1990], we show that the induced endomorphism on the open part

$$H^\bullet(\mathcal{M}_{1,n}(m))[\mathrm{sgn}]$$

coincides with the action of the Hecke operator on both cusp forms and Eisenstein series. It may be helpful to compare this proof with the proof of Proposition 4.2. Consider first the following diagram:

$$\begin{array}{ccccc}
\mathcal{M}_{1,n}(m) & \xleftarrow{\phi} & \mathcal{M}_{1,n}(m;\, p) & \xrightarrow{\psi} & \mathcal{M}_{1,n}(m) \\
\downarrow & & \downarrow & & \downarrow \\
\mathcal{M}_{1,1}(m) & \xleftarrow{\phi'} & \mathcal{M}_{1,1}(m;\, p) & \xrightarrow{\psi'} & \mathcal{M}_{1,1}(m)
\end{array}$$

By allowing markings to coincide we get an open embedding of all the spaces on the top row into fibered powers of the respective universal elliptic curves over the spaces on the bottom row:

$$\begin{array}{ccccc}
\mathcal{E}^{n-1} & \xleftarrow{\phi} & \mathcal{E}'^{n-1} & \xrightarrow{\psi} & \mathcal{E}^{n-1} \\
\downarrow & & \downarrow & & \downarrow \\
\mathcal{M}_{1,1}(m) & \xleftarrow{\phi'} & \mathcal{M}_{1,1}(m;\, p) & \xrightarrow{\psi'} & \mathcal{M}_{1,1}(m)
\end{array}$$

One checks that the definition of ϕ and ψ makes sense in exactly the same way also on these bigger spaces, and that ϕ and ψ are equal to the $(n-1)$-st fibered power of the morphism between universal curves induced by ϕ' and ψ'.

By the same arguments as in the proof of Proposition 4.2, one finds that: (i) these open embeddings induce an isomorphism on the alternating part of the cohomology, (ii) the degeneration of the Leray spectral sequence implies that the alternating part of the cohomology of each space on the top row is given by the cohomology of the local system $\mathrm{Sym}^{n-1} R^1\pi_*\mathbb{Q}$ on each space on the bottom row, where π is the projection from the universal curve. By the functoriality of the Leray spectral

sequence, the endomorphism on $H^\bullet(\mathcal{M}_{1,n}(m))[\mathrm{sgn}]$ induced by $[\phi_*][\psi^*]$ is the same as the one induced on

$$H^1(\mathcal{M}_{1,1}(m), \mathrm{Sym}^{n-1} R^1\pi_*\mathbb{Q})$$

by ϕ' and ψ'. As in Section 3 we may rigidify $\mathcal{M}_{1,1}(m)$ and $\mathcal{M}_{1,1}(m;\, p)$ with respect to the action of $(\mathbb{Z}/m\mathbb{Z})^2$; doing so, one finds by arguments very similar to those of Section 3 that the resulting spaces are isomorphic to the spaces called M_m and $M_{m,p}$, respectively, in [Deligne 1971], and that the maps ϕ' and ψ' coincide with the morphisms q_1 and q_2 defined in [Deligne 1971, Equation 3.14]. As in Theorem 5.2 rigidification induces an isomorphism on cohomology, and the proof follows by [Deligne 1971, Proposition 3.18]. □

Remark 6.3. As done by [Scholl 1990], the Hecke operators can be used to decompose the cusp form motives. Let f be a normalized newform of some weight and level. We would like to associate a motive to f, which should be a submotive of the motive M we have already associated to the space of all cusp forms of this weight and level. We consider now M as a Chow motive modulo *homological* equivalence (say with respect to Betti cohomology) instead, and consider the subalgebra H of $\mathrm{End}\, M$ generated by all T_p. This subalgebra is semisimple because its image under the Hodge realization is semisimple. The newform f lies in a 1-dimensional eigenspace for all the T_p, and this eigenspace is a simple H-submodule, so there exists an idempotent in the algebra H whose image is this eigenspace. This idempotent defines a Chow motive modulo homological equivalence which is associated to f.

Remark 6.4. Another way of decomposing cusp form motives into smaller pieces comes from looking also at the congruence subgroups $\Gamma_1(m)$ and $\Gamma_0(m)$. One may define a space of pointed stable curves with $\Gamma_1(m)$-level structure in much the same way as we have done in this article by considering the moduli spaces $\overline{\mathcal{M}}_{1,n}(B\mathbb{Z}/m\mathbb{Z})$ instead of $B(\mathbb{Z}/m\mathbb{Z})^2$. Explicitly, we look at the open and closed substack consisting of connected admissible torsors which are unramified over each marked point. The arguments in this article go through with only very minor changes. One finds by arguments similar to those in Section 3 that for $n = 1$ the curve $X_1(m)$ is recovered, and just as in this article it is seen that by projecting onto the alternating representation of $\mathbb{S}_n$ one isolates the part of the cohomology associated to cusp forms. Moreover, there is an action of $U(\mathbb{Z}/m\mathbb{Z})$ on the space, under which the cohomology decomposes into pieces indexed by the characters of $U(\mathbb{Z}/m\mathbb{Z})$. This way one can construct also motives associated to spaces of cusp forms of given level, weight and nebentypus. This has the advantage over the construction with Hecke operators that it does not take us out of the category of Chow motives modulo rational equivalence.

Acknowledgements

I am grateful to my advisor Carel Faber for patient discussions. I have also benefited from useful conversations with Nicola Pagani and Sergey Shadrin.

References

[Abramovich 2008] D. Abramovich, "Lectures on Gromov–Witten invariants of orbifolds", pp. 1–48 in *Enumerative invariants in algebraic geometry and string theory* (Cetraro, 2005), edited by K. Behrend and M. Manetti, Lecture Notes in Math. **1947**, Springer, Berlin, 2008. MR 2010b:14112 Zbl 1151.14005

[Abramovich and Vistoli 2002] D. Abramovich and A. Vistoli, "Compactifying the space of stable maps", *J. Amer. Math. Soc.* **15**:1 (2002), 27–75. MR 2002i:14030 Zbl 0991.14007

[Abramovich et al. 2003] D. Abramovich, A. Corti, and A. Vistoli, "Twisted bundles and admissible covers", *Comm. Algebra* **31**:8 (2003), 3547–3618. MR 2005b:14049 Zbl 1077.14034

[Abramovich et al. 2007] D. Abramovich, T. Graber, M. Olsson, and H.-H. Tseng, "On the global quotient structure of the space of twisted stable maps to a quotient stack", *J. Algebraic Geom.* **16**:4 (2007), 731–751. MR 2008k:14026 Zbl 1126.14002

[Abramovich et al. 2011] D. Abramovich, M. Olsson, and A. Vistoli, "Twisted stable maps to tame Artin stacks", *J. Algebraic Geom.* **20**:3 (2011), 399–477. MR 2012c:14024 Zbl 1225.14020

[Blasius and Rogawski 1993] D. Blasius and J. D. Rogawski, "Motives for Hilbert modular forms", *Invent. Math.* **114**:1 (1993), 55–87. MR 94i:11033 Zbl 0829.11028

[Conrad 2007] B. Conrad, "Arithmetic moduli of generalized elliptic curves", *J. Inst. Math. Jussieu* **6**:2 (2007), 209–278. MR 2008e:11073 Zbl 1140.14018

[Consani and Faber 2006] C. Consani and C. Faber, "On the cusp form motives in genus 1 and level 1", pp. 297–314 in *Moduli spaces and arithmetic geometry* (Kyoto, 2004), edited by S. Mukai et al., Adv. Stud. Pure Math. **45**, Math. Soc. Japan, Tokyo, 2006. MR 2008h:14013 Zbl 1115.14017

[Deligne 1971] P. Deligne, "Formes modulaires et représentations ℓ-adiques", pp. 139–172 in *Séminaire Bourbaki* 1968/1969 (Exposé 355), 1971. Zbl 0206.49901

[Deligne and Rapoport 1973] P. Deligne and M. Rapoport, "Les schémas de modules de courbes elliptiques", pp. 143–316 in *Modular functions of one variable, II* (Antwerp, 1972), edited by P. Deligne and W. Kuyk, Lecture Notes in Math. **349**, Springer, Berlin, 1973. MR 49 #2762 Zbl 0281.14010

[Diamond and Shurman 2005] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics **228**, Springer, New York, 2005. MR 2006f:11045 Zbl 1062.11022

[Faltings 1987] G. Faltings, "Hodge–Tate structures and modular forms", *Math. Ann.* **278** (1987), 133–149. MR 89e:11033 Zbl 0646.14026

[Getzler 1995] E. Getzler, "Mixed Hodge structures of configuration spaces", preprint 96-61, Max-Planck-Institut für Mathematik, Bonn, 1995. arXiv alg-geom/9510018

[Getzler 1998] E. Getzler, "The semi-classical approximation for modular operads", *Comm. Math. Phys.* **194**:2 (1998), 481–492. MR 99d:14017 Zbl 0912.18007

[Getzler and Kapranov 1998] E. Getzler and M. M. Kapranov, "Modular operads", *Compositio Math.* **110**:1 (1998), 65–126. MR 99f:18009 Zbl 0894.18005

[Grothendieck 1971] A. Grothendieck (editor), *Séminaire de Géométrie Algébrique du Bois Marie* 1960–1961: *Revêtements étales et groupe fondamental* (SGA 1), Lecture Notes in Mathematics

224, Springer, Berlin, 1971. Reprinted Société Math. de France, Paris, 2003. MR 50 #7129 Zbl 0234.14002

[Jarvis and Kimura 2002] T. J. Jarvis and T. Kimura, "Orbifold quantum cohomology of the classifying space of a finite group", pp. 123–134 in *Orbifolds in mathematics and physics* (Madison, WI, 2001), edited by A. Adem et al., Contemp. Mathematics **310**, Amer. Math. Soc., Providence, RI, 2002. MR 2004a:14056 Zbl 1065.14069

[Katz and Mazur 1985] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies **108**, Princeton University Press, 1985. MR 86i:11024 Zbl 0576.14026

[Kleiman 1994] S. L. Kleiman, "The standard conjectures", pp. 3–20 in *Motives* (Seattle, WA, 1991), edited by U. Jannsen et al., Proc. Sympos. Pure Math. **55**, Amer. Math. Soc., Providence, RI, 1994. MR 95k:14010 Zbl 0820.14006

[Kresch and Vistoli 2004] A. Kresch and A. Vistoli, "On coverings of Deligne–Mumford stacks and surjectivity of the Brauer map", *Bull. London Math. Soc.* **36**:2 (2004), 188–192. MR 2004j:14003 Zbl 1062.14004

[Macdonald 1995] I. G. Macdonald, *Symmetric functions and Hall polynomials*, 2nd ed., Oxford University Press, New York, 1995. MR 96h:05207 Zbl 0824.05059

[Manin 2005] Y. I. Manin, "Iterated Shimura integrals", *Mosc. Math. J.* **5**:4 (2005), 869–881, 973. MR 2007m:11069 Zbl 1215.11052

[Manin 2006] Y. I. Manin, "Iterated integrals of modular forms and noncommutative modular symbols", pp. 565–597 in *Algebraic geometry and number theory*, edited by V. Ginzburg, Progr. Math. **253**, Birkhäuser, Boston, MA, 2006. MR 2008a:11062 Zbl 1184.11019

[Niles 2012] A. Niles, "Moduli of elliptic curves via twisted stable maps", preprint, 2012. arXiv 1207.7280

[Peters and Steenbrink 2008] C. A. M. Peters and J. H. M. Steenbrink, *Mixed Hodge structures*, Ergeb. Math. Grenzgeb. (3) **52**, Springer, Berlin, 2008. MR 2009c:14018 Zbl 1138.14002

[Petersen 2012] D. Petersen, "A remark on Getzler's semi-classical approximation", pp. 309–316 in *Geometry and arithmetic*, edited by C. Faber et al., European Math. Soc., 2012. To appear.

[Romagny 2005] M. Romagny, "Group actions on stacks and applications", *Michigan Math. J.* **53**:1 (2005), 209–236. MR 2005m:14005 Zbl 1100.14001

[Scholl 1990] A. J. Scholl, "Motives for modular forms", *Invent. Math.* **100**:2 (1990), 419–430. MR 91e:11054 Zbl 0760.14002

[Toën 2000] B. Toën, "On motives for Deligne–Mumford stacks", *Internat. Math. Res. Notices* **2000**:17 (2000), 909–928. MR 2001h:14019 Zbl 1034.14008

Communicated by Yuri Manin
Received 2011-03-18 Accepted 2011-10-18

danpete@math.kth.se *Department of Mathematics, KTH Royal Institute of Technology, Institutionen för matematik, Kungliga Tekniska Högskolan, 100 44 Stockholm, Sweden*

msp

ALGEBRA AND NUMBER THEORY 6:6 (2012)
dx.doi.org/10.2140/ant.2012.6.1223

Ideals of degree one contribute most of the height

Aaron Levin and David McKinnon

Let k be a number field, $f(x) \in k[x]$ a polynomial over k with $f(0) \neq 0$, and $\mathbb{O}_{k,S}^*$ the group of S-units of k, where S is an appropriate finite set of places of k. In this note, we prove that outside of some natural exceptional set $T \subset \mathbb{O}_{k,S}^*$, the prime ideals of $\mathbb{O}_k$ dividing $f(u)$, $u \in \mathbb{O}_{k,S}^* \setminus T$, mostly have degree one over $\mathbb{Q}$; that is, the corresponding residue fields have degree one over the prime field. We also formulate a conjectural analogue of this result for rational points on an elliptic curve over a number field, and deduce our conjecture from Vojta's conjecture. We prove this conjectural analogue in certain cases when the elliptic curve has complex multiplication.

1. Introduction

If a is an algebraic integer in a number field k and $f(x) \in \mathbb{O}_k[x]$ a polynomial, then the ideals dividing $f(a)$ are simply the ideals I such that $f(a) \equiv 0 \pmod{I}$. Heuristically, the larger the cardinality of the residue ring $\mathbb{O}_k/I$, the smaller the probability that $f(a)$ and 0 are the same.

The purpose of this paper is to make this notion precise, to generalize it, and to prove it in the case described above. More specifically, in Theorem 2.1, using a result of Corvaja and Zannier, we prove a precise version of this notion for $\mathbb{G}_m$, and in Theorem 3.4, we state a conjectural analogue of Theorem 2.1 for elliptic curves over a number field, and show that it is a consequence of Vojta's conjecture [1987; 2011].

A theorem of the second author proves Vojta's conjecture in a relevant special case, and we deduce an unconditional version of Theorem 3.4 in that case. Specifically, if the elliptic curve E/k has complex multiplication, and if the algebraic point P is defined over the compositum of k with $\mathrm{End}(E) \otimes \mathbb{Q}$, then we can deduce Theorem 3.4 without the hypothesis that Vojta's conjectures are true.

MSC2010: primary 11G50; secondary 11J25.

Keywords: heights, Diophantine approximation, polynomial values, elliptic curves, Vojta's conjecture.

2. Main theorem

Let $f(x) \in k[x]$ be a polynomial over a number field k. The heuristic mentioned in the introduction suggests that a prime $\mathfrak{p}$ of k is likelier to divide $f(a)$ for $a \in k$ if the residue field $\mathbb{O}_k/\mathfrak{p}$ is small. Our main theorem will give one possible precise interpretation of this notion, where we view $\mathbb{O}_k/\mathfrak{p}$ as being small if $\mathbb{O}_k/\mathfrak{p}$ has degree one over its prime field. There is, however, an obvious way that our heuristic can fail. Suppose, for example, that f and a, and hence $f(a)$, are actually defined over a proper subfield k' of k. Then the size of $\mathbb{O}_{k'}/(\mathfrak{p} \cap \mathbb{O}_{k'})$, and not $\mathbb{O}_k/\mathfrak{p}$, is clearly the relevant quantity. In the simplest case, when $k/\mathbb{Q}$ is Galois and f is irreducible, our main theorem says, in essence, that for S-units u of k this is in fact the only way our heuristic can fail, that is, $f(u)$ is "mostly" supported on primes of k of degree one over $\mathbb{Q}$ unless $f(u)$ is rational, in an appropriate sense, over a proper subfield of k.

The statement of the main theorem requires a fair amount of notation. We summarize this notation as follows:

k	Extension of $\mathbb{Q}$ of degree $d \neq 1$
L	Galois closure of k over $\mathbb{Q}$
$\mathrm{Gal}(L/\mathbb{Q})$	The Galois group of L over $\mathbb{Q}$
$\mathbb{O}_k$	Ring of integers of k
$f(x)$	Nonconstant polynomial in $\mathbb{O}_k[x]$ with $f(0) \neq 0$
$f_1, \ldots, f_N$	The monic irreducible factors of f over L
S	Finite set of places of k containing the archimedean places such that if $v \in S$ and v and v' lie above the same rational prime $p \in \mathbb{Z}$ then $v' \in S$.
$\mathbb{O}_{k,S}$	Ring of S-integers of k
$\mathbb{O}_{k,S}^*$	Group of S-units of k
τ	The involution $\tau(u) = u^{-1}$ of $\mathbb{O}_{k,S}^*$.
$\mathbb{O}_{k,S}^{*\phi}$	For a homomorphism ϕ, the subgroup of $\mathbb{O}_{k,S}^*$ consisting of elements u such that $\phi(u) = u$.
$I(f(u))$	The ideal generated by $f(u)$ in the ring $\mathbb{O}_{k,S}$
$J(f(u))$	Smallest ideal dividing $I(f(u))$ such that for every prime $\mathfrak{p}$ dividing $J(f(u))$, $\mathbb{O}_{k,S}/\mathfrak{p}$ has degree greater than one over the prime field
$N(I)$	The norm of I over $\mathbb{Q}$, for any ideal I of $\mathbb{O}_k$ or $\mathbb{O}_{k,S}$
$H_k(x)$	The relative multiplicative Weil height of $x \in k$
$H(x)$	The absolute multiplicative Weil height of x, equal to $H_k(x)^{1/d}$ for $x \in k$
$h(x)$	The absolute logarithmic Weil height of x, equal to $\log H(x)$

We can now state the main theorem:

Theorem 2.1. *Let $\epsilon > 0$. Let $f(x) \in \mathbb{O}_k[x]$ satisfy $f(0) \neq 0$. Then there exists a finite set of places S' of L such that for every $u \in \mathbb{O}_{k,S}^*$ either*

(a) $$N(J(f(u))) < H(u)^{\epsilon}$$

or

(b) $$f_i(u)\mathbb{O}_{L,S'} = \alpha\mathbb{O}_{L,S'} \tag{1}$$

for some i and some α that lies in a proper subfield of L not containing k (in particular, if $k/\mathbb{Q}$ is Galois, α lies in a proper subfield of k).

With the exception of finitely many elements, the set of elements in $\mathbb{O}_{k,S}^*$ not satisfying (a) is contained in a finite union of cosets in $\mathbb{O}_{k,S}^*$ of the form

$$T = u_1\mathbb{O}_{k,S}^{*\sigma_1} \cup \cdots \cup u_{m'}\mathbb{O}_{k,S}^{*\sigma_{m'}} \cup u_{m'+1}\mathbb{O}_{k,S}^{*\sigma_{m'+1}\tau} \cup \cdots \cup u_m\mathbb{O}_{k,S}^{*\sigma_m\tau},$$

where $u_1, \ldots, u_m \in \mathbb{O}_{k,S}^*$ and $\sigma_1, \ldots, \sigma_m \in \mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(L/k)$ (not necessarily distinct) are effectively computable.

An alternative formulation of Theorem 2.1 involving only heights is given in Corollary 2.6. We mention also that the group $\mathbb{O}_{k,S}^{*\sigma_i}$ is the same as $\mathbb{O}_{F,S_F}^*$, where F is the fixed field of σ_i and S_F is the set of places of F lying below places of S.

Note that $H(f(u)) \ll H(u)^{\deg f}$ and that

$$H_k(f(u)) = C_u N(I(f(u))) = C_u N(J(f(u)))N(I(f(u))/J(f(u))),$$

where C_u is a real number (roughly equal to the archimedean part of the height of $f(u)^{-1}$) satisfying $C_u \ll H(u)^{\epsilon}$ (see Lemma 2.7). Thus, Theorem 2.1 implies that for $u \in \mathbb{O}_{k,S}^* \setminus T$, $f(u)$ is "mostly" supported on primes of k of degree one over $\mathbb{Q}$.

Finally, let us mention some possible generalizations of Theorem 2.1. Firstly, we note that for any integer n and $u \in \mathbb{O}_{k,S}^*$, we have $J(u^n f(u)) = J(f(u))$ and $u^n f(u)\mathbb{O}_{k,S} = f(u)\mathbb{O}_{k,S}$. Thus, Theorem 2.1 immediately extends to Laurent polynomials (that is, $f(x) \in k[x, 1/x]$). However, if $f(x)$ has a zero or pole at $x = 0$, then the interpretation that for $u \in \mathbb{O}_{k,S}^* \setminus T$, $f(u)$ is "mostly" supported on primes of k of degree one over $\mathbb{Q}$ is no longer necessarily valid (the inequality $N(I(f(u))) \gg H_k(f(u))^{1-\epsilon}$ may not hold in the previous remark). More generally, Theorem 2.1 may be extended in a straightforward way to rational functions (appropriately using fractional ideals in place of integral ideals). In a different direction, it seems to be an interesting problem to formulate an appropriate generalization of Theorem 2.1 that is valid for S-integers (as opposed to just S-units), or to prove a multivariable analogue.

Before we begin the proof, we introduce some notation. For a number field k we denote the set of inequivalent places of k by M_k. We define the function $\log^-$ for positive real numbers x by $\log^-(x) = \min\{0, \log(x)\}$. For a place $v \in M_k$, we

normalize the corresponding absolute value $|\cdot|_v$ in such a way that the product formula holds and $H(x) = \prod_{v \in M_k} \max\{1, |x|_v\}$.

Proof of Theorem 2.1. Consider the set

$$U = \{u \in \mathbb{O}_{k,S}^* \mid N(J(f(u))) \geq H(u)^{\epsilon}\}.$$

Let L be a Galois closure of k over $\mathbb{Q}$. Let $\mathfrak{p}$ be a prime of $\mathbb{O}_k$ of inertia degree greater than one over $\mathbb{Q}$, lying above a rational prime $p \in \mathbb{Z}$. Let $\mathfrak{q}$ be a prime of $\mathbb{O}_L$ lying above $\mathfrak{p}$. Then $\mathfrak{q}$ again has inertia degree greater than one over $\mathbb{Q}$. Let $D = D(\mathfrak{q}/p) \subset \mathrm{Gal}(L/\mathbb{Q})$ be the decomposition group of $\mathfrak{q}$ and let L^D be the decomposition field. Then $k \not\subset L^D$ since $\mathfrak{p}$ has inertia degree greater than one. It follows that there exists $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}$, $\sigma \notin \mathrm{Gal}(L/k)$.

Let S_L be the set of places of L lying above places of S. Let

$$J'(f(u)) = J(f(u))\mathbb{O}_{L,S_L}.$$

Let $\mathfrak{q}$ be a prime of $\mathbb{O}_{L,S_L}$ dividing $J'(f(u))$. From the above discussion and the definition of $J(f(u))$, there exists an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(L/k)$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}$. Let $\mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(L/k) = \{\sigma_1, \ldots, \sigma_m\}$. For $i = 1, \ldots, m$, define the ideal $J_i'(f(u))$ to be the smallest ideal of $\mathbb{O}_{L,S_L}$ dividing $J'(f(u))$ such that $\sigma_i(J_i'(f(u))) = J_i'(f(u))$. Then $J'(f(u))$ divides $J_1'(f(u)) \cdots J_m'(f(u))$. Note also that $N(J'(f(u))) \geq N(J(f(u)))$. Let

$$U_i = \{u \in U \mid N(J_i'(f(u))) \geq H(u)^{\epsilon/m}\}.$$

Then clearly $U \subset \bigcup_{i=1}^m U_i$.

Let $r \in \{1, \ldots, m\}$, and let f^{σ_r} denote the image of f under the natural action of σ_r. By definition, $J_r'(f(u))$ divides both $f(u)\mathbb{O}_{L,S_L}$ and $f^{\sigma_r}(\sigma_r(u))\mathbb{O}_{L,S_L}$ for all u. For $u \in U_r$, we therefore obtain

$$\begin{aligned}[L:\mathbb{Q}] \sum_{v \in M_L} \log^- \max\{|f(u)|_v, |f^{\sigma_r}(\sigma_r(u))|_v\} &\leq -\log N(J_r'(f(u))) \\ &\leq -\log H(u)^{\epsilon/m} \leq -\frac{\epsilon}{m} h(u).\end{aligned}$$

Theorem 2.1 will follow essentially from the following:

Lemma 2.2 [Corvaja and Zannier 2005, Proposition 4]. *Let $f(x), g(x) \in L[x]$ be polynomials that do not vanish at $x = 0$. Then, for every $\epsilon > 0$, all but finitely many solutions $(u, u') \in (\mathbb{O}_{L,S_L}^*)^2$ to the inequality*

$$\sum_{v \in M_L} \log^- \max\{|f(u)|_v, |g(u')|_v\} < -\epsilon(\max\{h(u), h(u')\})$$

are contained in finitely many effectively computable translates of one-dimensional subgroups of $\mathbb{G}_m^2$.

Since $h(u) = h(\sigma_r(u))$ and $u, \sigma_r(u) \in \mathbb{O}^*_{L,S_L}$, taking $g = f^{\sigma_r}$ it follows immediately from Lemma 2.2 that all but finitely many elements of the set

$$V_r = \{(u, \sigma_r(u)) \mid u \in U_r\}$$

are contained in finitely many effectively computable translates of one-dimensional subgroups of $\mathbb{G}_m^2$. Let X be a translate of a one-dimensional subgroup of $\mathbb{G}_m^2$ that contains infinitely many elements of V_r. Let $(v, \sigma_r(v)) \in X \cap V_r$. Taking $u = v'/v \in \mathbb{O}^*_{k,S}$, where $(v', \sigma_r(v')) \in X \cap V_r$, we see that infinitely many elements of the form $(u, \sigma_r(u))$, $u \in \mathbb{O}^*_{k,S}$, will lie in the associated one-dimensional subgroup in $\mathbb{G}_m^2$. We now classify the possibilities for such a one-dimensional subgroup.

Suppose there exists $a, b \in \mathbb{Z}$, not both zero, such that

$$u^a \sigma_r(u)^b = 1, \tag{2}$$

for infinitely many $u \in \mathbb{O}^*_{k,S}$. We claim that $a = \pm b$. Let l be the order of σ_r. Then

$$u^{b^l} = \sigma_r^l(u)^{b^l} = \sigma_r^{l-1}(u)^{-ab^{l-1}} = \cdots = u^{(-a)^l}.$$

So $u^{b^l-(-a)^l} = 1$ for infinitely many $u \in \mathbb{O}^*_{k,S}$. This implies that $b^l = (-a)^l$, or $a = \pm b$, as claimed.

Suppose first that $a = -b$. Then for any $u \in \mathbb{O}^*_{k,S}$ satisfying (2) we have $\sigma_r(u^a) = u^a$. So $u^a \in \mathbb{O}^{*\sigma_r}_{k,S} = F \cap \mathbb{O}^*_{k,S}$, where F is the fixed field of σ_r. It follows that $\mathbb{O}^{*\sigma_r}_{k,S}$ has finite index in $\{u \in \mathbb{O}^*_{k,S} \mid u^a \sigma_r(u)^{-a} = 1\}$ and that $\{u \in \mathbb{O}^*_{k,S} \mid (u, \sigma_r(u)) \in X \cap V_r\}$ is contained in a finite number of cosets of $\mathbb{O}^{*\sigma_r}_{k,S}$ in $\mathbb{O}^*_{k,S}$.

Suppose now that $a = b$. Then for any $u \in \mathbb{O}^*_{k,S}$ satisfying (2) we have $\sigma_r(u^a) = u^{-a}$. By definition, we have $u^{-a} \in \mathbb{O}^{*\sigma_r\tau}_{k,S}$. Then, as above, we find that

$$\{u \in \mathbb{O}^*_{k,S} \mid (u, \sigma_r(u)) \in X \cap V_r\}$$

is contained in a finite number of cosets of $\mathbb{O}^{*\sigma_r\tau}_{k,S}$ in $\mathbb{O}^*_{k,S}$.

Since there are only finitely many such X and finitely many r, we conclude that there exists a set T as in the statement of the theorem such that $U \setminus T$ is finite.

We now prove that all of the elements in T satisfy (1) for some choice of S', completing the proof of the theorem. Let $f_1, \ldots, f_N \in L[x]$ be the monic irreducible factors of $f(x)$ over L. First, consider cosets in $\mathbb{O}^*_{k,S}$ of the form $u_i \mathbb{O}^{*\sigma_r}_{k,S}$. From a slight modification of the first part of the proof above, we need only consider cosets $u_i \mathbb{O}^{*\sigma_r}_{k,S}$ such that for some $j \in \{1, \ldots, N\}$ and $\epsilon > 0$, there are infinitely many $u \in \mathbb{O}^{*\sigma_r}_{k,S}$ such that

$$\sum_{v \in M_L} \log^- \max\{|f_j(u_i u)|_v, |f_j^{\sigma_r}(\sigma_r(u_i u))|_v\} \le -\epsilon h(u_i u). \tag{3}$$

Note that $\sigma_r(u_i u) = \sigma_r(u_i)u$, since $u \in \mathbb{O}_{k,S}^{*\sigma_r}$. If $f_j(u_i x)$ and $f_j^{\sigma_r}(\sigma_r(u_i)x)$ are relatively prime in $L[x]$, then the left-hand side of (3) is bounded from below, independent of $u \in \mathbb{O}_{k,S}^{*\sigma_r}$. Since there are only finitely many $u \in \mathbb{O}_{k,S}^{*\sigma_r}$ with $h(u_i u)$ bounded, this contradicts the inequality (3) for all but finitely many $u \in \mathbb{O}_{k,S}^{*\sigma_r}$. So $f_j(u_i x)$ and $f_j^{\sigma_r}(\sigma_r(u_i)x)$ have a nontrivial common factor. Since $f_j(u_i x)$ and $f_j^{\sigma_r}(\sigma_r(u_i)x)$ are both irreducible over L, they must then be equal up to multiplication by a constant factor. Thus,

$$\frac{f_j(u_i x)}{u_i^e} = \frac{f_j^{\sigma_r}(\sigma_r(u_i)x)}{\sigma_r(u_i)^e},$$

where $e = \deg f_j$. It follows that for all u in $\mathbb{O}_{k,S}^{*\sigma_r}$,

$$\frac{f_j(u_i u)}{u_i^e} = \sigma_r\Big(\frac{f_j(u_i u)}{u_i^e}\Big).$$

So $f_j(u_i u)/u_i^e \in k'$, the fixed field of σ_r. Then, for all $u \in \mathbb{O}_{k,S}^{*\sigma_r}$, $f_j(u_i u)/u_i^e$ lies in a proper subfield of L not containing k. So in this case (1) holds with $S' = S_L$ (and u replaced by $u_i u$).

Now consider a coset of the form $u_i \mathbb{O}_{k,S}^{*\sigma_r\tau}$. Again, we may assume that for some j and some $\epsilon > 0$, (3) is satisfied for infinitely many $u \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$. By definition, for $u \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$ we have $\sigma_r(u) = u^{-1}$. Let $e = \deg f_j$. Similar to before, if $f_j(u_i x)$ and $x^e f_j^{\sigma_r}(\sigma_r(u_i)/x)$ are relatively prime in $L[x]$, then it follows that

$$\sum_{v \in M_L} \log^- \max\big\{ |f_j(u_i u)|_v \, , |f_j^{\sigma_r}(\sigma_r(u_i)/u)|_v \big\}$$

is bounded from below, independent of $u \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$. This again gives a contradiction with (3) and so $f_j(u_i x)$ and $x^e f_j^{\sigma_r}(\sigma_r(u_i)/x)$ must have a nontrivial common factor over L. Since f_j is irreducible over L, the two polynomials must be equal up to multiplication by a constant. Evaluating at any $x = u' \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$ with $f_j(u_i u') \neq 0$, we find that we must have that

$$\frac{f_j(u_i x)}{f_j(u_i u')} = \frac{x^e f_j^{\sigma_r}(\sigma_r(u_i)/x)}{u'^e \sigma_r(f_j(u_i u'))}.$$

Since $(\mathbb{O}_{k,S}^{*\sigma_r\tau})^2$ has finite index in $\mathbb{O}_{k,S}^{*\sigma_r\tau}$, we can find a finitely many elements $u_1', \ldots, u_{l'}' \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$ with $f_j(u_i u_l') \neq 0$, $l = 1, \ldots, l'$, and such that for any $u \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$, there exists some $l \in \{1, \ldots, l'\}$ with $u/u_l' \in (\mathbb{O}_{k,S}^{*\sigma_r\tau})^2$. Let $u \in \mathbb{O}_{k,S}^{*\sigma_r\tau}$ and u_l' chosen as above. Then we have the identity

$$\sigma_r\Big(\Big(\frac{u_l'}{u}\Big)^{e/2} \frac{f_j(u_i u)}{f_j(u_i u_l')}\Big) = \Big(\frac{u_l'}{u}\Big)^{e/2} \frac{f_j(u_i u)}{f_j(u_i u_l')}$$

and it follows that $(u_l'/u)^{e/2} f_j(u_i u)/f_j(u_i u_l') \in k'$, the fixed field of σ_r. We can enlarge S_L to a finite set of places S' of L such that $f_j(u_i u_l')$ is an S'-unit for all choices of i, j, and l. Then (1) holds for all $u \in u_i \mathbb{O}_{k,S}^{*\sigma_r\tau}$. □

In the case of a cyclic subgroup of k^* the theorem takes a particularly simple form.

Corollary 2.3. *Let $a \in k^*$. Let S be a finite set of places of k such that a is an S-unit. Assume that for all positive integers m,*

(a) *the element a^m does not lie in a proper subfield of k, and*

(b) *k is not a quadratic extension of a field k' with $N_{k'}^k(a^m) = 1$.*

Let $\epsilon > 0$ and let $f(x) \in \mathbb{O}_k[x]$ satisfy $f(0) \neq 0$. Then, for all but finitely many integers n,

$$N(J(f(a^n))) < H(a^n)^\epsilon.$$

Proof. Suppose that for infinitely many n, $N(J(f(a^n))) \geq H(a^n)^\epsilon$. Then by Theorem 2.1, there exists $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(k/\mathbb{Q})$ and $u \in \mathbb{O}_{k,S}^*$ such that for infinitely many n, a^n lies in a coset of the form $u\mathbb{O}_{k,S}^{*\sigma}$ or $u\mathbb{O}_{k,S}^{*\sigma\tau}$. This implies that for some $m \neq 0$, $a^m \in \mathbb{O}_{k,S}^{*\sigma}$ or $a^m \in \mathbb{O}_{k,S}^{*\sigma\tau}$. In the first case, a^m lies in the proper subfield $k \cap F$ of k, where F is the fixed field of σ. Suppose that $a^m \in \mathbb{O}_{k,S}^{*\sigma\tau}$ and that a^m does not lie in a proper subfield of k. Then $k = \mathbb{Q}(a^m)$. Since $\sigma(a^m) = a^{-m}$, σ restricts to an automorphism of k over $\mathbb{Q}$. Note that $\sigma^2(a^m) = a^m$, so σ is an automorphism of k of order 2. Let k' be the fixed field of σ. Then $[k : k'] = 2$, $\mathrm{Gal}(k/k') = \{\mathrm{id}, \sigma\}$, and $N_{k'}^k(a^m) = a^m \sigma(a^m) = 1$. □

We give an example related to Fibonacci numbers to show the likely necessity of the less obvious condition (b) in Corollary 2.3.

