Algebra & Number Theory

msp.org/ant

© 2016 Mathematical Sciences Publishers

Kummer theory for Drinfeld modules

Richard Pink

Let φ be a Drinfeld A-module of characteristic $\mathfrak{p}_0$ over a finitely generated field K. Previous articles determined the image of the absolute Galois group of K up to commensurability in its action on all prime-to-$\mathfrak{p}_0$ torsion points of φ, or equivalently, on the prime-to-$\mathfrak{p}_0$ adelic Tate module of φ. In this article we consider in addition a finitely generated torsion free A-submodule M of K for the action of A through φ. We determine the image of the absolute Galois group of K up to commensurability in its action on the prime-to-$\mathfrak{p}_0$ division hull of M, or equivalently, on the extended prime-to-$\mathfrak{p}_0$ adelic Tate module associated to φ and M.

1. Introduction

Let F be a finitely generated field of transcendence degree 1 over the prime field $\mathbb{F}_p$ of characteristic $p > 0$. Let A be the ring of elements of F which are regular outside a fixed place ∞ of F. Let K be another field that is finitely generated over $\mathbb{F}_p$, and let K^{sep} be a separable closure of K. Write $\mathrm{End}(\mathbb{G}_{a,K}) = K[\tau]$ with $\tau(x) = x^p$. Let $\varphi \colon A \to K[\tau], a \mapsto \varphi_a$ be a Drinfeld A-module of rank $r \geqslant 1$ and characteristic $\mathfrak{p}_0$. Then either $\mathfrak{p}_0$ is the zero ideal of A and φ is said to have generic characteristic; or $\mathfrak{p}_0$ is a maximal ideal of A and φ is said to have special characteristic.

For brevity we call any maximal ideal of A a prime of A. For any prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A the $\mathfrak{p}$-adic Tate module $T_{\mathfrak{p}}(\varphi)$ is a free module of rank r over the completion $A_{\mathfrak{p}}$, endowed with a continuous action of the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. The prime-to-$\mathfrak{p}_0$ adelic Tate module $T_{\mathrm{ad}}(\varphi) = \prod_{\mathfrak{p} \neq \mathfrak{p}_0} T_{\mathfrak{p}}(\varphi)$ is then a free module of rank r over

---

$A_{\mathrm{ad}} = \prod_{\mathfrak{p} \neq \mathfrak{p}_0} A_{\mathfrak{p}}$ carrying a natural action of Galois. This action corresponds to a continuous homomorphism

$$\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}_{A_{\mathrm{ad}}}(T_{\mathrm{ad}}(\varphi)) \cong \mathrm{GL}_r(A_{\mathrm{ad}}). \qquad (1.1)$$

Its image Γ_{ad} was determined up to commensurability in [Pink and Rütsche 2009] and [Devic and Pink 2012]; for special cases see Theorems 1.6 and 4.4 below.

Let $M \subset K$ be a finitely generated torsion free A-submodule of rank d for the action of A through φ. Then there is an associated prime-to-$\mathfrak{p}_0$ adelic Tate module $T_{\mathrm{ad}}(\varphi, M)$, which is a free module of rank $r + d$ over A_{ad} carrying a natural continuous action of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. This module lies in a natural Galois equivariant short exact sequence

$$0 \longrightarrow T_{\mathrm{ad}}(\varphi) \longrightarrow T_{\mathrm{ad}}(\varphi, M) \longrightarrow M \otimes_A A_{\mathrm{ad}} \longrightarrow 0. \qquad (1.2)$$

Define $\Gamma_{\mathrm{ad}, M}$ as the image of the associated continuous homomorphism

$$\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}_{A_{\mathrm{ad}}}(T_{\mathrm{ad}}(\varphi, M)) \cong \mathrm{GL}_{r+d}(A_{\mathrm{ad}}). \qquad (1.3)$$

Then the restriction to $T_{\mathrm{ad}}(\varphi)$ induces a surjective homomorphism $\Gamma_{\mathrm{ad}, M} \twoheadrightarrow \Gamma_{\mathrm{ad}}$, whose kernel we denote by $\Delta_{\mathrm{ad}, M}$. Since the action on $M \otimes_A A_{\mathrm{ad}}$ is trivial, there is a natural inclusion

$$\Delta_{\mathrm{ad}, M} \hookrightarrow \mathrm{Hom}_A(M, T_{\mathrm{ad}}(\varphi)). \qquad (1.4)$$

Any splitting of the sequence (1.2) induces an inclusion into the semidirect product

$$\Gamma_{\mathrm{ad}, M} \hookrightarrow \Gamma_{\mathrm{ad}} \ltimes \mathrm{Hom}_A(M, T_{\mathrm{ad}}(\varphi)). \qquad (1.5)$$

The aim of this article is to describe these subgroups up to commensurability.

In general the shape of these Galois groups is affected by the endomorphisms of φ over K^{sep}, and in special characteristic also by the endomorphisms of the restrictions of φ to all subrings of A. Any general results therefore involve further definitions and notation. In this introduction we avoid these and mention only a special case; the general case is addressed by Theorems 5.1, 6.6 and 6.7. Parts (a) and (b) of the following result can be found as [Pink and Rütsche 2009, Theorem 0.1] and [Devic and Pink 2012, Theorem 1.1], respectively, and part (c) is a special case of Theorem 5.1 below:

Theorem 1.6. *Assume that* $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) = A$, *and in special characteristic also that* $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi|B) = A$ *for every integrally closed infinite subring* $B \subset A$.

(a) *If* φ *has generic characteristic, then* Γ_{ad} *is open in* $\mathrm{GL}_r(A_{\mathrm{ad}})$.

(b) *If* φ *has special characteristic, then* Γ_{ad} *is commensurable with* $\overline{\langle a_0 \rangle} \cdot \mathrm{SL}_r(A_{\mathrm{ad}})$ *for some central element* $a_0 \in A$ *that generates a positive power of* $\mathfrak{p}_0$.

(c) *The inclusions (1.4) and (1.5) are both open.*

The method used to prove Theorem 1.6(c) and its generalizations is an adaptation of the Kummer theory for semiabelian varieties from Ribet [1979] and predecessors. The main ingredients are the above mentioned descriptions of Γ_{ad} and Poonen's tameness result [1995] concerning the structure of K as an A-module via φ. A standard procedure would be to first prove corresponding results for $\mathfrak{p}$-division points for almost all primes $\mathfrak{p} \neq \mathfrak{p}_0$ of A, and for $\mathfrak{p}$-power division points for all $\mathfrak{p} \neq \mathfrak{p}_0$, and then to combine these individual results by taking products, as in [Ribet 1979; Chi and Li 2001; Li 2001; Pink and Rütsche 2009; Devic and Pink 2012; Häberli 2011]. Instead, we have found a shorter way by doing everything adelically from the start. The core of the argument is the proof of Lemma 5.3. Therein we avoid the explicit use of group cohomology by trivializing an implicit 1-cocycle with the help of a suitable central element of Γ_{ad}. On first reading the readers may want to restrict their attention to the case of Theorem 1.6, which requires only Section 2, a little from Section 4, and Section 5 with simplifications, avoiding Sections 3 and 6 entirely. Some of this was worked out in [Häberli 2011]. Our results generalize those of [Chi and Li 2001] and [Li 2001].

The notation and the assumptions of this introduction remain in force throughout the article. For the general theory of Drinfeld modules see [Drinfeld 1974; Deligne and Husemöller 1987; Hayes 1979; Goss 1996].

2. Extended Tate modules

Following the usual convention in commutative algebra we let $A_{(\mathfrak{p}_0)} \subset F$ denote the localization of A at $\mathfrak{p}_0$; this is equal to F if and only if φ has generic characteristic. Observe that there is a natural isomorphism of A-modules

$$A_{(\mathfrak{p}_0)}/A \cong \bigoplus_{\mathfrak{p} \neq \mathfrak{p}_0} F_{\mathfrak{p}}/A_{\mathfrak{p}}, \tag{2.1}$$

where the product is extended over all maximal ideals $\mathfrak{p} \neq \mathfrak{p}_0$ of A and where $F_{\mathfrak{p}}$ and $A_{\mathfrak{p}}$ denote the corresponding completions of F and A. This induces a natural isomorphism for the prime-to-$\mathfrak{p}_0$ adelic completion of A:

$$A_{\mathrm{ad}} := \mathrm{End}_A(A_{(\mathfrak{p}_0)}/A) \cong \prod_{\mathfrak{p} \neq \mathfrak{p}_0} A_{\mathfrak{p}}. \tag{2.2}$$

As a consequence, for any torsion A-module X that is isomorphic to $(A_{(\mathfrak{p}_0)}/A)^{\oplus n}$ for some integer n, the construction

$$T(X) := \mathrm{Hom}_A(A_{(\mathfrak{p}_0)}/A, X) \tag{2.3}$$

yields a free A_{ad}-module of rank n. Reciprocally $T(X)$ determines X completely up to a natural isomorphism $X \cong T(X) \otimes_{A_{\mathrm{ad}}} (A_{(\mathfrak{p}_0)}/A)$. Thus any A-linear group

action on X determines and is determined by the corresponding A_{ad}-linear group action on $T(X)$. Moreover, with

$$T_{\mathfrak{p}}(X) := \mathrm{Hom}_A(F_{\mathfrak{p}}/A_{\mathfrak{p}}, X) \tag{2.4}$$

the decompositions (2.1) and (2.2) induce a decomposition

$$T(X) \cong \prod_{\mathfrak{p} \neq \mathfrak{p}_0} T_{\mathfrak{p}}(X). \tag{2.5}$$

This will give a concise way of defining the $\mathfrak{p}$-adic and adelic Tate modules associated to the given Drinfeld module φ.

We view K^{sep} as an A-module with respect to the action $A \times K^{\mathrm{sep}} \to K^{\mathrm{sep}}$, $(a, x) \mapsto \varphi_a(x)$ and are interested in certain submodules. One particular submodule is K. Let M be a finitely generated torsion free A-submodule of rank $d \geqslant 0$ contained in K. Then the *prime-to-$\mathfrak{p}_0$ division hull of M in K^{sep}* is the A-submodule

$$\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M) := \{x \in K^{\mathrm{sep}} \mid \exists a \in A \smallsetminus \mathfrak{p}_0 : \varphi_a(x) \in M\}. \tag{2.6}$$

Let $\mathrm{Div}_K^{(\mathfrak{p}_0)}(M)$ denote the intersection of $\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)$ with K. For later use we recall the following result proved in [Poonen 1995, Lemma 5] when K is a global field and φ has generic characteristic, and in [Wang 2001] in general:

Theorem 2.7. $[\mathrm{Div}_K^{(\mathfrak{p}_0)}(M) : M]$ *is finite.*

As a special case of the above, the prime-to-$\mathfrak{p}_0$ division hull of the zero module $\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(\{0\})$ is the module of all prime-to-$\mathfrak{p}_0$ torsion points of φ in K^{sep}. By direct calculation, which we leave to the reader, one proves:

Proposition 2.8. *There is a natural short exact sequence of A-modules*

$$0 \longrightarrow \mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(\{0\}) \longrightarrow \mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M) \longrightarrow M \otimes_A A_{(\mathfrak{p}_0)} \longrightarrow 1,$$

where the map on the right hand side is described by $x \mapsto \varphi_a(x) \otimes \frac{1}{a}$ for any $a \in A \smallsetminus \mathfrak{p}_0$ satisfying $\varphi_a(x) \in M$.

Dividing by M, the exact sequence from Proposition 2.8 yields a natural short exact sequence of A-modules

$$0 \longrightarrow \mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(\{0\}) \longrightarrow \mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)/M \longrightarrow M \otimes_A (A_{(\mathfrak{p}_0)}/A) \longrightarrow 0. \tag{2.9}$$

By the general theory of Drinfeld modules (see [Drinfeld 1974, Proposition 2.2]) the module on the left is isomorphic to $(A_{(\mathfrak{p}_0)}/A)^{\oplus r}$, where r is the rank of φ. Using the functor T from (2.3), the *prime-to-$\mathfrak{p}_0$ adelic Tate module of φ* can be described canonically as

$$T_{\mathrm{ad}}(\varphi) := T(\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(\{0\})) \tag{2.10}$$

and is a free A_{ad}-module of rank r. Since M is a projective A-module of rank d, the module on the right of (2.9) is isomorphic to $(A_{(\mathfrak{p}_0)}/A)^{\oplus d}$, and together it follows that the module in the middle is isomorphic to $(A_{(\mathfrak{p}_0)}/A)^{\oplus (r+d)}$. The *extended prime-to-$\mathfrak{p}_0$ adelic Tate module of φ and M*

$$T_{\mathrm{ad}}(\varphi, M) := T(\mathrm{Div}^{(\mathfrak{p}_0)}_{K^{\mathrm{sep}}}(M)/M) \tag{2.11}$$

is therefore a free A_{ad}-module of rank $r + d$. Moreover, the exact sequence (2.9) yields a natural short exact sequence of A_{ad}-modules

$$0 \longrightarrow T_{\mathrm{ad}}(\varphi) \longrightarrow T_{\mathrm{ad}}(\varphi, M) \longrightarrow M \otimes_A A_{\mathrm{ad}} \longrightarrow 0. \tag{2.12}$$

All this decomposes uniquely as $T_{\mathrm{ad}}(\varphi) = \prod_{\mathfrak{p} \neq \mathfrak{p}_0} T_{\mathfrak{p}}(\varphi)$ etc. as in (2.5).

By construction there is a natural continuous action of the Galois group

$$\mathrm{Gal}(K^{\mathrm{sep}}/K)$$

on all modules and arrows in Proposition 2.8 and in (2.9). This induces a continuous action on the short exact sequence (2.12), which in turn determines the former two by the following fact:

Proposition 2.13. *The action of* $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ *on* $\mathrm{Div}^{(\mathfrak{p}_0)}_{K^{\mathrm{sep}}}(M)$ *is completely determined by the action on* $T_{\mathrm{ad}}(\varphi, M)$.

Proof. For any $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$ the endomorphism $x \mapsto \sigma(x) - x$ of $\mathrm{Div}^{(\mathfrak{p}_0)}_{K^{\mathrm{sep}}}(M)$ is trivial on M, because that module is contained in K. Also, the image of this endomorphism is contained in $\mathrm{Div}^{(\mathfrak{p}_0)}_{K^{\mathrm{sep}}}(\{0\})$, because for any $a \in A \smallsetminus \mathfrak{p}_0$ with $\varphi_a(x) \in M$ we have

$$\varphi_a(\sigma(x) - x) = \sigma(\varphi_a(x)) - \varphi_a(x) = 0.$$

Thus the endomorphism factors through a homomorphism

$$\mathrm{Div}^{(\mathfrak{p}_0)}_{K^{\mathrm{sep}}}(M)/M \longrightarrow \mathrm{Div}^{(\mathfrak{p}_0)}_{K^{\mathrm{sep}}}(\{0\}).$$

But by (2.9) the latter homomorphism is determined completely by the action of σ on $\mathrm{Div}^{(\mathfrak{p}_0)}_{K^{\mathrm{sep}}}(M)/M$, and thus by the action of σ on $T_{\mathrm{ad}}(\varphi, M)$, as desired. $\square$

Let Γ_{ad} and $\Gamma_{\mathrm{ad}, M}$ denote the images of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ acting on $T_{\mathrm{ad}}(\varphi)$ and $T_{\mathrm{ad}}(\varphi, M)$, as in (1.1) and (1.3). Restricting to $T_{\mathrm{ad}}(\varphi)$ induces a surjective homomorphism $\Gamma_{\mathrm{ad}, M} \twoheadrightarrow \Gamma_{\mathrm{ad}}$, and we define $\Delta_{\mathrm{ad}, M}$ by the short exact sequence

$$1 \longrightarrow \Delta_{\mathrm{ad}, M} \longrightarrow \Gamma_{\mathrm{ad}, M} \longrightarrow \Gamma_{\mathrm{ad}} \longrightarrow 1. \tag{2.14}$$

For any $m \in M$ take an element $t \in T_{\mathrm{ad}}(\varphi, M)$ with image $m \otimes 1$ in $M \otimes_A A_{\mathrm{ad}}$. Since any $\delta \in \Delta_{\mathrm{ad}, M}$ acts trivially on $T_{\mathrm{ad}}(\varphi)$, the difference $\delta(t) - t$ depends only

on δ and m. Since δ also acts trivially on $M \otimes_A A_{\mathrm{ad}}$, the difference lies in $T_{\mathrm{ad}}(\varphi)$ and therefore defines a map

$$\Delta_{\mathrm{ad}, M} \times M \longrightarrow T_{\mathrm{ad}}(\varphi), \quad (\delta, m) \mapsto \langle \delta, m \rangle := \delta(t) - t. \qquad (2.15)$$

By direct calculation this map is additive in δ and A-linear in m. By the construction of $\Delta_{\mathrm{ad}, M}$ the adjoint of the pairing (2.15) is therefore a natural inclusion, already mentioned in (1.4):

$$\Delta_{\mathrm{ad}, M} \hookrightarrow \mathrm{Hom}_A(M, T_{\mathrm{ad}}(\varphi)). \qquad (2.16)$$

Let $R := \mathrm{End}_K(\varphi)$ denote the endomorphism ring of φ over K. This is an A-order in a finite dimensional division algebra over F (see [Drinfeld 1974, Corollary to Proposition 2.4]). It acts naturally on K and K^{sep} and therefore on $\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(\{0\})$ and $T_{\mathrm{ad}}(\varphi)$, turning the latter two into modules over $R_{\mathrm{ad}} := R \otimes_A A_{\mathrm{ad}}$. As this action commutes with the action of Γ_{ad}, it leads to an inclusion

$$\Gamma_{\mathrm{ad}} \subset \mathrm{Aut}_{R_{\mathrm{ad}}}(T_{\mathrm{ad}}(\varphi)). \qquad (2.17)$$

The decomposition (2.2) induces a decomposition

$$R_{\mathrm{ad}} = \prod_{\mathfrak{p} \neq \mathfrak{p}_0} R_{\mathfrak{p}},$$

where $R_{\mathfrak{p}} := R \otimes_A A_{\mathfrak{p}}$ acts naturally on $T_{\mathfrak{p}}(\varphi)$.

If M is an R-submodule of K, then R and hence R_{ad} also act on $\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)$ and $T_{\mathrm{ad}}(\varphi, M)$, and these actions commute with the action of $\Gamma_{\mathrm{ad}, M}$. The inclusion (2.16) then factors through an inclusion

$$\Delta_{\mathrm{ad}, M} \hookrightarrow \mathrm{Hom}_R(M, T_{\mathrm{ad}}(\varphi)). \qquad (2.18)$$

Moreover, any R-equivariant splitting of the sequence (2.12) then induces an embedding into the semidirect product

$$\Gamma_{\mathrm{ad}, M} \hookrightarrow \Gamma_{\mathrm{ad}} \ltimes \mathrm{Hom}_R(M, T_{\mathrm{ad}}(\varphi)). \qquad (2.19)$$

3. Reduction steps

For use in Section 6 we now discuss the behavior of extended Tate modules and their associated Galois groups under isogenies and under restriction of φ to subrings.

First consider another Drinfeld A-module φ' and an isogeny $f : \varphi \to \varphi'$ defined over K. Recall that there exists an isogeny $g : \varphi' \to \varphi$ such that $g \circ f = \varphi_a$ for some nonzero $a \in A$ (see [Drinfeld 1974, Corollary to Proposition 2.3]). From this it follows that $M' := f(M)$ is a torsion free finitely generated A-submodule of K for the action of A through φ'. Thus f induces A_{ad}-linear maps from the modules in (2.12) to those associated to φ' and M'. The existence of g implies that these maps

are inclusions of finite index. Together these maps yield a commutative diagram of A_{ad}-modules with exact rows

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & T_{\mathrm{ad}}(\varphi) & \longrightarrow & T_{\mathrm{ad}}(\varphi, M) & \longrightarrow & M \otimes_A A_{\mathrm{ad}} & \longrightarrow & 0 \\
& & \uparrow & & \uparrow & & \downarrow{\scriptstyle\wr} & & \\
0 & \longrightarrow & T_{\mathrm{ad}}(\varphi') & \longrightarrow & T_{\mathrm{ad}}(\varphi', M') & \longrightarrow & M' \otimes_A A_{\mathrm{ad}} & \longrightarrow & 0.
\end{array}
\tag{3.1}
$$

By construction all these maps are equivariant under $\mathrm{Gal}(K^{\mathrm{sep}}/K)$; hence the images of Galois in each column are canonically isomorphic. If we denote the analogues of the groups $\Delta_{\mathrm{ad},M} \subset \Gamma_{\mathrm{ad},M} \twoheadrightarrow \Gamma_{\mathrm{ad}}$ associated to φ' and M' by

$$
\Delta^{\varphi'}_{\mathrm{ad},M'} \subset \Gamma^{\varphi'}_{\mathrm{ad},M'} \twoheadrightarrow \Gamma^{\varphi'}_{\mathrm{ad}},
$$

this means that we have a natural commutative diagram

$$
\begin{array}{ccccccc}
\Gamma_{\mathrm{ad}} & \twoheadleftarrow & \Gamma_{\mathrm{ad},M} & \supset & \Delta_{\mathrm{ad},M} & \lhook\joinrel\longrightarrow & \mathrm{Hom}_A(M, T_{\mathrm{ad}}(\varphi)) \\
{\scriptstyle\wr}\| & & {\scriptstyle\wr}\| & & {\scriptstyle\wr}\| & & \downarrow \\
\Gamma^{\varphi'}_{\mathrm{ad}} & \twoheadleftarrow & \Gamma^{\varphi'}_{\mathrm{ad},M'} & \supset & \Delta^{\varphi'}_{\mathrm{ad},M'} & \lhook\joinrel\longrightarrow & \mathrm{Hom}_A(M', T_{\mathrm{ad}}(\varphi')),
\end{array}
\tag{3.2}
$$

where the vertical arrow on the right hand side is an inclusion of finite index.