Example 2.4. Let $k = \mathbb{Q}(\sqrt{5})$ and $a = \varphi = \frac{1+\sqrt{5}}{2} \in k^*$. Let S consist of the archimedean places of k and the prime lying above 5. Let $f(x) = x + 1$. For n odd, we have

$$\frac{\varphi^{2n}+1}{\varphi^n\sqrt{5}} = F_n,$$

where F_n is the n-th Fibonacci number. So

$$f(\varphi^{2n})\mathbb{O}_{k,S} = F_n \mathbb{O}_{k,S}.$$

A well-known naïve heuristic argument suggests that there should be infinitely many Fibonacci numbers that are prime and congruent to $\pm 2 \pmod 5$ (so that these primes are inert in k). In this case, there would be an $\epsilon > 0$ and infinitely many values of n such that $N(J(f(\varphi^n))) = N(f(\varphi^n)) > H(\varphi^n)^\epsilon$. This doesn't contradict Corollary 2.3 as $N_{\mathbb{Q}}^k(\varphi^2) = 1$.

We now give a slight reformulation of our results.

Definition 2.5. Let D be an effective divisor on $\mathbb{P}^1$ defined over k and supported on $\mathbb{P}^1 \setminus \{0, \infty\} = \mathbb{G}_m$. Let $a \in k^*$, $a \notin \operatorname{Supp} D$, where $\operatorname{Supp} D$ is the support of D. Let h_D be the absolute logarithmic height associated to D and let $h_D = \sum_{v \in M_k} h_{D,v}$ be a decomposition of h_D into local heights (Weil functions). For a place $v \in M_k$ associated to a prime $\mathfrak{p}$ lying above a prime $p \in \mathbb{Z}$, let $f_v = f_{\mathfrak{p}} = [\mathbb{O}_k/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$. Set $f_v = 1$ if $v|\infty$. We define the degree-one height of a with respect to k and D by

$$h_{D,\deg_1(k)}(a) = \sum_{\substack{v \in M_k \\ f_v = 1}} h_{D,v}(a).$$

Similarly, we define

$$h_{D,\deg_{>1}(k)}(a) = \sum_{\substack{v \in M_k \\ f_v > 1}} h_{D,v}(a).$$

Note that

$$h_D(a) = h_{D,\deg_1(k)}(a) + h_{D,\deg_{>1}(k)}(a)$$

and by standard properties of heights, $h_{D,\deg_1(k)}$ and $h_{D,\deg_{>1}(k)}$ depend on the choice of h_D and the local height functions only up to $O(1)$.

Corollary 2.6. *Let D be an effective divisor on $\mathbb{P}^1$ defined over k and supported on $\mathbb{P}^1 \setminus \{0, \infty\}$. Let $f(x) \in \mathbb{O}_k[x]$ be a polynomial defining D with monic irreducible factors $f_1, \ldots, f_n$ over L. Let $\epsilon > 0$. Then there exists a finite set of places S' of L such that for every $u \in \mathbb{O}_{k,S}^*$ either*

(a) $$h_{D,\deg_{>1}(k)}(u) < \epsilon h_D(u)$$

or

(b) $$f_i(u)\mathbb{O}_{L,S'} = \alpha \mathbb{O}_{L,S'}$$

for some i and some α that lies in a proper subfield of L not containing k.

All but finitely many elements not satisfying (a) are again contained in a set T as in Theorem 2.1. There is also a similar reformulation of Corollary 2.3 in terms of $h_{D,\deg_{>1}(k)}(u)$.

Lemma 2.7. *Let D be as in Corollary 2.6. For any finite set of places $S' \subset M_k$ and any $\epsilon > 0$,*

$$\sum_{v \in S'} h_{D,v}(u) < \epsilon h(u) + O(1) \tag{4}$$

for all $u \in \mathbb{O}_{k,S}^*$.

Proof. It suffices to show this for D a point (not equal to 0 or ∞) and $S' \supset S$. Let $E = 0 + \infty$. Since u is an S'-unit, we have

$$\sum_{v \in S'} h_{E,v}(u) = 2h(u) + O(1).$$

By Roth's theorem,

$$\sum_{v\in S'} h_{D+E,v}(u) = \sum_{v\in S'} h_{D,v}(u) + 2h(u) + O(1) < (2+\epsilon)h(u) + O(1),$$

which gives (4). □

In particular, it follows from Lemma 2.7 that Corollary 2.6 remains true if we add finitely many local heights to $h_{D,\deg_{>1}(k)}$ (e.g., all the archimedean ones).

Proof of Corollary 2.6. We may take as local height functions associated to D the functions

$$h_{D,v}(a) = -\log^- |f(a)|_v, \quad v \in M_k.$$

Using Theorem 2.1 and Lemma 2.7, we can write, for all $u \in \mathbb{O}_{k,S}^*$,

$$\begin{aligned} h_{D,\deg_{>1}(k)}(u) &= \sum_{\substack{v\in M_k\\ f_v>1}} h_{D,v}(u) = -\sum_{\substack{v\in M_k\setminus S\\ f_v>1}} \log^- |f(u)|_v + \sum_{\substack{v\in S\\ f_v>1}} h_{D,v}(u) \\ &= \frac{1}{[k:\mathbb{Q}]} \log N(J(f(u))) + \sum_{\substack{v\in S\\ f_v>1}} h_{D,v}(u) \\ &< \epsilon h(u) + O(1), \end{aligned}$$

□

3. Elliptic curves

Theorem 2.1 has a conjectural analogue for elliptic curves, following from a conjectural analogue of Lemma 2.2.

Conjecture 3.1 (Vojta). *Let E be an elliptic curve defined over a number field k. Let h be an ample height function on E. Let $B \subset E(\bar{k}) \times E(\bar{k})$ be a finite set of points with B defined over k. Let $\pi : X \to E \times E$ be the morphism obtained by blowing up the points in B and let Y be the exceptional divisor of π. Let h_Y be a logarithmic height function with respect to Y. Let $\epsilon > 0$. There exists a proper Zariski closed subset $Z(\epsilon)$ of X such that for every $(P, Q) \in (E \times E)(k) - \pi(Z(\epsilon))$, we have*

$$h_Y(\pi^{-1}(P, Q)) \le \epsilon(h(P) + h(Q)) + O(1).$$

(Conjecture 3.1 is a special case of a much more general set of conjectures made by Vojta [1987; 2011].)

This enables us to deduce an analogue of Theorem 2.1 for elliptic curves. As in the previous section, it will be convenient to list the notation used:

k	Fixed number field
ℓ/k	Fixed nontrivial extension of k
L	Galois closure of ℓ over k
$\mathrm{Gal}(L/k)$	Galois group of L over k
$\mathbb{O}_k$	Ring of integers of k
S	Fixed finite set of places of L, consisting of the archimedean places of L and the places of L ramified over k
$\mathbb{O}_{L,S}$	The ring of S-integers of L
E	Fixed elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$, $a, b \in \mathbb{O}_k$
$E(\ell)^{\nu\sigma}$	For $\nu \in \mathrm{Aut}(E)$ and $\sigma \in \mathrm{Gal}(L/k)$, the subgroup of points $x \in E(\ell)$ satisfying $\nu\sigma(x) = x$
D	Fixed effective and nontrivial ℓ-rational divisor on E
$D_1, \ldots, D_N$	The irreducible components of D over L
$I_D(P)$	Ideal associated to D and P (see Definition 3.2)
$J_D(P)$	The smallest divisor ideal of $I_D(P)$ supported on primes $\mathfrak{p}$ of $\mathbb{O}_\ell$ with $[\mathbb{O}_\ell/\mathfrak{p} : \mathbb{O}_k/(\mathbb{O}_k \cap \mathfrak{p})] > 1$
$N(I)$	Absolute norm of an ideal I of $\mathbb{O}_\ell$
$H_D(P)$	Multiplicative height function on E corresponding to D
$h_D(P)$	Logarithm of $H(P)$: $h_D(P) = \log H_D(P)$.

Definition 3.2. Let $E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{O}_k$, be an elliptic curve. Let L be a number field containing k, and let P, Q be distinct elements of $E(L)$. Let $P - Q = (x_0, y_0) \in E(L)$. Define

$$I_Q(P) = \prod_{\mathfrak{p} \subset \mathbb{O}_L} \mathfrak{p}^{\max\{-\frac{1}{2}\,\mathrm{ord}_{\mathfrak{p}}\, x_0, 0\}},$$

where $\mathfrak{p}$ runs over all (finite) primes of $\mathbb{O}_L$ (this is well-defined, independent of L, if we identify ideals $\mathfrak{a} \subset \mathbb{O}_L$ and $\mathfrak{a}\mathbb{O}_{L'}$, when $L \subset L'$). If $D = \sum_{i=1}^n Q_i$, $Q_i \in E(\bar{k})$, is a nontrivial effective divisor on E, then for $P \notin \mathrm{Supp}(D)$, we define

$$I_D(P) = \prod_{i=1}^n I_{Q_i}(P).$$

Definition 3.3. Let $P \in E(\ell)$, $P \notin \mathrm{Supp}(D)$. We define the height of P with respect to degree-one primes of ℓ/k by

$$h_{D,\deg_1(\ell/k)}(P) = \sum_{v \in M_k} \sum_{\substack{w \in M_\ell \\ w|v \\ f_{w/v}=1}} h_{D,w}(P),$$

where $h_{D,w}$ denotes a local Weil height with respect to D and w and $f_{w/v}$ is the inertia degree of w over v. Similarly, define

$$h_{D,\deg_{>1}(\ell/k)}(P) = \sum_{v \in M_k} \sum_{\substack{w \in M_\ell \\ w|v \\ f_{w/v}>1}} h_{D,w}(P).$$

Note that, as in the previous section, we have

$$h_{D,\deg_1(\ell/k)}(P) + h_{D,\deg_{>1}(\ell/k)}(P) = h_D(P) + O(1).$$

For $P \in E(\ell)$ and D a divisor on E defined over ℓ, the norm $N(I_D(P))$ is essentially just the nonarchimedean part of the (relative) height $H_{D,\ell}(P) = H_D(P)^{[\ell:\mathbb{Q}]}$ and $\log N(J_D(P)) = [\ell : \mathbb{Q}]\, h_{D,\deg_{>1}(\ell/k)}(P)$ (up to $O(1)$). We will assume the local heights are chosen so that this last statement is an equality.

We can now state the following theorem, which in the simplest case where ℓ/k is Galois, says, roughly, that the height of P with respect to D is "mostly" supported on the degree one primes of ℓ/k, unless the ideal $I_D(P)$ is coming from a proper subfield of ℓ. Note that the fields ℓ and k here play the roles of k and $\mathbb{Q}$, respectively, from the analogous Theorem 2.1.

Theorem 3.4. *Let $\epsilon > 0$. Assume that Conjecture 3.1 holds. Then, for every $P \in E(\ell)$, either*

(a) $$\frac{1}{[\ell : \mathbb{Q}]} \log N(J_D(P)) = h_{D,\deg_{>1}(\ell/k)}(P) < \epsilon h_D(P),$$

or

(b) $$I_{D_i}(P)\mathbb{O}_{L,S} = \mathfrak{a}\mathbb{O}_{L,S}$$

for some i and some ideal $\mathfrak{a} \subset \mathbb{O}_{k'}$, where k' is a proper subfield of L not containing ℓ (in particular, if ℓ/k is Galois, $\mathfrak{a}$ is contained in a proper subfield of ℓ).

The set of points in $E(\ell)$ not satisfying (a) *is contained in a finite union of cosets in $E(\ell)$ of the form*

$$T = \textstyle\bigcup_{i=1}^{m} P_i + E(\ell)^{\nu_i \sigma_i},$$

where $P_i \in E(\ell)$, $\sigma_i \in \mathrm{Gal}(L/k) \setminus \mathrm{Gal}(L/\ell)$, and $\nu_i \in \mathrm{Aut}(E)$ for $i = 1, \ldots, m$.

Proof. Let D_{red} be the reduced divisor associated to D. Then, for some positive integer c, $D < cD_{\mathrm{red}}$ and we have $h_D < ch_{D_{\mathrm{red}}} + O(1)$ and $h_{D,\deg_{>1}(\ell/k)} < ch_{D_{\mathrm{red}},\deg_{>1}(\ell/k)} + O(1)$. So without loss of generality we may assume that D is a reduced divisor. Let

$$U = \{P \in E(\ell) \mid h_{D,\deg_{>1}(\ell/k)}(P) \geq \epsilon h_D(P)\}.$$

Let L be a Galois closure of ℓ/k. Let $w' \in M_L$ lie above $w \in M_\ell$ and $v \in M_k$. As in the proof of Theorem 2.1, if $f_{w/v} > 1$, then there exists $\sigma \in \mathrm{Gal}(L/k) \setminus \mathrm{Gal}(L/\ell)$ such that $\sigma(w') = w'$. Let $\mathrm{Gal}(L/k) \setminus \mathrm{Gal}(L/\ell) = \{\sigma_1, \ldots, \sigma_m\}$. For $i = 1, \ldots, m$, let

$$h^{(i)}_{D,\deg_{>1}(L/k)}(P) = \sum_{v \in M_k} \sum_{\substack{w \in M_L \\ w|v,\ f_{w/v}>1 \\ \sigma_i(w)=w}} h_{D,w}(P).$$

Then

$$h_{D,\deg_{>1}(\ell/k)}(P) \leq \sum_{i=1}^{m} h^{(i)}_{D,\deg_{>1}(L/k)}(P).$$

Let

$$U_i = \left\{ P \in U \;\middle|\; h^{(i)}_{D,\deg_{>1}(L/k)}(P) \geq \frac{\epsilon}{m} h_D(P) \right\}.$$

Then $U \subset \bigcup_{i=1}^{m} U_i$. Let $r \in \{1, \ldots, m\}$. If $w \in M_L$ and $\sigma_r(w) = w$, then $h_{D,w}(P) = h_{\sigma_r(D),w}(\sigma_r(P))$ and so

$$\min\{ h_{D,w}(P), h_{\sigma_r(D),w}(\sigma_r(P))\} = h_{D,w}(P).$$

Let $\pi : X \to E \times E$ be the morphism obtained by blowing up the points in

$$D \times \sigma_r(D) \subset E \times E$$

and let Y be the exceptional divisor of π. By well-known properties of heights, for $(P, Q) \notin D \times \sigma_r(D)$ and $w \in M_L$, we can choose

$$h_{Y,w}(\pi^{-1}(P, Q)) = \min\{ h_{D,w}(P), h_{\sigma_r(D),w}(Q)\}.$$

Let $V_r = \{(P, \sigma_r(P)) \mid P \in U_r\}$. It follows that for $(P, \sigma_r(P)) \in V_r$, we have

$$\begin{aligned} h_Y(\pi^{-1}(P, \sigma_r(P))) &\geq h^{(r)}_{D,\deg_{>1}(L/k)}(P) \geq \frac{\epsilon}{m} h_D(P) \\ &> \frac{\epsilon}{2m}(h(P) + h(\sigma_r(P)) + O(1). \end{aligned}$$

Then by Conjecture 3.1 V_r is contained in a proper Zariski closed subset of $E \times E$. If V_r is a finite set, then U_r is contained in a set T as in the theorem. Otherwise, let C be a positive-dimensional component of the Zariski closure of V_r. Then C is a curve with infinitely many rational points on it. By Faltings' theorem, C is a translate of a one-dimensional abelian subvariety E' of $E \times E$.

Any irreducible one-dimensional abelian subvariety of $E \times E$ must be an elliptic curve isogenous to E, via projection onto E. Since E' is clearly not a fiber of either of the two projection maps, there are two isogenies $\phi, \psi : E' \to E$ induced by the two projection maps, with dual isogenies $\hat{\phi}$ and $\hat{\psi}$ from E to E'. If $R = (P, Q) \in E' \subset E \times E$, then $\hat{\phi}\phi(R) = \hat{\phi}(P) = (\deg \hat{\phi})R$ and similarly $\hat{\psi}(Q) = (\deg \hat{\psi})R$.

Thus, E' is contained in the set $\{(P, Q) \in E \times E \mid (\deg \hat{\psi})\hat{\phi}(P) = (\deg \hat{\phi})\hat{\psi}(Q)\}$. Composing with an isogeny to E we find that there are nonzero endomorphisms f and g of E such that $E' \subset \{(P, Q) \in E \times E \mid f(P) = g(Q)\}$. Note that if $(P_0, \sigma_r(P_0)), (P, \sigma_r(P)) \in V_r \cap C$ then $(P - P_0, \sigma_r(P - P_0)) \in E'$. It follows that there are points of the form $(P, \sigma_r(P)) \in E'$ with $P \in E(\ell)$ such that $f(P) = g(\sigma_r(P))$.

Let $K = \mathrm{End}_L(E) \otimes \mathbb{Q}$, where $\mathrm{End}_L(E)$ is the endomorphism ring of E over L. Then σ_r is an element of a finite group acting on the finite-dimensional K-vector space $V = E(L) \otimes_{\mathrm{End}_L(E)} K$. Thus, the eigenvalues of the action of σ_r must be roots of unity. But from the above, f/g is an eigenvalue of σ_r. So we deduce that $f/g \in K$ is a root of unity. Since K is contained in a quadratic extension of $\mathbb{Q}$, this means that $f/g \in \{\pm 1, \pm i, \pm\gamma, \pm\gamma^2\}$, where γ denotes a primitive sixth root of unity. Write $g = \nu f$. Composing both sides with the dual endomorphism to f, we may assume that $f = m$, where m is a positive integer. Then, for $(P, \sigma_r(P)), (P_0, \sigma_r(P_0)) \in V_r \cap C$, we have $m(P - P_0) = \nu\sigma_r(m(P - P_0))$. This implies that U_r is contained in finitely many cosets of the form $P_i + E(\ell)^{\nu_i \sigma_r}$ in $E(\ell)$, where $P_i \in E(\ell)$ and $\nu_i \in \mathrm{Aut}(E)$. So the set of points in $E(\ell)$ not satisfying (a) is contained in a set T as in the theorem.

We now show that the set of points in the set T not satisfying condition (a) satisfies condition (b). Let $D_1, \ldots, D_N$ be the irreducible components of D over L. Consider a coset in $E(\ell)$ of the form $P_r + E(\ell)^{\nu_r \sigma_r}$, where $P_r \in E(\ell)$, $\nu_r \in \mathrm{Aut}(E)$, and $\sigma_r \in \mathrm{Gal}(L/k) \setminus \mathrm{Gal}(L/\ell)$. From the first part of the proof, we need only consider cosets such that for some i, some $\epsilon > 0$, and infinitely many elements $P \in E(\ell)^{\nu_r \sigma_r}$, we have

$$\sum_{w \in M_L} \min\{h_{D_i, w}(P + P_r), h_{\sigma_r(D_i), w}(\sigma_r(P + P_r))\} > \epsilon h(P).$$

Let $\phi : E \to E$ be the morphism $\phi(P) = \nu_r^{-1} P + \sigma_r(P_r)$. Since $\sigma_r(P + P_r) = \nu_r^{-1} P + \sigma_r(P_r)$ for $P \in E(\ell)^{\nu_r \sigma_r}$, we have (up to $O(1)$)

$$h_{\sigma_r(D_i), w}(\sigma_r(P + P_r)) = h_{\sigma_r(D_i), w}(\phi(P)) = h_{\phi^* \sigma_r(D_i), w}(P).$$

Let τ be translation by P_r. So $h_{D_i, w}(P + P_r) = h_{\tau^* D_i, w}(P) + O(1)$. So for infinitely many $P \in E(\ell)$,

$$\sum_{w \in M_L} \min\{h_{\tau^* D_i, w}(P), h_{\phi^* \sigma_r(D_i), w}(P)\} > \epsilon h(P). \tag{5}$$

If $\tau^* D_i$ and $\phi^* \sigma_r(D_i)$ have empty intersection, then as is well known,

$$\sum_{w \in M_L} \min\{h_{\tau^* D_i, w}(P), h_{\phi^* \sigma_r(D_i), w}(P)\}$$

is bounded independent of P, contradicting (5). So $\tau^* D_i \cap \phi^* \sigma_r(D_i) \neq \varnothing$. Since D_i is irreducible over L, this implies that $\tau^* D_i = \phi^* \sigma_r(D_i)$.

It follows from the definition that for any translation τ_0 and any automorphism $\nu \in \mathrm{Aut}(E)$, $I_D(\tau_0(P)) = I_{\tau_0^* D}(P)$ and $I_D(\nu P) = I_{\nu^* D}(P)$. This implies that for all $P \in E(\ell)^{\nu_r \sigma_r}$,

$$\begin{aligned}\sigma_r(I_{D_i}(P + P_r)) &= I_{\sigma_r(D_i)}(\sigma_r(P) + \sigma_r(P_r)) = I_{\sigma_r(D_i)}(\phi(P)) = I_{\phi^* \sigma_r(D_i)}(P) \\ &= I_{\tau^* D_i}(P) \\ &= I_{D_i}(P + P_r).\end{aligned}$$

So σ_r fixes the ideal $I_{D_i}(P_r + P)$, $P_r + P \in P_r + E(\ell)^{\nu_r \sigma_r}$, which implies that $I_{D_i}(P + P_r)\mathbb{O}_{L,S} = \mathfrak{a}\mathbb{O}_{L,S}$ for some ideal $\mathfrak{a}$ of $\mathbb{O}_{k'}$, where k' is the fixed field of σ_r. □

If we restrict to cyclic subgroups of $E(\ell)$, we obtain the following simpler version of Theorem 3.4.

Corollary 3.5. *Let $P \in E(\ell)$ and $\epsilon > 0$. If Conjecture 3.1 holds, then either*

$$h_{D,\deg_{>1}(\ell/k)}(nP) < \epsilon h_D(nP)$$

for all but finitely many integers n, or there exists a proper subfield $k' \subsetneq \ell$ of ℓ, a positive integer m, an elliptic curve E'/k', and an isomorphism $\phi : E \to E'$ over ℓ such that $\phi(mP)$ is a k'-rational point on E'.

Proof. Suppose that for infinitely many n, $h_{D,\deg_{>1}(\ell/k)}(nP) < \epsilon h_D(nP)$. It follows from Theorem 3.4 that for some $m > 0$, $\sigma \in \mathrm{Gal}(L/k) \setminus \mathrm{Gal}(L/\ell)$, and $\nu \in \mathrm{Aut}(E)$, we have $mP \in E(\ell)^{\nu^{-1}\sigma}$, or $\sigma(mP) = \nu mP$. From this it follows that mP is a point on a twist of E, defined over $k' \cap \ell$, where k' is the fixed field of σ. □

At the time of writing, Conjecture 3.1 is known only in the following special case. See [McKinnon 2003] for a proof, and [Silverman 2005] for a discussion of the implications of Vojta's conjecture in this context.

Theorem 3.6 [McKinnon 2003]. *Let E be an elliptic curve over a number field ℓ. Let $R = \mathrm{End}_\ell(E)$. Let M be a cyclic R-submodule of $E(\ell)$. Then Conjecture 3.1 holds for $(P, Q) \in M \times M \subset (E \times E)(\ell)$; that is, in the notation of Conjecture 3.1, there exists a proper Zariski closed subset $Z(\epsilon)$ of X such that for every $(P, Q) \in M \times M - \pi(Z(\epsilon))$, we have*

$$h_Y(\pi^{-1}(P, Q)) \leq \epsilon(h(P) + h(Q)) + O(1),$$

where h_Y is a logarithmic height function associated to the exceptional divisor on the blowup X of $E \times E$ at a finite set of points and h is any fixed ample logarithmic height on E.

Theorem 3.7. *Let E be an elliptic curve over a number field k with complex multiplication. Let ℓ be the compositum of k with the imaginary quadratic field* $\mathrm{End}_{\bar{k}}(E) \otimes \mathbb{Q}$. *Let D be a nontrivial effective divisor on E defined over ℓ. Let $P \in E(\ell)$ and $\epsilon > 0$. Then either*

$$h_{D,\deg_{>1}(\ell/k)}(nP) < \epsilon h_D(nP)$$

for all but finitely many $n > 0$, or there exists a positive integer m, an elliptic curve E'/k, and an isomorphism $\phi : E \to E'$ over ℓ such that $\phi(mP)$ is a k-rational point on E'.

Proof. If $\ell = k$ then the theorem is vacuous. So suppose that ℓ is a quadratic extension of k. Let $R = \mathrm{End}_{\bar{k}}(E)$. First, we note that $R[E(k)]$ has finite index in $E(\ell)$. Indeed, as is well-known [Silverman 1992, Exercise X-10.16], we have $\mathrm{rk}\, E(\ell) = \mathrm{rk}\, E(k) + \mathrm{rk}\, E'(k)$, where E' is a quadratic twist of E over ℓ. If $\ell = k(\sqrt{N})$, $N \in \mathbb{Z}$, then any element $n\sqrt{N} \in R$, with n a positive integer, induces an isogeny (over k) between E and a quadratic twist E' of E over ℓ. Thus, $\mathrm{rk}\, E(k) = \mathrm{rk}\, E'(k)$ and we have $\mathrm{rk}\, E(\ell) = 2\,\mathrm{rk}\, E(k) = \mathrm{rk}\, R[E(k)]$.

Next, we claim that Theorem 3.6 actually holds under the slightly weaker assumption that M contains a cyclic R-submodule M' of finite index m. Indeed, one easily reduces to considering the case where X is the blow-up of $E \times E$ at the origin $(\mathbb{O}, \mathbb{O})$ and Y is the exceptional divisor. The claim then follows by applying Theorem 3.6 to M' and from the facts

$$h_Y(\pi^{-1}(P, Q)) \le h_Y(\pi^{-1}(mP, mQ)) + O(1),$$

$(P, Q) \neq (\mathbb{O}, \mathbb{O})$, and $h(mP) = m^2 h(P) + O(1)$.

Let m be the index of $R[E(k)]$ in $E(\ell)$. Let $P \in E(\ell)$. Then we have $mP = \phi(Q)$, for some $Q \in E(k)$ and some $\phi \in R$. Let σ be the unique nonidentity element of $\mathrm{Gal}(\ell/k)$. Then $m\sigma(P) = \sigma(mP) = \sigma(\phi(Q)) = (\sigma\phi)(Q)$, so mP and $m\sigma(P)$ both belong to the cyclic R-submodule RQ of $E(\ell)$ generated by Q. So RQ has finite index in the subgroup of $E(\ell)$ generated by RQ, P, and $\sigma(P)$. Then by our earlier claim, Conjecture 3.1 holds for the points $(nP, n\sigma(P)) \in (E \times E)(\ell)$, $n \in \mathbb{Z}$. But now the same proof as in Theorem 3.4 and Corollary 3.5 works, completing the proof. □

References

[Corvaja and Zannier 2005] P. Corvaja and U. Zannier, "A lower bound for the height of a rational function at S-unit points", *Monatsh. Math.* **144**:3 (2005), 203–224. MR 2005k:11140 Zbl 1086.11035

[McKinnon 2003] D. McKinnon, "Vojta's main conjecture for blowup surfaces", *Proc. Amer. Math. Soc.* **131**:1 (2003), 1–12. MR 2003g:11071 Zbl 1022.11027

[Silverman 1992] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1992. MR 95m:11054

[Silverman 2005] J. H. Silverman, "Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups", *Monatsh. Math.* **145**:4 (2005), 333–350. MR 2006e:11087 Zbl 1197.11070

[Vojta 1987] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics **1239**, Springer, Berlin, 1987. MR 91k:11049 Zbl 0609.14011

[Vojta 2011] P. Vojta, "Diophantine approximation and Nevanlinna theory", pp. 111–224 in *Arithmetic geometry* (Cetraro, 2007), edited by P. Corvaja and C. Gasbarri, Lecture Notes in Mathematics **2009**, Springer, Berlin, 2011. MR 2012i:11076 Zbl 05882118

Communicated by Bjorn Poonen
Received 2011-06-02 Revised 2011-10-18 Accepted 2011-12-10

adlevin@math.msu.edu *Department of Mathematics, Michigan State University, East Lansing, MI 48824, United States*

dmckinnon@math.uwaterloo.ca *Department of Pure Mathematics, University of Waterloo, Waterloo, ON, N2T 2M2, Canada*

msp

ALGEBRA AND NUMBER THEORY 6:6 (2012)
dx.doi.org/10.2140/ant.2012.6.1239

Torsion des modules de Drinfeld de rang 2 et formes modulaires de Drinfeld

Cécile Armana

On donne des résultats de non-existence pour les points rationnels de la courbe modulaire de Drinfeld affine $Y_1(\mathfrak{p})$ avec $\mathfrak{p}$ idéal premier de $\mathbb{F}_q[T]$. Cette courbe classifie les modules de Drinfeld de rang 2 munis d'un point de torsion d'ordre $\mathfrak{p}$. Le premier énoncé concerne les points définis sur les extensions de $\mathbb{F}_q(T)$ quadratiques pour $\mathfrak{p}$ de degré 3 et cubiques pour $\mathfrak{p}$ de degré 4 et $q \geq 7$. Le deuxième, conditionné à une dualité entre algèbre de Hecke et formes modulaires de Drinfeld, concerne les points sur les extensions de degré $\leq q$ pour $\deg \mathfrak{p}$ suffisamment grand. Comme conséquence, on déduit, sous la même condition, une borne uniforme pour la torsion des modules de Drinfeld de rang 2 définis sur les extensions de $\mathbb{F}_q(T)$ de degré $\leq q$, prédite par Poonen.

We give nonexistence results for rational points on the affine Drinfeld modular curve $Y_1(\mathfrak{p})$ with $\mathfrak{p}$ a prime ideal of $\mathbb{F}_q[T]$. This curve classifies Drinfeld modules of rank 2 with a torsion point of order $\mathfrak{p}$. The first statement concerns points defined over quadratic extensions of $\mathbb{F}_q(T)$ for $\mathfrak{p}$ of degree 3 and cubic extensions of $\mathbb{F}_q(T)$ for $\mathfrak{p}$ of degree 4 and $q \geq 7$. The second statement is valid under a duality condition between Hecke algebra and Drinfeld modular forms, and concerns points over extensions of degree $\leq q$ whenever $\deg \mathfrak{p}$ is sufficiently large. As a consequence we derive, under the same condition, a uniform bound for the torsion of rank-2 Drinfeld modules defined over extensions of $\mathbb{F}_q(T)$ of degree $\leq q$, as predicted by Poonen.

1. Introduction

L'objet de ce travail est d'exclure certaines structures de torsion sur les modules de Drinfeld de rang 2. Soit $\mathbb{F}_q$ un corps fini à q éléments, A l'anneau $\mathbb{F}_q[T]$ et K le corps des fractions rationnelles $\mathbb{F}_q(T)$ en l'indéterminée T. Considérons les couples donnés par un A-module de Drinfeld de rang 2 avec un point de torsion d'ordre $\mathfrak{n}$, pour $\mathfrak{n}$ idéal non nul de A (on renvoie aux rappels de la section 3). La courbe modulaire de Drinfeld $Y_1(\mathfrak{n})$ est une courbe algébrique affine sur K ainsi

MSC2010 : primary 11G09; secondary 11F52, 11G18, 14G05.
Mots-clefs : torsion of Drinfeld modules, Drinfeld modular forms, Drinfeld modular curves.

qu'un schéma de modules pour ces objets. En règle générale, on ne s'attend pas à ce qu'elle ait de points rationnels.

Conjecture 1.1 [Poonen 1997]. *Fixons q puissance d'un nombre premier et d un entier ≥ 1. Il existe une constante $C > 0$ telle que, si $\mathfrak{n}$ est de degré $\geq C$ et si L est une extension de K de degré $\leq d$, la courbe $Y_1(\mathfrak{n})$ n'a pas de point L-rationnel. Autrement dit, il existe une constante $C' > 0$ telle que, si L/K est de degré $\leq d$, tout A-module de Drinfeld de rang 2 sur L ait au plus C' points de torsion dans L.*

Les constantes C et C' dépendent de q et d. Il s'agit de la conjecture 2 de [Poonen 1997] dans le cas des $\mathbb{F}_q[T]$-modules de Drinfeld de rang 2 (une version plus faible avait été proposée auparavant par Denis [1995, problème 3]). À la lumière des fortes analogies entre courbes elliptiques et modules de Drinfeld de rang 2, cette conjecture s'apparente au théorème de borne uniforme pour la torsion des courbes elliptiques sur les corps de nombres de Merel [1996], après des travaux de Mazur [1977] notamment. Si on s'intéresse uniquement aux points K-rationnels, Schweizer a prédit un résultat plus précis :

Conjecture 1.2 (conséquence de [Schweizer 2003, conjecture 1]). *Si $\mathfrak{p}$ est un idéal premier de A de degré ≥ 3, la courbe $Y_1(\mathfrak{p})$ n'a pas de point K-rationnel.*

À l'heure actuelle, les résultats connus en direction de ces conjectures sont partiels et assez peu nombreux. Les plus avancés sont dus à Schweizer et Pál.

Théorème 1.3. *La courbe $Y_1(\mathfrak{n})$ n'a pas de point $\mathbb{F}_q(T)$-rationnel pour les idéaux $\mathfrak{n}$ suivants de $\mathbb{F}_q[T]$:*

(i) *$\mathfrak{n}$ idéal premier de degré ≥ 3 de $\mathbb{F}_2[T]$. En particulier la conjecture 1.1 est vérifiée pour $L = K = \mathbb{F}_2(T)$ (i.e., $q = 2$, $d = 1$)* [Pál 2010, théorèmes 1.2 et 1.4].

(ii) *$\mathfrak{n} \in \{(T^2+T+1)^2, T(T^2+T+1), T^3, (T^2(T+1)\}$ dans $\mathbb{F}_2[T]$* [Pál 2010, théorème 10.8; Schweizer 2003, lemme 1.3].

(iii) *$\mathfrak{n} \in \{T(T-1)(T+1), T^2(T-1)\}$ dans $\mathbb{F}_3[T]$* [Schweizer 2011, page 297].

(iv) *$\mathfrak{n}$ produit de trois facteurs linéaires distincts dans $\mathbb{F}_4[T]$* [Schweizer 2011, proposition 3.2].