Next let B be any integrally closed infinite subring of A. Then A is a finitely generated projective B-module of some rank $s \geqslant 1$. The restriction $\psi := \varphi|B$ is therefore a Drinfeld B-module of rank rs over K, and the given A-module M of rank d becomes a B-module of rank ds. Moreover, since the characteristic of φ is by definition the kernel of the derivative map $a \mapsto d\varphi_a$, the characteristic of ψ is simply $\mathfrak{q}_0 := \mathfrak{p}_0 \cap B$. In analogy to (2.2) we have

$$
B_{\mathrm{ad}} := \mathrm{End}_B(B_{(\mathfrak{q}_0)}/B) \cong \prod_{\mathfrak{q} \neq \mathfrak{q}_0} B_{\mathfrak{q}},
\tag{3.3}
$$

where the product is extended over all maximal ideals $\mathfrak{q} \neq \mathfrak{q}_0$ of B. Thus

$$
A \otimes_B B_{\mathrm{ad}} \cong \prod_{\mathfrak{p} \nmid \mathfrak{q}_0} A_{\mathfrak{p}}
\tag{3.4}
$$

is in a natural way a factor ring of A_{ad}. More precisely, it is isomorphic to A_{ad} if the characteristic $\mathfrak{p}_0$ and hence $\mathfrak{q}_0$ is zero; otherwise it is obtained from A_{ad} by removing the finitely many factors $A_{\mathfrak{p}}$ for all maximal ideals $\mathfrak{p} \neq \mathfrak{p}_0$ of A above $\mathfrak{q}_0$. In particular we have a natural isomorphism $A \otimes_B B_{\mathrm{ad}} \cong A_{\mathrm{ad}}$ if and only if $\mathfrak{p}_0$ is the unique prime ideal of A above $\mathfrak{q}_0$.

Proposition 3.5. *The exact sequence* (2.12) *for ψ and M is naturally isomorphic to that obtained from the exact sequence* (2.12) *for φ and M by tensoring with*

$A \otimes_B B_{\mathrm{ad}}$ *over* A_{ad}. *In particular we have a commutative diagram with surjective vertical arrows*

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & T_{\mathrm{ad}}(\varphi) & \longrightarrow & T_{\mathrm{ad}}(\varphi, M) & \longrightarrow & M \otimes_A A_{\mathrm{ad}} & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T_{\mathrm{ad}}(\psi) & \longrightarrow & T_{\mathrm{ad}}(\psi, M) & \longrightarrow & M \otimes_B B_{\mathrm{ad}} & \longrightarrow & 0.
\end{array}
$$

If $\mathfrak{p}_0$ is the only prime ideal of A above $\mathfrak{q}_0$, the vertical arrows are isomorphisms.

Proof. According to (2.6) the prime-to-$\mathfrak{p}_0$ division hull of M with respect to φ and the prime-to-$\mathfrak{q}_0$ division hull of M with respect to ψ are

$$
\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M) := \{x \in K^{\mathrm{sep}} \mid \exists a \in A \smallsetminus \mathfrak{p}_0 : \varphi_a(x) \in M\},
$$
$$
\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{q}_0)}(M) := \{x \in K^{\mathrm{sep}} \mid \exists b \in B \smallsetminus \mathfrak{q}_0 : \psi_b(x) \in M\}.
$$

Here the latter is automatically contained in the former, because any $b \in B \smallsetminus \mathfrak{q}_0$ with $\psi_b(x) \in M$ is by definition an element $a := b \in A \smallsetminus \mathfrak{p}_0$ with $\varphi_a(x) \in M$. Thus $\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{q}_0)}(M)/M$ is the subgroup of all elements of $\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)/M$ that are annihilated by some element of $B \smallsetminus \mathfrak{q}_0$. In other words, it is the subgroup of all prime-to-$\mathfrak{q}_0$ torsion with respect to B, or again, it is obtained from $\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)/M$ by removing the $\mathfrak{p}$-torsion for all maximal ideals $\mathfrak{p} \neq \mathfrak{p}_0$ of A above $\mathfrak{q}_0$. In the same way $A \otimes_B (B_{(\mathfrak{q}_0)}/B)$ is isomorphic to the submodule of $A_{(\mathfrak{p}_0)}/A$ obtained by removing the $\mathfrak{p}$-torsion for all $\mathfrak{p}|\mathfrak{q}_0$. The same process applied to the exact sequence (2.9) therefore yields the analogue for ψ and M. By definition the exact sequence (2.12) for ψ and M is obtained from this by applying the functor

$$
X \mapsto \mathrm{Hom}_B(B_{(\mathfrak{q}_0)}/B, X) \cong \mathrm{Hom}_A(A \otimes_B (B_{(\mathfrak{q}_0)}/B), X)
$$

analogous to (2.3). The total effect of this is simply to remove the $\mathfrak{p}$-primary factors for all $\mathfrak{p}|\mathfrak{q}_0$ from the exact sequence (2.12) for φ and M, from which everything follows. $\square$

By construction the diagram in Proposition 3.5 is equivariant under $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. It therefore induces a natural commutative diagram of Galois groups

$$
\begin{array}{ccccccc}
\mathrm{Aut}_{A_{\mathrm{ad}}}(T_{\mathrm{ad}}(\varphi)) \supset \Gamma_{\mathrm{ad}} & \longleftarrow & \Gamma_{\mathrm{ad}, M} \supset \Delta_{\mathrm{ad}, M} & \lhook\joinrel\longrightarrow & \mathrm{Hom}_A(M, T_{\mathrm{ad}}(\varphi)) \\
\downarrow \qquad \downarrow & & \downarrow \qquad \downarrow & & \downarrow \\
\mathrm{Aut}_{B_{\mathrm{ad}}}(T_{\mathrm{ad}}(\psi)) \supset \Gamma_{\mathrm{ad}}^{\psi} & \longleftarrow & \Gamma_{\mathrm{ad}, M}^{\psi} \supset \Delta_{\mathrm{ad}, M}^{\psi} & \lhook\joinrel\longrightarrow & \mathrm{Hom}_B(M, T_{\mathrm{ad}}(\psi)),
\end{array} \qquad (3.6)
$$

where the subgroups in the lower row are the analogues for ψ and M of those in the upper row. By construction the left two vertical arrows are surjective, and they are isomorphisms if $\mathfrak{p}_0$ is the only prime ideal of A above $\mathfrak{q}_0$. In that case the rightmost vertical arrow is injective and it follows that the map $\Delta_{\mathrm{ad}, M} \to \Delta_{\mathrm{ad}, M}^{\psi}$ is

an isomorphism as well. In general one can only conclude that $\Delta^{\psi}_{\mathrm{ad},M}$ contains the image of $\Delta_{\mathrm{ad},M}$. In any case the diagram (3.6) gives a precise way of determining $\Gamma^{\psi}_{\mathrm{ad},M}$ from $\Gamma_{\mathrm{ad},M}$.

4. Previous results on Galois groups

In this section we recall some previous results on the Galois group Γ_{ad}. Its precise description up to commensurability depends on certain endomorphism rings. The endomorphism ring of a Drinfeld module of generic characteristic is always commutative, but in special characteristic it can be noncommutative. In the latter case it can grow on restricting φ to a subring B of A, and this effect can impose additional conditions on Γ_{ad}. The question of whether the endomorphism ring becomes stationary or grows indefinitely with B depends on the following property:

Definition 4.1. We call a Drinfeld A-module of special characteristic over K *isotrivial* if over K^{sep} it is isomorphic to a Drinfeld A-module defined over a finite field.

The next definition is slightly ad hoc, but it describes particular kinds of Drinfeld modules to which we can reduce ourselves in all cases, allowing a unified treatment of Kummer theory later on.

Definition 4.2. We call the triple (A, K, φ) *primitive* if the following conditions hold:

(a) $R := \mathrm{End}_K(\varphi)$ is equal to $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$.

(b) The center of R is A.

(c) R is a maximal A-order in $R \otimes_A F$.

(d) If φ is nonisotrivial of special characteristic, then for every integrally closed infinite subring $B \subset A$ we have $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi|B) = R$.

(e) If φ is isotrivial of special characteristic, then $A = \mathbb{F}_p[a_0]$ with $\varphi_{a_0} = \tau^{[k/\mathbb{F}_p]}$, where k denotes the finite field of constants of K.

Proposition 4.3. *Let A' denote the normalization of the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$.*

(a) *There exist a Drinfeld A'-module $\varphi' \colon A' \to K^{\mathrm{sep}}[\tau]$ and an isogeny*

$$f \colon \varphi \to \varphi'|A$$

over K^{sep} such that A' is the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi')$.

(b) *The characteristic $\mathfrak{p}'_0$ of any φ' as in (a) is a prime ideal of A' above the characteristic $\mathfrak{p}_0$ of φ.*

(c) *There exist a finite extension $K' \subset K^{\mathrm{sep}}$ of K, a Drinfeld A'-module*

$$\varphi' \colon A' \to K'[\tau],$$

an isogeny $f \colon \varphi \to \varphi'|A$ over K', and an integrally closed infinite subring $B \subset A'$ such that A' is the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi')$ and $(B, K', \varphi'|B)$ is primitive.

(d) *The subring B in (c) is unique unless φ is isotrivial of special characteristic, in which case it is never unique.*

(e) *For any data as in (c) the characteristic $\mathfrak{p}_0'$ of φ' is the unique prime ideal of A' above the characteristic $\mathfrak{q}_0$ of $\varphi'|B$.*

Proof. Applying [Devic and Pink 2012, Proposition 4.3] to φ and the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$ yields a Drinfeld A-module $\tilde{\varphi} \colon A \to K^{\mathrm{sep}}[\tau]$ and an isogeny $f \colon \varphi \to \tilde{\varphi}$ over K^{sep} such that A' is mapped into $\mathrm{End}_{K^{\mathrm{sep}}}(\tilde{\varphi})$ under the isomorphism

$$\mathrm{End}_{K^{\mathrm{sep}}}(\varphi) \otimes_A F \cong \mathrm{End}_{K^{\mathrm{sep}}}(\tilde{\varphi}) \otimes_A F$$

induced by f. Then $A' \otimes_A F$ is the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\tilde{\varphi}) \otimes_A F$, and since A' is integrally closed, it follows that A' is the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\tilde{\varphi})$. The tautological homomorphism $A' \hookrightarrow \mathrm{End}_{K^{\mathrm{sep}}}(\tilde{\varphi}) \hookrightarrow K^{\mathrm{sep}}[\tau]$ thus constitutes a Drinfeld A'-module φ' with $\varphi'|A \cong \tilde{\varphi}$ and $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi') = \mathrm{End}_{K^{\mathrm{sep}}}(\tilde{\varphi})$. In particular the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi')$ is equal to A', proving (a).

For (b) recall that the characteristic of φ' is the kernel of the derivative map $a' \mapsto d\varphi'_{a'}$. Calling it $\mathfrak{p}_0'$, the characteristic of $\varphi'|A$ is then $\mathfrak{p}_0' \cap A$. As the characteristic of a Drinfeld module is invariant under isogenies, it follows that $\mathfrak{p}_0'$ lies above $\mathfrak{p}_0$, proving (b).

For the remainder of the proof we take any pair φ' and f as in (a). We also choose a finite extension $K' \subset K^{\mathrm{sep}}$ of K such that φ' and f are defined over K' and that $\mathrm{End}_{K'}(\varphi') = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi')$.