Pour les idéaux de cet énoncé, hormis $(T^2+T+1)^2 \in \mathbb{F}_2[T]$, le résultat est en fait établi pour la courbe modulaire de Drinfeld $Y_0(\mathfrak{n})$ qui paramètre les modules de Drinfeld de rang 2 munis d'une isogénie cyclique d'ordre $\mathfrak{n}$.

En ce qui concerne la conjecture 1.1, Poonen [1997, théorème 6] et Schweizer [2003, théorème 2.4] ont aussi obtenu une borne uniforme sur la composante $\mathfrak{p}$-primaire de la torsion, à rapprocher des énoncés de Manin [1969] et de Kamienny et Mazur [1995] pour les courbes elliptiques. Mentionnons enfin une preuve de

Nguyen et Yamada de la conjecture 1.1 en 2001 qui s'est avérée fausse (voir [Schweizer 2003] pour les détails).

Dans ce travail, on détermine les points rationnels de $Y_1(\mathfrak{p})$ pour certains premiers $\mathfrak{p}$ en suivant l'approche de Mazur et Merel pour les courbes modulaires classiques. Dans le cas des corps de fonctions, il s'avère que la propriété d'immersion formelle requise par Mazur [1978] est loin d'être évidente. L'objet principal de cet article, issu de la thèse [Armana 2008] débutée en 2003, est d'expliciter cette difficulté, ce qui n'avait pas été fait dans la littérature, et de détailler les liens entre immersion formelle, formes modulaires de Drinfeld et symboles modulaires. Ainsi ce travail s'appuie en partie sur [Armana 2011b]. Précisons que l'approche de Mazur a aussi été employée par Pál [2010] : la différence réside dans le choix d'une place auxiliaire de réduction ($\infty = (1/T)$ pour Pál, place $\mathfrak{l}$ distincte de ∞ ici).

D'autres outils nécessaires à la mise en place de la méthode de Mazur sur les corps de fonctions sont développés dans ce travail. Un premier est le quotient d'enroulement de la jacobienne $J_0(\mathfrak{p})$ de la courbe modulaire de Drinfeld compactifiée $X_0(\mathfrak{p})$. C'est le plus grand quotient de $J_0(\mathfrak{p})$ de rang analytique nul et il fait l'objet de la section 4. Pour établir les théorèmes principaux, on utilisera aussi une borne effective sur le degré de la torsion des modules de Drinfeld de rang 2 à bonne réduction potentielle (proposition 5.2).

Lorsque $\mathfrak{p}$ est premier de petit degré, la situation se trouve simplifiée. Le quotient d'enroulement est alors essentiellement la jacobienne $J_0(\mathfrak{p})$ ou son quotient sur lequel l'involution d'Atkin–Lehner opère comme -1, d'après la connaissance du degré de la fonction L de $J_0(\mathfrak{p})$. L'immersion formelle pour les puissances symétriques de $X_0(\mathfrak{p})$ provient alors d'un argument de point de Weierstrass ou de gonalité (section 7D1). Cela fournit l'énoncé suivant, résultat non trivial en direction de la conjecture 1.2. Comparé au théorème 1.3, il a l'avantage d'être sans condition forte sur le cardinal q du corps fini de base et d'autoriser des extensions de K de degré > 1.

Théorème 1.4. *Soit* $\mathfrak{p}$ *un idéal premier.*

(i) *Si* $\mathfrak{p}$ *est de degré* 3, *la courbe* $Y_1(\mathfrak{p})$ *n'a pas de point* L*-rationnel pour toute extension* L/K *de degré* ≤ 2.

(ii) *Supposons* $\mathfrak{p}$ *de degré* 4 *et* $d = 1$ *si* q *quelconque*, $d = 2$ *si* $q = 5$, $d = 3$ *si* $q \geq 7$. *Alors la courbe* $Y_1(\mathfrak{p})$ *n'a pas de point* L*-rationnel pour toute extension* L/K *de degré* $\leq d$.

En d'autres termes, pour de tels q, $\mathfrak{p}$ *et* L, *il n'existe pas de* A*-module de Drinfeld de rang* 2 *sur* L *ayant un point de torsion dans* L *d'ordre* $\mathfrak{p}$.

Il se déduit du théorème 7.5, plus général, qui concerne les niveaux $\mathfrak{p}$ tels que toute forme primitive associée est de rang analytique ≤ 1. Considérons l'espace

$\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$ des cochaînes harmoniques paraboliques pour $\Gamma_0(\mathfrak{p}) \subset \mathrm{GL}_2(A)$ à valeurs complexes. D'après Drinfeld, elles s'identifient naturellement à des formes automorphes paraboliques pour GL_2 sur les adèles de K. L'algèbre de Hecke $\mathbb{T}$ est la sous $\mathbb{Z}$-algèbre commutative de $\mathrm{End}(\mathrm{H}_{\mathfrak{p}}(\mathbb{C}))$ engendrée par les opérateurs de Hecke. Le théorème 7.5(ii) est alors valable pour les premiers $\mathfrak{p}$ tels que la fonction L de toute forme primitive de $\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$ pour Hecke s'annule à l'ordre ≤ 1 au centre de symétrie (on dira que $\mathfrak{p}$ satisfait la condition $\mathscr{C}$). Signalons aussi le théorème 7.8 qui donne $Y_0(\mathfrak{p})(K) = \varnothing$ pour $q \geq 5$ et $\mathfrak{p}$ de degré ≥ 5 vérifiant $\mathscr{C}$. La condition $\mathscr{C}$ présente l'avantage d'être testable sur machine, par exemple à l'aide des symboles modulaires pour $\mathbb{F}_q(T)$ [Teitelbaum 1992]. On l'a ainsi vérifiée pour tous les premiers de degré 5 dans $\mathbb{F}_2[T]$ (déjà couverts par le théorème 1.3(i)) et, par exemple, pour les premiers suivants de $\mathbb{F}_3[T]$: $(T^5 + T^3 - T^2 - T + 1)$, $(T^5 + T^4 + T^3 - T^2 + T - 1)$, $(T^5 - T^4 - T^2 - 1)$. L'ensemble $Y_1(\mathfrak{p})(K)$ est donc vide pour de tels $\mathfrak{p}$.

Cette condition $\mathscr{C}$ n'est certainement pas vérifiée par tout idéal premier $\mathfrak{p}$. En effet, d'après Ulmer [2002] il existe des courbes elliptiques non-isotriviales sur $\mathbb{F}_q(T)$, pour q premier, de rang arithmétique arbitrairement grand. Par le théorème de modularité pour les courbes elliptiques sur K (corollaire des travaux de Grothendieck, Deligne, Jacquet–Langlands et Drinfeld, voir [Gekeler et Reversat 1996]) et en supposant la conjecture de Birch et Swinnerton-Dyer pour ces courbes, on voit que la condition $\mathscr{C}$ n'est pas satisfaite pour tout $\mathfrak{p}$. Cependant, on s'attend à ce qu'elle le soit assez fréquemment car une philosophie courante prédit que les courbes elliptiques de rangs élevés (≥ 2) sont rares. Heath-Brown, Young et récemment Bhargava et Shankar ont obtenu des résultats en ce sens pour les courbes elliptiques sur $\mathbb{Q}$. De façon générale, déterminer la densité d'idéaux $\mathfrak{p}$ vérifiant $\mathscr{C}$ semble être un problème délicat.

Le deuxième énoncé relie l'existence de points rationnels sur $Y_1(\mathfrak{p})$ aux formes modulaires de Drinfeld, en exploitant la méthode de Mazur dans le cas général. Commençons par des notations. Soit $\mathrm{S}_{\mathfrak{p}}$ le $A[1/\mathfrak{p}]$-module des différentielles relatives globales de degré 1 de $X_0(\mathfrak{p})$ sur $A[1/\mathfrak{p}]$. Ce sont des formes modulaires de Drinfeld algébriques doublement paraboliques de poids 2 pour $\Gamma_0(\mathfrak{p})$. Pour $\mathfrak{l}$ un idéal premier non nul de A et distinct de $\mathfrak{p}$, notons $\mathbb{F}_{\mathfrak{l}}$ le corps fini $A/\mathfrak{l}$ et $\mathrm{S}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{l}}) = \mathrm{S}_{\mathfrak{p}} \otimes_{A[1/\mathfrak{p}]} \mathbb{F}_{\mathfrak{l}}$. L'algèbre $\mathbb{T}$ agit sur $\mathrm{S}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{l}})$ *via* son quotient $\mathbb{T}/p\mathbb{T}$ où p désigne la caractéristique de $\mathbb{F}_q$. De plus, tout élément f de $\mathrm{S}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{l}})$ possède un développement de la forme $\sum_{i\geq 1} b_i(f)t^{1+i(q-1)} \in \mathbb{F}_{\mathfrak{l}}[\![t]\!]$ en la pointe infinie de $X_0(\mathfrak{p})$ (voir section 6).

Dans [Armana 2011b], on a défini un symbole modulaire parabolique $\mathbf{e}$ relativement à $\Gamma_0(\mathfrak{p})$ au sens de Teitelbaum [1992]. C'est l'analogue de l'élément d'enroulement de Mazur [1977]. L'algèbre de Hecke $\mathbb{T}$ agit aussi sur les symboles modulaires pour $\mathbb{F}_q(T)$. Soient $I_{\mathbf{e}}$ et $\tilde{I}_{\mathbf{e}}$ les idéaux annulateurs dans $\mathbb{T}$ de $\mathbf{e}$ et

(**e** mod p) respectivement (sections 4A et 4D). On note $S_{\mathfrak{p}}(\mathbb{F}_\mathfrak{l})[\tilde{I}_{\mathbf{e}}]$ le sous-espace de $S_{\mathfrak{p}}(\mathbb{F}_\mathfrak{l})$ annulé par $\tilde{I}_{\mathbf{e}}$.

Théorème 1.5. *Soit* $\mathfrak{p}$ *premier de degré* ≥ 3. *Supposons qu'il existe* :
- *Un idéal saturé* I *de* $\mathbb{T}$, *d'annulateur noté* $\hat{I}$, *vérifiant* $I_{\mathbf{e}} \subset I \subset \tilde{I}_{\mathbf{e}}$ *et* $\hat{I} + \tilde{I}_{\mathbf{e}} = \mathbb{T}$.
- *Un idéal* $\mathfrak{l}$ *de* A *de degré* 1 *tel que l'application* $\mathbb{F}_\mathfrak{l}$*-linéaire*

$$\Phi_\mathfrak{l} : (\mathbb{T}/\tilde{I}_{\mathbf{e}}) \otimes_{\mathbb{Z}} \mathbb{F}_\mathfrak{l} \longrightarrow \mathrm{Hom}(S_{\mathfrak{p}}(\mathbb{F}_\mathfrak{l})[\tilde{I}_{\mathbf{e}}], \mathbb{F}_\mathfrak{l}),$$

qui envoie la classe de $u \in \mathbb{T}$ *sur la forme linéaire* $f \mapsto b_1(uf)$, *est un isomorphisme.*

Alors

(i) *si* $\deg \mathfrak{p} \geq \max(q+1, 5)$, *la courbe* $Y_1(\mathfrak{p})$ *n'a de point* L*-rationnel pour toute extension* L/K *de degré* $\leq q$;

(ii) *si* $\deg \mathfrak{p} \geq 3$, *la courbe* $Y_1(\mathfrak{p})$ *n'a pas de point* K*-rationnel.*

L'hypothèse sur l'existence de l'idéal I est vraisemblablement de nature technique. Elle évite un problème lié au passage de suites exactes de variétés abéliennes sur K aux espaces cotangents de leur modèles de Néron. De fait, elle permet la construction d'un raffinement du quotient d'enroulement possédant de bonnes propriétés (sections 4D et 7E2). On démontre que $I_{\mathbf{e}}$ vérifie cette hypothèse pour tout $\mathfrak{p}$ de degré 3, ou de degré 4 avec $p \neq 2$ (proposition 4.12). Un critère est aussi donné en section 4D2.

L'hypothèse sur $\Phi_\mathfrak{l}$ est certainement plus profonde. Elle permet de traduire l'immersion formelle (critère de Kamienny) en une indépendance linéaire de symboles modulaires sur les corps de fonctions, qui a fait l'objet d'un travail précédent [Armana 2011b]. Si on supprime l'idéal $\tilde{I}_{\mathbf{e}}$ de sa formulation, l'hypothèse s'apparente à un accouplement entre formes modulaires de Drinfeld et algèbre de Hecke, qui entraînerait un énoncé de multiplicité un dans $S_{\mathfrak{p}}(\mathbb{F}_\mathfrak{l})$. Depuis [Goss 1980a], on sait que des formes modulaires de Drinfeld pour $\mathrm{GL}_2(A)$ de poids distincts peuvent avoir les mêmes valeurs propres de Hecke en caractéristique générique. Cependant, le problème de multiplicité un, dans $S_{\mathfrak{p}}$ ou $S_{\mathfrak{p}}(\mathbb{F}_\mathfrak{l})$ à $\mathfrak{p}$ fixé, est semble-t-il ouvert à l'heure actuelle. Ici, on démontre notre hypothèse sur $\Phi_\mathfrak{l}$, a priori plus faible, ainsi que la multiplicité un, dans le cas où $\mathfrak{p}$ est de degré 3 avec $\mathfrak{l}$ quelconque (proposition 7.14). Le cas général requerrait une étude plus approfondie.

Quant à la condition sur le degré de l'extension L/K du théorème 1.5, elle provient de relations entre coefficients du développement des formes modulaires de Drinfeld et opérateurs de Hecke de degré 1 (théorème 6.15 et proposition 7.14).

À nouveau, le théorème 1.5 est sans hypothèse sur q, autorise des extensions non triviales de K et va dans le sens de la conjecture 1.2. Il contient même le résultat de Pál sur $Y_1(\mathfrak{p})$ (théorème 1.3(i)) si les hypothèses peuvent être levées.

Remarquons que, pour $\mathfrak{p}$ de degré 3, on retrouve $Y_1(\mathfrak{p})(K) = \varnothing$ de façon inconditionnelle (théorème 1.4(i)). Comme conséquence du théorème 1.5 et du travail de Schweizer [2003], on obtient une borne uniforme conditionnelle sur la torsion des modules de Drinfeld de rang 2.

Corollaire 1.6. *Fixons q. Supposons qu'il existe une constante $B_q > 0$ telle que pour tout premier $\mathfrak{p}$ de degré $\geq B_q$ on peut trouver des idéaux I de $\mathbb{T}$ et $\mathfrak{l}$ de A comme dans l'énoncé du théorème 1.5. Alors la conjecture 1.1 est vraie pour les A-modules de Drinfeld de rang 2 sur les extensions de K de degré $1 \leq d \leq q$.*

2. Notations

Soient q une puissance d'un nombre premier p, $\mathbb{F}_q$ (respectivement $\mathbb{F}_p$) un corps fini à q (respectivement p) éléments, $A = \mathbb{F}_q[T]$ l'anneau en l'indéterminée T et $K = \mathbb{F}_q(T)$ son corps des fractions. On note deg le degré usuel sur A avec la convention $\deg 0 = -\infty$. Le *degré d'un idéal* non nul de A est celui de l'un de ses générateurs. Pour P, Q dans A, on note (P) l'idéal engendré par P et $P \mid Q$ si P divise Q.

Les lettres gothiques désigneront des idéaux de A. En particulier, $\mathfrak{p}$ désignera un *premier* (c'est-à-dire un idéal premier non nul) de A. Le corps fini $A/\mathfrak{p}$ est noté $\mathbb{F}_\mathfrak{p}$. Pour un idéal $\mathfrak{n}$, le sous-groupe $\Gamma_0(\mathfrak{n})$ de $\mathrm{GL}_2(A)$ est formé des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ avec $c \in \mathfrak{n}$.

Pour un corps F, on désigne par F^{alg} une clôture algébrique et F^{sep} une clôture séparable. Le cardinal d'un ensemble fini S est noté $\#S$.

3. Rappels

3A. ***Courbes modulaires de Drinfeld.*** Soit L un A-corps c'est-à-dire un corps L muni d'un homomorphisme d'anneaux $\iota : A \to L$. Soit $L\{\tau\}$ l'anneau des polynômes tordus sur L avec multiplication donnée par $\tau l = l^q \tau$ $(l \in L)$. Fixons $r \geq 1$ entier. Un *A-module de Drinfeld* (on abrègera en module de Drinfeld) de rang r sur L est un homomorphisme d'anneaux

$$\phi : A \longrightarrow L\{\tau\}, \quad a \longmapsto \phi_a,$$

tel que le terme constant de ϕ_a est $\iota(a)$ et $\deg_\tau \phi_a = r \deg a$. Si ϕ est de rang 2, il est déterminé de façon unique par l'image de $T : \phi_T = \iota(T)\tau^0 + g\tau + \Delta\tau^2$ avec $g \in L$ et $\Delta \in L^\times$. En identifiant τ à l'automorphisme $x \mapsto x^q$ de L, on identifie $L\{\tau\}$ à l'anneau des polynômes (additifs) combinaisons linéaires de $\{x^{q^i}\}_{i \geq 0}$ à coefficients dans L, avec pour loi de multiplication la composition. En faisant agir un élément a de A sur $x \in L$ par $\phi_a(x)$, on obtient une nouvelle structure de A-module sur le corps L, notée ${}^\phi L$.

Soit $\mathfrak{a}$ un idéal de A. On fixe un générateur a de $\mathfrak{a}$. Les *points de* $\mathfrak{a}$*-torsion* de ϕ dans une extension F/L sont les éléments du A-module

$$\phi[\mathfrak{a}](F) = (\ker \phi_a)(F) \subset {}^{\phi}F$$

(il ne dépend pas du choix de a). Les points de torsion dans F forment le A-module $({}^{\phi}F)_{\text{tors}}$, le sous-module de torsion de ${}^{\phi}F$. L'*ordre* d'un élément de $({}^{\phi}F)_{\text{tors}}$ est son idéal annulateur dans A. On pose $\phi[\mathfrak{a}] = \phi[\mathfrak{a}](L^{\text{alg}})$. Si le noyau de ι ne contient pas $\mathfrak{a}$, le polynôme ϕ_a est alors séparable et le A-module $\phi[\mathfrak{a}]$ est en fait contenu dans $({}^{\phi}L^{\text{sep}})_{\text{tors}}$.

Un *homomorphisme* de modules de Drinfeld $u : \phi \to \psi$ sur L est un élément $u \in L\{\tau\}$ tel que $\phi_a u = u\psi_a$ pour tout $a \in A$. C'est un *isomorphisme* si $u \in L^{\times}$. Une *isogénie* est un homomorphisme non nul ; il n'en existe qu'entre modules de Drinfeld de même rang. Une isogénie est *cyclique d'ordre* $\mathfrak{a}$ si $\deg_{\tau} u = \deg \mathfrak{a}$ et si son noyau $C = (\ker u)(L^{\text{alg}})$ est un sous-module de $({}^{\phi}L^{\text{alg}})_{\text{tors}}$ isomorphe à $A/\mathfrak{a}$. On note alors ϕ/C le module de Drinfeld ψ isogène à ϕ. Il y a une bijection entre l'ensemble des isogénies L-rationnelles (*i.e.*, définies sur L) cycliques d'ordre $\mathfrak{a}$ de ϕ et les sous-modules C de $({}^{\phi}L^{\text{alg}})_{\text{tors}}$ stables par $\text{Gal}(L^{\text{sep}}/L)$ et isomorphes à $A/\mathfrak{a}$ comme A-modules.

On peut étendre la notion de module de Drinfeld d'un A-corps à un A-schéma quelconque S [Drinfeld 1974]. Soit $\mathfrak{n}$ un idéal non nul de A. Considérons le foncteur qui associe à S l'ensemble des classes d'isomorphisme de couples (ϕ, C), où ϕ est un module de Drinfeld de rang 2 sur S et C est un sous-groupe cyclique de ϕ d'ordre $\mathfrak{n}$ au sens de Katz–Mazur. Il possède un schéma de modules grossier $\mathcal{Y}_0(\mathfrak{n})$ sur A. De même, en considérant les classes d'isomorphisme de couples (ϕ, P) où P est un point de ϕ d'ordre $\mathfrak{n}$, on obtient un schéma de modules grossier $\mathcal{Y}_1(\mathfrak{n})$ sur A. Les schémas $\mathcal{Y}_0(\mathfrak{n})$ et $\mathcal{Y}_1(\mathfrak{n})$ sont affines, de type fini sur A et de dimension relative pure 1.

On définit les courbes $Y_0(\mathfrak{n}) = \mathcal{Y}_0(\mathfrak{n}) \times_A K$ et $Y_1(\mathfrak{n}) = \mathcal{Y}_1(\mathfrak{n}) \times_A K$. Pour L une extension de K, les points L-rationnels de $Y_0(\mathfrak{n})$ (respectivement $Y_1(\mathfrak{n})$) sont en bijection avec les classes d'isomorphisme sur L^{alg} de modules de Drinfeld de rang 2 sur L munis d'une isogénie L-rationnelle cyclique d'ordre $\mathfrak{n}$ (respectivement d'un point de torsion d'ordre $\mathfrak{n}$ défini sur L).

Pour mémoire, rappelons le versant analytique de ces courbes. On désigne par $\mathbb{C}_{\infty}$ le complété d'une clôture algébrique de $\mathbb{F}_q(\!(1/T)\!)$. Les analytifiées de $Y_0(\mathfrak{n})$ et $Y_1(\mathfrak{n})$ sur $\mathbb{C}_{\infty}$ sont alors les espaces analytiques rigides obtenus comme quotients du demi-plan de Drinfeld $\mathbb{C}_{\infty} - \mathbb{F}_q(\!(1/T)\!)$ par l'action de certains sous-groupes de congruence de $\text{GL}_2(A)$ [Drinfeld 1974, section 6].

On a une compactification canonique $\mathcal{X}_0(\mathfrak{n})$ de $\mathcal{Y}_0(\mathfrak{n})$ et $\mathcal{X}_1(\mathfrak{n})$ de $\mathcal{Y}_1(\mathfrak{n})$ sur $\text{Spec}(A)$ [Drinfeld 1974, section 9 ; Gekeler 1986] et un homomorphisme canonique $\mathcal{X}_1(\mathfrak{n}) \to \mathcal{X}_0(\mathfrak{n})$. L'énoncé suivant se déduit de [Drinfeld 1974].

Théorème 3.1. *Soit* $i \in \{0, 1\}$.

(i) *Le schéma* $\mathscr{X}_i(\mathfrak{n})$ *est propre, normal, plat et irréductible de dimension relative pure* 1 *sur* A.

(ii) *Le morphisme structurel* $\mathscr{X}_i(\mathfrak{n}) \to \operatorname{Spec} A[1/\mathfrak{n}]$ *est lisse et propre.*

(iii) *La courbe* $X_i(\mathfrak{n}) = \mathscr{X}_i(\mathfrak{n}) \times_A K$ *est lisse, propre et géométriquement connexe sur* K.

D'après Drinfeld, on sait aussi que l'ensemble $X_0(\mathfrak{n})(K^{\mathrm{alg}}) - Y_0(\mathfrak{n})(K^{\mathrm{alg}})$ est fini. Ses éléments sont appelés les *pointes* de $X_0(\mathfrak{n})$. Elles sont en bijection avec l'ensemble quotient $\Gamma_0(\mathfrak{n})\backslash\mathbb{P}^1(K)$ (on a fait opérer le groupe $\Gamma_0(\mathfrak{n})$ par homographies sur $\mathbb{P}^1(K)$). En particulier, pour $\mathfrak{n} = \mathfrak{p}$ premier, la courbe $X_0(\mathfrak{p})$ possède exactement deux pointes notées 0 et ∞ et elles sont K-rationnelles.

Gekeler a donné des formules pour le genre $g(X_0(\mathfrak{n}))$ [Gekeler 1980, 3.4.18 ; Gekeler et Nonnengardt 1995], dont l'énoncé suivant est un cas particulier.

Proposition 3.2. *Pour* $\mathfrak{p}$ *de degré* d, *le genre de* $X_0(\mathfrak{p})$ *est*

$$g(X_0(\mathfrak{p})) = \begin{cases} \dfrac{q^d - q^2}{q^2 - 1} & \text{si } d \text{ est pair,} \\ \dfrac{q^d - q}{q^2 - 1} & \text{si } d \text{ est impair.} \end{cases}$$

La courbe $X_0(\mathfrak{n})$ est munie de correspondances de Hecke [Gekeler 1986, 5.3 ; Gekeler et Reversat 1996, 4.12 ; Gekeler 1997a, section 7]. Pour $\mathfrak{m}$ idéal non nul, la correspondance $T_{\mathfrak{m}}$ est définie sur le problème de modules par

$$(\phi, C) \mapsto \sum_{D \cap C = \{0\}} (\phi/D, (C + D)/D),$$

la somme portant sur les sous-modules cycliques D de ϕ d'ordre $\mathfrak{m}$. De même, pour un idéal $\mathfrak{m}$ divisant $\mathfrak{n}$ et premier à $\mathfrak{n}/\mathfrak{m}$, l'involution $w_{\mathfrak{m}}$ de $X_0(\mathfrak{n})$ est définie par $(\phi, C) \mapsto (\phi/C, \phi[\mathfrak{m}]/C)$. Ces correspondances stabilisent l'ensemble des pointes de $X_0(\mathfrak{n})$. Si $\mathfrak{n} = \mathfrak{p}$ premier, $w_{\mathfrak{p}}$ échange 0 et ∞ et $T_{\mathfrak{m}}$ opère par multiplication par $(1 + q^{\deg \mathfrak{m}})$ sur chaque pointe, pour $\mathfrak{m}$ étranger à $\mathfrak{p}$.

La jacobienne $J_0(\mathfrak{n})$ de $X_0(\mathfrak{n})$ est une variété abélienne sur K de dimension $g(X_0(\mathfrak{n}))$. Elle a bonne réduction en-dehors de $\mathfrak{n} \cdot (\infty)$ et, pour $\mathfrak{n} = \mathfrak{p}$, réduction torique en $\mathfrak{p}$. La structure de la fibre spéciale de $\mathscr{X}_0(\mathfrak{p})$ et le groupe des composantes de $J_0(\mathfrak{p})$ en $\mathfrak{p}$ ont été déterminés par Gekeler [1986].

3B. ***Cochaînes harmoniques.*** Les cochaînes harmoniques paraboliques pour $\Gamma_0(\mathfrak{p})$ à valeurs dans $\mathbb{Z}$ sont des fonctions sur les arêtes de l'arbre de Bruhat–Tits de $\mathrm{PGL}_2(\mathbb{F}_q((1/T)))$ (on se réfère à [Gekeler et Reversat 1996] pour leurs définitions et propriétés). Elles forment un $\mathbb{Z}$-module libre de rang $g(X_0(\mathfrak{p}))$, noté $\mathrm{H}_{\mathfrak{p}}$. Soit

$\mathrm{H}_{\mathfrak{p}}(\mathbb{C}) = \mathrm{H}_{\mathfrak{p}} \otimes_{\mathbb{Z}} \mathbb{C}$ le $\mathbb{C}$-espace vectoriel des cochaînes paraboliques à valeurs dans $\mathbb{C}$. La plupart du temps, on omettra la dépendance en $\mathfrak{p}$ et on notera H et $\mathrm{H}(\mathbb{C})$. D'après Drinfeld et le théorème d'approximation faible, $\mathrm{H}(\mathbb{C})$ s'identifie à un espace de formes automorphes paraboliques pour GL_2 sur les adèles de K. Toute cochaîne de $\mathrm{H}(\mathbb{C})$ admet un développement de Fourier indexé par les idéaux de A (voir [Weil 1971 ; Tan 1993 ; Gekeler 1980 ; 1995b] pour différents points de vue).

Pour $\mathfrak{m}$ idéal non nul de A, on définit l'opérateur de Hecke $T_{\mathfrak{m}}$ comme l'endomorphisme de $\mathrm{H}(\mathbb{C})$ provenant de l'action à gauche des matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ (a, b, d dans A, $(ad) = \mathfrak{m}$, $(a) + \mathfrak{p} = A$, $\deg b < \deg d$, a et d unitaires) sur les arêtes de l'arbre. Soit $w_{\mathfrak{p}}$ l'involution de $\mathrm{H}(\mathbb{C})$ induite par l'action de $\left(\begin{smallmatrix} 0 & -1 \\ P & 0 \end{smallmatrix}\right)$ où P désigne le générateur unitaire de l'idéal $\mathfrak{p}$. Le lien avec les correspondances $T_{\mathfrak{m}}$ et $w_{\mathfrak{p}}$ sera explicité en section 3D. Soit $\mathbb{T}$ la sous-algèbre commutative de $\operatorname{End} \mathrm{H}(\mathbb{C})$ engendrée sur $\mathbb{Z}$ par $w_{\mathfrak{p}}$ et les $T_{\mathfrak{m}}$ pour $\mathfrak{m}$ et $\mathfrak{p}$ étrangers. Ces opérateurs sont hermitiens pour le produit de Petersson sur $\mathrm{H}(\mathbb{C})$ induit par celui sur les formes automorphes. On a $w_{\mathfrak{p}} = -T_{\mathfrak{p}}$. L'*algèbre de Hecke* $\mathbb{T}$ stabilise la structure entière H. Le $\mathbb{Z}$-module $\mathbb{T}$ est libre de type fini car il en est de même de H.

Par le théorème spectral, il existe une base de $\mathrm{H}(\mathbb{C})$ constituée de formes propres pour tous les opérateurs de Hecke et normalisées (*i.e.*, le coefficient de Fourier associé à l'idéal A est 1). On les appelle *formes primitives*. Elles sont propres pour $w_{\mathfrak{p}}$ de valeur propre $+1$ ou -1.

La fonction $L(F, s)$ est la série de Dirichlet associée aux coefficients de Fourier de $F \in \mathrm{H}(\mathbb{C})$ (s variable complexe). Cette fonction s'écrit aussi comme transformée de Mellin de F. Pour $L(F, s)$, on en déduit un prolongement holomorphe à $\mathbb{C}$, l'équation fonctionnelle

$$L(F, s) = -q^{(\deg(\mathfrak{p})-3)(1-s)} L(w_{\mathfrak{p}} F, 2-s) \quad (s \in \mathbb{C}) \tag{1}$$

et la propriété que $L(F, s)$ est un polynôme non nul en q^{-s} de degré $\leq \deg(\mathfrak{p}) - 3$ (voir [Tan 1993], proposition 2, équation (3.4) et le corollaire à la page 305 pour ces affirmations). En particulier, en $s = 1$, la fonction $L(F, s)$ a un zéro d'ordre impair si $w_{\mathfrak{p}} F = +F$ et un zéro d'ordre pair (ou pas de zéro) si $w_{\mathfrak{p}} F = -F$. On complète ces rappels par des propriétés élémentaires.

Lemme 3.3. *Soit F primitive dans* $\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$.

(i) *La fonction $L(F, s)$ est un polynôme en q^{-s} de degré* $\deg(\mathfrak{p}) - 3$ *et de terme constant* 1.

(ii) *Supposons que l'ordre d'annulation de $L(F, s)$ en $s = 1$ est ≤ 1 (c'est le cas si* $\deg \mathfrak{p} \leq 4$*). Alors*

$$w_{\mathfrak{p}} F = -F \iff L(F, 1) \neq 0.$$

Démonstration. (i) Voir [Tan 1993, page 305].

(ii) La condition est vérifiée si $\deg \mathfrak{p} \leq 4$ car la fonction L est alors un polynôme en q^{-s} de degré ≤ 1. D'après (1), on a $L(F, 1) = -L(w_{\mathfrak{p}}F, 1)$. Donc $L(F, 1) \neq 0$ entraîne $w_{\mathfrak{p}}F = -F$, sans condition sur l'ordre d'annulation. Réciproquement, supposons $w_{\mathfrak{p}}F = -F$. Alors l'ordre d'annulation est pair ≥ 2 ou bien $L(F, 1) \neq 0$. Comme $L(F, s)$ s'annule à l'ordre ≤ 1, seul le deuxième cas est possible. □

Soit $\mathcal{F}$ l'ensemble des formes primitives de $\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$. Le groupe de Galois absolu de $\mathbb{Q}$ opère sur $\mathcal{F}$ *via* son action sur les coefficients de Fourier. Notons $\mathcal{O}$ l'ensemble des orbites, $[F]$ l'orbite de $F \in \mathcal{F}$ et $a_{[F]}$ l'idéal annulateur de F dans $\mathbb{T}$. L'application $[F] \mapsto a_{[F]}$ est une bijection entre $\mathcal{O}$ et l'ensemble des idéaux premiers minimaux de $\mathbb{T}$.

Soit K_F le corps de nombres totalement réel engendré par les coefficients de Fourier de F. Son degré sur $\mathbb{Q}$ est le cardinal de $[F]$. L'application $u \mapsto uF/F$ de $\mathbb{T}$ dans K_F induit un isomorphisme de $\mathbb{Q}$-algèbres $(\mathbb{T}/a_{[F]}) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq K_F$. La $\mathbb{Q}$-algèbre $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$ est alors semi-simple : elle est isomorphe au produit des K_F pour $[F] \in \mathcal{O}$. Le rang de $\mathbb{T}$ sur $\mathbb{Z}$ est donc $g(X_0(\mathfrak{p}))$.

La variété abélienne $J_{[F]}$ est définie comme le quotient de $J_0(\mathfrak{p})$ par la sous-variété abélienne $a_{[F]}J_0(\mathfrak{p})$. Elle est simple sur K et sa dimension est $\#[F]$. Sa fonction L de Hasse–Weil se factorise en

$$L(J_{[F]}, s) = \prod_{G \in [F]} L(G, s) \quad (s \in \mathbb{C}), \tag{2}$$

l'égalité étant valable pour les facteurs locaux. (Pour les places étrangères à $\mathfrak{p}$, cela provient d'une relation d'Eichler et Shimura ; dans le cas général, de [Deligne 1973; Drinfeld 1984, théorème A et remarque 2]. Voir aussi [Tamagawa 1995, (3.3)].)

3C. ***Symboles modulaires pour*** $\mathbb{F}_q(T)$**.** Les rappels suivants sur la théorie de Teitelbaum se basent sur [Teitelbaum 1992], auquel on renvoie pour les détails. Les symboles modulaires paraboliques pour $\mathbb{F}_q(T)$ à valeurs dans $\mathbb{Z}$ relativement au sous-groupe $\Gamma_0(\mathfrak{p})$ forment un $\mathbb{Z}$-module qu'on note $\mathrm{M}_{\mathfrak{p}}^0$ ou encore M^0. Il est de type fini et de rang $g(X_0(\mathfrak{p}))$. On note qu'il peut avoir une torsion non nulle. Soit $\mathrm{M}^0(\mathbb{Q}) = \mathrm{M}^0 \otimes_{\mathbb{Z}} \mathbb{Q}$ (respectivement $\mathrm{M}^0(\mathbb{C}) = \mathrm{M}^0 \otimes_{\mathbb{Z}} \mathbb{C}$) l'espace vectoriel des symboles modulaires paraboliques à valeurs dans $\mathbb{Q}$ (respectivement $\mathbb{C}$).

Comme auparavant, les matrices

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right\}_{a,b,d} \quad \text{et} \quad \begin{pmatrix} 0 & -1 \\ P & 0 \end{pmatrix}$$

définissent des éléments de $\operatorname{End} \mathrm{M}^0(\mathbb{C})$ notés $T_{\mathfrak{m}}$ et $w_{\mathfrak{p}}$. Par ailleurs, Teitelbaum a défini un accouplement parfait $\langle \cdot, \cdot \rangle : \mathrm{M}^0(\mathbb{C}) \times \mathrm{H}(\mathbb{C}) \to \mathbb{C}$. Il est compatible aux opérateurs de Hecke et parfait sur $\mathrm{M}^0(\mathbb{Q}) \times \mathrm{H}(\mathbb{Q})$ où $\mathrm{H}(\mathbb{Q}) = \mathrm{H} \otimes_{\mathbb{Z}} \mathbb{Q}$. Il permet donc d'identifier $\mathbb{T}$ à la sous-algèbre de $\operatorname{End} \mathrm{M}^0(\mathbb{C})$ engendrée sur $\mathbb{Z}$ par les

opérateurs d'indice étranger à $\mathfrak{p}$. On désigne encore par $\mathbb{T}$ cette algèbre. À nouveau, elle stabilise la structure entière M^0.

Lemme 3.4. *Le* $(\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q})$*-module* $\mathrm{M}^0(\mathbb{Q})$ *est libre de rang* 1.

Démonstration. Pour $F\in\mathrm{H}$, on note $c_A(F)$ le coefficient de Fourier de F associé à l'idéal A. On a un accouplement de groupes abéliens

$$\mathbb{T}\times\mathrm{H}\to\mathbb{Z},\quad (u,F)\mapsto c_A(uF),$$

qui est équivariant par $\mathbb{T}$. D'après le théorème 3.17 de [Gekeler 1995a], l'accouplement est parfait après extension des scalaires à $\mathbb{Z}[1/p]$. Ainsi $\mathrm{H}(\mathbb{Q})$ est un $(\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q})$-module libre de rang 1. Par l'accouplement $\langle\cdot,\cdot\rangle$ de Teitelbaum, on sait que $\mathrm{H}(\mathbb{Q})$ et $\mathrm{M}^0(\mathbb{Q})$ sont des $(\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q})$-modules isomorphes, ce qui permet de conclure. □

3D. ***Compatibilité de l'action de Hecke.*** Les correspondances de Hecke sur la courbe $X_0(\mathfrak{p})$ induisent des endomorphismes de $J_0(\mathfrak{p})$ définis sur K. Considérons la sous-algèbre de $\mathrm{End}_K J_0(\mathfrak{p})$ engendrée sur $\mathbb{Z}$ par $w_{\mathfrak{p}}$ et les $T_{\mathfrak{m}}$ pour $\mathfrak{m}$ étranger à $\mathfrak{p}$. Un théorème fondamental de Drinfeld [1974, théorème 2] permet de l'identifier à l'algèbre de Hecke $\mathbb{T}\subset\mathrm{End}\,\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$. Cette compatibilité peut aussi se déduire de la construction explicite de $J_0(\mathfrak{p})$, en tant que variété analytique rigide sur $\mathbb{C}_\infty$, comme tore modulo le réseau des périodes de certaines fonctions thêta d'après [Gekeler et Reversat 1996, sections 5 à 9 ; Gekeler 1997a, 7.6]. L'algèbre de Hecke $\mathbb{T}$ agit ainsi de façon fidèle et compatible sur plusieurs objets : la jacobienne $J_0(\mathfrak{p})$, les structures entières $\mathrm{H}_{\mathfrak{p}}$ de cochaînes et $\mathrm{M}^0_{\mathfrak{p}}$ de symboles modulaires.

4. Le quotient d'enroulement de $J_0(\mathfrak{p})$

4A. ***Définition et groupe de Mordell–Weil.*** Par l'accouplement $\langle\cdot,\cdot\rangle$, la forme linéaire $F\mapsto(q-1)L(F,1)$ définit un élément $\mathbf{e}$ de $\mathrm{M}^0(\mathbb{Q})$ appelé *élément d'enroulement* [Armana 2011b, définition 7.1].

Définition 4.1. Notons $I_{\mathbf{e}}$ l'idéal annulateur de $\mathbf{e}$ dans $\mathbb{T}$ et $I_{\mathbf{e}}J_0(\mathfrak{p})$ la sous-variété abélienne de $J_0(\mathfrak{p})$ engendrée par ux pour $u\in I_{\mathbf{e}}$ et $x\in J_0(\mathfrak{p})$. Le *quotient d'enroulement* $J_{\mathbf{e}}(\mathfrak{p})$ est la variété abélienne $J_0(\mathfrak{p})/I_{\mathbf{e}}J_0(\mathfrak{p})$, définie sur K.

Cette construction est similaire à celle de Merel [1996] pour la courbe modulaire classique. On commence par donner deux propriétés de $I_{\mathbf{e}}$ qui serviront pour l'étude de $J_{\mathbf{e}}(\mathfrak{p})$.

Lemme 4.2. (i) *On a*

$$I_{\mathbf{e}}=\bigcap_{\substack{[F]\in\mathcal{C}\\ L(F,1)\neq0}} a_{[F]}. \tag{3}$$

(ii) *Soit* $F\in\mathrm{H}(\mathbb{C})$ *une cochaîne propre pour* $\mathbb{T}$ *et non nulle. Alors*

$$I_{\mathbf{e}}F=0\iff L(F,1)\neq0.$$

Démonstration. (i) Voir la preuve du lemme 7.12 de [Armana 2011b].

(ii) Si $L(F,1)\neq 0$, l'idéal $I_{\mathbf{e}}$ est contenu dans $a_{[F]}$ d'après (3). Cela démontre un sens de l'équivalence. Passons à l'autre. Le $(\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q})$-module $\mathrm{M}^0(\mathbb{Q})$ est semi-simple, par semi-simplicité de $\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q}$, et libre de rang 1 par le lemme 3.4. On a donc décomposition en somme directe $\mathrm{M}^0(\mathbb{Q})=(\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q})\mathbf{e}\oplus I_{\mathbf{e}}\mathrm{M}^0(\mathbb{Q})$. Soit F non nulle dans $\mathrm{H}(\mathbb{C})$, propre pour $\mathbb{T}$ et annulée par $I_{\mathbf{e}}$. Elle est orthogonale à la seconde composante de $\mathrm{M}^0(\mathbb{Q})$ pour $\langle\cdot,\cdot\rangle$. Cet accouplement étant non dégénéré, il existe $u\in\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q}$ tel que $0\neq\langle u\mathbf{e},F\rangle=\langle\mathbf{e},uF\rangle$. Comme F est propre, on obtient $\langle\mathbf{e},F\rangle\neq 0$. Cela revient à dire $L(F,1)\neq 0$. □

Si F est primitive avec $L(F,1)\neq 0$, on a $(1+w_{\mathfrak{p}})\in a_{[F]}$ d'après l'équation (1). Donc par le lemme 4.2, l'idéal $I_{\mathbf{e}}$ contient $(1+w_{\mathfrak{p}})$. En posant

$$J_0(\mathfrak{p})^-=J_0(\mathfrak{p})/(1+w_{\mathfrak{p}})J_0(\mathfrak{p})$$

on a alors un homomorphisme canonique surjectif $J_0(\mathfrak{p})^-\to J_{\mathbf{e}}(\mathfrak{p})$.

Proposition 4.3. *La variété abélienne $J_{\mathbf{e}}(\mathfrak{p})$ est isogène sur K au produit de variétés abéliennes simples*

$$\prod_{\substack{[F]\in\mathbb{C}\\ L(F,1)\neq 0}} J_{[F]}.$$

On a donc, pour $s\in\mathbb{C}$,

$$L(J_{\mathbf{e}}(\mathfrak{p}),s)\;=\prod_{\substack{F\in\mathcal{F}\\ L(F,1)\neq 0}} L(F,s). \tag{4}$$

Le groupe de Mordell–Weil $J_{\mathbf{e}}(\mathfrak{p})(K)$ est fini.

Démonstration. D'après la théorie d'Eichler–Shimura, due dans ce cadre à Drinfeld [1974], les variétés abéliennes $J_{\mathbf{e}}(\mathfrak{p})$ et $\prod_{[F]\in\mathbb{C},\,I_{\mathbf{e}}\subset a_{[F]}}J_{[F]}$ sont isogènes sur K (c'est un cas particulier du lemme 4.1 de [Tamagawa 1995]). Donc leurs fonctions L de Hasse–Weil coïncident. D'après le lemme 4.2, on peut remplacer la condition $I_{\mathbf{e}}\subset a_{[F]}$ par $L(F,1)\neq 0$. En combinant à (2), on obtient l'égalité (4) pour tout $s\in\mathbb{C}$. En particulier, $L(J_{\mathbf{e}}(\mathfrak{p}),1)$ est non nul. Par une inégalité connue dans la conjecture de Birch et Swinnerton-Dyer pour les variétés abéliennes sur K (théorème 11(i) de [Schneider 1982]), le groupe de Mordell–Weil $J_{\mathbf{e}}(\mathfrak{p})(K)$ est alors fini. □

Pál [2010, définition 5.10] a construit un objet qui coïncide probablement avec notre quotient d'enroulement. Il est possible de montrer que $J_{\mathbf{e}}(\mathfrak{p})$ est le plus grand quotient optimal de $J_0(\mathfrak{p})$ dont la fonction L ne s'annule pas en $s=1$, en suivant les lignes de la proposition 5.11(iii) de [Pál 2010]. Selon la conjecture de Birch et

Swinnerton-Dyer, $J_{\mathbf{e}}(\mathfrak{p})$ serait alors le plus grand quotient optimal de $J_0(\mathfrak{p})$ n'ayant qu'un nombre fini de points K-rationnels.

Dans la situation classique, il résulte de travaux de Mazur que l'homomorphisme canonique induit une bijection entre le groupe des points $\mathbb{Q}$-rationnels d'ordre fini de la jacobienne et le groupe des points $\mathbb{Q}$-rationnels du quotient d'enroulement (conséquence du corollaire III/1.4 et du théorème II/8.10 de [Mazur 1977]). Par analogie, on s'attend ici à une bijection naturelle entre $J_0(\mathfrak{p})(K)_{\mathrm{tors}}$ et $J_{\mathbf{e}}(\mathfrak{p})(K)$.

4B. ***Étude pour $\mathfrak{p}$ de petit degré.*** En nous appuyant sur des résultats de Schweizer, on décrit le quotient d'enroulement lorsque le premier $\mathfrak{p}$ est de degré 3 ou 4.

4B1. *Quotients d'enroulement triviaux.*

Proposition 4.4. *On a $J_{\mathbf{e}}(\mathfrak{p}) = J_0(\mathfrak{p})$ si et seulement si $\mathfrak{p}$ est de degré* 3. *Dans cette situation, on a les propriétés suivantes* :

- *L'idéal $I_{\mathbf{e}}$ est nul.*
- *La fonction $L(J_{\mathbf{e}}(\mathfrak{p}), s)$ est constante égale à* 1.
- *Le groupe $J_0(\mathfrak{p})(K)$ est cyclique d'ordre q^2+q+1.*
- *Le groupe de Tate–Shafarevich de $J_0(\mathfrak{p})$ est trivial.*

Démonstration. Supposons $J_{\mathbf{e}}(\mathfrak{p}) = J_0(\mathfrak{p})$. Comme l'idéal $I_{\mathbf{e}}$ contient $(1 + w_{\mathfrak{p}})$, l'involution $w_{\mathfrak{p}}$ agit comme -1 sur la jacobienne. Cela signifie que la courbe $X_0(\mathfrak{p})$ est hyperelliptique. Or, d'après Schweizer (théorème 20 de [Schweizer 1997]), les seuls premiers $\mathfrak{p}$ pour lesquels $X_0(\mathfrak{p})$ est hyperelliptique sont ceux de degré 3.

Réciproquement, supposons $\mathfrak{p}$ premier de degré 3. Alors d'après le lemme 3.3, la fonction L de toute forme primitive est constante égale à 1. Par le lemme 4.2, on en déduit $I_{\mathbf{e}} = \bigcap_{[F]\in\mathcal{C}} a_{[F]} = \{0\}$. Donc la sous-variété abélienne $I_{\mathbf{e}}J_0(\mathfrak{p})$ est nulle et $J_{\mathbf{e}}(\mathfrak{p}) = J_0(\mathfrak{p})$. Avec la proposition 4.3, on obtient $L(J_{\mathbf{e}}(\mathfrak{p}), s) = 1$ et $J_0(\mathfrak{p})(K)$ est fini.

Par ailleurs, le théorème 1.2 de [Pál 2005] dit que le sous-groupe de torsion de $J_0(\mathfrak{p})(K)$ est cyclique (pour $\mathfrak{p}$ premier quelconque) et, si $\mathfrak{p}$ est de degré 3, d'ordre q^2+q+1. Donc ici $J_0(\mathfrak{p})(K)$ est cyclique d'ordre q^2+q+1.

On constate que le rang de $J_0(\mathfrak{p})(K)$ coïncide avec l'ordre d'annulation en $s=1$ de $L(J_0(\mathfrak{p}), s)$, car ils sont tous deux nuls. D'après le théorème de Kato et Trihan [2003], la formulation forte de la conjecture de Birch et Swinnerton-Dyer est vérifiée pour $J_0(\mathfrak{p})$, donc

$$L(J_0(\mathfrak{p}), 1) = \frac{Sc_{\mathfrak{p}}c_\infty}{(\#J_0(\mathfrak{p})(K))^2},$$

où S est l'ordre du groupe de Tate–Shafarevich de $J_0(\mathfrak{p})$ (il est alors fini), $c_{\mathfrak{p}}$ et c_∞ sont les ordres du groupe des composantes du modèle de Néron de $J_0(\mathfrak{p})$ en $\mathfrak{p}$ et $\infty = (1/T)$, respectivement (ce sont les seules places de mauvaise réduction de $J_0(\mathfrak{p})$). On a vu précédemment que $\#J_0(\mathfrak{p})(K) = q^2+q+1$. De plus, d'après

Gekeler, on a $c_{\mathfrak{p}} = q^2+q+1$ [1986, lemme 5.9 et proposition 5.10] et $c_\infty = q^2+q+1$ [1997b, 6.3(ii)]. On trouve donc $S = 1$. □

4B2. *Exemples en degré supérieur.* Soit I un idéal de $\mathbb{T}$. On rappelle qu'il est dit saturé si le groupe abélien $\mathbb{T}/I$ est sans torsion. On note I^{sat} le plus petit idéal saturé de $\mathbb{T}$ contenant I.

Une cochaîne de $\mathrm{H}(\mathbb{C})$ sera dite de *rang analytique* r si sa fonction L s'annule à l'ordre r en $s = 1$.

Proposition 4.5. *Soit* $\mathfrak{p}$ *un premier tel que toute forme primitive de* $\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$ *est de rang analytique* ≤ 1 (*c'est le cas si* $\deg \mathfrak{p} = 4$). *Alors* $I_{\mathbf{e}} = (1 + w_{\mathfrak{p}})^{\mathrm{sat}}$ *et la variété abélienne* $J_{\mathbf{e}}(\mathfrak{p})$ *est isogène à* $J_0(\mathfrak{p})^-$ *sur* K. *Notons* $d = \deg \mathfrak{p}$ *et* P *le générateur unitaire de* $\mathfrak{p}$.

– *Si* q *est impair* : *soient* $h(\sqrt{f})$ *le nombre de classes d'idéaux de l'ordre* $\mathbb{F}_q[T, \sqrt{f}]$ *pour* $f \in A$ *et* α *un élément qui n'est pas un carré de* $\mathbb{F}_q^\times$. *Alors*

$$\dim J_{\mathbf{e}}(\mathfrak{p}) = \begin{cases} \frac{1}{2}\left(\frac{q^d-q^2}{q^2-1} + \frac{h(\sqrt{\alpha P})}{2} - 1\right) & \text{si } d \text{ est pair,} \\ \frac{1}{2}\left(\frac{q^d-q}{q^2-1} + \frac{h(\sqrt{P})+h(\sqrt{\alpha P})}{2} - 1\right) & \text{si } d \text{ est impair.} \end{cases}$$

– *Si* q *est pair* : *soit* (S, R) *l'unique couple de* $A \times A$ *tel que* $P = S^2 + T R^2$. *Posons* $Q = \prod_a a^{\mathrm{ord}_a(R)}$, *le produit fini portant sur les polynômes unitaires irréductibles de* A. *Alors*

$$\dim J_{\mathbf{e}}(\mathfrak{p}) = \begin{cases} \frac{1}{2}\left(\frac{q^d-q^2}{q^2-1} + \sum_{f|Q} q^{\deg f} - 1\right) & \text{si } d \text{ est pair,} \\ \frac{1}{2}\left(\frac{q^d-q}{q^2-1} + \sum_{f|Q} q^{\deg f} - 1\right) & \text{si } d \text{ est impair.} \end{cases}$$

Démonstration. On a vu que $(1 + w_{\mathfrak{p}}) \subset I_{\mathbf{e}}$, donc $(1 + w_{\mathfrak{p}})^{\mathrm{sat}} \subset I_{\mathbf{e}}$ car $I_{\mathbf{e}}$ est saturé. Passons à l'inclusion réciproque. Soit $[F] \in \mathcal{O}$ tel que $(1 + w_{\mathfrak{p}})^{\mathrm{sat}} \in a_{[F]}$. L'idéal $a_{[F]}$ contenant $(1 + w_{\mathfrak{p}})$, on a $w_{\mathfrak{p}} F = -F$. Par l'hypothèse sur l'ordre d'annulation et le lemme 3.3, $L(F, 1)$ est non nul. Par ailleurs, la description de $I_{\mathbf{e}}$ donnée en (3) assure que $a_{[F]}$ contient $I_{\mathbf{e}}$. L'idéal $(1 + w_{\mathfrak{p}})^{\mathrm{sat}}$ étant saturé, il est l'intersection des idéaux premiers minimaux de $\mathbb{T}$ le contenant. Donc $I_{\mathbf{e}} \subset (1 + w_{\mathfrak{p}})^{\mathrm{sat}}$.

Posons $I = (1 + w_{\mathfrak{p}})$, $J = J_0(\mathfrak{p})$ et montrons que les variétés abéliennes $J/I^{\mathrm{sat}}J$ et J/IJ sont isogènes. Le $\mathbb{Z}$-module I^{sat}/I est de torsion et de type fini (pour la dernière affirmation, car I^{sat} est de type fini comme sous-module de $\mathbb{T}$). Donc I^{sat}/I est fini. La surjection canonique $J \to J/I^{\mathrm{sat}}J$ induit un homomorphisme surjectif de variétés abéliennes $J/IJ \to J/I^{\mathrm{sat}}J$. Son noyau $I^{\mathrm{sat}}J/IJ$ est fini par ce qui précède. Cet homomorphisme est donc l'isogénie cherchée.

Notons g la dimension de J et g^+ celle de IJ. La suite exacte de variétés abéliennes $0 \to IJ \to J \to J/IJ \to 0$ donne $\dim J_{\mathbf{e}}(\mathfrak{p}) = \dim(J/IJ) = g - g^+$. Avec la formule de Riemann–Hurwitz, Schweizer [1997, proposition 7] a établi

des expressions pour g^+. On en déduit

$$\dim J_{\mathbf{e}}(\mathfrak{p}) = \begin{cases} \frac{1}{2}(g-1+\frac{n}{2}) & \text{si } q \text{ est impair,} \\ \frac{1}{2}(g-1+n) & \text{si } q \text{ est pair,} \end{cases}$$

où n est le nombre de points fixes de l'involution $w_{\mathfrak{p}}$ sur $X_0(\mathfrak{p})$. Ces points fixes sont dénombrés dans [Schweizer 1997, proposition 11 et lemme 12] :

$$n = \begin{cases} h(\sqrt{\alpha P}) & \text{si } q \text{ est impair et } \deg \mathfrak{p} \text{ pair.} \\ h(\sqrt{P}) + h(\sqrt{\alpha P}) & \text{si } q \text{ est impair et } \deg \mathfrak{p} \text{ impair.} \\ \sum_{f \mid Q} q^{\deg f} & \text{si } q \text{ est pair.} \end{cases}$$

En substituant la formule pour g (proposition 3.2), on trouve les dimensions annoncées. □

4C. ***Minoration de la dimension.*** La dimension de $J_{\mathbf{e}}(\mathfrak{p})$ est, d'après la proposition 4.3,

$$\dim J_{\mathbf{e}}(\mathfrak{p}) = \sum_{\substack{[F]\in\mathbb{O} \\ L(F,1)\neq 0}} \dim J_{[F]} = \sum_{\substack{[F]\in\mathbb{O} \\ L(F,1)\neq 0}} \#[F] = \#\{F \in \mathscr{F} \mid L(F,1) \neq 0\}.$$

Dans [Armana 2011b], on a minoré cette quantité *via* une indépendance linéaire dans $\mathbb{T}\mathbf{e}$.

Théorème 4.6 (reformulation du théorème 1.3 de [Armana 2011b]). *Si* $\mathfrak{p}$ *est premier de degré* ≥ 3 *et* r *est la partie entière de* $(\deg(\mathfrak{p})-3)/2$, *on a*

$$\dim J_{\mathbf{e}}(\mathfrak{p}) \geq \frac{q^{r+1}-1}{q-1} \geq \frac{(q^2-1)^{1/2}}{q^2}(\dim J_0(\mathfrak{p}))^{1/2}.$$

Cette estimation est meilleure que celle obtenue pour le quotient d'enroulement classique par une approche similaire (liberté d'une famille de symboles modulaires). En effet, Parent [1999, remarque page 89] et VanderKam [2000] obtiennent des minorants en $(\dim J_0(p^n))^{1/6}$ et $\dim(J_0(p))^{1/2+\varepsilon}$ pour tout $\varepsilon > 0$, pour les jacobiennes de courbes modulaires classiques $X_0(p^n)$ et $X_0(p)$ respectivement. Toujours dans le cas classique, des méthodes de théorie analytique des nombres fournissent même des estimations linéaires en la dimension de la jacobienne : $(\frac{1}{6} + o(1)) \dim J_0(p)$ chez Kowalski et Michel [1999, théorème 3], amélioré en $(\frac{1}{4} + o(1)) \dim J_0(p)$ par Iwaniec et Sarnak [2000, corollaire 13]. Sur $\mathbb{F}_q(T)$, on pourrait s'attendre à une borne linéaire.

Corollaire 4.7. *Les propriétés suivantes sont équivalentes pour un premier* $\mathfrak{p}$:

(i) *La variété abélienne* $J_{\mathbf{e}}(\mathfrak{p})$ *est non nulle.*

(ii) $\deg \mathfrak{p} \geq 3$.

(iii) $g(X_0(\mathfrak{p})) > 0$.

Démonstration. L'équivalence des deux dernières affirmations provient des formules pour le genre (proposition 3.2). Si le genre est nul, la variété jacobienne est nulle, et de même pour $J_{\mathbf{e}}(\mathfrak{p})$. Enfin, si $\deg \mathfrak{p} \geq 3$, le théorème 4.6 assure que la variété abélienne $J_{\mathbf{e}}(\mathfrak{p})$ est de dimension > 0, donc n'est pas la variété abélienne nulle. □

4D. *Une version raffinée de* $J_{\mathbf{e}}(\mathfrak{p})$.

4D1. *Construction.* Notons $\overline{\mathrm{M}^0}$ le quotient maximal sans torsion $\mathrm{M}^0/(\mathrm{M}^0)_{\mathrm{tors}}$. Il s'identifie à un sous $\mathbb{Z}$-module de $\mathrm{M}^0(\mathbb{Q})$. L'élément d'enroulement $\mathbf{e}$ étant défini sur $\mathbb{Q}$, il possède un dénominateur $d_{\mathbf{e}}$ qui est le plus petit entier strictement positif n tel que $n\mathbf{e} \in \overline{\mathrm{M}^0}$. Dans [Armana 2011b, proposition 7.5], on a vu que $d_{\mathbf{e}}$ est premier à p.

Notation 4.8. On note $\tilde{\mathbf{e}}$ la classe de $d_{\mathbf{e}}\mathbf{e}$ dans $\overline{\mathrm{M}^0}/p\overline{\mathrm{M}^0}$. Soit $\tilde{I}_{\mathbf{e}}$ l'annulateur de $\tilde{\mathbf{e}}$ dans $\mathbb{T}$ c'est-à-dire l'ensemble des $u \in \mathbb{T}$ tels que $d_{\mathbf{e}}u\mathbf{e} \in p\overline{\mathrm{M}^0}$. Il contient $I_{\mathbf{e}} + p\mathbb{T}$. Si I est un idéal de $\mathbb{T}$, on note $\hat{I}$ l'idéal annulateur de I dans $\mathbb{T}$.

Dans la section 7E, nous serons amenés à considérer une variante du quotient d'enroulement. *Jusqu'à la fin de section 4D1, nous faisons l'hypothèse suivante afin de construire cette variante.*

Hypothèse 4.9. *Il existe un idéal saturé I de $\mathbb{T}$ vérifiant* :

($\mathfrak{I}1$) $I_{\mathbf{e}} \subset I$.

($\mathfrak{I}2$) $I \subset \tilde{I}_{\mathbf{e}}$.

($\mathfrak{I}3$) $\hat{I} + \tilde{I}_{\mathbf{e}} = \mathbb{T}$.

Définition 4.10. Soit $I\,J_0(\mathfrak{p})$ la sous-variété abélienne de $J_0(\mathfrak{p})$ engendrée par ux pour $u \in I$ et $x \in J_0(\mathfrak{p})$. Le *quotient raffiné* $J'_{\mathbf{e}}(\mathfrak{p})$ *relatif à* I est la variété abélienne quotient $J_0(\mathfrak{p})/I\,J_0(\mathfrak{p})$, définie sur K.

Il satisfait des propriétés analogues à celles du quotient d'enroulement.

Proposition 4.11. (i) *Le groupe abélien* $J'_{\mathbf{e}}(\mathfrak{p})(K)$ *est fini.*

(ii) *Soient* $\mathfrak{p}$ *premier de degré* $d \geq 3$ *et* r *la partie entière de* $(d-3)/2$. *On a*

$$\dim J'_{\mathbf{e}}(\mathfrak{p}) \geq \frac{q^{r+1}-1}{q-1}.$$

En particulier, la variété abélienne $J'_{\mathbf{e}}(\mathfrak{p})$ *est non nulle.*

Démonstration. (i) Par le lemme 4.10 de [Tamagawa 1995], la variété abélienne $J'_{\mathbf{e}}(\mathfrak{p})$ est isogène sur K à

$$\prod_{\substack{[F]\in\mathbb{O}\\ IF=0}} J_{[F]}.$$

La propriété ($\mathfrak{J}1$) assure que toute forme primitive F annulée par I l'est aussi par $I_{\mathbf{e}}$, donc vérifie $L(F, 1) \neq 0$ par le lemme 4.2. On conclut comme dans la preuve de la proposition 4.3.

(ii) D'après l'isogénie évoquée précédemment, la dimension de $J'_{\mathbf{e}}(\mathfrak{p})$ est

$$\sum_{\substack{[F]\in\mathbb{O}\\ IF=0}} \dim J_{[F]} = \sum_{\substack{[F]\in\mathbb{O}\\ I\subset a_{[F]}}} \dim_{\mathbb{Q}}((\mathbb{T}/a_{[F]})\otimes_{\mathbb{Z}}\mathbb{Q}).$$

La projection canonique donne un isomorphisme $\mathbb{T}/I \to \prod_{I\subset a_{[F]}} \mathbb{T}/a_{[F]}$ car l'idéal I est saturé. Donc la dimension de $J'_{\mathbf{e}}(\mathfrak{p})$ est égale au rang du $\mathbb{Z}$-module libre $\mathbb{T}/I$. Elle est minorée par le rang de $\mathbb{T}/\tilde{I}_{\mathbf{e}}$, puisque $\tilde{I}_{\mathbf{e}}$ contient I (propriété ($\mathfrak{J}2$)). Par ailleurs, on trouve dans [Armana 2011b, théorème 7.10(ii)] l'énoncé suivant dans $\mathbb{T}\tilde{\mathbf{e}}$: les symboles modulaires $T_{\mathfrak{m}}\tilde{\mathbf{e}}$, pour $\mathfrak{m}$ de degré $\leq r$, sont libres sur $\mathbb{F}_p$. Le rang sur $\mathbb{Z}$ de $\mathbb{T}/\tilde{I}_{\mathbf{e}}$, qui coïncide avec sa dimension comme $\mathbb{F}_p$-espace vectoriel, est donc $\geq (q^{r+1}-1)/(q-1)$. Donc $\dim J'_{\mathbf{e}}(\mathfrak{p}) \geq (q^{r+1}-1)/(q-1) > 0$. □

4D2. *Des situations dans lesquelles l'hypothèse 4.9 est vérifiée.* On commence par vérifier l'hypothèse pour l'idéal $I_{\mathbf{e}}$ avec $\mathfrak{p}$ de petit degré. De manière générale, l'idéal $I_{\mathbf{e}}$ est saturé et vérifie les propriétés ($\mathfrak{J}1$) et ($\mathfrak{J}2$) ; il vérifie ($\mathfrak{J}3$) dès que $I_{\mathbf{e}} + \hat{I}_{\mathbf{e}} + p\mathbb{T} = \mathbb{T}$.

Proposition 4.12. *Supposons que* $\mathfrak{p}$ *vérifie l'une des deux conditions suivantes* :

(i) $\mathfrak{p}$ *est de degré* 3.

(ii) $p \neq 2$ *et toute forme primitive de* $\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$ *est de rang analytique* ≤ 1 (*c'est le cas si* $\deg \mathfrak{p} = 4$).

Alors l'idéal $I_{\mathbf{e}}$ *vérifie l'hypothèse 4.9.*

Démonstration. (i) Si $\mathfrak{p}$ est de degré 3, l'idéal $I_{\mathbf{e}}$ est nul d'après la proposition 4.4. Donc son annulateur est $\mathbb{T}$ et les trois propriétés de l'hypothèse 4.9 sont satisfaites.

(ii) Soit $\mathfrak{p}$ comme dans l'énoncé. Par la proposition 4.5, on a $I_{\mathbf{e}} = (1 + w_{\mathfrak{p}})^{\mathrm{sat}}$. De $(1 - w_{\mathfrak{p}})(1 + w_{\mathfrak{p}}) = 0$, on déduit $(1 - w_{\mathfrak{p}})I_{\mathbf{e}} = 0$. Ainsi, $I_{\mathbf{e}} + \hat{I}_{\mathbf{e}}$ contient l'idéal $(1 + w_{\mathfrak{p}})\mathbb{T} + (1 - w_{\mathfrak{p}})\mathbb{T}$ et donc $2\mathbb{T}$. On obtient les inclusions

$$2\mathbb{T} + p\mathbb{T} \subset I_{\mathbf{e}} + \hat{I}_{\mathbf{e}} + p\mathbb{T} \subset \mathbb{T}.$$

Comme 2 et p sont premiers entre eux, ces inclusions sont des égalités. □

On définit maintenant un idéal $I'_{\mathbf{e}}$ qui vérifie les propriétés ($\mathfrak{J}2$) et ($\mathfrak{J}3$) et on donne une condition pour qu'il vérifie ($\mathfrak{J}1$).

Notation 4.13. On note $\mathcal{P}$ l'ensemble des idéaux premiers minimaux de $\mathbb{T}$ et $\mathcal{P}'$ l'ensemble des $\mathfrak{q} \in \mathcal{P}$ tels qu'il existe un idéal maximal $\mathfrak{m}$ de $\mathbb{T}$ contenant $\mathfrak{q}$ et $\tilde{I}_{\mathbf{e}}$. Enfin, $I'_{\mathbf{e}}$ désigne l'idéal $\bigcap_{\mathfrak{q}\in\mathcal{P}'} \mathfrak{q}$ de $\mathbb{T}$.

L'idéal $I'_{\mathbf{e}}$ est donc l'intersection des idéaux premiers minimaux $\mathfrak{q}$ de $\mathbb{T}$ tels que l'inclusion $\mathfrak{q}+\tilde{I}_{\mathbf{e}} \subset \mathbb{T}$ est stricte.

Lemme 4.14. *On a* $\prod_{\mathfrak{q}\notin\mathcal{P}'} \mathfrak{q} \subset \hat{I}'_{\mathbf{e}}$.

Démonstration. Il suffit de voir que les générateurs $\prod_{\mathfrak{q}\notin\mathcal{P}'} x_{\mathfrak{q}}$ (avec $x_{\mathfrak{q}} \in \mathfrak{q}$) de l'idéal produit annulent $I'_{\mathbf{e}}$. Posons $y = u\prod_{\mathfrak{q}\notin\mathcal{P}'} x_{\mathfrak{q}}$ avec $u \in I'_{\mathbf{e}}$. Soit $\mathfrak{m}$ un idéal premier minimal de $\mathbb{T}$. Si $\mathfrak{m} \notin \mathcal{P}'$ alors $x_{\mathfrak{m}}$ appartient à $\mathfrak{m}$, donc y aussi. Si $\mathfrak{m} \in \mathcal{P}'$ alors $I'_{\mathbf{e}} \subset \mathfrak{m}$, donc u appartient à $\mathfrak{m}$ et il en est de même de y. Ainsi, y est dans l'intersection des idéaux premiers minimaux de $\mathbb{T}$. Donc y est nul. □

Proposition 4.15. (i) *L'idéal $I'_{\mathbf{e}}$ est saturé.*

(ii) *On a $I'_{\mathbf{e}} = \bigcap_{k\geq 1}(\tilde{I}_{\mathbf{e}})^k$. En particulier, $I'_{\mathbf{e}}$ est contenu dans $\tilde{I}_{\mathbf{e}}$.*

(iii) *On a $\hat{I}'_{\mathbf{e}} + \tilde{I}_{\mathbf{e}} = \mathbb{T}$.*

Démonstration. (i) Supposons qu'on ait $nu \in I'_{\mathbf{e}}$ avec $u \in \mathbb{T}$ et n non nul dans $\mathbb{Z}$. Soit $\mathfrak{q}$ un idéal de $\mathcal{P}'$. Alors nu appartient à $\mathfrak{q}$ par définition de $I'_{\mathbf{e}}$. Si $n \in \mathfrak{q}$, on aurait $nF = 0$ pour une forme primitive F dans l'orbite correspondant à $\mathfrak{q}$, donc $F = 0$, ce qui est exclu. Comme l'idéal $\mathfrak{q}$ est premier, u appartient donc à $\mathfrak{q}$. Cela prouve que u est dans $I'_{\mathbf{e}}$.