Suppose first that φ' has generic characteristic. Then $\mathrm{End}_{K'}(\varphi')$ is commutative (see [Drinfeld 1974, Corollary to Proposition 2.4]) and hence equal to A', and so the triple (A', K', φ') is already primitive. This proves (c) with $B = A'$. Also, for any integrally closed infinite subring $B \subset A'$ the ring $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ is commutative and hence again equal to $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi') = A'$. Thus $(B, K', \varphi'|B)$ being primitive requires that $B = A'$, proving (d). Since $B = A'$, the assertion of (e) is then trivially true.

Suppose next that φ' is nonisotrivial of special characteristic. Then by [Pink 2006, Theorem 6.2] there exists a unique integrally closed infinite subring $B \subset A'$ such that B is the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ and that $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B') \subset \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ for every integrally closed infinite subring $B' \subset A'$. For use below we note that both properties are invariant under isogenies of φ', because isogenies induce isomorphisms on the

rings $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B') \otimes_{B'} \mathrm{Quot}(B')$. By uniqueness it follows that B, too, is invariant under isogenies of φ'.

After replacing K' by a finite extension we may assume that $\mathrm{End}_{K'}(\varphi'|B) = \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$. Then the triple $(B, K', \varphi'|B)$ satisfies the conditions in Definition 4.2 except that $\mathrm{End}_{K'}(\varphi'|B)$ may not be a maximal order in $\mathrm{End}_{K'}(\psi') \otimes_B \mathrm{Quot}(B)$. But applying [Devic and Pink 2012, Proposition 4.3] to $\varphi'|B$ and $\mathrm{End}_{K'}(\varphi'|B)$ yields a Drinfeld B-module $\psi' \colon B \to K'[\tau]$ and an isogeny $g \colon \varphi'|B \to \psi'$ over K' such that $\mathrm{End}_{K'}(\psi')$ is a maximal order in $\mathrm{End}_{K'}(\psi') \otimes_B \mathrm{Quot}(B)$ which contains $\mathrm{End}_{K'}(\varphi'|B)$. By the preceding remarks we now find that (B, K', ψ') is primitive. Moreover, the composite homomorphism

$$A' \hookrightarrow \mathrm{End}_{K'}(\varphi') \hookrightarrow \mathrm{End}_{K'}(\varphi'|B) \hookrightarrow \mathrm{End}_{K'}(\psi') \hookrightarrow K'[\tau]$$

constitutes a Drinfeld A'-module φ'' with $\varphi''|B \cong \psi'$. After replacing (φ', f) by $(\varphi'', g \circ f)$ the data then satisfies all the requirements of (c). Assertion (d) follows from the above stated uniqueness of B, and (e) follows from [Pink 2006, Proposition 3.5].

It remains to consider the case where φ' is isotrivial of special characteristic. In this case we may assume that φ' is defined over the constant field k' of K'. Any endomorphism of φ' over K^{sep} is then defined over a finite extension of k', but by assumption also over K'; hence it is defined over k'. In other words we have $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi') \subset k'[\tau]$. Since $\tau^{[k'/\mathbb{F}_p]}$ lies in the center of the $k'[\tau]$, it thus corresponds to an element of the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi')$. As this center is equal to A' by assumption, there is therefore an element $a_0 \in A'$ with $\varphi'_{a_0} = \tau^{[k'/\mathbb{F}_p]}$. Set $B := \mathbb{F}_p[a_0] \subset A'$ which, being isomorphic to a polynomial ring, is an integrally closed infinite subring of A'. Then $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B)$ is the commutant of $\tau^{[k'/\mathbb{F}_p]}$ in $K^{\mathrm{sep}}[\tau]$ and hence just $k'[\tau]$. By a standard construction this is a maximal B-order in a (cyclic) central division algebra over $\mathrm{Quot}(B)$; hence $(B, K', \varphi'|B)$ is primitive, proving (c). For (d) observe that replacing K' and k' by finite extensions amounts to replacing a_0 by an arbitrary positive power a_0^i. Thus the ring B is really not unique in this case, proving (d). Finally, assertion (e) follows from [Devic and Pink 2012, Proposition 6.4(a)]. This finishes the proof of Proposition 4.3. $\square$

Assume now that (A, K, φ) is primitive and that φ has rank r. Then $R \otimes_A F$ is a central division algebra of dimension m^2 over F for some factorization $r = mn$. Thus for all primes $\mathfrak{p} \neq \mathfrak{p}_0$ of A, the ring $R_{\mathfrak{p}} := R \otimes_A A_{\mathfrak{p}}$ is an $A_{\mathfrak{p}}$-order in the central simple algebra $R \otimes_A F_{\mathfrak{p}}$ of dimension m^2 over $F_{\mathfrak{p}}$ and is isomorphic to the matrix ring $\mathrm{Mat}_{m \times m}(A_{\mathfrak{p}})$ for almost all $\mathfrak{p}$. Let $D_{\mathfrak{p}}$ denote the commutant of $R_{\mathfrak{p}}$ in $\mathrm{End}_{A_{\mathfrak{p}}}(T_{\mathfrak{p}}(\varphi))$. This is an $A_{\mathfrak{p}}$-order in a central simple algebra of dimension n^2 over $F_{\mathfrak{p}}$ and is isomorphic to the matrix ring $\mathrm{Mat}_{n \times n}(A_{\mathfrak{p}})$ for almost all $\mathfrak{p}$. Let $D_{\mathfrak{p}}^1$

denote the multiplicative group of elements of $D_{\mathfrak{p}}$ of reduced norm 1. Set

$$D_{\mathrm{ad}} := \prod_{\mathfrak{p} \neq \mathfrak{p}_0} D_{\mathfrak{p}} \subset \mathrm{End}_{A_{\mathrm{ad}}}(T_{\mathrm{ad}}(\varphi))$$

and

$$D^1_{\mathrm{ad}} := \prod_{\mathfrak{p} \neq \mathfrak{p}_0} D^1_{\mathfrak{p}} \subset D^\times_{\mathrm{ad}} \subset \mathrm{Aut}_{A_{\mathrm{ad}}}(T_{\mathrm{ad}}(\varphi)).$$

If φ has generic characteristic, we have $m = 1$ and therefore

$$D_{\mathfrak{p}} = \mathrm{End}_{A_{\mathfrak{p}}}(T_{\mathfrak{p}}(\varphi)) \cong \mathrm{Mat}_{r \times r}(A_{\mathfrak{p}})$$

for all $\mathfrak{p}$.

If φ is nonisotrivial of special characteristic $\mathfrak{p}_0$, let a_0 be any element of A that generates a positive power of $\mathfrak{p}_0$. If φ is isotrivial, the element a_0 from Definition 4.2(d) already has the same property. In both cases we view a_0 as a scalar element of $D^\times_{\mathrm{ad}}$ via the diagonal embedding $A \subset A_{\mathrm{ad}} \subset D_{\mathrm{ad}}$, and let $\overline{\langle a_0 \rangle}$ denote the procyclic subgroup that is topologically generated by it.

In general the group Γ_{ad} was described up to commensurability in our earlier work. In the primitive case, Theorem 0.1 of [Pink and Rütsche 2009] and Theorem 1.1 and Proposition 6.3 of [Devic and Pink 2012] imply:

Theorem 4.4. *Assume that (A, K, φ) is primitive.*

(a) *If φ has generic characteristic, then Γ_{ad} is open in $D^\times_{\mathrm{ad}}$.*

(b) *If φ is nonisotrivial of special characteristic, then $n \geqslant 2$ and Γ_{ad} is commensurable with $\overline{\langle a_0 \rangle} \cdot D^1_{\mathrm{ad}}$.*

(c) *If φ is isotrivial of special characteristic, then $n = 1$ and $\Gamma_{\mathrm{ad}} = \overline{\langle a_0 \rangle}$ with a_0 from 4.2(c).*

Corollary 4.5. *Assume that (A, K, φ) is primitive.*

(a) *Let Θ_{ad} denote the closure of the $\mathbb{F}_p$-subalgebra of D_{ad} generated by Γ_{ad}. Then there exists a nonzero ideal $\mathfrak{a}$ of A with $\mathfrak{a} \not\subset \mathfrak{p}_0$ such that $\mathfrak{a}D_{\mathrm{ad}} \subset \Theta_{\mathrm{ad}}$.*

(b) *There exist a scalar element $\gamma \in \Gamma_{\mathrm{ad}}$ and a nonzero ideal $\mathfrak{b}$ of A with $\mathfrak{b} \not\subset \mathfrak{p}_0$ such that $\gamma \equiv 1$ modulo $\mathfrak{b}A_{\mathrm{ad}}$ but not modulo $\mathfrak{p}\mathfrak{b}A_{\mathrm{ad}}$ for any prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A.*

Proof. Any open subgroup of $D^\times_{\mathrm{ad}}$, and for $n \geqslant 2$ any open subgroup of D^1_{ad}, generates an open subring of D_{ad}. Thus the assertion (a) follows from Theorem 4.4 unless φ is isotrivial of special characteristic. But in that case we have $\Theta_{\mathrm{ad}} = \overline{\mathbb{F}_p[a_0]} = A_{\mathrm{ad}} = D_{\mathrm{ad}}$ and (a) follows as well.

In generic characteristic the assertion (b) follows directly from the openness of Γ_{ad}. In special characteristic some positive power a_0^i lies in Γ_{ad}, and so (b) holds with $\gamma = a_0^i$ and the ideal $\mathfrak{b} = (a_0^i - 1)$. $\square$

5. The primitive case

Now we prove the following result, of which Theorem 1.6(c) is a special case:

Theorem 5.1. *Assume that (A, K, φ) is primitive. Set $R := \mathrm{End}_K(\varphi)$ and let M be a finitely generated torsion free R-submodule of K. Then the inclusions $\Delta_{\mathrm{ad},M} \subset \mathrm{Hom}_R(M, T_{\mathrm{ad}}(\varphi))$ and $\Gamma_{\mathrm{ad},M} \subset \Gamma_{\mathrm{ad}} \ltimes \mathrm{Hom}_R(M, T_{\mathrm{ad}}(\varphi))$ are both open.*

So assume that (A, K, φ) is primitive. Let the subring $\Theta_{\mathrm{ad}} \subset D_{\mathrm{ad}}$, the element $\gamma \in \Gamma_{\mathrm{ad}}$, and the ideals $\mathfrak{a}, \mathfrak{b} \subset A$ be as in Corollary 4.5. Since $M \subset \mathrm{Div}_K^{(\mathfrak{p}_0)}(M)$ has finite index by Theorem 2.7, we can also choose a nonzero ideal $\mathfrak{c}$ of A with $\mathfrak{c} \not\subset \mathfrak{p}_0$ such that $\mathfrak{c} \cdot \mathrm{Div}_K^{(\mathfrak{p}_0)}(M) \subset M$. With this data we prove the following more precise version of Theorem 5.1:

Theorem 5.2. *In the above situation we have $\mathfrak{abc} \cdot \mathrm{Hom}_R(M, T_{\mathrm{ad}}(\varphi)) \subset \Delta_{\mathrm{ad},M}$.*

In the rest of this section we abbreviate $T_{\mathrm{ad}} := T_{\mathrm{ad}}(\varphi)$ and $M^*_{\mathrm{ad}} := \mathrm{Hom}_R(M, T_{\mathrm{ad}})$. Recall that the embedding $\Delta_{\mathrm{ad},M} \subset M^*_{\mathrm{ad}}$ is adjoint to the pairing $\langle \, , \, \rangle$ from (2.15). The arithmetic part of the proof is a calculation in $\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)$ with the following result:

Lemma 5.3. *For any prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A and any element $m \in M$ satisfying $\langle \Delta_{\mathrm{ad},M}, m \rangle \subset \mathfrak{pbc}T_{\mathrm{ad}}$ we have $m \in \mathfrak{p}M$.*

Proof. The assumption on γ, viewed as an element of A_{ad}, means that

$$\gamma - 1 \in \mathfrak{b}A_{\mathrm{ad}} \smallsetminus \mathfrak{pb}A_{\mathrm{ad}}.$$

By the Chinese remainder theorem we can find an element $b \in A \smallsetminus \mathfrak{p}_0$ satisfying $b \equiv \gamma - 1$ modulo $\mathfrak{pbc}A_{\mathrm{ad}}$. Then by construction we have $b \in \mathfrak{b} \smallsetminus \mathfrak{pb}$, and γ acts on all $\mathfrak{pbc}$-torsion points of φ through the action of $1 + b \in A$. By the Chinese remainder theorem we can also find elements $a, c \in A \smallsetminus \mathfrak{p}_0$ with $a \in \mathfrak{p} \smallsetminus \mathfrak{p}^2$ and $c \in \mathfrak{c} \smallsetminus \mathfrak{pc}$. Then the product abc lies in $\mathfrak{pbc} \smallsetminus (\mathfrak{p}^2\mathfrak{bc} \cup \mathfrak{p}_0)$. In particular the order of abc at $\mathfrak{p}$ is equal to that of $\mathfrak{pbc}$, and so we can also choose an element $d \in A \smallsetminus \mathfrak{p}$ such that $d\mathfrak{pbc} \subset (abc)$.

For better readability we abbreviate the action of any element $e \in A$ on an element $x \in K^{\mathrm{sep}}$ by $ex := \varphi_e(x)$. Since $abc \in A \smallsetminus \mathfrak{p}_0$, we can select an element $\widetilde{\widetilde{m}} \in \mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)$ with $abc\widetilde{\widetilde{m}} = m$. Then $\widetilde{m} := d\widetilde{\widetilde{m}}$ is an element of $\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)$ which satisfies $abc\widetilde{m} = dm$. By construction $\widetilde{m}$ lies in K^{sep}, but we shall see that it actually lies in a specific subfield.

Choosing a compatible system of division points of $\widetilde{m}$ we can find an A-linear map $\widetilde{t} \colon A_{(\mathfrak{p}_0)} \to \mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)$ satisfying $\widetilde{t}\left(\frac{1}{abc}\right) = \widetilde{m}$. Then $\widetilde{t}(1) = abc\widetilde{m} = dm$ lies in M; hence $\widetilde{t}$ induces an A-linear map $t \colon A_{(\mathfrak{p}_0)}/A \to \mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)/M$. By the construction (2.11) this map is an element of $T_{\mathrm{ad}}(\varphi, M)$ whose image in $M \otimes_A A_{\mathrm{ad}}$

is $dm \otimes 1$. For any $\delta \in \Delta_{\mathrm{ad},M}$ the definition (2.15) of the pairing now says that $\langle \delta, dm \rangle = \delta(t) - t$. But the assumption $\langle \Delta_{\mathrm{ad},M}, m \rangle \subset \mathfrak{p}\mathfrak{b}\mathfrak{c}T_{\mathrm{ad}}$ implies that

$$\langle \Delta_{\mathrm{ad},M}, dm \rangle \subset d\mathfrak{p}\mathfrak{b}\mathfrak{c}T_{\mathrm{ad}} \subset abcT_{\mathrm{ad}}$$

and therefore $\delta(t) - t \in abcT_{\mathrm{ad}}$. Thus $\delta(t) - t$ is the multiple by abc of an A-linear map $A_{(\mathfrak{p}_0)}/A \to \mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(\{0\})$; hence it is zero on the residue class of $\frac{1}{abc}$. By the construction of t this means that $\delta(\widetilde{m}) - \widetilde{m} = 0$. Varying δ we conclude that $\widetilde{m}$ is fixed by $\Delta_{\mathrm{ad},M}$; in other words, it lies in the subfield $K_{\mathrm{ad}} \subset K^{\mathrm{sep}}$ with $\mathrm{Gal}(K_{\mathrm{ad}}/K) = \Gamma_{\mathrm{ad}}$.

Now consider any element $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$. The fact that m lies in K implies that

$$abc(\sigma - 1)(\widetilde{\widetilde{m}}) = (\sigma - 1)(abc\widetilde{\widetilde{m}}) = (\sigma - 1)(m) = 0.$$

Thus $(\sigma - 1)(\widetilde{\widetilde{m}})$ is annihilated by abc and hence by the ideal $d\mathfrak{p}\mathfrak{b}\mathfrak{c} \subset (abc)$. The element $(\sigma - 1)(\widetilde{m}) = d(\sigma - 1)(\widetilde{\widetilde{m}})$ is therefore annihilated by the ideal $\mathfrak{p}\mathfrak{b}\mathfrak{c}$. Since γ acts on all $\mathfrak{p}\mathfrak{b}\mathfrak{c}$-torsion points through the action of $1 + b \in A$, it follows that

$$(1 + b - \gamma)((\sigma - 1)(\widetilde{m})) = 0.$$

On the other hand we have $\widetilde{m} \in K_{\mathrm{ad}}$, and since γ lies in the center of Γ_{ad}, its action on K_{ad} commutes with the action of σ on K_{ad}. Thus the last equation is equivalent to

$$(\sigma - 1)((1 + b - \gamma)(\widetilde{m})) = 0.$$

As $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$ was arbitrary, it follows that $(1 + b - \gamma)(\widetilde{m}) \in K$.

Since $\widetilde{m}$ lies in $\mathrm{Div}_{K^{\mathrm{sep}}}^{(\mathfrak{p}_0)}(M)$, we can now deduce that $(1 + b - \gamma)(\widetilde{m}) \in \mathrm{Div}_K^{(\mathfrak{p}_0)}(M)$. By the choice of $\mathfrak{c}$ and c it follows that $c(1 + b - \gamma)(\widetilde{m}) \in M$. The fact that $dm = abc\widetilde{m}$ thus implies that

$$(1 + b - \gamma)(dm) = (1 + b - \gamma)(abc\widetilde{m}) = abc(1 + b - \gamma)(\widetilde{m}) \in abM.$$

But dm is an element of K and therefore satisfies $(1 - \gamma)(dm) = 0$. Thus the last relation shows that actually $bdm \in abM$ and so $dm \in aM$. Since $a \in \mathfrak{p}$ and $d \notin \mathfrak{p}$, this implies that $m \in \mathfrak{p}M$, as desired. $\square$

The rest of the proof of Theorem 5.2 is a technical argument involving rings and modules. It is easier to understand if $R = A$, in which case $D_{\mathfrak{p}} \cong \mathrm{Mat}_{r \times r}(A_{\mathfrak{p}})$ for all $\mathfrak{p}$, so the readers may want to restrict themselves to that case on first reading. For general facts on maximal orders in semisimple algebras, see [Reiner 2003].

Using Corollary 11.6 of that reference, the assumptions in Definition 4.2 imply that for any prime $\mathfrak{p} \neq \mathfrak{p}_0$ of A the ring $R_{\mathfrak{p}} := R \otimes_A A_{\mathfrak{p}}$ is a maximal order in a finite dimensional central simple algebra over $F_{\mathfrak{p}}$. By [Reiner 2003, Theorem 17.3] we can therefore identify it with the matrix ring $\mathrm{Mat}_{n_{\mathfrak{p}} \times n_{\mathfrak{p}}}(S_{\mathfrak{p}})$, where $S_{\mathfrak{p}}$ is the maximal

order in a finite dimensional central division algebra over $F_{\mathfrak{p}}$. Here $n_{\mathfrak{p}} \geqslant 1$ may vary with $\mathfrak{p}$. Let $L_{\mathfrak{p}} := S_{\mathfrak{p}}^{\oplus n_{\mathfrak{p}}}$ denote the tautological left $R_{\mathfrak{p}}$-module. Since $T_{\mathfrak{p}} := T_{\mathfrak{p}}(\varphi)$ is a nontrivial finitely generated torsion free left $R_{\mathfrak{p}}$-module, it is isomorphic to $L_{\mathfrak{p}}^{\oplus m_{\mathfrak{p}}}$ for some $m_{\mathfrak{p}} \geqslant 1$ by [ibid., Theorem 18.10]. Thus

$$D_{\mathfrak{p}} := \mathrm{End}_{R_{\mathfrak{p}}}(T_{\mathfrak{p}})$$

is isomorphic to the matrix ring $\mathrm{Mat}_{m_{\mathfrak{p}} \times m_{\mathfrak{p}}}(S_{\mathfrak{p}}^{\mathrm{opp}})$ over the opposite algebra $S_{\mathfrak{p}}^{\mathrm{opp}}$. Let $N_{\mathfrak{p}} := (S_{\mathfrak{p}}^{\mathrm{opp}})^{\oplus m_{\mathfrak{p}}}$ denote the tautological left $D_{\mathfrak{p}}$-module; then as a $D_{\mathfrak{p}}$-module $T_{\mathfrak{p}}$ is isomorphic to $N_{\mathfrak{p}}^{\oplus n_{\mathfrak{p}}}$. Moreover, by biduality, using Morita equivalence [ibid., Theorem 16.14] or direct computation, we have

$$R_{\mathfrak{p}} \cong \mathrm{End}_{D_{\mathfrak{p}}}(T_{\mathfrak{p}}). \tag{5.4}$$

Next, since R is a maximal order in a division algebra over the Dedekind ring A, and M is a finitely generated torsion free R-module, M is a projective R-module by [ibid., Corollary 21.5], say of rank $\ell \geqslant 0$. For each $\mathfrak{p} \neq \mathfrak{p}_0$ we therefore have $M_{\mathfrak{p}} := M \otimes_A A_{\mathfrak{p}} \cong R_{\mathfrak{p}}^{\oplus \ell}$ as an $R_{\mathfrak{p}}$-module. Consequently $M_{\mathfrak{p}}^* := \mathrm{Hom}_R(M, T_{\mathfrak{p}}) \cong T_{\mathfrak{p}}^{\oplus \ell}$ as a $D_{\mathfrak{p}}$-module via the action of $D_{\mathfrak{p}}$ on $T_{\mathfrak{p}}$. Using the biduality (5.4) we obtain a natural isomorphism

$$M_{\mathfrak{p}} \cong \mathrm{Hom}_{D_{\mathfrak{p}}}(M_{\mathfrak{p}}^*, T_{\mathfrak{p}}). \tag{5.5}$$

Taking the product over all $\mathfrak{p} \neq \mathfrak{p}_0$ yields adelic versions of all this with $T_{\mathrm{ad}} = \prod T_{\mathfrak{p}}$ and $R_{\mathrm{ad}} = \prod R_{\mathfrak{p}}$ and $D_{\mathrm{ad}} = \prod D_{\mathfrak{p}}$ and $M_{\mathrm{ad}}^* = \prod M_{\mathfrak{p}}^*$.