(ii) C'est une conséquence de l'énoncé d'algèbre commutative suivant. *Soient R un anneau noethérien et J un idéal de R. Soit $\mathcal{P}$ l'ensemble des idéaux premiers minimaux de R. Alors on a*

$$\bigcap_{\substack{\mathfrak{q}\in\mathcal{P}\\ J+\mathfrak{q}\neq R}} \mathfrak{q} = \bigcap_{k\geq 1} J^k. \tag{5}$$

En effet, soit $R_{\mathfrak{m}}$ le localisé de R par rapport à la partie multiplicative $R-\mathfrak{m}$ pour un idéal maximal $\mathfrak{m}$ de R. Comme R est noethérien, le théorème de Krull donne $\bigcap_{k\geq 1} J^k = \bigcap_{\mathfrak{m},\, J\subset\mathfrak{m}} \ker(R \to R_{\mathfrak{m}})$ [Atiyah et Macdonald 1969, exercice 10/3]. Par ailleurs, le noyau de $R \to R_{\mathfrak{m}}$ est $\bigcap_{\mathfrak{q}\in\mathcal{P},\, \mathfrak{q}\subset\mathfrak{m}} \mathfrak{q}$ [ibid, corollaire 10.21]. En combinant ces observations, on obtient l'égalité (5).

(ii) Supposons que $\hat{I}'_{\mathbf{e}} + \tilde{I}_{\mathbf{e}} \neq \mathbb{T}$. Alors il existe un idéal maximal $\mathfrak{m}$ de $\mathbb{T}$ contenant $\hat{I}'_{\mathbf{e}}$ et $\tilde{I}_{\mathbf{e}}$. Le lemme 4.14 permet d'exhiber un idéal premier minimal $\mathfrak{q} \notin \mathcal{P}'$ contenu dans $\mathfrak{m}$. Comme $\tilde{I}_{\mathbf{e}} \subset \mathfrak{m}$, l'idéal $\mathfrak{q}$ appartient alors à $\mathcal{P}'$ par définition de cet ensemble. C'est impossible. □

Proposition 4.16. *Si $d_{\mathbf{e}}\mathbf{e}$ engendre le $\mathbb{T}$-module $\overline{\mathrm{M}^0}/I'_{\mathbf{e}}\overline{\mathrm{M}^0}$, on a $I_{\mathbf{e}} \subset I'_{\mathbf{e}}$, et donc $I'_{\mathbf{e}}$ vérifie* ($\mathfrak{J}1$).

Démonstration. L'idéal $I'_{\mathbf{e}}$ étant saturé, il est l'intersection des idéaux premiers minimaux de $\mathbb{T}$ le contenant. Soient $\mathfrak{q}$ un tel idéal et F une forme primitive de l'orbite correspondant à $\mathfrak{q}$. Pour montrer que $I_{\mathbf{e}} \subset I'_{\mathbf{e}}$, il s'agit d'établir $uF = 0$ pour tout $u \in I_{\mathbf{e}}$. L'accouplement entre $\mathrm{M}^0(\mathbb{C})$ et $\mathrm{H}(\mathbb{C})$ étant parfait, cela revient à

prouver que uF est orthogonal à $\mathrm{M}^0(\mathbb{C})$. Comme $d_{\mathbf{e}}\mathbf{e}$ engendre $\overline{\mathrm{M}^0}/I'_{\mathbf{e}}\overline{\mathrm{M}^0}$, on a la décomposition en sous $\mathbb{T}$-modules $\overline{\mathrm{M}^0} = \mathbb{T}d_{\mathbf{e}}\mathbf{e} + I'_{\mathbf{e}}\overline{\mathrm{M}^0}$. Par extension des scalaires, on en déduit

$$\mathrm{M}^0(\mathbb{C}) = (\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{C})\mathbf{e} + (I'_{\mathbf{e}} \otimes_{\mathbb{Z}} \mathbb{C})\mathrm{M}^0(\mathbb{C}).$$

On utilise ensuite l'équivariance de l'accouplement par Hecke. L'élément u annulant $\mathbf{e}$, il reste à montrer que uF est orthogonal à $(I'_{\mathbf{e}} \otimes_{\mathbb{Z}} \mathbb{C})\mathrm{M}^0(\mathbb{C})$. Mais c'est le cas puisque $I'_{\mathbf{e}}$ annule F. □

5. L'uniformisation et le module de Tate–Drinfeld

5A. *Uniformisation de Tate–Drinfeld.*

5A1. *Réduction des modules de Drinfeld.* D'après [Drinfeld 1974, proposition 7.1], tout module de Drinfeld ϕ sur un A-corps local L a réduction potentiellement stable. En d'autres termes, il existe un module de Drinfeld ϕ' sur une extension F/L, à coefficients dans l'anneau de valuation $\mathbb{O}$ de F, tel que ϕ est isomorphe à ϕ' sur F et la réduction $\overline{\phi'}$ de ϕ' est un module de Drinfeld sur le corps résiduel. On appellera un tel ϕ' un *modèle potentiellement stable* de ϕ.

Supposons ϕ de rang 2. Alors ϕ a bonne réduction potentielle (*i.e.*, $\overline{\phi'}$ est de rang 2) ou réduction potentiellement stable de rang 1 ($\overline{\phi'}$ est de rang 1). Si ϕ est muni d'un point $x \in {}^{\phi}L$, on obtient par l'isomorphisme un point y de ${}^{\phi'}F$. Si on part d'un point x entier (*i.e.*, dans l'anneau de valuation de L), y n'est pas nécessairement dans $\mathbb{O}$. Cependant, si y est dans $\mathbb{O}$, on peut vérifier que l'image de x dans tout autre modèle potentiellement stable de ϕ est encore dans $\mathbb{O}$.

5A2. *Uniformisation de Tate–Drinfeld.* C'est l'analogue de l'uniformisation de Tate pour les courbes elliptiques à réduction multiplicative. Soit L un A-corps local dont l'anneau de valuation discrète $\mathbb{O}$ est complet. Si ψ est un module de Drinfeld sur L, un *ψ-réseau de rang* 1 est un sous A-module projectif, discret, de rang 1 et invariant par $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ de ${}^{\psi}L^{\mathrm{sep}}$. D'après [Drinfeld 1974, paragraphe 7], il existe une bijection entre les ensembles de classes d'isomorphisme sur L de

- modules de Drinfeld ϕ de rang 2 sur L à réduction potentiellement stable de rang 1,
- couples (ψ, Γ) où ψ est un module de Drinfeld de rang 1 sur L et Γ est un ψ-réseau de rang 1,

respectivement. L'uniformisation permet aussi de décrire les points de torsion de ϕ. Soit e la fonction exponentielle associée au réseau Γ (voir [Drinfeld 1974] pour sa définition). Soit $\mathfrak{a}$ un idéal non nul de A, dont on fixe un générateur a. Par construction, on a $\phi_a e = e\psi_a$ et l'isomorphisme de A-modules

$$e : \psi_a^{-1}(\Gamma)/\Gamma \xrightarrow{\sim} \phi[\mathfrak{a}], \tag{6}$$

où $\psi_a^{-1}(\Gamma)$ est l'image réciproque de Γ par ψ_a. Supposons ϕ à coefficients dans $\mathbb{O}$. Alors ψ est à coefficients dans $\mathbb{O}$ et on a des A-modules ${}^{\phi}\mathbb{O}$ et ${}^{\psi}\mathbb{O}$ induits par ϕ et ψ respectivement.

Lemme 5.1. *Si ϕ est à coefficients dans $\mathbb{O}$, on a pour tout $a \in A - \{0\}$,*

$$\phi[\mathfrak{a}](\mathbb{O}) = e(\psi[\mathfrak{a}](\mathbb{O})).$$

Démonstration. C'est une adaptation d'arguments de Rosen. On esquisse la preuve et renvoie à [Rosen 2003, lemme 5.3 et théorème 5.4] pour les détails. D'abord, l'inclusion $\supset$ est immédiate car e et ψ sont à coefficients dans $\mathbb{O}$. Passons à l'autre inclusion. Fixons une racine primitive λ_a de ψ_a dans L^{alg} (*primitive* signifiant : λ_a engendre $\psi[\mathfrak{a}]$ comme A-module). D'après l'uniformisation de Tate–Drinfeld, le réseau Γ est le noyau de e et il est de la forme $\psi_A(\gamma) = \{\psi_b(\gamma) \mid b \in A\}$ pour un $\gamma \in \Gamma$. Fixons aussi une racine γ_a de $\psi_a(x) = \gamma$ dans L^{alg}. On note w l'unique prolongement de la valuation de L à L^{alg}. L'ensemble $\psi_a^{-1}(\Gamma)/\Gamma$ a pour système de représentants :

$$\{\psi_c(\lambda_a) + \psi_d(\gamma_a) \mid (c, d) \in A \times A, \deg c < \deg a, \deg d < \deg a\} \subset \psi_a^{-1}(\Gamma).$$

De plus, pour un tel (c, d) avec $d \neq 0$, on a $w(\psi_c(\lambda_a)) \geq 0$ et $w(\psi_d(\gamma_a)) < 0$. On en déduit $w(e(\psi_c(\lambda_a))) \geq 0$ et $w(e(\psi_d(\gamma_a))) < 0$. Par linéarité de e et l'isomorphisme (6), on a alors $\phi[\mathfrak{a}](\mathbb{O}) \subset e(\psi[\mathfrak{a}])$. En raisonnant comme à la page 254 de [Rosen 2003], on voit que $\phi[\mathfrak{a}](\mathbb{O})$ est en fait contenu dans $e(\psi[\mathfrak{a}](L))$. Mais tout élément de $\psi[\mathfrak{a}](L)$ est dans $\mathbb{O}$, car il est racine du polynôme ψ_a dont le coefficient dominant est inversible dans $\mathbb{O}$. Finalement, on obtient $\phi[\mathfrak{a}](\mathbb{O}) \subset e(\psi[\mathfrak{a}](\mathbb{O}))$. □

5B. ***Estimation locale pour la torsion.*** Par un argument local, Poonen a donné un résultat quantitatif sur la torsion des modules de Drinfeld de rang quelconque à bonne réduction potentielle (théorèmes 5 et 7 de [Poonen 1997]). La borne qu'il obtient peut être rendue explicite, mais est loin d'être optimale en rang 2. On raffine l'estimation dans le cas des modules de Drinfeld de rang 2.

Proposition 5.2. *Soit $K_{\mathfrak{l}}$ la complétion de K en un premier $\mathfrak{l}$. Soient L une extension de $K_{\mathfrak{l}}$ de degré $\leq d$, ϕ un module de Drinfeld de rang 2 sur L et x un point de $({}^{\phi}L)_{\mathrm{tors}}$ d'ordre $\mathfrak{n}$ avec $\mathfrak{n} \neq A$ et $\mathfrak{l} \nmid \mathfrak{n}$. Supposons vérifiée l'une des conditions suivantes* :

(i) *ϕ a bonne réduction potentielle.*

(ii) *ϕ a réduction potentiellement stable de rang 1 et x donne un point entier d'un modèle potentiellement stable de ϕ.*

Alors on a $\deg \mathfrak{n} \leq d \deg \mathfrak{l}$.

Démonstration. Notons $r = 2$ dans le premier cas, $r = 1$ dans le deuxième. Le module de Drinfeld ϕ est défini par $\phi_T = T\tau^0 + g\tau + \Delta\tau^2 \in L\{\tau\}$ avec $g \in L$

et $\Delta \in L^\times$. Notons v la valuation de L et P une uniformisante. Le polynôme $X^{q^r-1} - P$ est d'Eisenstein donc irréductible dans $L[X]$. Soit α une racine de ce polynôme et $F = L(\alpha)$. L'extension F/L est séparable et totalement ramifiée de degré $q^r - 1$. Notons O l'anneau de valuation de F et w l'unique valuation de F prolongeant v. Supposons vérifiée l'assertion :

> Il existe un module de Drinfeld ψ de rang r sur F, à coefficients dans O et à bonne réduction, et un point y de $({}^{\psi}O)_{\text{tors}}$ d'ordre $\mathfrak{n}$.

Soit B le sous A-module de $({}^{\psi}F)_{\text{tors}}$ engendré par y (en fait, B est contenu dans ${}^{\psi}O$). Soit $\pi : B \to k$ l'homomorphisme de groupes additifs donné par la réduction sur le corps résiduel k de F. Démontrons qu'il est injectif. Un élément z de B est de $\mathfrak{n}$-torsion pour ψ, donc si N est un générateur de $\mathfrak{n}$, on a

$$\psi_N(z) = Nz + \sum_{i=1}^{r \deg N} l_i z^{q^i} = 0,$$

avec $l_1, \ldots, l_{r \deg N} \in O$ et $l_{r \deg N} \in O^\times$ (car ψ a bonne réduction). S'il existe z non nul dans le noyau de π, on aurait $N + \sum_{1 \le i \le r \deg N} l_i z^{q^i - 1} = 0$. De $w(z) > 0$, on déduirait $w(N) > 0$, ce qui contredit $\mathfrak{l} \nmid \mathfrak{n}$. Donc π est injectif.

Comme F/L est totalement ramifiée, les corps résiduels de F et L sont égaux. De plus, celui de L est une extension de degré au plus d de $\mathbb{F}_\mathfrak{l}$. En combinant ce qui précède, on trouve $\#B \le (\#\mathbb{F}_\mathfrak{l})^d \le q^{d \deg \mathfrak{l}}$. Par ailleurs, y est d'ordre $\mathfrak{n}$ dans ${}^{\psi}O$, donc B est isomorphe à $A/\mathfrak{n}$ comme A-module. On en déduit $\#B = q^{\deg \mathfrak{n}}$. Ainsi on a l'inégalité $\deg \mathfrak{n} \le d \deg \mathfrak{l}$. Maintenant, démontrons l'assertion.

Supposons la condition (i) vérifiée. Posons $u = \alpha^{-v(\Delta)}$ dans $F^\times$ de sorte que $w(u) = -v(\Delta)/(q^2 - 1)$. Le module de Drinfeld ϕ ayant bonne réduction potentielle, son invariant modulaire $j = g^{q+1}/\Delta$ est entier, donc $v(\Delta) \le (q+1)v(g)$. Ainsi, on a $w(u) \ge -v(g)/(q-1)$. On définit le module de Drinfeld ρ de rang 2 sur F par $\rho_T = T\tau^0 + u^{q-1} g \tau + u^{q^2-1} \Delta \tau^2$. Il est isomorphe à ϕ sur F et, par construction, à coefficients dans O et de terme dominant dans $O^\times$. Par l'isomorphisme avec ϕ, le point x de $({}^{\phi}L)_{\text{tors}}$ définit un point y de $({}^{\psi}F)_{\text{tors}}$ d'ordre $\mathfrak{n}$. De plus, y est racine du polynôme $\psi_N(z)$ qui est à coefficients dans O et de terme dominant inversible (car ψ est de rang 2 et a bonne réduction). Donc y est dans O.

Supposons la condition (ii) vérifiée. Posons $u = \alpha^{-v(g)}$ dans $F^\times$ de sorte que $w(u) = -v(g)/(q-1)$. Le module de Drinfeld ϕ n'ayant pas bonne réduction potentielle, on a $(q+1)w(g) < w(\Delta)$ d'où $w(u^{q^2-1}\Delta) > 0$. Soit φ le module de Drinfeld sur F de rang 2 défini par $\varphi_T = T\tau^0 + u^{q-1} g \tau + u^{q^2-1} \Delta \tau^2$. Il est isomorphe à ϕ sur F, à coefficients dans O et sa réduction est de rang 1. C'est un modèle potentiellement stable de ϕ sur F. Par hypothèse sur x, on a un point x' de $({}^{\varphi}O)_{\text{tors}}$ d'ordre $\mathfrak{n}$. Considérons une uniformisation de Tate–Drinfeld (ρ, Γ) de φ sur F. Le module de Drinfeld ρ est de rang 1, à coefficients dans O et a bonne

réduction. Par le lemme 5.1, il existe $y \in \rho[\mathfrak{n}](O)$ tel que $x' = e(y)$. Comme x' est d'ordre $\mathfrak{n}$, on en déduit que l'ordre de y dans ${}^{\rho}O$ est aussi $\mathfrak{n}$. □

5C. ***Le module de Tate–Drinfeld.*** Ce nom désigne l'objet analogue à la courbe de Tate classique dans le cadre de Drinfeld. Il a été étudié par Goss [1980b, définitions 1.51 et 1.54], Gekeler [1988, paragraphe 11.3], Böckle [2002, sections 2.2 à 2.4] et van der Heiden [2006, section 6]. Nous rappelons les résultats adaptés à notre situation.

5C1. *Construction.* Soit $K(\!(t)\!)$ le corps des séries de Laurent formelles sur K en l'indéterminée t. Considérons le module de Carlitz $\rho : A \to K(\!(t)\!)\{\tau\}$ de rang 1 défini par $\rho_T = T\tau^0 + \tau$. Posons $\Gamma = \rho_A(1/t) = \{\rho_a(1/t) \mid a \in A\} \subset A(\!(t)\!)$. Ce sous A-module de ${}^{\rho}K(\!(t)\!)^{\mathrm{sep}}$ est projectif, de rang 1, discret et invariant par le groupe de Galois absolu de $K(\!(t)\!)$. D'après l'uniformisation de Tate–Drinfeld, la donnée de (ρ, Γ) définit un module de Drinfeld TD sur $K(\!(t)\!)$ de rang 2 et à réduction potentiellement stable de rang 1. On appelle TD le *module de Tate–Drinfeld*. Si $e_\Gamma \in K(\!(t)\!)\{\tau\}$ désigne l'exponentielle de Γ, on a alors

$$\mathrm{TD}_a e_\Gamma = e_\Gamma \rho_a \quad (a \in A).$$

De plus, les réductions modulo (t) de TD et ρ coïncident. En fait, TD est un module de Drinfeld de rang 2 sur $A(\!(t)\!)$ à coefficients dans $A[\![t]\!]$ (voir par exemple les lemmes 6.5 de [van der Heiden 2006] et 2.10 de [Böckle 2002]). Le polynôme TD_T est donc de la forme $T\tau^0 + g^*(t)\tau + \Delta^*(t)\tau^2$ avec $g^*(t)$ dans $A[\![t]\!]^\times$ et $\Delta^*(t)$ dans $A(\!(t)\!)^\times \cap tA[\![t]\!]$.

La construction précédente est inchangée si on remplace $\rho_A(1/t)$ par $\rho_A(1/(\lambda t))$ pour $\lambda \in \mathbb{F}_q^\times$: en effet, l'uniformisation de Tate–Drinfeld fournit alors un module de Drinfeld qui est isomorphe à TD sur $\mathbb{F}_q$, donc égal à TD. On en déduit que les séries formelles $g^*(t)$ et $\Delta^*(t)$ sont en fait dans $A(\!(t^{q-1})\!)$ et TD est un module de Drinfeld de rang 2 sur $A(\!(t^{q-1})\!)$ à coefficients dans $A[\![t^{q-1}]\!]$.

Ces séries $g^*(t)$ et $\Delta^*(t)$ peuvent être vues comme développements formels des formes modulaires de Drinfeld g et Δ au voisinage de l'infini (voir [Goss 1980b] ou [Gekeler 1988] pour leur définition). Plus précisément, par la théorie analytique des modules de Drinfeld, le module de Carlitz sur $\mathbb{C}_\infty$ correspond à un réseau de $\mathbb{C}_\infty$ de rang 1 de la forme $\overline{\pi}A$, où la période fondamentale $\overline{\pi} \in \mathbb{C}_\infty^\times$ est définie à multiplication près par un élément de $\mathbb{F}_q^\times$. Dorénavant, on fixe un tel choix de $\overline{\pi}$. Notons e_A l'exponentielle associée au réseau A de rang 1 de $\mathbb{C}_\infty$. Suivant la convention de [Gekeler 1988, 4.1], on pose $t(z) = \overline{\pi}^{-1}/e_A(z)$ pour $z \in \mathbb{C}_\infty - A$. En substituant $t(z)$ à t dans TD, on obtient un module de Drinfeld $\mathrm{TD}(z)$. On peut voir que c'est aussi le module de Drinfeld de rang 2 sur $\mathbb{C}_\infty$ associé au réseau $\overline{\pi}Az \oplus \overline{\pi}A$ de rang 2. Ses coefficients sont reliés à g et Δ par $g^*(t(z)) = \overline{\pi}^{1-q} g(z)$

et $\Delta^*(t(z)) = \overline{\pi}^{1-q^2}\Delta(z)$ (les formes modulaires g et Δ sont de poids $q-1$ et q^2-1, respectivement).

5C2. *Points de torsion.*

Notation 5.3. Pour tout $a \in A$, on fixe :
- Une racine primitive λ_a de ρ_a dans K^{alg}.
- Une racine γ_a de l'équation $\rho_a(x) = 1/t$ dans $K(\!(t)\!)^{\mathrm{alg}}$.

Notons N le générateur unitaire d'un idéal non nul $\mathfrak{n}$. D'après (6), l'ensemble des points de $\mathfrak{n}$-torsion du module de Tate–Drinfeld est

$$\mathrm{TD}[\mathfrak{n}] = e_\Gamma(\rho_N^{-1}(\Gamma)/\Gamma) = \{e_\Gamma(\rho_c(\lambda_N) + \rho_d(\gamma_N)) \mid (c,d) \in A/\mathfrak{n} \times A/\mathfrak{n}\},$$

le dernier ensemble étant bien défini et indépendant des choix de λ_N et γ_N. Donc les sous A-modules de $\mathrm{TD}(K(\!(t)\!)^{\mathrm{sep}})_{\mathrm{tors}}$ isomorphes à $A/\mathfrak{n}$ et stables par le groupe de Galois absolu de $K(\!(t)\!)$ sont :

$$\mathrm{TD}_A e_\Gamma(\rho_c(\lambda_N) + \rho_d(\gamma_N)) \quad \text{avec } (c,d) \text{ d'ordre } \mathfrak{n} \text{ dans } (A/\mathfrak{n} \times A/\mathfrak{n})/(A/\mathfrak{n})^\times$$

(on fait agir $(A/\mathfrak{n})^\times$ diagonalement sur $A/\mathfrak{n} \times A/\mathfrak{n}$). Cet ensemble est en bijection naturelle avec la droite projective $\mathbb{P}^1(A/\mathfrak{n})$, donc avec l'ensemble $\Gamma_0(\mathfrak{n})\backslash\mathbb{P}^1(K)$ des pointes de $\mathscr{X}_0(\mathfrak{n})$.

5C3. *Interprétation modulaire.* Soit $C_\mathfrak{n}$ le sous-module de TD correspondant à $(1:0) = \infty$ dans $\mathbb{P}^1(A/\mathfrak{n})$, *i.e.*, $C_\mathfrak{n} = \mathrm{TD}_A e_\Gamma(\lambda_N)$. Le module de Tate–Drinfeld TD muni de $C_\mathfrak{n}$ définit, par interprétation modulaire, une section

$$\mathbf{s} : \mathrm{Spec}\, A[1/\mathfrak{n}][\![t^{q-1}]\!] \to \mathscr{Y}_0(\mathfrak{n})$$

du morphisme structurel. Soit $r : \mathrm{Spec}\, A[1/\mathfrak{n}] \to \mathrm{Spec}\, A[1/\mathfrak{n}][\![t^{q-1}]\!]$ le morphisme de schémas induit par $t^{q-1} \mapsto 0$ sur les anneaux.

Proposition 5.4. *Le morphisme* $\mathbf{s}$ *se prolonge en un morphisme*

$$\mathbf{s} : \mathrm{Spec}\, A[1/\mathfrak{n}][\![t^{q-1}]\!] \to \mathscr{X}_0(\mathfrak{n}),$$

qui vérifie $\mathbf{s} \circ r = \infty$. *De plus*, $\mathbf{s}$ *induit un isomorphisme entre le spectre formel de* $A[1/\mathfrak{n}][\![t^{q-1}]\!]$ *et le complété formel de* $\mathscr{X}_0(\mathfrak{n})$ *le long de la section* ∞.

Démonstration. Pour le prolongement, on se réfère à la démonstration du lemme 9.3 de [van der Heiden 2006]. Les autres assertions se déduisent de la proposition 9.1 et des théorèmes 9.2 et 10.3 de [loc.cit]. □

Le module de Tate–Drinfeld satisfait une propriété universelle : par changement de base, il décrit les modules de Drinfeld de rang 2 à réduction potentiellement stable de rang 1 *via* l'uniformisation de Tate–Drinfeld (théorème 7.8 de [van der Heiden 2006]). Conjointement à la proposition 5.4 et au lemme 5.1, cela amène au résultat suivant concernant l'interprétation modulaire de la pointe ∞.

Proposition 5.5. *Soit L une extension finie de K, d'anneau des entiers $\mathbb{O}_L$. Soit ϕ un module de Drinfeld de rang 2 sur L et P un point de $({}^{\phi}L)_{\mathrm{tors}}$ d'ordre $\mathfrak{n}$. En prenant ϕ et le sous-module cyclique engendré par P on définit un point de $X_0(\mathfrak{n})(L)$ qui se prolonge de façon unique en une section $x : \operatorname{Spec}\mathbb{O}_L \to X_0(\mathfrak{n})$. Supposons que ϕ a réduction potentiellement stable de rang 1 en une place $\mathfrak{L}$ de L. Alors la section x se spécialise comme ∞ en $\mathfrak{L}$ si et seulement si P donne un point entier d'un modèle potentiellement stable de ϕ.*

6. Formes modulaires de Drinfeld

6A. ***Formes modulaires de Drinfeld algébriques de poids 2.*** Les formes modulaires pour $\mathbb{F}_q[T]$, ou formes modulaires de Drinfeld, ont été introduites par Goss [1980a; 1980b] puis étudiées notamment par Gekeler [1988]. Dans cette section on présente un point de vue algébrique sur les formes modulaires de Drinfeld doublement paraboliques de poids 2 et de type 1 pour $\Gamma_0(\mathfrak{n})$, sans supposer $\mathfrak{n}$ premier.

Pour les formes modulaires classiques, on dispose de plusieurs constructions algébriques à la Serre, Katz [1973] ou encore Deligne et Rapoport [1973]. Elles ont été comparées notamment dans [Mazur 1977, section II.4] en poids 2 pour $\Gamma_0(n) \subset \mathrm{SL}_2(\mathbb{Z})$. Pour les formes modulaires de Drinfeld, on trouve dans la littérature les théories algébriques suivantes. Gekeler [1988, section 12] a donné un point de vue à la Serre des formes modulaires pour $\mathrm{GL}_2(A)$ modulo un idéal premier. Pour les formes modulaires de niveau $\Gamma(\mathfrak{n})$, Goss [1980b] a mis en place une théorie à la Katz. Nous présentons ici un point de vue algébrique pour $\Gamma_0(\mathfrak{n})$ *via* les sections du faisceau des différentielles relatives, qui couvrira nos besoins. Toutefois, il resterait à faire le lien entre cette approche et celles de Gekeler et Goss.

6A1. *Définition et t-développement.* Soit R une algèbre sur $A[1/\mathfrak{n}]$. Considérons le R-schéma $\mathscr{X}_R = \mathscr{X}_0(\mathfrak{n})_R = \mathscr{X}_0(\mathfrak{n}) \times_A R$ et son faisceau $\Omega^1_{\mathscr{X}_R/R}$ des différentielles relatives de degré 1. On adopte la définition suivante.

Définition 6.1. Soit $\mathrm{S}(R)$ le R-module $H^0(\mathscr{X}_R, \Omega^1_{\mathscr{X}_R/R})$ des sections globales de $\Omega^1_{\mathscr{X}_R/R}$. Un élément de $\mathrm{S}(R)$ est appelé une *forme modulaire sur R pour* $\Gamma_0(\mathfrak{n})$.

Posons $s = t^{q-1}$ où t désigne encore une indéterminée. Du morphisme

$$\mathbf{s}_R : \operatorname{Spec} R[\![s]\!] \to \mathscr{X}_R$$

déduit de $\mathbf{s}$, et de l'inclusion $i : R[\![s]\!] \hookrightarrow R[\![t]\!]$, on déduit un morphisme de schémas

$$\mathbf{t}_R : \operatorname{Spec} R[\![t]\!] \longrightarrow \mathscr{X}_R.$$

Définition 6.2. Soit $f \in \mathrm{S}(R)$. Il existe une unique série formelle $F(t) \in t^2 R[\![t]\!]$ telle que le tiré-en-arrière $\mathbf{t}_R^*(f)$ de f par $\mathbf{t}_R$ soit $(F(t)/t^2)\,\mathrm{d}t$. On appelle $F(t)$ le *t-développement de f* (en la pointe ∞).

Le facteur de normalisation $1/t^2$ sera justifié en 6A4.

Lemme 6.3. *On a* $F(t)/t \in sR[\![s]\!]$.

Démonstration. Comme $\mathbf{t}_R = \mathbf{s}_R \circ \mathrm{Spec}(i)$, on a $\mathbf{t}_R^*(f) = \mathrm{Spec}(i)^*(\mathbf{s}_R^*(f)) = \mathbf{s}_R^*(f)$. Or $\mathrm{d}s/s = -\mathrm{d}t/t$ en caractéristique p. Donc

$$\mathbf{t}_R^*(f) = \frac{F(t)}{t^2}\,\mathrm{d}t = -\frac{F(t)}{t}\,\frac{\mathrm{d}s}{s}.$$

La conclusion suit. □

Notation 6.4. En vertu du lemme 6.3, le t-développement de f est de la forme $F(t) = \sum_{i\geq 1} a_{1+i(q-1)} t^{1+i(q-1)} \in t^2 R[\![t]\!]$ soit encore, en posant $b_i = a_{1+i(q-1)}$ pour $i \geq 1$,

$$F(t) = \sum_{i\geq 1} b_i t^{1+i(q-1)} = t \sum_{i\geq 1} b_i s^i. \tag{7}$$

Proposition 6.5 (principe du t-développement). *L'homomorphisme de R-modules*

$$\mathrm{S}(R) \to t^2 R[\![t]\!], \quad f \mapsto F(t),$$

est injectif.

Démonstration. La démonstration de [Katz 1973, théorème 1.6.1] est encore valable dans notre contexte, en utilisant le fait que le schéma $\mathscr{X}_R$ est de Cohen–Macaulay, car il est lisse sur R. □

6A2. *Changement de base.* On pourra comparer l'énoncé suivant à la proposition II.3.3 de [Mazur 1977] pour les formes modulaires classiques.

Proposition 6.6. *Considérons un corps F qui est une extension de K ou le corps $\mathbb{F}_\mathfrak{l}$ (pour $\mathfrak{l}$ un premier étranger à $\mathfrak{n}$). L'application F-linéaire canonique*

$$\mathrm{S}(A[1/\mathfrak{n}]) \otimes_{A[1/\mathfrak{n}]} F \xrightarrow{\sim} \mathrm{S}(F)$$

est un isomorphisme.

Démonstration. Pour alléger les notations, on pose $\mathscr{X} = \mathscr{X}_0(\mathfrak{n})$ et $\Omega = \Omega^1_{\mathscr{X}_0(\mathfrak{n})/A[1/\mathfrak{n}]}$. Toute extension F de K, munie de sa structure canonique de $A[1/\mathfrak{n}]$-module, est plate. L'isomorphisme provient alors d'un théorème de changement de base plat pour la cohomologie des faisceaux quasi-cohérents et du fait que la formation de Ω commute aux changements de base sur $\mathrm{Spec}\, A[1/\mathfrak{n}]$ [Hartshorne 1977, III.9.3 et II.8.10].

Supposons maintenant $F = \mathbb{F}_\mathfrak{l}$ avec $\mathfrak{l}$ comme dans l'énoncé. Soit P un générateur de $\mathfrak{l}$. Le morphisme structurel $\mathscr{X} \to \mathrm{Spec}\, A[1/\mathfrak{n}]$ étant lisse, le faisceau Ω est inversible. En particulier, il est sans $A[1/\mathfrak{n}]$-torsion. Le morphisme de multiplication par P sur Ω est donc injectif. On a la suite exacte de faisceaux cohérents sur $\mathscr{X}$

$$0 \longrightarrow \Omega \xrightarrow{\cdot P} \Omega \longrightarrow \Omega/P\Omega = \Omega \otimes_{A[1/\mathfrak{n}]} \mathbb{F}_\mathfrak{l} = \Omega^1_{\mathscr{X}_{\mathbb{F}_\mathfrak{l}}/\mathbb{F}_\mathfrak{l}} \longrightarrow 0$$

car la formation de Ω commute aux changements de base. On en déduit la suite exacte longue en cohomologie

$$0 \to H^0(\mathscr{X}, \Omega) \xrightarrow{\cdot P} H^0(\mathscr{X}, \Omega) \to H^0(\mathscr{X}_{\mathbb{F}_\mathfrak{l}}, \Omega^1_{\mathscr{X}_{\mathbb{F}_\mathfrak{l}}/\mathbb{F}_\mathfrak{l}}) \to H^1(\mathscr{X}, \Omega) \xrightarrow{\cdot P} H^1(\mathscr{X}, \Omega).$$

L'application canonique

$$H^0(\mathscr{X}, \Omega) \otimes_{A[1/\mathfrak{n}]} \mathbb{F}_\mathfrak{l} \longrightarrow H^0(\mathscr{X}_{\mathbb{F}_\mathfrak{l}}, \Omega^1_{\mathscr{X}_{\mathbb{F}_\mathfrak{l}}/\mathbb{F}_\mathfrak{l}}) \tag{8}$$

est donc injective. De plus, son conoyau est le noyau de la multiplication par P sur $H^1(\mathscr{X}, \Omega)$. Le schéma $\mathscr{X}$ est régulier donc son faisceau dualisant est Ω. Par dualité de Grothendieck, $H^1(\mathscr{X}, \Omega)$ est le $A[1/\mathfrak{n}]$-dual de $H^0(\mathscr{X}, \mathbb{O}_\mathscr{X}) \simeq A[1/\mathfrak{n}]$. La multiplication par P sur $A[1/\mathfrak{n}]$ étant injective, l'application (8) est un isomorphisme. □

Proposition 6.7. *Le $A[1/\mathfrak{n}]$-module $\mathrm{S}(A[1/\mathfrak{n}])$ est libre de rang $g(X_0(\mathfrak{n}))$. Si F est comme dans la proposition 6.6, le F-espace vectoriel $\mathrm{S}(F)$ est de dimension $g(X_0(\mathfrak{n}))$.*

Démonstration. Reprenons les notations de la démonstration précédente et notons X la courbe $X_0(\mathfrak{n})$ sur K. Le faisceau Ω étant localement libre, le $A[1/\mathfrak{n}]$-module $H^0(\mathscr{X}, \Omega)$ est sans torsion, donc libre. Par ailleurs, d'après la proposition 6.6, on a

$$H^0(\mathscr{X}, \Omega) \otimes_{A[1/\mathfrak{n}]} K \simeq H^0(X, \Omega^1_{X/K}).$$

Donc le rang du $A[1/\mathfrak{n}]$-module $\mathrm{S}(A[1/\mathfrak{n}]) = H^0(\mathscr{X}, \Omega)$ est égal à la dimension sur K de $H^0(X, \Omega^1_{X/K})$ c'est-à-dire au genre géométrique de X. Cela démontre l'énoncé pour $\mathrm{S}(A[1/\mathfrak{n}])$. Celui pour $\mathrm{S}(F)$ s'en déduit par changement de base avec la proposition 6.6. □

6A3. *Opérateurs de Hecke.* On note $\mathcal{J}_0(\mathfrak{n})$ le modèle de Néron de $J_0(\mathfrak{n})$ sur $A[1/\mathfrak{n}]$. C'est un schéma abélien sur $A[1/\mathfrak{n}]$. Si G est un schéma en groupes lisse sur un schéma T, $\mathrm{Cot}\, G$ désigne l'espace cotangent de G le long de la section nulle. L'énoncé suivant s'inspire de [Mazur 1978, 2e].