Recall that $\Delta_{\mathrm{ad}, M}$ is a closed additive subgroup of $M_{\mathrm{ad}}^* = \prod M_{\mathfrak{p}}^*$. Let $\Delta_{\mathfrak{p}}$ denote its image under the projection to $M_{\mathfrak{p}}^*$.

Lemma 5.6. *For any $\mathfrak{p} \neq \mathfrak{p}_0$ and any $D_{\mathfrak{p}}$-linear map $f: M_{\mathfrak{p}}^* \to N_{\mathfrak{p}}$ satisfying $f(\Delta_{\mathfrak{p}}) \subset \mathfrak{p}\mathfrak{b}\mathfrak{c}N_{\mathfrak{p}}$, we have $f(M_{\mathfrak{p}}^*) \subset \mathfrak{p}N_{\mathfrak{p}}$.*

Proof. Since $N_{\mathfrak{p}}$ is a $D_{\mathfrak{p}}$-module isomorphic to a direct summand of $T_{\mathfrak{p}}$, it is equivalent to show that for every $D_{\mathfrak{p}}$-linear map $g: M_{\mathfrak{p}}^* \to T_{\mathfrak{p}}$ with $g(\Delta_{\mathfrak{p}}) \subset \mathfrak{p}\mathfrak{b}\mathfrak{c}T_{\mathfrak{p}}$ we have $g(M_{\mathfrak{p}}^*) \subset \mathfrak{p}T_{\mathfrak{p}}$. Let $\langle\,,\,\rangle: M_{\mathfrak{p}}^* \times M_{\mathfrak{p}} \to T_{\mathfrak{p}}$ denote the natural $A_{\mathfrak{p}}$-bilinear map. Then the biduality (5.5) says that $g = \langle \_, m_{\mathfrak{p}} \rangle$ for an element $m_{\mathfrak{p}} \in M_{\mathfrak{p}}$. Write $\mathfrak{p}\mathfrak{b}\mathfrak{c} = \mathfrak{p}^i \mathfrak{d}$ for an integer $i \geqslant 1$ and an ideal $\mathfrak{d}$ of A that is prime to $\mathfrak{p}$. Choose any element $m \in M$ which is congruent to $m_{\mathfrak{p}}$ modulo $\mathfrak{p}^i M_{\mathfrak{p}}$ and congruent to 0 modulo $\mathfrak{d}M$. Then the assumption $\langle \Delta_{\mathfrak{p}}, m_{\mathfrak{p}} \rangle = g(\Delta_{\mathfrak{p}}) \subset \mathfrak{p}\mathfrak{b}\mathfrak{c}T_{\mathfrak{p}}$ implies that $\langle \Delta_{\mathrm{ad}, M}, m \rangle \subset \mathfrak{p}\mathfrak{b}\mathfrak{c}T_{\mathrm{ad}}$. By Lemma 5.3 it follows that $m \in \mathfrak{p}M$. Consequently $m_{\mathfrak{p}} \in \mathfrak{p}M_{\mathfrak{p}}$ and therefore $g(M_{\mathfrak{p}}^*) = \langle \Delta_{\mathfrak{p}}, m_{\mathfrak{p}} \rangle \subset \mathfrak{p}T_{\mathfrak{p}}$, as desired. $\qquad\square$

Now observe that $\Delta_{\mathrm{ad}, M} \subset M_{\mathrm{ad}}^*$ is a closed additive subgroup that is invariant under the action of Γ_{ad}. It is therefore a submodule with respect to the subring $\Theta_{\mathrm{ad}} := \overline{\mathbb{F}_p[\Gamma_{\mathrm{ad}}]}$ of D_{ad} from Corollary 4.5(a). By Corollary 4.5(a) we therefore

have

$$\Delta'_{\mathrm{ad}} := \mathfrak{a} D_{\mathrm{ad}} \Delta_{\mathrm{ad},M} \subset \Delta_{\mathrm{ad},M}. \tag{5.7}$$

By construction Δ'_{ad} is a submodule over $D_{\mathrm{ad}} = \prod D_{\mathfrak{p}}$ and therefore itself a product $\Delta'_{\mathrm{ad}} = \prod \Delta'_{\mathfrak{p}}$ for $D_{\mathfrak{p}}$-submodules $\Delta'_{\mathfrak{p}} \subset M^*_{\mathfrak{p}}$.

Lemma 5.8. *For any* $\mathfrak{p} \neq \mathfrak{p}_0$ *and any* $D_{\mathfrak{p}}$-*linear map* $f \colon M^*_{\mathfrak{p}} \to N_{\mathfrak{p}}$ *satisfying* $f(\Delta'_{\mathfrak{p}}) \subset \mathfrak{pabc}N_{\mathfrak{p}}$, *we have* $f(M^*_{\mathfrak{p}}) \subset \mathfrak{p}N_{\mathfrak{p}}$.

Proof. The definition of $\Delta'_{\mathfrak{p}}$ implies that $\mathfrak{a}D_{\mathfrak{p}}\Delta_{\mathfrak{p}} \subset \Delta'_{\mathfrak{p}}$. Thus by assumption we have $\mathfrak{a}f(\Delta_{\mathfrak{p}}) \subset f(\mathfrak{a}D_{\mathfrak{p}}\Delta_{\mathfrak{p}}) \subset f(\Delta'_{\mathfrak{p}}) \subset \mathfrak{pabc}N_{\mathfrak{p}}$ and therefore $f(\Delta_{\mathfrak{p}}) \subset \mathfrak{pbc}N_{\mathfrak{p}}$. By Lemma 5.6 this implies that $f(M^*_{\mathfrak{p}}) \subset \mathfrak{p}N_{\mathfrak{p}}$. $\square$

Lemma 5.9. *For any* $\mathfrak{p} \neq \mathfrak{p}_0$ *we have* $\mathfrak{abc}M^*_{\mathfrak{p}} \subset \Delta'_{\mathfrak{p}}$.

Proof. Let $\mathfrak{m}_{\mathfrak{p}}$ denote the maximal ideal of $S^{\mathrm{opp}}_{\mathfrak{p}}$. Then by [Reiner 2003, Theorem 13.2] we have $\mathfrak{p}S^{\mathrm{opp}}_{\mathfrak{p}} = \mathfrak{m}^e_{\mathfrak{p}}$ for some integer $e \geqslant 1$. The general theory says the following about the structure of the module $M^*_{\mathfrak{p}}/\Delta'_{\mathfrak{p}}$ over the maximal order $D_{\mathfrak{p}}$. On the one hand, by [Knebusch 1967, Satz 7] the torsion submodule of $M^*_{\mathfrak{p}}/\Delta'_{\mathfrak{p}}$ is a finite direct sum of indecomposable modules isomorphic to $N_{\mathfrak{p}}/\mathfrak{m}^{j_\nu}_{\mathfrak{p}}N_{\mathfrak{p}}$ for certain integers $j_\nu \geqslant 1$. On the other hand, the factor module of $M^*_{\mathfrak{p}}/\Delta'_{\mathfrak{p}}$ by its torsion submodule is projective by [Reiner 2003, Corollary 21.5] and hence isomorphic to a direct sum of copies of $N_{\mathfrak{p}}$. That the factor module is projective also implies that $M^*_{\mathfrak{p}}/\Delta'_{\mathfrak{p}}$ is isomorphic to the direct sum of its torsion submodule with the factor module. Together it follows that $M^*_{\mathfrak{p}}/\Delta'_{\mathfrak{p}}$ is a finite direct sum of modules isomorphic to $N_{\mathfrak{p}}$ or to $N_{\mathfrak{p}}/\mathfrak{m}^{j_\nu}_{\mathfrak{p}}N_{\mathfrak{p}}$ for certain integers $j_\nu \geqslant 1$.

To use this fact, let $\mathfrak{p}^i$ denote the highest power of $\mathfrak{p}$ dividing $\mathfrak{abc}$. If no summand isomorphic to $N_{\mathfrak{p}}$ occurs in $M^*_{\mathfrak{p}}/\Delta'_{\mathfrak{p}}$ and all exponents j_ν are $\leqslant ei$, then $M^*_{\mathfrak{p}}/\Delta'_{\mathfrak{p}}$ is annihilated by $\mathfrak{p}^i S^{\mathrm{opp}}_{\mathfrak{p}} = \mathfrak{m}^{ei}_{\mathfrak{p}}$. In this case it follows that $\mathfrak{abc}M^*_{\mathfrak{p}} = \mathfrak{p}^i M^*_{\mathfrak{p}} \subset \Delta'_{\mathfrak{p}}$, as desired.

Otherwise there exists a surjective $D_{\mathfrak{p}}$-linear map $M^*_{\mathfrak{p}}/\Delta'_{\mathfrak{p}} \twoheadrightarrow N_{\mathfrak{p}}/\mathfrak{m}^{ei+1}_{\mathfrak{p}}N_{\mathfrak{p}}$. Composed with the isomorphism

$$N_{\mathfrak{p}}/\mathfrak{m}^{ei+1}_{\mathfrak{p}}N_{\mathfrak{p}} \cong \mathfrak{m}^{e-1}_{\mathfrak{p}}N_{\mathfrak{p}}/\mathfrak{p}^{i+1}N_{\mathfrak{p}} = \mathfrak{m}^{e-1}_{\mathfrak{p}}N_{\mathfrak{p}}/\mathfrak{pabc}N_{\mathfrak{p}},$$

this yields a $D_{\mathfrak{p}}$-linear map $M^*_{\mathfrak{p}}/\Delta'_{\mathfrak{p}} \to N_{\mathfrak{p}}/\mathfrak{pabc}N_{\mathfrak{p}}$ whose image is not contained in $\mathfrak{p}N_{\mathfrak{p}}/\mathfrak{pabc}N_{\mathfrak{p}} = \mathfrak{m}^e_{\mathfrak{p}}N_{\mathfrak{p}}/\mathfrak{pabc}N_{\mathfrak{p}}$. As $M^*_{\mathfrak{p}}$ is a projective $D_{\mathfrak{p}}$-module, the latter map can be lifted to a $D_{\mathfrak{p}}$-linear map $f \colon M^*_{\mathfrak{p}} \to N_{\mathfrak{p}}$. By construction this map then satisfies $f(\Delta'_{\mathfrak{p}}) \subset \mathfrak{pabc}N_{\mathfrak{p}}$ and $f(M^*_{\mathfrak{p}}) \not\subset \mathfrak{p}N_{\mathfrak{p}}$. But that contradicts Lemma 5.8; hence this case is not possible and the lemma is proved. $\square$

Taking the product over all $\mathfrak{p}$, Lemma 5.9 and the inclusion (5.7) imply that $\mathfrak{abc}M^*_{\mathrm{ad}} \subset \Delta'_{\mathrm{ad}} \subset \Delta_{\mathrm{ad},M}$. This finishes the proof of Theorem 5.2. In particular it proves the first assertion of Theorem 5.1, from which the second assertion directly follows.