Lemme 6.8. *On a un isomorphisme canonique*

$$\mathrm{Cot}(\mathcal{J}_0(\mathfrak{n})) \xrightarrow{\sim} \mathrm{S}(A[1/\mathfrak{n}]).$$

Démonstration. On pose $\mathscr{X} = X_0(\mathfrak{n})$ et $U = \mathrm{Spec}(A[1/\mathfrak{n}])$. Comme $\mathscr{X}$ est propre sur U, le foncteur $Pic^0_{\mathscr{X}/U}$ est représentable par un U-schéma lisse et séparé, noté $\mathrm{Pic}^0_{\mathscr{X}/U}$ [Bosch et al. 1990, théorème 9.4/2]. D'après le théorème 9.5/4 du même livre, le morphisme naturel $\mathrm{Pic}^0_{\mathscr{X}/U} \to \mathcal{J}_0(\mathfrak{n})$ identifie $\mathrm{Pic}^0_{\mathscr{X}/U}$ à la composante connexe de l'identité de $\mathcal{J}_0(\mathfrak{n})$. En passant aux espaces tangents en la section nulle sur U, on obtient l'isomorphisme $H^1(\mathscr{X}, \mathbb{O}_\mathscr{X}) \simeq \mathrm{Tan}\, \mathcal{J}_0(\mathfrak{n})$ (théorème 8.4/1 de [Bosch et al. 1990]). Par ailleurs, le schéma $\mathscr{X}$ sur U est régulier donc de Cohen–Macaulay.

Son faisceau dualisant est donc le faisceau $\Omega^1_{\mathscr{X}/U}$ des différentielles relatives de degré 1. La dualité de Grothendieck permet alors de voir $H^0(\mathscr{X}, \Omega^1_{\mathscr{X}/U})$ comme le $\mathbb{C}_U$-dual de $H^1(\mathscr{X}, \mathbb{C}_{\mathscr{X}})$. Par ailleurs, $\mathrm{Cot}\, \mathscr{J}_0(\mathfrak{n})$ est naturellement le $\mathbb{C}_U$-dual de $\mathrm{Tan}\, \mathscr{J}_0(\mathfrak{n})$. Par dualité, on obtient l'isomorphisme $H^0(\mathscr{X}, \Omega^1_{\mathscr{X}/U}) \simeq \mathrm{Cot}\, \mathscr{J}_0(\mathfrak{n})$. □

On utilise le lemme 6.8 pour faire opérer l'algèbre de Hecke $\mathbb{T}$ sur les formes modulaires de Drinfeld. Soit $\mathfrak{m}$ un idéal non nul de A. Les endomorphismes $T_\mathfrak{m}$ et $w_\mathfrak{m}$ de la jacobienne $J_0(\mathfrak{n})$ s'étendent en des endomorphismes de $\mathscr{J}_0(\mathfrak{n})$ (par propriété universelle des modèles de Néron), de l'espace cotangent $\mathrm{Cot}\, \mathscr{J}_0(\mathfrak{n})$ puis de $\mathrm{S}(A[1/\mathfrak{n}])$ (par le lemme). Pour F comme dans la proposition 6.6, on obtient des endomorphismes $T_\mathfrak{m}$ et $w_\mathfrak{m}$ de $\mathrm{S}(F)$ par extension des scalaires. Pour $\mathfrak{n} = \mathfrak{p}$ premier, l'espace de formes modulaires $\mathrm{S}(F)$ est donc muni d'une action de l'algèbre de Hecke $\mathbb{T}$, vue comme sous-algèbre de $\mathrm{End}_K\, J_0(\mathfrak{p})$. Comme F est de caractéristique p, l'algèbre $\mathbb{T}$ agit sur $\mathrm{S}(F)$ *via* son quotient $\mathbb{T}/p\mathbb{T}$. Cette action n'a pas de raison d'être fidèle.

Pour $\mathfrak{m}$ étranger à $\mathfrak{n}$ et $k \geq 0$, on a l'identité $T_{\mathfrak{m}^k} T_\mathfrak{m} = T_{\mathfrak{m}^{k+1}}$ dans $\mathrm{End}\, \mathrm{S}(F)$ à cause de la caractéristique positive, comme l'a remarqué Goss [1980b, proposition 3.3]. Ainsi, $T_{\mathfrak{q}\mathfrak{r}} = T_\mathfrak{q} T_\mathfrak{r}$ pour *tous* $\mathfrak{q}$ et $\mathfrak{r}$ premiers à $\mathfrak{n}$. C'est une différence importante avec les opérateurs de Hecke sur les formes modulaires classiques et sur les formes automorphes de $\mathrm{H}(\mathbb{C})$.

6A4. *Lien avec la théorie analytique.* Bien que nous n'en ferons usage qu'un usage limité (dans la proposition 7.17), on précise le lien entre les formes modulaires algébriques définies précédemment et les formes modulaires de Drinfeld analytiques. Soit $M^2_{2,1}(\Gamma_0(\mathfrak{n}))$ le $\mathbb{C}_\infty$-espace vectoriel des formes modulaires de Drinfeld de poids 2, de type 1 et doublement paraboliques pour $\Gamma_0(\mathfrak{n})$, au sens de [Gekeler et Reversat 1996]. Une telle forme modulaire possède un développement analytique en la pointe ∞ par rapport au paramètre $t(z) = \overline{\pi}^{-1}/e_A(z)$. Comme elle est doublement parabolique, ce développement est de la forme $\sum_{i\geq 2} a_i t(z)^i$, valable pour $|t(z)|$ suffisamment petit ($|\cdot|$ désigne la valeur absolue sur $\mathbb{C}_\infty$). Le groupe $\Gamma_0(\mathfrak{n})$ contenant les matrices $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix}\right)$ pour $\lambda \in \mathbb{F}_q^\times$, un calcul élémentaire montre que le développement est en fait de la forme $\sum_{i\geq 2} a_{1+i(q-1)} t(z)^{1+i(q-1)}$.

Proposition 6.9. *Soit $H^0(X_0(\mathfrak{n})^{\mathrm{an}}, \Omega^1_{\mathrm{an}})$ l'espace des formes différentielles holomorphes sur l'analytifiée $X_0(\mathfrak{n})^{\mathrm{an}}$ de $X_0(\mathfrak{n})$ sur $\mathbb{C}_\infty$. On a l'isomorphisme de $\mathbb{C}_\infty$-espaces vectoriels*

$$\begin{aligned} M^2_{2,1}(\Gamma_0(\mathfrak{n})) &\xrightarrow{\sim} H^0(X_0(\mathfrak{n})^{\mathrm{an}}, \Omega^1_{\mathrm{an}}) \simeq \mathrm{S}(\mathbb{C}_\infty) \\ f &\longmapsto -\frac{1}{\overline{\pi}} f(z)\mathrm{d}z. \end{aligned}$$

De plus, si f a pour développement $\sum_{i\geq 2} a_i t(z)^i$, la forme modulaire associée de $\mathrm{S}(\mathbb{C}_\infty)$ a pour t-développement $\sum_{i\geq 2} a_i t^i$.

Démonstration. Pour le premier isomorphisme, on renvoie au paragraphe 2.10 de [Gekeler et Reversat 1996] (leur définition de $t(z)$ diffère par une constante multiplicative). L'apparition des formes *doublement* paraboliques provient de la relation $\mathrm{d}z = -\overline{\pi}\,\mathrm{d}(t(z))\,/t(z)^2$, remarquée initialement par Goss [1980b]. Enfin, un énoncé de type GAGA identifie les formes différentielles algébriques sur la courbe projective $X_0(\mathfrak{n})_{\mathbb{C}_\infty}$ et analytiques sur $X_0(\mathfrak{n})^{\mathrm{an}}$. □

On peut voir que, par l'isomorphisme de la proposition 6.9, l'action de $T_{\mathfrak{m}}$ sur $\mathrm{S}(\mathbb{C}_\infty)$ correspond à l'endomorphisme de $M^2_{2,1}(\Gamma_0(\mathfrak{n}))$ défini par

$$T_{\mathfrak{m}}(f)(z) = \frac{1}{P} \sum_{\substack{a,b,d\in A \\ \deg b<\deg d \\ a,d \text{ unitaires} \\ (ad)=\mathfrak{m},(a)+\mathfrak{n}=A}} a^k f\left(\frac{az+b}{cz+d}\right),$$

où P est le générateur unitaire de $\mathfrak{m}$ (cette formule diffère de celles de [Goss 1980a,1980b, Gekeler 1988] par le facteur $1/P$).

6B. *Action de Hecke sur le t-développement.*

6B1. *Polynômes de Goss, opérateurs de Hecke et t-développement.* Ces rappels sur les polynômes de Goss sont dans le cas des réseaux finis issus de la torsion du module de Carlitz. Un traitement plus général est donné par Goss [1980b] et Gekeler [1988] pour les réseaux discrets de $\mathbb{C}_\infty$. On lui substitue une présentation algébrique plus adaptée à notre contexte.

Soit $\mathfrak{a}$ un idéal non nul de A, de générateur unitaire noté a et de degré d. Ici, ρ désigne le module de Carlitz sur K et $\Lambda_a = \rho[\mathfrak{a}]$. Le polynôme $\rho_a(x)$ étant additif, Λ_a est un $\mathbb{F}_q$-espace vectoriel de dimension finie. En s'inspirant de Goss, on introduit dans $K^{\mathrm{alg}}(X)$ avec une indéterminée X les quantités

$$S_{0,a}(X) = 0, \quad S_{j,a}(X) = \sum_{\lambda\in\Lambda_a} \frac{1}{(X+\lambda)^j}, \quad t_{\Lambda_a}(X) = \sum_{\lambda\in\Lambda_a} \frac{1}{X-\lambda} = \frac{1}{e_{\Lambda_a}(X)},$$

où $j \geq 1$ et $e_{\Lambda_a}(X) = X\prod_{\lambda\in\Lambda_a-\{0\}}(1 - X/\lambda)$ est l'exponentielle associée à Λ_a.

Proposition 6.10 [Goss 1980b, section 2 ; [Gekeler 1988, sections 3.4–3.9]]. *Pour tout entier $j \geq 1$, il existe un unique polynôme $G_{j,a}(X)$ dans $K[X]$ vérifiant $S_{j,a}(X) = G_{j,a}(t_{\Lambda_a}(X))$. Pour $j = 0$, on pose $G_{0,a}(X) = 0$. On a la formule explicite*

$$G_{j,a}(X) = \sum_{0\leq k<j} \sum_{\underline{i}} \binom{k}{\underline{i}} l^{\underline{i}} a^{-k} X^{k+1}, \tag{9}$$

avec les notations suivantes :

$\underline{i} = (i_0, \ldots, i_d)$ *parcourt les $(d+1)$-uplets d'entiers naturels vérifiant*

$$i_0 + \cdots + i_d = k \quad \text{et} \quad i_0 + i_1 q + \cdots + i_d q^d = j - 1.$$

$\binom{k}{\underline{i}}$ *est le coefficient multinomial* $k!/i_0!\cdots i_d!$ *évalué dans* $\mathbb{F}_p \subset K$.

$l^{\underline{i}} = l_0(a)^{i_0}\cdots l_d(a)^{i_d}$ *avec* $l_j(a) \in A$, *défini par* $\rho_a = \sum l_j(a)\tau^j \in A\{\tau\}$.

La formule (9) découle de [Gekeler 1988, 3.8] en remarquant que l'exponentielle $e_{\Lambda_a}(X)$ n'est autre que $\rho_a(X)/a$. De (9), on déduit que le polynôme $G_{j,a}(aX)$ est à coefficients dans A.

Notation 6.11. On garde les notations du paragraphe 5C2. Pour d diviseur unitaire de a, et b dans A de degré $< \deg b$, on pose

$$\chi_{a,d,b}(t) = \frac{1}{\rho_b(\lambda_d)+\rho_{a/d}(\gamma_d)} \in K(\!(t)\!)^{\mathrm{alg}}$$

et $\varphi_a(t) = \chi_{a,1,0}(t) = 1/(\rho_a(1/t)) \in A[\![t]\!]$. Noter que $\chi_{a,d,b}(t)$ dépend des choix de λ_d et γ_d.

Lemme 6.12. *Pour tout* $i \geq 0$, *on a l'égalité dans* $dA[\![t]\!]$

$$\sum_{\substack{b\in A\\ \deg b<\deg d}} \big(\chi_{a,d,b}(t)\big)^i = G_{i,d}(d\cdot\varphi_{a/d}(t)). \tag{10}$$

Cette quantité est indépendante des choix de λ_d *et* γ_d.

Démonstration. L'ensemble $\{\rho_b(\lambda_d) \mid \deg b < \deg d\}$ est le réseau $\Lambda_d = \rho[(d)]$. En utilisant la proposition 6.10, on voit que le membre de gauche de (10) est

$$\sum_{\lambda\in\Lambda_d} (\rho_{a/d}(\gamma_d)+\lambda)^{-i} = S_{i,d}(\rho_{a/d}(\gamma_d)) = G_{i,d}\Big(\frac{1}{e_{\Lambda_d}(\rho_{a/d}(\gamma_d))}\Big).$$

Par ailleurs, comme $e_{\Lambda_d}(X) = \rho_d(X)/d$, on a

$$d\cdot e_{\Lambda_d}(\rho_{a/d}(\gamma_d)) = \rho_d\rho_{a/d}(\gamma_d) = \rho_{a/d}\rho_d(\gamma_d) = \rho_{a/d}(1/t),$$

d'où l'égalité annoncée. Le membre de droite de (10) est dans $dA[\![t]\!]$, comme remarqué précédemment, et indépendant des choix de λ_d et γ_d. □

Jusqu'à la fin de la section 6B, la lettre F *désigne au choix l'anneau* $A[1/\mathfrak{n}]$, *une extension de corps de* K *ou le corps fini* $\mathbb{F}_\mathfrak{l}$ (*pour* $\mathfrak{l}$ *premier étranger à* $\mathfrak{n}$). L'énoncé qui suit est une généralisation de [Gekeler 1988, 7.3] pour les formes modulaires algébriques et les opérateurs de Hecke d'indice non nécessairement premier. Une version analytique en poids quelconque se trouve dans [Armana 2011a, proposition 5.2].

Proposition 6.13. *Soit* $f \in \mathrm{S}(F)$ *de* t*-développement* $\sum_{i\geq 2} a_i t^i$ *dans* $F[\![t]\!]$. *Soit* $\mathfrak{m}$ *premier à* $\mathfrak{n}$, *de générateur unitaire* M. *Alors le* t*-développement de la forme modulaire* $T_\mathfrak{m} f$ *est donné par*

$$\sum_{i\geq 2} \sum_{\substack{d\mid M\\ d\ \text{unitaire}}} \frac{M}{d^2} a_i G_{i,d}(d\cdot\varphi_{M/d}(t)) \in F[\![t]\!]. \tag{11}$$

Démonstration. L'expression est bien dans $F[\![t]\!]$ d'après le lemme 6.12. Par la proposition 6.6 de changement de base, il suffit d'établir (11) pour tout f dans $\mathrm{S}(A[1/\mathfrak{n}])$.

Explicitons la correspondance $T_\mathfrak{m}$. Reprenons les notations de la section 5C. Soit TD le module de Tate–Drinfeld sur $A[\![t]\!]$, construit à partir du module de Carlitz ρ et du réseau $\Gamma = \rho_A(1/t)$, qu'on munit de son A-module $C_\mathfrak{n}$. Comme $\mathfrak{m}$ est premier à $\mathfrak{n}$, les sous-groupes cycliques intervenant dans la définition de $T_\mathfrak{m}(\mathrm{TD}, C_\mathfrak{n})$ sont

$$C_\mathfrak{m} = \mathrm{TD}_A e_\Gamma(\lambda_M) \quad \text{et} \quad C_{d,b} = \mathrm{TD}_A e_\Gamma(\rho_b(\lambda_d) + \rho_{M/d}(\gamma_d)),$$

pour $(d, b) \in A \times A$ avec d diviseur unitaire de M, $d \neq 1$ et $\deg b < \deg d$.

Notons $E_{1,0}$ le module de Drinfeld de rang 2 construit à partir de ρ et du ρ-réseau $\Gamma' = \rho_A(1/\varphi_M(t)) = \rho_\mathfrak{m}(1/t)$ par uniformisation de Tate–Drinfeld. L'inclusion de réseaux $\Gamma' \subset \Gamma$ définit une isogénie $\mathrm{TD} \to E_{1,0}$ de noyau $C_\mathfrak{m}$. Donc $\mathrm{TD}/C_\mathfrak{m}$ n'est autre que $E_{1,0}$ et $(C_\mathfrak{n} + C_\mathfrak{m})/C_\mathfrak{m}$ est le A-module $C'_\mathfrak{n} = (E_{1,0})_A e_{\Gamma'}(\lambda_N)$.

On notera $E_{d,b}$ le module de Drinfeld de rang 2 construit à partir de ρ et du ρ-réseau $\Gamma'' = \rho_A(1/\chi_{M,d,b}(t))$ par uniformisation de Tate–Drinfeld. Nous avons $\rho_d(\Gamma'') = \rho_{(M/d)}(1/t) \subset \Gamma$. Le morphisme injectif et de conoyau fini $\rho_d : \Gamma'' \to \Gamma$ définit une isogénie $\mathrm{TD} \to E_{d,b}$ de noyau $C_{d,b}$. Donc $\mathrm{TD}/C_{d,b}$ n'est autre que $E_{d,b}$ et $(C_\mathfrak{n} + C_{d,b})/C_{d,b}$ est le A-module $C''_\mathfrak{n} = (E_{d,b})_A e_{\Gamma''}(\lambda_N)$.

On trouve donc

$$T_\mathfrak{m}(\mathrm{TD}, C_\mathfrak{n}) = (E_{1,0}, C'_\mathfrak{n}) + \sum_{d,b} (E_{d,b}, C''_\mathfrak{n}) = \sum_{(d,b)\in\mathscr{E}} (E_{d,b}, C), \tag{12}$$

avec $\mathscr{E}$ l'ensemble des $(d, b) \in A \times A$ avec d diviseur unitaire de M et $\deg b < \deg d$, et C vaut $C'_\mathfrak{n}$ si $d = 1$, $C''_\mathfrak{n}$ sinon.

Soit $\mathbf{t} = \mathbf{t}_{A[1/\mathfrak{n}]} : \mathrm{Spec}\, A[1/\mathfrak{n}][\![t]\!] \to \mathscr{X}_0(\mathfrak{n})$ le morphisme de 6A1. Soit $\chi_{d,b}$ l'homomorphisme d'anneaux $A[1/\mathfrak{n}][\![t]\!] \to K^{\mathrm{sep}}(\!(\gamma_d)\!)$ donné par $t \mapsto \chi_{M,d,b}(t)$. En composant $\mathrm{Spec}\, \chi_{d,b}$ avec $\mathbf{t}$, on obtient un morphisme de schémas

$$\mathbf{t}_{d,b} : \mathrm{Spec}\, K^{\mathrm{sep}}(\!(\gamma_d)\!) \to \mathscr{X}_0(\mathfrak{n}).$$

Soit $f \in \mathrm{S}(A[1/\mathfrak{n}])$ de t-développement $F(t)$. D'après (12), le t-développement de $T_\mathfrak{m} f$ est donné par

$$\mathbf{t}^*(T_\mathfrak{m} f) = \sum_{(d,b)\in\mathscr{E}} \mathbf{t}^*_{d,b}(f).$$

Un calcul élémentaire donne

$$\frac{\mathrm{d}(\chi_{M,d,b}(t))}{\chi_{M,d,b}(t)^2} = \frac{M}{d^2}\frac{\mathrm{d}t}{t^2}.$$

Donc $\mathbf{t}^*(T_\mathfrak{m} f)$ vaut

$$\sum_{(d,b)\in\mathscr{E}} (\mathrm{Spec}\, \chi_{d,b})^* \mathbf{t}^*(f) = \sum_{(d,b)} (\mathrm{Spec}\, \chi_{d,b})^* \Big(F(t)\frac{\mathrm{d}t}{t^2} \Big) = \sum_{(d,b)} F(\chi_{M,d,b}(t)) \frac{M}{d^2}\frac{\mathrm{d}t}{t^2}.$$

Comme $F(t)=\sum_{i\geq 2} a_i t^i$, le t-développement de $T_{\mathfrak{m}} f$ est donné par

$$\sum_{i\geq 2} a_i \sum_{(d,b)\in\mathscr{E}} \frac{M}{d^2}(\chi_{M,d,b}(t))^i = \sum_{i\geq 2} a_i \sum_{\substack{d\mid M\\ d \text{ unitaire}}} \frac{M}{d^2} \sum_{\deg b<\deg d} (\chi_{M,d,b}(t))^i.$$

On conclut alors à l'aide du lemme 6.12. □

Proposition 6.14. *Soit* $\mathfrak{m}$ *étranger à* $\mathfrak{n}$, *de degré* d *et générateur unitaire* M. *Soit* $f\in \mathrm{S}(F)$ *une forme modulaire de* t*-développement* $\sum_{i\geq 2} a_i(f)t^i$. *Alors le premier coefficient de* $T_{\mathfrak{m}} f$ *est* :

$$b_1(T_{\mathfrak{m}} f)=a_q(T_{\mathfrak{m}} f)=\sum_{\underline{m}} \binom{q-1}{\underline{m}} l^{\underline{m}} a_{1+m_0+m_1 q+\cdots+m_d q^d}(f),$$

la somme portant sur les $(d+1)$*-uplets d'entiers naturels* $(m_0,\dots,m_d)$ *vérifiant* $m_0+\cdots+m_d=q-1$. *La notation* $l^{\underline{m}}$ *désigne le produit de coefficients du module de Carlitz* : $l_0(M)^{m_0}\cdots l_d(M)^{m_d}$.

Démonstration. Cela provient de la proposition 6.13 et de (9) pour les polynômes de Goss. Pour les détails, on renvoie à [Armana 2011a, proposition 5.5]. □

6B2. *Opérateurs de Hecke de degré* 1 *et coefficients du* t*-développement.* Pour $\mathfrak{m}$ de degré 1, la proposition 6.14 donne

$$a_q(T_{\mathfrak{m}} f)=\sum_{i=0}^{q-1}\binom{q-1}{i} M^{q-i-1} a_{q+i(q-1)}(f) \tag{13}$$

(voir [Gekeler 1988, 7.4] pour un résultat similaire sur les formes modulaires de Drinfeld analytiques pour $\mathrm{GL}_2(A)$). Remarquons que le coefficient binomial $\binom{q-1}{i}$ est non nul dans $\mathbb{F}_p$, pour $0\leq i\leq q-1$, par le théorème de Lucas.

Théorème 6.15. *Considérons les éléments suivants de l'algèbre de Hecke* $\mathbb{T}\otimes_{\mathbb{Z}} A$:

$$\theta_j=-\binom{q-1}{j-1}^{-1}\sum_{\deg \mathfrak{m}=1} M^{j-1} T_{\mathfrak{m}} \quad (1\leq j\leq q-1).$$

$$\theta_q=-\sum_{\deg \mathfrak{m}=1}(M^{q-1}-1)T_{\mathfrak{m}}.$$

Supposons que $\mathfrak{n}$ *ne possède pas de diviseur de degré* 1. *Pour toute forme modulaire* $f\in \mathrm{S}(F)$ *pour* $\Gamma_0(\mathfrak{n})$, *on a*

$$b_j(f)=b_1(\theta_j f)\quad (1\leq j\leq q).$$

Un énoncé sensiblement plus général a été établi dans [Armana 2011a, théorème 7.2] pour les formes modulaires de Drinfeld analytiques de poids quelconque. Par commodité, on donne ici une preuve simplifiée du théorème 6.15.

Démonstration. On pose $a_i = a_i(f)$. Pour $n \geq 0$, notons $s_1(n)$ la somme des puissances $n$èmes des polynômes de degré 1 de A. À partir de (13), on obtient pour tout $j \geq 0$

$$a_q\Big(\sum_{\deg \mathfrak{m}=1} M^j T_{\mathfrak{m}} f\Big) = \sum_{i=0}^{q-1} s_1(j+q-i-1)\binom{q-1}{i} a_{q+i(q-1)}. \tag{14}$$

Il est bien connu que $s_1(n)$ vaut -1 pour $n > 0$ divisible par $q-1$, et 0 sinon. Donc pour $0 \leq j \leq q-2$, l'équation (14) se simplifie en

$$\begin{aligned} a_q\Big(\sum_{\deg \mathfrak{m}=1} M^j T_{\mathfrak{m}} f\Big) &= s_1(q-1)\binom{q-1}{j} a_{q+j(q-1)} \\ &= -\binom{q-1}{j} a_{1+(j+1)(q-1)}, \end{aligned} \tag{15}$$

et pour $j = q-1$, en

$$a_q\Big(\sum_{\deg \mathfrak{m}=1} M^{q-1} T_{\mathfrak{m}} f\Big) = -a_{q+(q-1)^2} - a_q.$$

En particulier, on trouve $a_{q+(q-1)^2} = a_q(-\sum_{\deg \mathfrak{m}=1} M^{q-1} T_{\mathfrak{m}} f - f)$. Or, pour $j=0$ l'équation (15) donne $a_q(\sum_{\deg \mathfrak{m}=1} T_{\mathfrak{m}} f) = -a_q$, d'où

$$a_{q+(q-1)^2} = a_q\Big(\sum_{\deg \mathfrak{m}=1} (1 - M^{q-1} T_{\mathfrak{m}}) f\Big) = a_q(\theta_q f). \qquad \square$$

6B3. *Points de Weierstrass et t-développement. Dans cette section, on suppose $\mathfrak{n} = \mathfrak{p}$ premier.* D'après la proposition 6.5, une forme modulaire de Drinfeld est déterminée de façon unique par son t-développement. Pour savoir combien de coefficients successifs du t-développement suffisent à la déterminer, on s'intéresse aux points de Weierstrass de la courbe $X_0(\mathfrak{p})$ sur K et en spécialisant aux places de bonne réduction.

Soit C une courbe algébrique projective lisse de genre $g \geq 2$ sur un corps k. On rappelle qu'un point x de C est de Weierstrass s'il existe une différentielle régulière non nulle dans $H^0(C, \Omega^1_{C/k})$ s'annulant à l'ordre $\geq g$ en x. De façon équivalente, par le théorème de Riemann–Roch, cela revient à l'existence d'une fonction rationnelle non nulle sur C régulière en-dehors de x et ayant un pôle d'ordre $\leq g$ en x.

Proposition 6.16 (d'après Ogg, Gekeler, Schweizer). *Soit $\mathfrak{p}$ premier de degré ≥ 3.*

(i) *Considérons un point K-rationnel de $X_0(\mathfrak{p})$ dont la réduction modulo $\mathfrak{p}$ n'est pas supersingulière (c'est-à-dire dont le module de Drinfeld de rang 2 sous-jacent n'est pas supersingulier sur $\mathbb{F}_{\mathfrak{p}}{}^{\mathrm{alg}}$; c'est le cas des pointes 0 et ∞). Alors ce point n'est pas de Weierstrass.*

(ii) *Soient* $\mathfrak{p}$ *premier de degré* 3 *et* $\mathfrak{l} \neq \mathfrak{p}$ *premier. La courbe* $X_0(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}} = \mathscr{X}_0(\mathfrak{p}) \times_A \mathbb{F}_\mathfrak{l}$ *est hyperelliptique sur* $\mathbb{F}_\mathfrak{l}$. *Les pointes* $0_{\mathbb{F}_\mathfrak{l}}$ *et* $\infty_{\mathbb{F}_\mathfrak{l}}$ *ne sont pas des points de Weierstrass sur cette courbe.*

Démonstration. (i) On adapte l'argument géométrique de Ogg [1978] pour les courbes modulaires classiques. Les détails se trouvent dans la preuve du lemme 7.6 de [Armana 2011a]. Ils sont énoncés pour la pointe ∞ mais restent valables pour les points de $X_0(\mathfrak{p})$ à réduction non supersingulière.

(ii) D'après [Gekeler 1986, corollaire 3.8], la courbe $X_0(\mathfrak{p})$ sur K est hyperelliptique pour $\deg \mathfrak{p} = 3$. On applique alors un argument de spécialisation remarqué par Schweizer [1997, lemme 17] : la courbe $X_0(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$ est hyperelliptique sur $\mathbb{F}_\mathfrak{l}$, dès que $\mathfrak{l}$ est distinct de $\mathfrak{p}$.

On sait que les points de Weierstrass d'une courbe hyperelliptique C sur un corps k sont les points de ramification de son morphisme séparable $C \to \mathbb{P}^1_k$ de degré 2, c'est-à-dire les points fixes de son involution hyperelliptique (voir par exemple [Liu 2002, exercice 7/4.7]). D'après [Gekeler 1986, corollaire 3.8], l'involution hyperelliptique de $X_0(\mathfrak{p})$ est $w_\mathfrak{p}$ (résultat étendu en niveau non premier par Schweizer [1997, théorème 20]). Donc l'involution hyperelliptique de $X_0(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$ est $(w_\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$. Les pointes $0_{\mathbb{F}_\mathfrak{l}}$ et $\infty_{\mathbb{F}_\mathfrak{l}}$ étant distinctes et échangées par $(w_\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$, ce ne sont pas des points fixes de $(w_\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$ ni des points de Weierstrass de $X_0(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$. □

Proposition 6.17. *Supposons l'une des conditions vérifiées* :

(i) F *est une extension de* K *et* $\deg \mathfrak{p} \geq 3$.

(ii) $F = \mathbb{F}_\mathfrak{l}$ *avec* $\mathfrak{l}$ *premier* $\neq \mathfrak{p}$ *et* $\deg \mathfrak{p} = 3$.

Posons $g = g(X_0(\mathfrak{p}))$. *Alors l'application* F*-linéaire*

$$\mathrm{S}(F) \to F^g, \quad f \mapsto (b_1(f), \ldots, b_g(f)),$$

est un isomorphisme.

Démonstration. Soit F comme dans l'énoncé. Posons $X_0(\mathfrak{p})_F = \mathscr{X}_0(\mathfrak{p}) \times_A F$. En la section ∞ sur $X_0(\mathfrak{p})$, on a le paramètre formel local $s = t^{q-1}$ (proposition 5.4). D'après l'équation (7), le développement formel d'une différentielle $f \in \mathrm{S}(F)$ est alors $\mathbf{t}_F^*(f) = -\sum_{i \geq 1} b_i(f) s^{i-1}\, ds$. Donc ∞ n'est pas un point de Weierstrass de $X_0(\mathfrak{p})_F$ si et seulement si toute différentielle s'annule à l'ordre $< g(X_0(\mathfrak{p})_F)$ en ∞, c'est-à-dire si l'application linéaire

$$\mathrm{S}(F) \to F^{g(X_0(\mathfrak{p})_F)}, \quad f \mapsto (b_1(f), \ldots, b_{g(X_0(\mathfrak{p})_F)}(f)),$$

est injective.

Le genre de la courbe $X_0(\mathfrak{p})_F$ est g. En effet, si F est une extension de K, c'est une conséquence du théorème de changement de base plat pour les faisceaux

quasi-cohérents (voir par exemple [Liu 2002, corollaire 5/2.27]). Par ailleurs, l'homomorphisme structurel $\mathscr{X}_0(\mathfrak{p}) \to \operatorname{Spec} A[1/\mathfrak{p}]$ est lisse et projectif, donc le genre arithmétique des fibres est égal au genre arithmétique de $X_0(\mathfrak{p})$. Donc la courbe $X_0(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}}$ est aussi de genre g.

Par la proposition 6.16, l'application linéaire de l'énoncé est donc injective pour $F = K$ et $F = \mathbb{F}_\mathfrak{l}$. Comme $\mathrm{S}(F)$ est aussi de dimension g (proposition 6.7), c'est un isomorphisme. Si F est une extension de K, on en déduit que $\mathrm{S}(F) \to F^g$ est un isomorphisme en étendant les scalaires de K à F par la proposition 6.6. □

Remarque 6.18. (i) La preuve montre que ∞ n'est pas un point de Weierstrass de $X_0(\mathfrak{p})_F$ pour tout extension F de K. Cela complète la proposition 6.16.

(ii) On a la conséquence suivante, dont on ne connaît pas d'autre démonstration : sous les hypothèses de la proposition 6.17, il existe une forme modulaire de Drinfeld f dans $\mathrm{S}(F)$ avec $b_1(f) \neq 0$.

7. Points rationnels de courbes modulaires de Drinfeld

7A. ***Spécialisation dans les quotients optimaux de $J_0(\mathfrak{p})$.*** La méthode de Mazur utilisait un résultat de spécialisation de Raynaud : si G est un schéma en groupes sur $\mathbb{Z}_l$ avec l premier ≥ 3, tout point d'ordre fini de $G(\mathbb{Z}_l)$ a même ordre que sa spécialisation en l [Mazur 1978, 1c]. Ce n'est plus vrai sur un anneau de valuation discrète de caractéristique p puisqu'on peut y construire des courbes elliptiques ayant un point d'ordre p et de spécialisation nulle. Cependant, on peut contourner cet écueil dans le cas des quotients optimaux de $J_0(\mathfrak{p})$.