6. The general case

First we note the following general fact on homomorphisms of modules:

Proposition 6.1. *Let S be a unitary ring, not necessarily commutative, and let M and N be left S-modules. Let X be a subset of M and SX the S-submodule generated by it. Let $\operatorname{Hom}_{(S)}(X, N)$ denote the set of maps $\ell\colon X \to N$ such that for any finite collection of $s_i \in S$ and $x_i \in X$ with $\sum_i s_i x_i = 0$ in M we have $\sum_i s_i \ell(x_i) = 0$ in N.*

(a) *The restriction of maps induces a bijection $\operatorname{Hom}_S(SX, N) \overset{\sim}{\to} \operatorname{Hom}_{(S)}(X, N)$.*

(b) *If R is a unitary subring of S such that X is an R-submodule and the natural map $S \otimes_R X \to M$, $\sum_i s_i \otimes x_i \mapsto \sum_i s_i x_i$ is injective, then $\operatorname{Hom}_{(S)}(X, N) = \operatorname{Hom}_R(X, N)$.*

(c) *If X is an S-submodule of M, then $\operatorname{Hom}_{(S)}(X, N) = \operatorname{Hom}_S(X, N)$.*

Proof. Let $F := \bigoplus_{x \in X} S \cdot [x]$ be the free left S-module over the set X and consider the natural S-linear map $F \to M$, $\sum_i s_i[x_i] \mapsto \sum_i s_i x_i$. Since S is unitary, the image of this map is SX. Let T denote its kernel. Then giving an S-linear map $SX \to N$ is equivalent to giving an S-linear map $F \to N$ which vanishes on T. Using the universal property of F we find that the latter is equivalent to giving an element of $\operatorname{Hom}_{(S)}(X, N)$. The total correspondence is given by restriction of maps, proving (a).

In (b) we have $S \otimes_R X \overset{\sim}{\to} SX$; hence the adjunction between tensor product and Hom yields bijections $\operatorname{Hom}_S(SX, N) \overset{\sim}{\to} \operatorname{Hom}_S(S \otimes_R X, N) \overset{\sim}{\to} \operatorname{Hom}_R(X, N)$. Their composite is again just restriction of maps; so by (a) the restriction map $\operatorname{Hom}_{(S)}(X, N) \to \operatorname{Hom}_R(X, N)$ is also bijective, proving (b).

Finally, (c) is a special case of (a) or (b), according to taste.   □

Now we return to the situation of Section 4. We choose data (A', K', φ', f, B) as in Proposition 4.3(c), that is: We let A' denote the normalization of the center of $\operatorname{End}_{K^{\mathrm{sep}}}(\varphi)$, take a finite extension $K' \subset K^{\mathrm{sep}}$ of K, a Drinfeld A'-module $\varphi'\colon A' \to K'[\tau]$, an isogeny $f\colon \varphi \to \varphi'|A$ over K', and an integrally closed infinite subring $B \subset A'$ such that A' is the center of $\operatorname{End}_{K^{\mathrm{sep}}}(\varphi')$ and $(B, K', \varphi'|B)$ is primitive. By Proposition 4.3(e) the characteristic $\mathfrak{p}_0'$ of φ' is then the only prime ideal of A' above the characteristic $\mathfrak{q}_0$ of $\varphi'|B$. We will apply the reduction steps from Section 3 to the isogeny f and to each of the inclusions $A \subset A' \supset B$.

Specifically, let us set $\psi' := \varphi'|B$ and $S' := \operatorname{End}_{K^{\mathrm{sep}}}(\psi')$. Then $M' := A'f(M)$ is a finitely generated A'-submodule of K' for the action of A' through φ', and so $N' := S'M'$ is a finitely generated B-submodule for the action of B through ψ'. The modules M' and N' may have torsion, but since they are finitely generated, their torsion is annihilated by some nonzero element $a' \in A'$. Replacing the isogeny

f by $\varphi'_{a'} \circ f$ replaces M' by $a'M'$ and N' by $a'N'$; hence we may without loss of generality assume that M' and N' are torsion free.

Let $\Delta^{\varphi'}_{\mathrm{ad},M'} \subset \Gamma^{\varphi'}_{\mathrm{ad},M'} \twoheadrightarrow \Gamma^{\varphi'}_{\mathrm{ad}}$ denote the Galois groups as in (2.14) associated to (K', φ', M') in place of (K, φ, M), and similarly for (K', φ', N'), respectively for (K', ψ', N'), and so on. Then Proposition 3.5 for the inclusion $A' \supset B$ yields a natural commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & T_{\mathrm{ad}}(\varphi') & \longrightarrow & T_{\mathrm{ad}}(\varphi', N') & \longrightarrow & N' \otimes_{A'} A'_{\mathrm{ad}} & \longrightarrow & 0 \\
& & \| \wr & & \| \wr & & \| \wr & & \\
0 & \longrightarrow & T_{\mathrm{ad}}(\psi') & \longrightarrow & T_{\mathrm{ad}}(\psi', N') & \longrightarrow & N' \otimes_B B_{\mathrm{ad}} & \longrightarrow & 0.
\end{array} \tag{6.2}$$

The action of S' on the lower row thus yields a natural action on the upper row. Recall from (2.19) that any S'-equivariant splitting induces an embedding

$$\Gamma^{\psi'}_{\mathrm{ad},N'} \hookrightarrow \Gamma^{\psi'}_{\mathrm{ad}} \ltimes \mathrm{Hom}_{S'}(N', T_{\mathrm{ad}}(\psi')). \tag{6.3}$$

Since (B, K', ψ') is primitive, this embedding is open by Theorem 5.1. The isomorphisms from (3.6) thus yield an open embedding

$$\Gamma^{\varphi'}_{\mathrm{ad},N'} \hookrightarrow \Gamma^{\varphi'}_{\mathrm{ad}} \ltimes \mathrm{Hom}_{S'}(N', T_{\mathrm{ad}}(\varphi')). \tag{6.4}$$

Since $N' = S'M'$, the Galois action on $T_{\mathrm{ad}}(\varphi', N')$ is completely determined by the action on $T_{\mathrm{ad}}(\varphi', M')$; in other words the restriction induces a natural isomorphism $\Gamma^{\varphi'}_{\mathrm{ad},N'} \cong \Gamma^{\varphi'}_{\mathrm{ad},M'}$. This together with Proposition 6.1(a) yields an open embedding

$$\Gamma^{\varphi'}_{\mathrm{ad},M'} \hookrightarrow \Gamma^{\varphi'}_{\mathrm{ad}} \ltimes \mathrm{Hom}_{(S')}(M', T_{\mathrm{ad}}(\varphi')). \tag{6.5}$$

The next natural step would be the passage from (K', φ', M') to $(K', \varphi'|A, M')$. However, this runs into the problem that S' does not necessarily act on $T_{\mathrm{ad}}(\varphi'|A)$, because $T_{\mathrm{ad}}(\varphi'|A)$ is obtained from $T_{\mathrm{ad}}(\varphi') \cong \prod_{\mathfrak{p}' \neq \mathfrak{p}'_0} T_{\mathfrak{p}'}(\varphi')$ by removing all factors with $\mathfrak{p}'|\mathfrak{p}'_0$, which are not necessarily preserved by the noncommutative ring S'. Thus if $\mathfrak{p}'_0$ is not the only prime above $\mathfrak{p}_0$, it would be ugly to precisely describe the image of $\mathrm{Hom}_{(S')}(M', T_{\mathrm{ad}}(\varphi'))$ in $\mathrm{Hom}_A(M', T_{\mathrm{ad}}(\varphi'|A))$ in general, though of course it can be done. We therefore restrict ourselves to two special cases, with the following results:

Theorem 6.6. *Assume that A is the center of $\mathrm{End}_{K^{\mathrm{sep}}}(\varphi)$. With $A' := A$ let (K', φ', f, B) be as in Proposition 4.3(c), and set $S := \mathrm{End}_{K^{\mathrm{sep}}}(\varphi|B)$. Let M be a finitely generated torsion free A-submodule of K. Then $\Delta_{\mathrm{ad},M}$ is commensurable with the subgroup $\mathrm{Hom}_{(S)}(M, T_{\mathrm{ad}}(\varphi))$ of $\mathrm{Hom}_A(M, T_{\mathrm{ad}}(\varphi))$, and $\Gamma_{\mathrm{ad},M}$ is commensurable with $\Gamma_{\mathrm{ad}} \ltimes \mathrm{Hom}_{(S)}(M, T_{\mathrm{ad}}(\varphi))$.*

Proof. With the above notation f induces an isomorphism $M \xrightarrow{\sim} M'$ and an embedding of finite index $T_{\mathrm{ad}}(\varphi) \hookrightarrow T_{\mathrm{ad}}(\varphi')$. It also induces an isomorphism

$S \otimes_B \mathrm{Quot}(B) \cong S' \otimes_B \mathrm{Quot}(B)$ under which the intersection of S and S' has finite index in both. Since $T_{\mathrm{ad}}(\varphi)$ and $T_{\mathrm{ad}}(\varphi')$ are torsion free A_{ad}-modules, this implies the equalities and an inclusion of finite index in the diagram

$$\begin{array}{ccc}
\mathrm{Hom}_{(S)}(M, T_{\mathrm{ad}}(\varphi)) & = & \mathrm{Hom}_{(S \cap S')}(M, T_{\mathrm{ad}}(\varphi)) \\
& & \cap \downarrow f \circ (\;) \circ f^{-1} \\
\mathrm{Hom}_{(S')}(M', T_{\mathrm{ad}}(\varphi')) & = & \mathrm{Hom}_{(S \cap S')}(M', T_{\mathrm{ad}}(\varphi')).
\end{array}$$

With (3.2) and the open embedding (6.5) this shows that the image of $\mathrm{Gal}(K^{\mathrm{sep}}/K')$ associated to (K', φ, M) is an open subgroup of $\Gamma_{\mathrm{ad}} \ltimes \mathrm{Hom}_{(S)}(M, T_{\mathrm{ad}}(\varphi))$. This implies the assertion about $\Gamma_{\mathrm{ad}, M}$, from which the assertion about $\Delta_{\mathrm{ad}, M}$ directly follows. $\qquad\square$

In the other special case we drop all assumptions on endomorphisms, but instead assume something about M:

Theorem 6.7. *Let (A', K', φ', f, B) be as in* Proposition 4.3*(c), and set*

$$S' := \mathrm{End}_{K^{\mathrm{sep}}}(\varphi'|B).$$

Let M be a finitely generated torsion free A-submodule of K such that the natural map

$$S' \otimes_A M \to K^{\mathrm{sep}}, \quad \textstyle\sum_i s_i \otimes m_i \mapsto \sum_i s_i f(m_i)$$

is injective. Then $\Delta_{\mathrm{ad}, M}$ is an open subgroup of $\mathrm{Hom}_A(M, T_{\mathrm{ad}}(\varphi))$, and $\Gamma_{\mathrm{ad}, M}$ is an open subgroup of $\Gamma_{\mathrm{ad}} \ltimes \mathrm{Hom}_A(M, T_{\mathrm{ad}}(\varphi))$.