Proposition 7.1. *Soit J' un quotient optimal de $J_0(\mathfrak{p})$ sur K c'est-à-dire un quotient de $J_0(\mathfrak{p})$ par une sous-variété abélienne définie sur K.*

(i) *La composante p-primaire de $J'(K)_{\mathrm{tors}}$ est nulle.*

(ii) *L'application de réduction $J'(K)_{\mathrm{tors}} \to J'(\mathbb{F}_\mathfrak{l})$ en un premier $\mathfrak{l}$ distinct de $\mathfrak{p}$ est injective.*

Démonstration. La première affirmation est le lemme 3.4 de [Pál 2010]. Notons $\mathscr{J}'$ le modèle de Néron de J' sur $A[1/\mathfrak{p}]$. L'application de réduction est définie comme suit : par propriété universelle des modèles de Néron, on a un isomorphisme canonique $J'(K) \simeq \mathscr{J}'(A[1/\mathfrak{p}])$ et la spécialisation en $\mathfrak{l} \neq \mathfrak{p}$ induit $J'(K) \to J'(\mathbb{F}_\mathfrak{l})$. La deuxième affirmation de l'énoncé, qui se déduit de la première, est essentiellement la proposition 9.4 de [Pál 2010] : elle reste valable en remplaçant $W(\mathfrak{p})$ par J', à condition de restreindre la spécialisation aux points d'ordre fini de $J'(K)$. □

7B. ***Gonalité de $X_0(\mathfrak{p})$.*** On utilisera à plusieurs reprises un résultat de Schweizer sur la gonalité de la courbe modulaire $X_0(\mathfrak{p})$. La gonalité d'une courbe algébrique C sur un corps k est le plus petit degré $\gamma_k(C)$ d'un morphisme k-rationnel dominant

$C \to \mathbb{P}^1$. Si C a un point rationnel, alors la gonalité est 1 si et seulement si le genre de C est nul, et la gonalité est 2 si et seulement si C est elliptique ou hyperelliptique. Pour une extension k' de k, notons $\gamma_{k'}(C)$ la gonalité de $C_{k'} = C \times_k k'$. On voit facilement que $\gamma_k(C) \geq \gamma_{k'}(C)$.

Proposition 7.2 [Schweizer 2003, lemme 2.2]. *On suppose encore* $\mathfrak{p}$ *premier. Si* $\widetilde{K}$ *est une extension finie purement inséparable de* K, *on a*

$$\gamma_K(X_0(\mathfrak{p})) \geq \gamma_{\widetilde{K}}(X_0(\mathfrak{p})) > \frac{q^{\deg \mathfrak{p}}}{(q^2+1)(q+1)}.$$

7C. ***Préliminaires.***

Notation 7.3. Pour simplifier, on pose dorénavant $\mathscr{X} = \mathscr{X}_0(\mathfrak{p})$, $X = X_0(\mathfrak{p})$, $J = J_0(\mathfrak{p})$ et J' un quotient optimal de J. Soient $\mathscr{J}$ et $\mathscr{J}'$ les modèles de Néron de J et J' sur $A[1/\mathfrak{p}]$.

Soit $d \geq 1$ entier. La puissance symétrique $d$ème $X^{(d)}$ est une variété lisse sur K [Milne 1986, sections 3–5]. Ses points sur K s'identifient aux diviseurs K-rationnels sur $X_{K^{\mathrm{sep}}}$ (c'est-à-dire invariants par l'action du groupe de Galois absolu de K) et effectifs de degré d. Notons $\infty^{(d)}$ et $0^{(d)}$ les sections $\operatorname{Spec} A[1/\mathfrak{p}] \to X^{(d)}$ déduites de ∞ et 0.

On définit un homomorphisme $\varphi^{(d)} : X^{(d)} \to J$ en associant à un diviseur effectif D de degré d la classe d'équivalence linéaire de $D - d(\infty)$. En composant avec le morphisme canonique $J \to J'$, on obtient

$$u^{(d)} : X^{(d)} \to J'.$$

Considérons un point de $Y_1(\mathfrak{p})$ défini sur une extension L/K de degré d. Son image par l'homomorphisme canonique $X_1(\mathfrak{p}) \to X$ est un point P de $X(L)$. Notons s et p^e ($e \geq 0$) les degrés séparable et inséparable de l'extension L/K et $\sigma_1, \ldots, \sigma_s$ les plongements de L dans K^{alg} fixant K. Le diviseur $\sum_{i=1}^{s} p^e \sigma_i(P)$ de $X_{K^{\mathrm{sep}}}$ est K-rationnel de degré $p^e s = d$. Il définit donc un point de $X^{(d)}(K)$.

Lemme 7.4. *On suppose* $J'(K)$ *fini et* $d < \deg \mathfrak{p}$. *Notons* E *l'ensemble des points de* $X^{(d)}(K)$ *provenant de* $Y_1(\mathfrak{p})(L)$ *pour* L/K *une extension de degré* d. *Alors* $u^{(d)}(w_{\mathfrak{p}}(E)) = \{0\}$ *dans* $J'(K)$.

Démonstration. Soit $x \in E$. Notons $y \in Y_1(\mathfrak{p})(L)$ et $P \in X(L)$ les points dont il provient. La variété $X^{(d)}$ possède un modèle $\mathscr{X}^{(d)}$ propre sur $A[1/\mathfrak{p}]$. Donc x se prolonge naturellement en une section du morphisme structurel $\mathscr{X}^{(d)} \to \operatorname{Spec} A[1/\mathfrak{p}]$ encore notée x. Fixons un premier $\mathfrak{l}$ de degré 1 (en particulier, $\mathfrak{l} \neq \mathfrak{p}$). D'après la proposition 5.2, en toute place $\mathfrak{L}$ de L au-dessus de $\mathfrak{l}$, le module de Drinfeld sous-jacent à P n'a ni bonne réduction potentielle, ni réduction potentiellement stable de rang 1 avec point entier. Comme il n'a pas bonne réduction potentielle,

la spécialisation de P en $\mathfrak{L}$ est nécessairemment une pointe, c'est-à-dire 0 ou ∞. Or, par la proposition 5.5, cette spécialisation est nécessairemment 0. Donc x se spécialise comme $0^{(d)}$ en $\mathfrak{l}$. Posons $x' = w_{\mathfrak{p}}(x)$. L'involution échangeant les pointes, x' et $\infty^{(d)}$ ont même spécialisation. Donc $u^{(d)}(x')$ se spécialise en 0 dans $J'(\mathbb{F}_{\mathfrak{l}})$. Par ailleurs, comme $J'(K)$ est fini, le point $u^{(d)}(x')$ est de torsion dans $J'(K)$. Donc $u^{(d)}(x')$ est nul par le résultat de spécialisation (proposition 7.1(ii)). □

7D. *Points rationnels pour $\mathfrak{p}$ de petit degré.*

7D1. *Points de $Y_1(\mathfrak{p})$ pour $\mathfrak{p}$ de petit degré.*

Théorème 7.5. (i) *Soit $\mathfrak{p}$ de degré 3. La courbe $Y_1(\mathfrak{p})$ n'a pas de point L-rationnel pour toute extension L/K de degré ≤ 2.*

(ii) *Supposons que $\mathfrak{p}$ est tel que toute forme primitive de $\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$ est de rang analytique ≤ 1. Soit L/K une extension de degré*

$$[L:K] < \min\left(\deg \mathfrak{p},\ \frac{q^{\deg \mathfrak{p}}}{2(q^2+1)(q+1)}\right).$$

Ces conditions sont vérifiées pour $\deg \mathfrak{p} = 4$ et $[L:K] \leq d$ avec $d = 2$ si $q = 5$, $d = 3$ si $q \geq 7$. Alors la courbe $Y_1(\mathfrak{p})$ n'a pas de point L-rationnel.

(iii) *Soit $\mathfrak{p}$ de degré 4. La courbe $Y_1(\mathfrak{p})$ n'a pas de point K-rationnel.*

Revenons sur la condition sur le rang analytique des formes primitives de $\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$. Elle se reformule ainsi : pour toute orbite $[F] \in \mathbb{O}$, la variété abélienne $J_{[F]}$ est de rang analytique inférieur ou égal à sa dimension sur K. Calculer l'ordre d'annulation des fonctions L de formes primitives de $\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$ peut se faire sur machine, par exemple grâce aux symboles modulaires pour $\mathbb{F}_q(T)$. La condition peut être donc testée numériquement. Nous l'avons vérifiée pour tous les idéaux premiers $\mathfrak{p}$ de degré 5 dans $\mathbb{F}_2[T]$ et, par exemple, pour

$$(T^5+T^3-T^2-T+1),\ (T^5+T^4+T^3-T^2+T-1),\ (T^5-T^4-T^2-1) \subset \mathbb{F}_3[T].$$

Comme expliqué dans l'introduction, la condition n'est certainement pas vérifiée de façon systématique, mais on s'attend à ce qu'elle le soit assez fréquemment.

Démonstration. Supposons qu'il existe un point y de $Y_1(\mathfrak{p})(L)$ sur une extension L/K de degré d. Par la construction donnée en 7C, il définit des points $P \in X(L)$ et $x \in X^{(d)}(K)$.

(i) Comme $d \leq 2 < \deg \mathfrak{p}$ et $J(K)$ est fini (proposition 4.4), on peut appliquer le lemme 7.4 à J : le point $z = u^{(d)}(w_{\mathfrak{p}}(x))$ est nul dans $J(K)$. Donc le diviseur $\sum_{i=1}^{s} p^e \sigma_i(w_{\mathfrak{p}}(P)) - d(\infty)$ est principal sur K^{alg}. L'interprétation modulaire de P assure qu'il est non nul. Notons f une fonction rationnelle non nulle sur X définie sur K^{alg} dont c'est le diviseur. La courbe $X_{K^{\mathrm{alg}}}$ est de genre $g(X_0(\mathfrak{p}))$ qui est,

d'après la proposition 3.2, supérieur ou égal à $\deg(\mathfrak{p})-1$ dès que $\deg\mathfrak{p}\geq 3$. Donc la fonction f possède un pôle unique en ∞ d'ordre $d\leq\deg(\mathfrak{p})-1\leq g(X_0(\mathfrak{p}))$ et est régulière ailleurs. Cela contredit le fait que ∞ n'est pas un point de Weierstrass de $X_{K^{\mathrm{alg}}}$ (voir la remarque 6.18).

(ii) D'après l'hypothèse sur $\mathfrak{p}$, la variété abélienne $J'=J_0(\mathfrak{p})^-$ est de groupe de Mordell–Weil fini sur K (propositions 4.3 et 4.5). Comme $d<\deg\mathfrak{p}$, on peut appliquer le lemme 7.4 à J' : le point $z=u^{(d)}(w_{\mathfrak{p}}(x))$ est nul dans $J'(K)$. Donc $\varphi^{(d)}(w_{\mathfrak{p}}(x))$ appartient à la sous-variété abélienne $(1+w_{\mathfrak{p}})J$. On en déduit que $(1-w_{\mathfrak{p}})\varphi^{(d)}(w_{\mathfrak{p}}(x))$ est nul dans $J(K)$. Le diviseur

$$D=w_{\mathfrak{p}}(x)-d(0)-(x)+d(\infty)=\sum_i p^e w_{\mathfrak{p}}(\sigma_i(P))+d(\infty)-\sum_i p^e\sigma_i(P)-d(0)$$

est principal sur K^{alg}, donc sur une extension finie purement inséparable $\widetilde{K}$ de K. De plus, il est non nul : en effet, on a $\infty\neq 0$ et $\sigma_i(P)\neq\infty$ pour tout i, par interprétation modulaire de P. Ainsi, le diviseur D définit un morphisme $\widetilde{K}$-rationnel non constant $X_{\widetilde{K}}\to\mathbb{P}^1$ de degré $p^e s+d=2d$. La borne de Schweizer pour la gonalité (proposition 7.2) donne $2d>q^{\deg\mathfrak{p}}/((q^2+1)(q+1))$. Cela contredit l'hypothèse de l'énoncé sur d.

(iii) Reprenons l'argument et les notations de (ii) avec $\deg\mathfrak{p}=4$ et $d=1$. On obtient un morphisme $\widetilde{K}$-rationnel non constant $X_{\widetilde{K}}\to\mathbb{P}^1$ de degré 2. Donc la courbe $X_{\widetilde{K}}$ est rationnelle, elliptique ou hyperelliptique. Par le lemme 6 de [Schweizer 1997], la courbe $X_0(\mathfrak{p})$ a la même propriété sur K. Comme $\deg\mathfrak{p}=4$, cela contredit la classification de [Schweizer 1997, théorème 20]. □

7D2. *Résultats partiels sur les points de* $Y_0(\mathfrak{p})$. Ils sont obtenus par une variante des démonstrations précédentes.

Proposition 7.6. *Soit* $\mathfrak{p}$ *de degré* 3 *ou* 4. *Soit* ϕ *un module de Drinfeld de rang* 2 *sur* K *possédant une isogénie* K*-rationnelle cyclique d'ordre* $\mathfrak{p}$. *Alors* ϕ *a bonne réduction potentielle en tout idéal premier distinct de* $\mathfrak{p}$.

Démonstration. On pourra comparer l'argument suivant avec [Mazur 1978, corollaire 4.3]. Un module de Drinfeld comme dans l'énoncé correspond, par l'interprétation modulaire, à un point x de $Y_0(\mathfrak{p})(K)$. Notons encore x son prolongement en une section du morphisme structurel $\mathscr{X}\to\operatorname{Spec}A[1/\mathfrak{p}]$. Supposons qu'il existe un premier $\mathfrak{l}\neq\mathfrak{p}$ en lequel ϕ n'a pas bonne réduction potentielle. Alors ϕ a réduction potentiellement stable de rang 1. Donc x se spécialise en $\mathfrak{l}$ comme ∞ ou 0. Les pointes étant permutées par $w_{\mathfrak{p}}$, quitte à remplacer x par $w_{\mathfrak{p}}(x)$, on peut supposer que x et ∞ ont même spécialisation. Si $\mathfrak{p}$ est de degré 3 (respectivement de degré 4), on prend pour J' la jacobienne $J=J_0(\mathfrak{p})$ (respectivement le quotient $J_0(\mathfrak{p})^-$). On a vu dans la section 4B que le groupe de Mordell–Weil de ces variétés abéliennes est fini. Comme $u^{(1)}(x)$ se spécialise en $\mathfrak{l}$ comme 0, la proposition 7.1 assure que

$u^{(1)}(x) = 0$ dans J'. On conclut alors comme dans le théorème 7.5 (i) et (iii) pour $d = 1$. □

Lemme 7.7. *Soient $q \geq 5$ et $\mathfrak{p}$ de degré ≥ 4. Pour $\mathfrak{l}$ premier distinct de $\mathfrak{p}$, on pose $\eta_\mathfrak{l} = T_\mathfrak{l} - (q^{\deg \mathfrak{l}} + 1)$ dans $\mathbb{T}$. L'ensemble des éléments x de $X(K)$ tels que $\eta_\mathfrak{l}(x) = \eta_\mathfrak{l}(w_\mathfrak{p}(x))$, comme diviseurs de degré nul sur X, est égal à $\{0, \infty\}$.*

Démonstration. Pour un tel x, on a l'égalité de diviseurs sur X

$$T_\mathfrak{l}(x) + (q^{\deg \mathfrak{l}} + 1)(w_\mathfrak{p}(x)) = T_\mathfrak{l}(w_\mathfrak{p}(x)) + (q^{\deg \mathfrak{l}} + 1)(x). \tag{16}$$

Pour $\deg \mathfrak{n} \geq 3$ avec $\mathfrak{n}$ non nécessairemment premier, Schweizer [2003, remarque 4.6] a établi la liste des points K-rationnels CM de $X_0(\mathfrak{n})$. Lorsque $\mathfrak{n} = \mathfrak{p}$ premier, il n'en existe que si $\deg \mathfrak{p} = 3$. Donc ici x n'est pas un point K-rationnel CM de X, c'est-à-dire $w_\mathfrak{p}(x) \neq x$. D'après l'équation (16), on en déduit que le diviseur $T_\mathfrak{l}(x) - (q^{\deg \mathfrak{l}} + 1)(x)$ est effectif. Par ailleurs, il est de degré nul. Donc $T_\mathfrak{l}(x) = (q^{\deg \mathfrak{l}} + 1)(x)$.

La conjecture de Ramanujan–Petersson, démontrée dans ce cadre par Drinfeld [1988], affirme que les valeurs propres de $T_\mathfrak{l}$, opérant sur $\mathrm{H}(\mathbb{C})$, sont des entiers algébriques de valeur absolue $\leq 2q^{(\deg \mathfrak{l})/2}$. Ainsi, les valeurs propres de $\eta_\mathfrak{l}$ sont non nulles. Le noyau de $\eta_\mathfrak{l}$, vu comme élément de $\mathbb{T} \otimes_\mathbb{Z} \mathbb{Q} \subset \mathrm{End}_K\, J \otimes \mathbb{Q}$, est alors nul. De $\eta_\mathfrak{l}(x) = 0 = \eta_\mathfrak{l}(\infty)$, on déduit $(x) - (\infty) = 0$ dans $J(K) \otimes_\mathbb{Z} \mathbb{Q}$. Donc la classe du diviseur $(x) - (\infty)$ appartient à $J(K)_{\mathrm{tors}}$. Par un théorème de Pál [2005, théorème 1.4], ce groupe est égal au sous-groupe cuspidal. Ce dernier étant annulé par $(1 + w_\mathfrak{p})$, la classe de $(1 + w_\mathfrak{p})((x) - (\infty))$ est donc nulle dans $J(K)$.

Notons X^+ la courbe $w_\mathfrak{p} \backslash X$ sur K, ∞^+ son unique pointe et J^+ sa jacobienne. On a le diagramme commutatif

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & J \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi_*} \\ X^+ & \xrightarrow{\varphi^+} & J^+, \end{array}$$

où π est la projection canonique, π_* le morphisme qui s'en déduit par fonctorialité d'Albanese, $\varphi = \varphi^{(1)}$ l'application d'Abel–Jacobi normalisée par $\varphi(\infty) = 0$, de même pour φ^+ normalisée par $\varphi^+(\infty^+) = 0$. D'après ce qui précède, le diviseur $\pi_*((1+w_\mathfrak{p})((x)-(\infty))) = 2((x^+)-(\infty^+))$ est linéairement équivalent à 0 dans J^+.

Supposons x^+ distinct de ∞^+. Alors le diviseur $(x^+) - (\infty^+)$ est non nul et sa classe est d'ordre 1 ou 2 dans $J^+(K)$. Supposons qu'elle soit d'ordre 2. Le diviseur $2((x^+) - (\infty^+))$ étant non nul et principal sur K, il définit un morphisme K-rationnel non constant $X^+ \to \mathbb{P}^1$ de degré 2. En composant avec $\pi : X \to X^+$ qui est dominant, on obtient un morphisme K-rationnel dominant $X \to \mathbb{P}^1$ de degré 4. Donc la gonalité de X sur K est ≤ 4. Comme $q \geq 5$ et $\deg \mathfrak{p} \geq 4$, cela contredit

la minoration de la proposition 7.2. Ainsi, le diviseur $(x^+) - (\infty^+)$ est non nul et linéairement équivalent à 0. Comme précédemment, on en déduit un morphisme K-rationnel dominant $X^+ \to \mathbb{P}^1$ de degré 1. Donc la courbe X^+ serait de genre nul. En particulier, le morphisme K-rationnel $\pi : X \to X^+ \simeq \mathbb{P}^1$ est dominant de degré 2. La courbe modulaire X serait rationnelle, elliptique ou hyperelliptique. Mais comme $\deg \mathfrak{p} \geq 4$, elle est de genre > 1 et n'est pas hyperelliptique d'après [Schweizer 1997, théorème 20]. En conclusion on a $x^+ = \infty^+$ c'est-à-dire x est dans $\{0, \infty\}$. □

Théorème 7.8. *Soit $q \geq 5$. Supposons $\mathfrak{p}$ de degré ≥ 5 tel que toute forme primitive de $\mathrm{H}_{\mathfrak{p}}(\mathbb{C})$ est de rang analytique ≤ 1. Alors la courbe $Y_0(\mathfrak{p})$ n'a pas de point K-rationnel* (i.e., *il n'existe pas de module de Drinfeld de rang 2 sur K avec une isogénie K-rationnelle cyclique d'ordre $\mathfrak{p}$*).

Cet énoncé partage la même condition sur le rang analytique des formes primitives que le théorème 7.5(ii). Des outils appropriés sur machine devraient permettre d'exhiber des couples $(q, \mathfrak{p})$ où le théorème 7.8 s'applique (nous n'avons pas eu l'occasion de le faire).

Démonstration. Supposons qu'il existe $x \in Y_0(\mathfrak{p})(K)$. Considérons le morphisme $f : X \to J$ qui envoie P sur la classe d'équivalence linéaire de $(P) - (w_{\mathfrak{p}}(P))$. L'image de f, qui est anti-invariante par $w_{\mathfrak{p}}$, est donc contenue dans la plus grande sous-variété abélienne de J annulée par $(1 + w_{\mathfrak{p}})$. Cette variété abélienne est notée J_-. Elle est naturellement isogène à $J^- = J/(1 + w_{\mathfrak{p}})J$ sur K, dont le groupe de Mordell–Weil est fini d'après l'hypothèse sur $\mathfrak{p}$ et la proposition 4.5. Donc $f(x)$ appartient à $J_-(K) \hookrightarrow J(K)_{\mathrm{tors}}$. Par un théorème de Pál [2005, théorème 1.4] ce sous-groupe de torsion est égal au sous-groupe cuspidal. Ce dernier étant annulé par $\eta_{\mathfrak{l}}$, on a alors $\eta_{\mathfrak{l}}(f(x)) = 0$ dans $J(K)$ pour un premier $\mathfrak{l} \neq \mathfrak{p}$. Le diviseur $T_{\mathfrak{l}}(x) + (q+1)(w_{\mathfrak{p}}(x)) - T_{\mathfrak{l}}(w_{\mathfrak{p}}(x)) - (q+1)(x)$ est non nul, d'après le lemme 7.7, et principal sur K. Il définit donc une fonction K-rationnelle non constante $X \to \mathbb{P}^1$ de degré $\leq 2(q+1)$. Donc la gonalité de X sur K est $\leq 2(q+1)$. Comme $q \geq 5$ et $\deg \mathfrak{p} \geq 5$, on obtient une contradiction avec la proposition 7.2. □

7E. *Points rationnels : étude du cas général.*

7E1. *L'argument de Mazur.* On reprend les notations introduites en 7C. Par propriété universelle, $\varphi^{(d)}$ et $u^{(d)}$ se prolongent de façon unique en des homomorphismes de $A[1/\mathfrak{p}]$-schémas $\varphi^{(d)} : \mathscr{X}^{(d)} \to \mathscr{J}$ et $u^{(d)} : \mathscr{X}^{(d)} \to \mathscr{J}'$.

L'argument de Mazur utilise une propriété des immersions formelles. Soient $f : Y \to Z$ un morphisme de schémas noethériens, y un point de Y et $z = f(y)$. On dit que f est une *immersion formelle en y* si le morphisme d'anneaux $\widehat{\mathcal{O}}_{Z,z} \to \widehat{\mathcal{O}}_{Y,y}$ déduit de f par passage aux complétés est surjectif. D'après le lemme de Nakayama, cela revient à demander à ce que f induise une bijection entre les corps

résiduels en z et y et l'application déduite de f par passage aux espaces cotangents en z et y soit surjective. Si de plus Y est séparé de type fini, une immersion formelle f vérifie la propriété suivante : soient T un schéma intègre noethérien et t un point de T ; deux morphismes $T \to Y$ envoyant t sur y et qui coïncident après composition par f sont alors égaux.

On pourra comparer l'énoncé suivant à [Mazur 1978, corollaire 4.3] et [Kamienny 1992b, lemme 3.2, théorème 3.3].

Proposition 7.9. *Fixons un premier* $\mathfrak{l}$. *Soit* $\mathfrak{p}$ *un premier de degré* $> d \deg \mathfrak{l}$ *tel que les propriétés suivantes sont vérifiées* :

(i) $J'(K)$ *est fini.*

(ii) $u^{(d)} : \mathscr{X}^{(d)} \to \mathscr{J}'$ *est une immersion formelle en* $\infty_{\mathfrak{l}}^{(d)}$ (*la restriction de* $\infty^{(d)}$ *à la fibre spéciale en* $\mathfrak{l}$).

Alors pour toute extension L/K *de degré* d, *la courbe* $Y_1(\mathfrak{p})$ *n'a pas de point* L-*rationnel.*

Démonstration. S'il existe, un point y de $Y_1(\mathfrak{p})(L)$ définit $P \in X(L)$ et $x \in X^{(d)}(K)$ comme expliqué au paragraphe 7C. Par le lemme 7.4, on trouve que $u^{(d)}(w_{\mathfrak{p}}(x))$ est nul dans $J'(K)$. En particulier, on a $u^{(d)}(w_{\mathfrak{p}}(x)) = u^{(d)}(w_{\mathfrak{p}}(0))$ dans $\mathscr{J}'(A[1/\mathfrak{p}])$. De plus, $w_{\mathfrak{p}}(x)$ et $\infty^{(d)}$ ont même spécialisation en $\mathfrak{l}$ (voir la preuve du lemme 7.4). La propriété rappelée pour l'immersion formelle $u^{(d)}$ en $\infty_{\mathfrak{l}}^{(d)}$ assure que les sections $w_{\mathfrak{p}}(x)$ et $\infty^{(d)}$ coïncident. Donc P est la pointe 0. Cela contredit l'interprétation modulaire de P. □

7E2. *Espaces cotangents et immersion formelle.* Implicitement, les espaces cotangents aux variétés abéliennes seront pris en la section nulle, ceux à $\mathscr{X}^{(d)}$ en la section $\infty^{(d)}$.

L'algèbre $\mathbb{T}$ opère naturellement sur l'espace cotangent $\mathrm{Cot}\,\mathscr{J}$ comme suit. Tout élément u de $\mathbb{T}$, vu comme endomorphisme de J sur K, s'étend de façon unique au modèle de Néron $\mathscr{J}$. Par passage aux espaces cotangents, il induit un endomorphisme de $\mathrm{Cot}\,\mathscr{J}$ qu'on note $\mathrm{cot}(u)$.

Jusqu'à la fin de 7E2, on suppose l'hypothèse 4.9 satisfaite par un idéal I *de* $\mathbb{T}$. Soit $J'_{\mathbf{e}}(\mathfrak{p})$ le quotient raffiné relatif à I et $\mathscr{J}'_{\mathbf{e}}(\mathfrak{p})$ son modèle de Néron. Commençons par donner un critère pour l'immersion formelle. Pour un idéal $\mathscr{I}$ de $\mathbb{T}$ et un espace V sur lequel $\mathbb{T}$ opère, on note $V[\mathscr{I}]$ le sous-espace annulé par $\mathscr{I}$.

Proposition 7.10. *Soit* $\mathfrak{l}$ *un premier distinct de* $\mathfrak{p}$. *Si l'application naturelle*

$$(\mathrm{Cot}\,\mathscr{J}_{\mathbb{F}_{\mathfrak{l}}})[\tilde{I}_{\mathbf{e}}] \longrightarrow \mathrm{Cot}\,\mathscr{X}^{(d)}_{\mathbb{F}_{\mathfrak{l}}}$$

déduite de $\varphi^{(d)}$ *est surjective*, *le morphisme* $u^{(d)} : \mathscr{X}^{(d)} \to \mathscr{J}'_{\mathbf{e}}(\mathfrak{p})$ *est une immersion formelle en* $\infty_{\mathfrak{l}}^{(d)}$.

Démonstration. Soit $\pi : J \to J'_{\mathbf{e}}(\mathfrak{p})$ le morphisme canonique, qui s'étend aux modèles de Néron, et $\pi^* : \mathrm{Cot}\, \mathcal{J}'_{\mathbf{e}}(\mathfrak{p}) \to \mathrm{Cot}\, \mathcal{J}$ le morphisme obtenu par passage aux espaces cotangents. On commence par montrer que l'image de π^* contient $(\mathrm{Cot}\, \mathcal{J})[\tilde{I}_{\mathbf{e}}]$.

Par (J3) de l'hypothèse 4.9, il existe des éléments $\hat{t}$ dans $\hat{I}$ et $\tilde{t}$ dans $\tilde{I}_{\mathbf{e}}$ avec $1 = \hat{t} + \tilde{t}$ dans $\mathbb{T}$. Regardons $\hat{t}$ comme un endomorphisme de J. Comme $\hat{t}$ annule I, le morphisme $\hat{t} : J \to J$ se factorise par π. Le diagramme se prolonge aux modèles de Néron, par propriété universelle. En passant aux espaces cotangents, on en déduit le diagramme commutatif :

$$\begin{array}{ccc} \mathrm{Cot}\, \mathcal{J} & \longrightarrow & \mathrm{Cot}\, \mathcal{J}'_{\mathbf{e}}(\mathfrak{p}) \\ & \searrow^{\cot(\hat{t})} & \downarrow \pi^* \\ & & \mathrm{Cot}\, \mathcal{J}. \end{array}$$

En particulier, l'image du morphisme π^* contient $\cot(\hat{t})(\mathrm{Cot}\, \mathcal{J})[\tilde{I}_{\mathbf{e}}]$. Comme la relation $1 = \hat{t} + \tilde{t}$ est encore valable sur $\mathcal{J}$, on a

$$\cot(\hat{t})(\mathrm{Cot}\, \mathcal{J})[\tilde{I}_{\mathbf{e}}] = \cot(1 - \tilde{t})(\mathrm{Cot}\, \mathcal{J})[\tilde{I}_{\mathbf{e}}] = (\mathrm{Cot}\, \mathcal{J})[\tilde{I}_{\mathbf{e}}].$$

Donc l'image de π^* contient $(\mathrm{Cot}\, \mathcal{J})[\tilde{I}_{\mathbf{e}}]$. En passant aux fibres en $\mathfrak{l}$ et en utilisant l'hypothèse de l'énoncé, on voit que l'homomorphisme $\mathrm{Cot}\, \mathcal{J}'_{\mathbf{e}}(\mathfrak{p})_{\mathbb{F}_\mathfrak{l}} \to \mathrm{Cot}\, \mathscr{X}^{(d)}_{\mathbb{F}_\mathfrak{l}}$ déduit de $u^{(d)}$ est alors surjectif. Donc $u^{(d)}$ est une immersion formelle en $\infty^{(d)}_\mathfrak{l}$. □

Afin de reformuler la surjectivité de $(\mathrm{Cot}\, \mathcal{J}_{\mathbb{F}_\mathfrak{l}})[\tilde{I}_{\mathbf{e}}] \longrightarrow \mathrm{Cot}\, \mathscr{X}^{(d)}_{\mathbb{F}_\mathfrak{l}}$, on rend explicite ce morphisme. Notons $\mathrm{S}_\mathfrak{p} = \mathrm{S}(A[1/\mathfrak{p}])$ comme dans l'introduction. Rappelons que, d'après le lemme 6.8, on a un isomorphisme canonique

$$\mathrm{Cot}\, \mathcal{J} \xrightarrow{\sim} \mathrm{S}_\mathfrak{p}.$$

Par la proposition 5.4, le complété formel de $\mathscr{X}$ le long de la section ∞ est isomorphe, *via* le module de Tate–Drinfeld, au spectre formel de $A[1/\mathfrak{p}][\![t^{q-1}]\!]$. En d'autres termes, $\mathscr{X}$ admet la coordonnée formelle locale $s = t^{q-1}$ en ∞. L'espace cotangent à $\mathscr{X}$ en la section ∞ est alors isomorphe, comme $A[1/\mathfrak{p}]$-module, à sR/s^2R où $R = A[1/\mathfrak{p}][\![s]\!]$. Il est de libre de rang 1 de base ds (on utilise d pour la notation différentielle). Notons $s_1, \ldots, s_d$ les coordonnées formelles locales du schéma-produit $\mathscr{X}^d$. Par construction du produit symétrique, les fonctions symétriques élémentaires $\sigma_1 = s_1 + \cdots + s_d, \ldots, \sigma_d = s_1 \cdots s_d$ sont des coordonnées formelles locales de $\mathscr{X}^{(d)}$ en $\infty^{(d)}$. Donc le $A[1/\mathfrak{p}]$-module $\mathrm{Cot}_{\infty^{(d)}}\, \mathscr{X}^{(d)}$ est libre de rang d de base d$\sigma_1, \ldots,$ dσ_d. Notons $\varphi^{(d)*} : \mathrm{Cot}\, \mathcal{J} \to \mathrm{Cot}\, \mathscr{X}^{(d)}$ le morphisme déduit de $\varphi^{(d)}$. On pourra comparer l'énoncé suivant avec les preuves de [Kamienny 1992a, proposition 3.2] et [Kamienny 1992b, proposition 3.1].

Proposition 7.11. *Avec les identifications précédentes, $\varphi^{(d)*}$ correspond à l'homomorphisme de $A[1/\mathfrak{p}]$-modules*

$$\mathrm{S}_{\mathfrak{p}} \to (A[1/\mathfrak{p}])^d, \quad f \mapsto \big(-b_1(f), b_2(f), \ldots, (-1)^d b_d(f)\big),$$

où $\sum_{i\geq 1} b_i(f)t^{1+i(q-1)}$ est le t-développement de f.

Démonstration. Posons $\Omega = \Omega^1_{\mathscr{X}/A[1/\mathfrak{p}]}$. On note temporairement δ l'exposant de la puissance symétrique afin d'éviter toute confusion avec la notation différentielle d. Par propriété de la puissance symétrique [Milne 1986, proposition 5.3], on a l'isomorphisme canonique β obtenu par composition :

$$\mathrm{S}_{\mathfrak{p}} \xrightarrow{\sim} H^0(\mathscr{X}, \Omega) \xrightarrow{\sim} H^0(\mathscr{X}^{(\delta)}, \Omega).$$

Soit $r : H^0(\mathscr{X}^{(\delta)}, \Omega) \to \mathrm{Cot}\,\mathscr{X}^{(\delta)}$ le morphisme naturel qui associe à une section sa restriction au fibré cotangent en $\infty^{(\delta)}$. On a le diagramme suivant :

$$\begin{array}{ccccc}
\mathrm{Cot}\,\mathscr{J} & \xrightarrow{\varphi^{(\delta)*}} & \mathrm{Cot}\,\mathscr{X}^{(\delta)} & \xrightarrow{\sim} & (A[1/\mathfrak{p}])^{\delta}. \\
\downarrow \sim & & \nearrow r & & \\
\mathrm{S}_{\mathfrak{p}} & & & & \\
\beta \downarrow \sim & & & & \\
H^0(\mathscr{X}^{(\delta)}, \Omega) & & & &
\end{array}$$

Le triangle est commutatif par l'argument du lemme 2.1 de [Mazur 1978]. Explicitons $r \circ \beta$. Soit $f \in \mathrm{S}_{\mathfrak{p}}$ de t-développement $\sum_{i\geq 1} b_i t^{1+i(q-1)}$. Pour $s = t^{q-1}$ le paramètre formel local de $X_0(\mathfrak{p})$ en ∞, le développement de toute différentielle $f \in \mathrm{S}(F)$ en ∞ est $-\sum_{i\geq 1} b_i s^{i-1}\,\mathrm{d}s$ (équation (7)). Donc l'image de f dans $H^0(\mathscr{X}^{\delta}, \Omega)$ par l'application canonique est la différentielle régulière globale de développement formel

$$-\sum_{1\leq i\leq \delta}\sum_{k\geq 1} b_k s_i^{k-1}\,\mathrm{d}s_i.$$

Signalons qu'à partir de cette étape, les calculs menés dans [Kamienny 1992a, proposition 3.2] ne sont plus valables en caractéristique p. Posons $u_j = \sum_{1\leq i\leq \delta} s_i^j\,\mathrm{d}s_i$ pour $j \geq 0$. On a l'identité

$$-\sum_{1\leq i\leq \delta}\sum_{k\geq 1} b_k s_i^{k-1}\,\mathrm{d}s_i = -\sum_{k\geq 1} b_k u_{k-1}. \tag{17}$$

Pour obtenir l'image de f par $r \circ \beta$, il suffit de considérer l'image de (17) dans $H^0(\mathscr{X}^{(\delta)}, \Omega)$ puis prendre la partie linéaire de son développement.

En notant comme auparavant $\sigma_1 = s_1 + \cdots + s_\delta, \ldots, \sigma_\delta = s_1 \cdots s_\delta$, on a les identités suivantes dans le module des différentielles de Kähler de $A[1/\mathfrak{p}, s_1, \ldots, s_\delta]$

sur $A[1/\mathfrak{p}]$:

$$\sigma_m u_0 - \sigma_{m-1} u_1 + \cdots + (-1)^m u_m = \mathrm{d}\sigma_{m+1} \quad (1 \le m \le \delta - 1), \tag{18}$$

$$(-1)^\delta \sigma_\delta u_{m-\delta} + \cdots - \sigma_1 u_{m-1} + u_m = 0 \qquad (m \ge \delta). \tag{19}$$

La première est le lemme 5.4 de [Milne 1986]. Pour démontrer la deuxième, on considère les relations de Newton $s_i^\delta - \sigma_1 s_i^\delta + \cdots + (-1)^\delta \sigma_\delta = 0$ pour $1 \le i \le \delta$, qu'on multiplie par $s_i^{m-\delta}\,\mathrm{d}s_i$ pour $m \ge \delta$, puis on somme ces relations sur $1 \le i \le \delta$. En évaluant en l'infini (18) et (19), on obtient les égalités dans $\mathrm{Cot}\,\mathscr{X}^{(\delta)}$:

$$(-1)^m u_m = \mathrm{d}\sigma_{m+1} \quad (1 \le m \le \delta - 1).$$
$$u_m = 0 \qquad (m \ge \delta).$$

En substituant dans (17), on obtient pour la partie linéaire :

$$(r \circ \beta)(f) = -\sum_{1 \le k \le \delta} (-1)^{k+1} b_k\,\mathrm{d}\sigma_k \in \mathrm{Cot}\,\mathscr{X}^{(\delta)}. \qquad \square$$

Corollaire 7.12. *Si* $\mathfrak{p}$ *est premier de degré* 3, *le morphisme* $u^{(q)} : \mathscr{X}^{(q)} \to \mathscr{J}$ *est une immersion formelle en* $\infty_\mathfrak{l}^{(q)}$ *pour tout* $\mathfrak{l}$ *premier* $\neq \mathfrak{p}$.

Démonstration. Comme $\deg \mathfrak{p} = 3$, le quotient d'enroulement est égal à J par la proposition 4.4. Donc $u^{(q)} = \varphi^{(q)} : \mathscr{X}^{(q)} \to \mathscr{J}$. Pour l'immersion formelle, il suffit alors de voir que

$$\mathrm{S}(\mathbb{F}_\mathfrak{l}) \to (\mathbb{F}_\mathfrak{l})^q, \quad f \mapsto (b_1(f), \ldots, b_q(f))$$

est surjective d'après la proposition 7.11. C'est précisément le résultat de la proposition 6.17 car X est ici de genre $g = q$ (proposition 3.2). $\square$

On obtient ainsi une nouvelle démonstration du théorème 7.5(i) : il s'agit de combiner le corollaire, la méthode de Mazur pour $J' = J$ (proposition 7.9) et la proposition 4.4.

Maintenant, donnons un critère pour l'immersion formelle en termes de formes modulaires de Drinfeld.

Théorème 7.13. *Supposons l'application linéaire*

$$\mathrm{S}(\mathbb{F}_\mathfrak{l})[\tilde{I}_\mathbf{e}] \to (\mathbb{F}_\mathfrak{l})^d, \quad f \mapsto (b_1(f), \ldots, b_d(f))$$

surjective. Alors le morphisme $u^{(d)} : \mathscr{X}^{(d)} \to \mathscr{J}'_\mathbf{e}(\mathfrak{p})$ *est une immersion formelle en* $\infty_\mathfrak{l}^{(d)}$.

Démonstration. Par le lemme 6.8 et le changement de base (proposition 6.6), on a un isomorphisme canonique $\mathrm{Cot}(\mathscr{J}_{\mathbb{F}_\mathfrak{l}}) \simeq \mathrm{S}(\mathbb{F}_\mathfrak{l})$ pour tout $\mathfrak{l}$ premier distinct de $\mathfrak{p}$. On conclut alors avec les propositions 7.10 et 7.11. $\square$

7E3. *Critère de Kamienny.* On fixe un premier ℓ distinct de $\mathfrak{p}$. Comme dans la section précédente, *on suppose qu'il existe un idéal I vérifiant l'hypothèse 4.9* et son quotient raffiné est noté $J'_{\mathbf{e}}(\mathfrak{p})$. L'énoncé qui suit s'apparente à un critère de Kamienny [1992b, corollaire 3.4].

Proposition 7.14. *Supposons les conditions suivantes vérifiées* :

(i) *L'application $\mathbb{F}_\ell$-linéaire*

$$\Phi_\ell : (\mathbb{T}/\tilde{I}_{\mathbf{e}}) \otimes_{\mathbb{Z}} \mathbb{F}_\ell \longrightarrow \mathrm{Hom}(\mathrm{S}(\mathbb{F}_\ell)[\tilde{I}_{\mathbf{e}}], \mathbb{F}_\ell),$$

qui envoie la classe de $u \in \mathbb{T}$ sur la forme linéaire $f \mapsto b_1(uf)$, est un isomorphisme.

(ii) *Il existe des éléments $u_1, \dots, u_d$ de $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ vérifiant $b_i = b_1 \circ u_i$ $(1 \le i \le d)$ et dont les images dans $(\mathbb{T}/\tilde{I}_{\mathbf{e}}) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ sont libres sur $\mathbb{F}_\ell$.*

La condition (i) *est vérifiée lorsque* $\deg \mathfrak{p} = 3$. *La condition* (ii) *est vérifiée pour* $d = 1$, $\deg \mathfrak{p} \ge 3$ *et pour* $1 \le d \le q$, $\deg \mathfrak{p} \ge 5$. *Alors le morphisme $u^{(d)} : \mathscr{X}^{(d)} \to \mathscr{J}'_{\mathbf{e}}(\mathfrak{p})$ est une immersion formelle en $\infty^{(d)}_\ell$.*

Démonstration. D'après le théorème 7.13, il suffit de voir les formes linéaires $b_1, \dots, b_d$ sur $\mathrm{S}(\mathbb{F}_\ell)[\tilde{I}_{\mathbf{e}}]$ sont linéairement indépendantes. Par l'isomorphisme Φ_ℓ, la forme linéaire b_i correspond à la classe de u_i dans $(\mathbb{T}/\tilde{I}_{\mathbf{e}}) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$. La condition (ii) dit que ces classes sont libres et le résultat se transpose à $b_1, \dots, b_d$ par l'isomorphisme Φ_ℓ. Donc $u^{(d)}$ est une immersion formelle.

Supposons $\mathfrak{p}$ de degré 3. On commence par démontrer que l'idéal $(q-1)d_{\mathbf{e}}\tilde{I}_{\mathbf{e}}$ est contenu dans $p\mathbb{T}$. Soit $t \in \tilde{I}_{\mathbf{e}}$ c'est-à-dire vérifiant $d_{\mathbf{e}} t\mathbf{e} \in p\overline{\mathrm{M}^0}$. Comme $\deg \mathfrak{p} = 3$, d'après la proposition 8.2 de [Armana 2011b] on a $\overline{\mathrm{M}^0} = \mathrm{M}^0$ et l'isomorphisme de $\mathbb{T}$-modules

$$I_E \to \mathrm{M}^0, \quad u \mapsto u\mathbf{e}/(q-1),$$

où I_E est l'idéal d'Eisenstein de $\mathbb{T}$, c'est-à-dire, celui engendré par les éléments $T_{\mathfrak{m}} - (q^{\deg \mathfrak{m}} + 1)$ pour tout $\mathfrak{m}$ premier distinct de $\mathfrak{p}$. Donc il existe u dans I_E tel que l'élément $(q-1)d_{\mathbf{e}}t - pu$ de l'algèbre de Hecke annule $\mathbf{e}$. Il est nul par la proposition 4.4. Donc $(q-1)d_{\mathbf{e}}t$ appartient à $p\mathbb{T}$. Cela démontre l'affirmation.

Un calcul mené en [Armana 2011b, 7.1.2] montre que le dénominateur $d_{\mathbf{e}}$ est ici q^2+q+1. Donc, comme $\mathbb{F}_\ell$ est de caractéristique p et $(q^3-1)\tilde{I}_{\mathbf{e}} \subset p\mathbb{T}$, on a $\tilde{I}_{\mathbf{e}} \otimes \mathbb{F}_\ell = (q^3-1)\tilde{I}_{\mathbf{e}} \otimes \mathbb{F}_\ell = 0$. De même, on a

$$\mathrm{S}(\mathbb{F}_\ell) = \mathrm{S}(\mathbb{F}_\ell)[p\mathbb{T}] \subset \mathrm{S}(\mathbb{F}_\ell)[(q^3-1)\tilde{I}_{\mathbf{e}}] = \mathrm{S}(\mathbb{F}_\ell)[\tilde{I}_{\mathbf{e}}]$$

donc l'inclusion est une égalité. Par ces considérations, la condition (i) revient à montrer que $\Phi_\ell : \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_\ell \to \mathrm{Hom}(\mathrm{S}(\mathbb{F}_\ell), \mathbb{F}_\ell)$ est bijectif. Les espaces considérés sont de dimension $g = q$ sur $\mathbb{F}_\ell$ (car $\mathbb{T}$ est libre de rang g sur $\mathbb{Z}$ et, pour $\mathrm{S}(\mathbb{F}_\ell)$, d'après la proposition 6.7). Montrons simplement la surjectivité de Φ_ℓ. D'après le

théorème 6.15, les images de $\theta_1, \dots, \theta_q$ dans $\mathbb{T} \otimes \mathbb{F}_\mathfrak{l}$ s'envoient par $\Phi_\mathfrak{l}$ sur les formes linéaires $b_1, \dots, b_q$ respectivement. Or, ces formes linéaires constituent une base du dual de $\mathrm{S}(\mathbb{F}_\mathfrak{l})$ par la proposition 6.17. Donc $\Phi_\mathfrak{l}$ est bijective.

Passons maintenant à la condition (ii). Supposons $d = 1$ et $\deg \mathfrak{p} \geq 3$. L'élément $u_1 = T_{(1)} = \mathrm{id}$ de l'algèbre de Hecke vérifie naturellement $b_1 = b_1 \circ u_1$. Il s'agit ensuite de voir que $T_{(1)}$ est non nul dans $(\mathbb{T}/\tilde{I}_\mathbf{e}) \otimes \mathbb{F}_\mathfrak{l}$. Il suffit de le vérifier dans $\mathbb{T}/\tilde{I}_\mathbf{e}$, vu comme espace vectoriel sur $\mathbb{F}_p$. Or cela découle de la propriété : $\tilde{\mathbf{e}}$ est non nul dès que $\deg \mathfrak{p} \geq 3$ [Armana 2011b, théorème 7.10(ii)].

Supposons $\deg \mathfrak{p} \geq 5$ et vérifions la condition (ii) pour $d = q$. Les éléments $\theta_1, \dots, \theta_q$ de $\mathbb{T} \otimes_\mathbb{Z} A$ donnés par le théorème 6.15 vérifient $b_i = b_1 \circ \theta_i$ pour $1 \leq i \leq q$ dans le dual de $\mathrm{S}(A[1/\mathfrak{p}])$, donc aussi dans le dual de $\mathrm{S}(\mathbb{F}_\mathfrak{l})$. Montrons que leurs images $u_1, \dots, u_q$ dans $(\mathbb{T}/\tilde{I}_\mathbf{e}) \otimes_\mathbb{Z} \mathbb{F}_\mathfrak{l}$ forment une famille libre. Pour cela, on commence par se ramener à d'autres éléments de l'algèbre de Hecke. Notons $\mathfrak{m}_1, \dots, \mathfrak{m}_q$ les idéaux de A de degré 1 et $M_1, \dots, M_q$ leurs générateurs unitaires respectifs. Par définition de θ_i, on a

$$\begin{pmatrix} \theta_1 \\ \vdots \\ \theta_q \end{pmatrix} = R \begin{pmatrix} T_{\mathfrak{m}_1} \\ \vdots \\ T_{\mathfrak{m}_q} \end{pmatrix} \text{ avec } R = (-1)^q \begin{pmatrix} \binom{q-1}{0}^{-1} & \cdots & \binom{q-1}{0}^{-1} \\ \binom{q-1}{1}^{-1} M_1 & \cdots & \binom{q-1}{1}^{-1} M_q \\ \vdots & & \vdots \\ \binom{q-1}{q-2}^{-1} M_1^{q-2} & \cdots & \binom{q-1}{q-2}^{-1} M_q^{q-2} \\ 1 - M_1^{q-1} & \cdots & 1 - M_q^{q-1} \end{pmatrix}.$$

Quitte à soustraire la première ligne de la dernière, on voit que le déterminant de R est de Vandermonde et vaut

$$(-1)^{q+1} \prod_{1 \leq i \leq q-2} \binom{q-1}{i}^{-1} \prod_{j<k} (M_j - M_k) \in \mathbb{F}_q^\times.$$

Donc R appartient à $\mathrm{GL}_q(A)$. Ainsi, il suffit de démontrer l'indépendance linéaire des images de $T_{\mathfrak{m}_1}, \dots, T_{\mathfrak{m}_q}$ dans $(\mathbb{T}/\tilde{I}_e) \otimes_\mathbb{Z} \mathbb{F}_\mathfrak{l}$. Là encore, il suffit de le vérifier dans le $\mathbb{F}_p$-espace vectoriel $\mathbb{T}/\tilde{I}_e$. Or, cela découle de [Armana 2011b, théorème 7.10(ii)] pour $\deg \mathfrak{p} \geq 5$. □

Remarque 7.15. Pour établir la condition (ii) pour $d > q$, il faudrait déjà disposer d'un élément u_{q+1} de $\mathbb{T} \otimes_\mathbb{Z} \mathbb{F}_\mathfrak{l}$ vérifiant $b_{q+1} = b_1 \circ u_{q+1}$. Pour cela, une idée naturelle est de généraliser le théorème 6.15 à des opérateurs de Hecke dont l'indice est de degré > 1. C'est ce qui a été fait dans [Armana 2011a], mais un tel u_{q+1} n'a pas pu être exhibé. Lorsque $\deg \mathfrak{p} = 3$, on verra l'existence d'un tel u_{q+1} (proposition 7.17), sans en avoir une formule explicite.

Maintenant, nous sommes en mesure de prouver les résultats annoncés en introduction. En combinant les propositions 4.11, 7.9 et 7.14, on obtient le théorème 1.5 sur les points de $Y_1(\mathfrak{p})$. Un argument similaire, dans l'esprit de la proposition 7.6, démontre un résultat partiel sur les points de $Y_0(\mathfrak{p})$ (on laisse la preuve au lecteur).

Proposition 7.16. *Soit* $\mathfrak{p}$ *de degré* ≥ 3. *Supposons qu'il existe un premier* $\mathfrak{l}$ *tel que* $\Phi_\mathfrak{l}$ *est un isomorphisme. Alors tout module de Drinfeld de rang* 2 *sur* K *possédant une isogénie* K*-rationnelle cyclique d'ordre* $\mathfrak{p}$ *a bonne réduction potentielle en* $\mathfrak{l}$.

La borne uniforme de Schweizer sur la $\mathfrak{p}$-torsion [2003, théorème 2.4 et remarque 2.5] ramène la conjecture 1.1 pour q et d fixés à un problème, *a priori* plus faible, sur la torsion première : *montrer qu'il n'y a qu'un nombre fini de premiers* $\mathfrak{p}$ *pour lesquels il existe une extension* L/K *de degré* d, *un module de Drinfeld* ϕ *de rang* 2 *sur* L *et un point de* $({}^{\phi}L)_{\mathrm{tors}}$ *d'ordre* $\mathfrak{p}$. Cela revient à voir que le degré des premiers $\mathfrak{p}$ comme ci-dessus est borné par une constante dépendant de q et d. Le théorème 1.5 établit ce fait si $1 \leq d \leq q$, à condition que ses hypothèses soient vérifiées. C'est ainsi qu'on obtient le corollaire 1.6 (on applique le théorème 1.5 aux $\mathfrak{p}$ de degrés $\geq \max(q+1, 5, B_q)$).

Pour terminer, on revient sur la condition (i) de la proposition 7.14. Dans une version antérieure [Armana 2009] de ce travail, la condition (i) était remplacée par l'hypothèse plus forte : l'application $\Phi'_\mathfrak{l} : \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_\mathfrak{l} \to \mathrm{Hom}(\mathrm{S}(\mathbb{F}_\mathfrak{l}), \mathbb{F}_\mathfrak{l})$, qui envoie la classe de u sur $(f \mapsto b_1(uf))$, est un isomorphisme. Elle ne semble pas être systématiquement vérifiée. En effet, le théorème 6.15 permet de voir que $\sum_{\deg \mathfrak{m} \leq 1} T_\mathfrak{m}$ est dans le noyau de $\Phi'_\mathfrak{l}$. Mais des investigations numériques suggèrent que, pour $\deg \mathfrak{p} \geq 5$, cet élément est non nul dans $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_\mathfrak{l}$, car non nul dans $\mathrm{H}/p\mathrm{H}$ (voir [Armana 2011a, paragraphe 6.4 et conjecture 6.9]).

Lorsque $\deg \mathfrak{p} = 3$, on a vu dans la preuve de la proposition 7.14 que $\Phi'_\mathfrak{l}$ est un isomorphisme pour tout $\mathfrak{l}$. De cette dualité, on tire des informations sur la structure de Hecke des formes modulaires de Drinfeld.

Proposition 7.17. *Soit* $\mathfrak{p}$ *premier de degré* 3.

(i) *L'algèbre* $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_\mathfrak{l}$ *opère fidèlement sur* $\mathrm{S}(\mathbb{F}_\mathfrak{l})$; *l'algèbre* $\mathbb{T}/p\mathbb{T}$ *opère fidèlement sur* $\mathrm{H}/p\mathrm{H}$.

(ii) *Pour tout* $i \geq 1$, *il existe* $u_i \in \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_\mathfrak{l}$ *avec* $b_i = b_1 \circ u_i$.

(iii) *Toute forme modulaire de Drinfeld de* $\mathrm{S}(\mathbb{F}_\mathfrak{l})$ *propre pour* $(T_\mathfrak{m})_{\deg \mathfrak{m}=1}$ *est déterminée par ses valeurs propres, à un facteur multiplicatif près.*

(iv) *Le* $\mathbb{F}_p$*-espace vectoriel* $\mathbb{T}/p\mathbb{T}$ *a pour base* $(T_\mathfrak{m})_{\deg \mathfrak{m}=1}$.

Démonstration. (i) La première affirmation découle de l'isomorphisme $\Phi'_\mathfrak{l}$. Une preuve de la deuxième se trouve dans [Armana 2011b, corollaire 8.3]. On donne ici un autre argument, indépendant, utilisant $\Phi'_\mathfrak{l}$. Soit u un élément de $\mathbb{T}/p\mathbb{T}$, nul comme endomorphisme de $\mathrm{H}/p\mathrm{H}$. D'après Gekeler–Reversat, le $\mathbb{T}/p\mathbb{T}$-module

$\mathrm{H}/p\mathrm{H}$ s'identifie à une certaine $\mathbb{F}_p$-structure de l'espace $\mathrm{S}(\mathbb{C}_\infty)$ de formes modulaires analytiques (proposition 6.9 et [Gekeler et Reversat 1996, diagramme 6.5]). Donc u, vu comme endomorphisme de $\mathrm{S}(\mathbb{C}_\infty)$, est nul. Il en est de même sur $\mathrm{S}(A[1/\mathfrak{p}])$. Par extension des scalaires (proposition 6.6), il en va de même sur $\mathrm{S}(\mathbb{F}_\mathfrak{l})$. Donc u est dans le noyau du morphisme composé

$$\mathbb{T}/p\mathbb{T} \longrightarrow \mathbb{T}/p\mathbb{T} \otimes_{\mathbb{F}_p} \mathbb{F}_\mathfrak{l} = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_\mathfrak{l} \xrightarrow{\Phi'_\mathfrak{l}} \mathrm{Hom}(\mathrm{S}(\mathbb{F}_\mathfrak{l}), \mathbb{F}_\mathfrak{l}).$$

Le premier est naturellement injectif. Comme $\Phi'_\mathfrak{l}$ est un isomorphisme, u est nul.

(ii) L'affirmation provient de la surjectivité de $\Phi'_\mathfrak{l}$.

(iii) Soit f propre pour $(T_\mathfrak{m})_{\deg \mathfrak{m}=1}$ de valeurs propres $(\lambda_\mathfrak{m})_{\deg \mathfrak{m}=1}$. Par le théorème 6.15, on peut exprimer les coefficients $b_1(f), \ldots, b_q(f)$ en fonction des valeurs propres $(\lambda_\mathfrak{m})_{\deg \mathfrak{m}=1}$ et $b_1(f)$. Par ailleurs, comme le genre est $g = q$, la forme modulaire f est déterminée de façon unique par ses coefficients $b_1(f), \ldots, b_q(f)$ (proposition 6.17) Donc f est déterminée, à un facteur multiplicatif près, par les valeurs propres $(\lambda_\mathfrak{m})_{\deg \mathfrak{m}=1}$.

(iv) Dans la preuve de la proposition 7.14, on a vu que $\theta_1, \ldots, \theta_q$ est une base de $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_\mathfrak{l}$ sur $\mathbb{F}_\mathfrak{l}$ pour $\deg \mathfrak{p} = 3$. *Via* la matrice $R \in \mathrm{GL}_q(A)$ de la preuve, on en déduit que $(T_\mathfrak{m})_{\deg \mathfrak{m}=1}$ est aussi une base. En prenant pour $\mathfrak{l}$ une place de degré 1, on a $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_\mathfrak{l} \simeq \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{F}_p \simeq \mathbb{T}/p\mathbb{T}$, d'où le résultat. □

Remerciements

Je tiens à remercier Loïc Merel pour ses conseils lors de l'élaboration de ce travail de doctorat ainsi que le rapporteur pour ses remarques et sa relecture attentive. Je suis reconnaissante au Max-Planck-Institut für Mathematik pour son accueil lors de la rédaction de l'article.

Bibliographie

[Armana 2008] C. Armana, *Torsion rationnelle des modules de Drinfeld*, thèse, Université Paris Diderot, 2008, Disponible à http://tel.archives-ouvertes.fr/docs/00/34/93/10/PDF/these-armana.pdf.

[Armana 2009] C. Armana, "Torsion des modules de Drinfeld de rang 2 et formes modulaires de Drinfeld", *C. R. Math. Acad. Sci. Paris* **347**:13-14 (2009), 705–708. MR 2010h:11079 Zbl 1207.11055

[Armana 2011a] C. Armana, "Coefficients of Drinfeld modular forms and Hecke operators", *J. Number Theory* **131**:8 (2011), 1435–1460. MR 2012f:11096 Zbl 05899186

[Armana 2011b] C. Armana, "Une base explicite de symboles modulaires sur les corps de fonctions", prépublication, 2011, Disponible à http://tinyurl.com/armana-symbolesmodulaires-pre.

[Atiyah et Macdonald 1969] M. F. Atiyah et I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, MA, 1969. MR 39 #4129 Zbl 0175.03601

[Böckle 2002] G. Böckle, "An Eichler–Shimura isomorphism over function fields between Drinfeld modular forms and cohomology classes of crystals", prépublication, 2002, Disponible à http://tinyurl.com/boeckleES2002.

[Bosch et al. 1990] S. Bosch, W. Lütkebohmert et M. Raynaud, *Néron models*, Ergeb. Math. Grenzgeb. (3) **21**, Springer, Berlin, 1990. MR 91i:14034 Zbl 0705.14001

[Deligne 1973] P. Deligne, "Les constantes des équations fonctionnelles des fonctions L", pp. 501–597 dans *Modular functions of one variable* (Antwerp, 1972), vol. 2, édité par P. Deligne et W. Kuyk, Lecture Notes in Math. **349**, Springer, Berlin, 1973. MR 50 #2128 Zbl 0271.14011

[Deligne et Rapoport 1973] P. Deligne et M. Rapoport, "Les schémas de modules de courbes elliptiques", pp. 143–316 dans *Modular functions of one variable* (Antwerp,1972), vol. 2, Lecture Notes in Math. **349**, Springer, Berlin, 1973. MR 49 #2762 Zbl 0281.14010

[Denis 1995] L. Denis, "Problèmes diophantiens sur les t-modules" (*Les dix-huitièmes journées arithmétiques*, Bordeaux, 1993)*, J. Théor. Nombres Bordeaux* **7**:1 (1995), 97–110. MR 98f:11061 Zbl 0842.11026

[Drinfeld 1974] V. G. Drinfeld, "Elliptic modules", *Mat. Sb.* (*N.S.*) **94(136)** (1974), 594–627. En russe ; traduction anglaise : *Math. USSR-Sb* **23**:4 (1974), 561–592. MR 52 #5580

[Drinfeld 1984] V. G. Drinfeld, "Two-dimensional l-adic representations of the Galois group of a global field of characteristic p and automorphic forms on GL(2): Automorphic functions and number theory, II", *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov.* **134** (1984), 138–156. En russe ; traduction anglaise : J. Soviet Math. **36**(1), 93–105 (1987). MR 86i:11066

[Drinfeld 1988] V. G. Drinfeld, "Proof of the Petersson conjecture for GL(2) over a global field of characteristic p", *Funktsional. Anal. i Prilozhen.* **22**:1 (1988), 34–54. En russe ; traduction anglaise : *Funct. Anal. Appl.* **22** (1988), 28–43. MR 90c:11038

[Gekeler 1980] E.-U. Gekeler, *Drinfeld–Moduln und modulare Formen über rationalen Funktionenkörpern*, Bonner Math. Schriften **119**, Universität Bonn Mathematisches Institut, Bonn, 1980. MR 83a:10042 Zbl 0446.14018

[Gekeler 1986] E.-U. Gekeler, "Über Drinfeldsche Modulkurven vom Hecke-Typ", *Compositio Math.* **57**:2 (1986), 219–236. MR 87d:11041 Zbl 0599.14032

[Gekeler 1988] E.-U. Gekeler, "On the coefficients of Drinfeld modular forms", *Invent. Math.* **93**:3 (1988), 667–700. MR 89g:11043 Zbl 0653.14012

[Gekeler 1995a] E.-U. Gekeler, "Analytical construction of Weil curves over function fields", pp. 27–49 dans *Les dix-huitièmes journées arithmétiques* (Bordeaux, 1993), J. Théor. Nombres Bordeaux **7**, 1995. MR 97g:11060 Zbl 0846.11037

[Gekeler 1995b] E.-U. Gekeler, "Improper Eisenstein series on Bruhat–Tits trees", *Manuscripta Math.* **86**:3 (1995), 367–391. MR 95m:11043 Zbl 0884.11025

[Gekeler 1997a] E.-U. Gekeler, "Jacquet–Langlands theory over K and relations with elliptic curves", pp. 224–257 dans *Drinfeld modules, modular schemes and applications* (Alden–Biesen, 1996), édité par E.-U. Gekeler et al., World Sci. Publ., River Edge, NJ, 1997. MR 99e:11078 Zbl 0929.11051

[Gekeler 1997b] E.-U. Gekeler, "On the cuspidal divisor class group of a Drinfeld modular curve", *Doc. Math.* **2** (1997), 351–374. MR 98m:11057 Zbl 0895.11024

[Gekeler et Nonnengardt 1995] E.-U. Gekeler et U. Nonnengardt, "Fundamental domains of some arithmetic groups over function fields", *Internat. J. Math.* **6**:5 (1995), 689–708. MR 96i:11043 Zbl 0858.11025

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

[Goss 1980a] D. Goss, "Modular forms for $\mathbf{F}_r[T]$", *J. Reine Angew. Math.* **317** (1980), 16–39. MR 82m:10049 Zbl 0422.10021

[Goss 1980b] D. Goss, "π-adic Eisenstein series for function fields", *Compositio Math.* **41**:1 (1980), 3–38. MR 82e:10053 Zbl 0422.10020

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977. MR 57 #3116 Zbl 0367.14001

[van der Heiden 2006] G.-J. van der Heiden, "Drinfeld modular curve and Weil pairing", *J. Algebra* **299**:1 (2006), 374–418. MR 2007b:11086 Zbl 1177.11049

[Iwaniec et Sarnak 2000] H. Iwaniec et P. Sarnak, "The non-vanishing of central values of automorphic L-functions and Landau–Siegel zeros", *Israel J. Math.* **120**:part A (2000), 155–177. MR 2002b:11115 Zbl 0992.11037

[Kamienny 1992a] S. Kamienny, "Torsion points on elliptic curves and q-coefficients of modular forms", *Invent. Math.* **109**:2 (1992), 221–229. MR 93h:11054 Zbl 0773.14016

[Kamienny 1992b] S. Kamienny, "Torsion points on elliptic curves over fields of higher degree", *Internat. Math. Res. Notices* **1992**:6 (1992), 129–133. MR 93e:11072 Zbl 0807.14022

[Kamienny et Mazur 1995] S. Kamienny et B. Mazur, "Rational torsion of prime order in elliptic curves over number fields", pp. 81–100 dans *Columbia University Number Theory Seminar* (New York, 1992), Astérisque **228**, Société Mathématique de France, Paris, 1995. MR 96c:11058 Zbl 0846.14012

[Kato et Trihan 2003] K. Kato et F. Trihan, "On the conjectures of Birch and Swinnerton–Dyer in characteristic $p > 0$", *Invent. Math.* **153**:3 (2003), 537–592. MR 2004h:11058 Zbl 1046.11047

[Katz 1973] N. M. Katz, "p-adic properties of modular schemes and modular forms", pp. 69–190 dans *Modular functions of one variable, III* (Antwerp, 1972), édité par W. Kuyk et J.-P. Serre, Lecture Notes in Mathematics **350**, Springer, Berlin, 1973. MR 56 #5434 Zbl 0271.10033

[Kowalski et Michel 1999] E. Kowalski et P. Michel, "The analytic rank of $J_0(q)$ and zeros of automorphic L-functions", *Duke Math. J.* **100**:3 (1999), 503–542. MR 2001b:11060 Zbl 1161.11359

[Liu 2002] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics **6**, Oxford University Press, 2002. MR 2003g:14001 Zbl 0996.14005

[Manin 1969] Y. Manin, "The p-torsion of elliptic curves is uniformly bounded", *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 459–465. En russe ; traduction anglaise : *Math. USSR-Izv.* **3**:3 (1969), 433–438. MR 42 #7667

[Mazur 1977] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186. MR 80c:14015 Zbl 0394.14008

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162. MR 80h:14022 Zbl 0386.14009

[Merel 1996] L. Merel, "Bornes pour la torsion des courbes elliptiques sur les corps de nombres", *Invent. Math.* **124**:1-3 (1996), 437–449. MR 96i:11057 Zbl 0936.11037

[Milne 1986] J. S. Milne, "Jacobian varieties", pp. 167–212 dans *Arithmetic geometry* (Storrs, CT, 1984), édité par G. Cornell et J. H. Silverman, Springer, New York, 1986. MR 861976 Zbl 0604.14018

[Ogg 1978] A. P. Ogg, "On the Weierstrass points of $X_0(N)$", *Illinois J. Math.* **22**:1 (1978), 31–35. MR 57 #3136 Zbl 0374.14005

[Pál 2005] A. Pál, "On the torsion of the Mordell–Weil group of the Jacobian of Drinfeld modular curves", *Doc. Math.* **10** (2005), 131–198. MR 2006c:11070 Zbl 1119.11031

[Pál 2010] A. Pál, "On the torsion of Drinfeld modules of rank two", *J. Reine Angew. Math.* **640** (2010), 1–45. MR 2011i:11087 Zbl 05697008

[Parent 1999] P. Parent, "Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres", *J. Reine Angew. Math.* **506** (1999), 85–116. MR 99k:11080 Zbl 0919.11040

[Poonen 1997] B. Poonen, "Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture", *Math. Ann.* **308**:4 (1997), 571–586. MR 98h:11073 Zbl 0891.11034

[Rosen 2003] M. Rosen, "Formal Drinfeld modules", *J. Number Theory* **103**:2 (2003), 234–256. MR 2004j:11056 Zbl 1049.11060

[Schneider 1982] P. Schneider, "Zur Vermutung von Birch und Swinnerton–Dyer über globalen Funktionenkörpern", *Math. Ann.* **260**:4 (1982), 495–510. MR 84i:14027 Zbl 0509.14022

[Schweizer 1997] A. Schweizer, "Hyperelliptic Drinfeld modular curves", pp. 330–343 dans *Drinfeld modules, modular schemes and applications* (Alden–Biesen, 1996), édité par E.-U. Gekeler et al., World Sci. Publ., River Edge, NJ, 1997. MR 99h:11061 Zbl 0930.11039

[Schweizer 2003] A. Schweizer, "On the uniform boundedness conjecture for Drinfeld modules", *Math. Z.* **244**:3 (2003), 601–614. MR 2004e:11062 Zbl 1037.11041

[Schweizer 2011] A. Schweizer, "Strong Weil curves over $\mathbb{F}_q(T)$ with small conductor", *J. Number Theory* **131**:2 (2011), 285–299. MR 2012f:11110 Zbl 1218.11059

[Tamagawa 1995] A. Tamagawa, "The Eisenstein quotient of the Jacobian variety of a Drinfel′d modular curve", *Publ. Res. Inst. Math. Sci.* **31**:2 (1995), 203–246. MR 96b:11077 Zbl 1045.11510

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

[Teitelbaum 1992] J. T. Teitelbaum, "Modular symbols for $\mathbf{F}_q(T)$", *Duke Math. J.* **68**:2 (1992), 271–295. MR 93h:11055 Zbl 0777.11021

[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

[VanderKam 2000] J. VanderKam, "Linear independence of Hecke operators in the homology of $X_0(N)$", *J. London Math. Soc.* (2) **61**:2 (2000), 349–358. MR 2001e:11045 Zbl 0963.11023

[Weil 1971] A. Weil, *Dirichlet series and automorphic forms: Lezioni fermiane*, Lecture Notes in Mathematics **189**, Berlin, 1971. Zbl 0218.10046

Communicated by Bjorn Poonen
Received 2011-07-14 Revised 2011-11-08 Accepted 2011-12-10

armana@math.jussieu.fr *Max-Planck Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany*

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@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 6 No. 6 2012

1937-0652(2012)6:6;1-9