Proof. With the above notation the assumption implies that the natural map

$$S' \otimes_A f(M) \to S' f(M) = N', \quad \textstyle\sum_i s_i' \otimes m_i' \mapsto \sum_i s_i' m_i'$$

is injective and therefore an isomorphism. Thus by Proposition 6.1 the restriction induces a natural isomorphism

$$\mathrm{Hom}_{S'}(N', T_{\mathrm{ad}}(\varphi')) \xrightarrow{\;\sim\;} \mathrm{Hom}_A(f(M), T_{\mathrm{ad}}(\varphi')).$$

The openness of the embedding (6.4), together with the surjectivity in (3.6) for the inclusion $A \subset A'$, thus implies the openness of the embedding

$$\Gamma^{\varphi'|A}_{\mathrm{ad}, f(M)} \hookrightarrow \Gamma^{\varphi'|A}_{\mathrm{ad}} \ltimes \mathrm{Hom}_A(f(M), T_{\mathrm{ad}}(\varphi'|A)).$$

With (3.2) it follows that

$$\Gamma_{\mathrm{ad}, M} \hookrightarrow \Gamma_{\mathrm{ad}} \ltimes \mathrm{Hom}_A(M, T_{\mathrm{ad}}(\varphi))$$

is an open embedding. This proves the assertion about $\Gamma_{\mathrm{ad}, M}$, from which the assertion about $\Delta_{\mathrm{ad}, M}$ directly follows. $\qquad\square$

References

[Chi and Li 2001] W.-C. Chi and A. Li, "Kummer theory of division points over Drinfeld modules of rank one", *J. Pure Appl. Algebra* **156**:2-3 (2001), 171–185. MR 2001k:11233 Zbl 1029.11018

[Deligne and Husemöller 1987] P. Deligne and D. Husemöller, "Survey of Drinfel′d modules", pp. 25–91 in *Current trends in arithmetical algebraic geometry* (Arcata, California, 1985), edited by K. A. Ribet, Contemp. Math. **67**, Amer. Math. Soc., Providence, RI, 1987. MR 89f:11081

[Devic and Pink 2012] A. Devic and R. Pink, "Adelic openness for Drinfeld modules in special characteristic", *J. Number Theory* **132**:7 (2012), 1583–1625. MR 2903172 Zbl 06033752

[Drinfeld 1974] V. G. Drinfel′d, "Elliptic modules", *Mat. Sb.* (*N.S.*) **94**:136 (1974), 594–627, 656. In Russian; translated in *Math. USSR Sbornik* **23**:4 (1974), 561–592. MR 52 #5580

[Goss 1996] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **35**, Springer, Berlin, 1996. MR 97i:11062 Zbl 0874.11004

[Häberli 2011] S. Häberli, *Kummer theory of Drinfeld modules*, Master's thesis, ETH Zürich, 2011, Available at http://www.math.ethz.ch/~pink/Theses/2011-Master-Simon-Haeberli.pdf.

[Hayes 1979] D. R. Hayes, "Explicit class field theory in global function fields", pp. 173–217 in *Studies in algebra and number theory*, edited by G.-C. Rota, Adv. in Math. Suppl. Stud. **6**, Academic Press, New York, 1979. MR 81d:12011 Zbl 0476.12010

[Knebusch 1967] M. Knebusch, "Elementarteilertheorie über Maximalordnungen", *J. Reine Angew. Math.* **226** (1967), 175–183. MR 35 #5433 Zbl 0217.33704

[Li 2001] A. Li, "A note on Kummer theory of division points over singular Drinfeld modules", *Bull. Austral. Math. Soc.* **64**:1 (2001), 15–20. MR 2002f:11065 Zbl 0984.11026

[Pink 2006] R. Pink, "The Galois representations associated to a Drinfeld module in special characteristic, II: Openness", *J. Number Theory* **116**:2 (2006), 348–372. MR 2006k:11108 Zbl 1173.11037

[Pink and Rütsche 2009] R. Pink and E. Rütsche, "Adelic openness for Drinfeld modules in generic characteristic", *J. Number Theory* **129**:4 (2009), 882–907. MR 2010f:11092 Zbl 1246.11122

[Poonen 1995] B. Poonen, "Local height functions and the Mordell–Weil theorem for Drinfel′d modules", *Compositio Math.* **97**:3 (1995), 349–368. MR 96k:11075

[Reiner 2003] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series **28**, The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original. MR 2004c:16026 Zbl 1024.16008

[Ribet 1979] K. A. Ribet, "Kummer theory on extensions of abelian varieties by tori", *Duke Math. J.* **46**:4 (1979), 745–761. MR 81g:14019 Zbl 0428.14018

[Wang 2001] J. T.-Y. Wang, "The Mordell–Weil theorems for Drinfeld modules over finitely generated function fields", *Manuscripta Math.* **106**:3 (2001), 305–314. MR 2002k:11086 Zbl 0992.11039

pink@math.ethz.ch   *Department of Mathematics, ETH Zürich, CH-8092 Zürich, Switzerland*

Parity and symmetry in intersection and ordinary cohomology

Shenghao Sun and Weizhe Zheng

To the memory of Torsten Ekedahl

We show that the Galois representations provided by ℓ-adic cohomology of proper smooth varieties, and more generally by ℓ-adic intersection cohomology of proper varieties, over any field, are orthogonal or symplectic according to the degree. We deduce this from a preservation result of orthogonal and symplectic pure perverse sheaves by proper direct image. We show, moreover, that the subgroup of the Grothendieck group generated by orthogonal pure perverse sheaves of even weights and symplectic pure perverse sheaves of odd weights are preserved by Grothendieck's six operations. Over a finite field, we deduce parity and symmetry results for Jordan blocks appearing in the Frobenius action on intersection cohomology of proper varieties, and virtual parity results for the Frobenius action on ordinary cohomology of arbitrary varieties.

1. Introduction

The n-th cohomology of a compact Kähler manifold X is equipped with a pure Hodge structure of weight n,

$$\mathrm{H}^n(X, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} = \bigoplus_{p+q=n} \mathrm{H}^{pq},$$

where $\mathrm{H}^{pq} \simeq \mathrm{H}^q(X, \Omega_X^p)$ satisfies $\overline{\mathrm{H}^{pq}} = \mathrm{H}^{qp}$. In particular, $\mathrm{H}^n(X, \mathbb{Q})$ is even-dimensional for n odd. Hodge decomposition and Hodge symmetry extend to proper smooth schemes over $\mathbb{C}$ [Deligne 1968, Proposition 5.3] by Chow's lemma and resolution of singularities. Thus, in this case, $\mathrm{H}^n(X(\mathbb{C}), \mathbb{Q})$ is also even-dimensional

for n odd. Moreover, the pure Hodge structure of weight n on $\mathrm{H}^n(X(\mathbb{C}), \mathbb{Q})$ is polarizable, in the sense that there exists a morphism of Hodge structures

$$\mathrm{H}^n(X(\mathbb{C}), \mathbb{Q}) \otimes \mathrm{H}^n(X(\mathbb{C}), \mathbb{Q}) \to \mathbb{Q}(-n),$$

symmetric for n even and alternating for n odd, satisfying certain positivity conditions, which implies that the pairing is perfect.

Now let $\bar{k}$ be a separably closed field of characteristic $p \geq 0$ and let $\ell \neq p$ be a prime number. For a projective smooth scheme X of finite type over $\bar{k}$, the hard Lefschetz theorem [Deligne 1980, Théorème 4.1.1] and Poincaré duality equip the n-th ℓ-adic cohomology $\mathrm{H}^n(X, \mathbb{Q}_\ell)$ of X with a nondegenerate bilinear form that is symmetric for n even and alternating for n odd. In particular, $\mathrm{H}^n(X, \mathbb{Q}_\ell)$ is even-dimensional for n odd. Deligne predicts, in a remark following [1980, Corollaire 4.1.5], that the evenness of the odd-degree Betti numbers should hold more generally for proper smooth schemes over $\bar{k}$. This was recently shown by Suh [2012, Corollary 2.2.3] using crystalline cohomology.

The goal of this article is to study problems of parity and symmetry in more general settings, including symmetry of Galois actions on cohomology. Our approach is different from that of Suh as we do not use p-adic cohomology.

For a general scheme X of finite type over $\bar{k}$, the n-th cohomology $\mathrm{H}^n(X, \mathbb{Q}_\ell)$ is not "pure" and not necessarily even-dimensional for n odd. Before going into results for such mixed situations, let us first state our results in the pure case for intersection cohomology.

Theorem 1.1. *Let k be an arbitrary field of characteristic $p \geq 0$ and let $\bar{k}$ be its separable closure. Let X be a proper, equidimensional scheme over k. Then, for n even (resp. odd), the n-th ℓ-adic intersection cohomology group admits a* $\mathrm{Gal}(\bar{k}/k)$-*equivariant symmetric (resp. alternating) perfect pairing*

$$\mathrm{IH}^n(X_{\bar{k}}, \mathbb{Q}_\ell) \otimes \mathrm{IH}^n(X_{\bar{k}}, \mathbb{Q}_\ell) \to \mathbb{Q}_\ell(-n).$$

Here $\mathrm{Gal}(\bar{k}/k)$ *denotes the Galois group of k, and $X_{\bar{k}} = X \otimes_k \bar{k}$.*

By definition, we have $\mathrm{IH}^n(X_{\bar{k}}, \mathbb{Q}_\ell) = \mathrm{H}^{n-d}(X_{\bar{k}}, \mathrm{IC}_X)$, where $\mathrm{IC}_X = j_{!*}(\mathbb{Q}_\ell[d])$ and $d = \dim(X)$, and where $j : U \to X$ is an open dense immersion such that U_{red} is regular. For X proper smooth, we have $\mathrm{IH}^n(X_{\bar{k}}, \mathbb{Q}_\ell) = \mathrm{H}^n(X_{\bar{k}}, \mathbb{Q}_\ell)$, and the theorem takes the following form. The statement was suggested to us by Takeshi Saito. One may compare such pairings with polarizations of pure Hodge structures, mentioned at the beginning of the Introduction.

Corollary 1.2. *Let X be a proper smooth scheme over k. Then, for n even (resp. odd), the n-th ℓ-adic cohomology group admits a* $\mathrm{Gal}(\bar{k}/k)$-*equivariant symmetric (resp. alternating) perfect pairing*

$$\mathrm{H}^n(X_{\bar{k}}, \mathbb{Q}_\ell) \otimes \mathrm{H}^n(X_{\bar{k}}, \mathbb{Q}_\ell) \to \mathbb{Q}_\ell(-n).$$

Ignoring Galois actions, we obtain the following corollary. For X proper smooth, this gives another proof of Suh's result mentioned earlier.

Corollary 1.3. *Let X be a proper, equidimensional scheme over k. Then $\mathrm{IH}^n(X_{\bar{k}}, \mathbb{Q}_\ell)$ is even-dimensional for n odd.*

To demonstrate the strength of Theorem 1.1, we give a reformulation in the case where $k = \mathbb{F}_q$ is a finite field. In this case, the Galois action is determined by Frobenius action. We let $\mathrm{Frob}_q \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ denote the geometric Frobenius $x \mapsto x^{1/q}$. The eigenvalues of Frob_q acting on $\mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ are q-*Weil integers of weight n*, by which we mean algebraic integers λ such that, for every embedding $\alpha : \mathbb{Q}(\lambda) \to \mathbb{C}$, we have $|\alpha(\lambda)|^2 = q^n$. We let $\mu_\lambda \in \mathbb{Z}_{\geq 0}$ denote the multiplicity of the eigenvalue λ for the action of Frob_q on $\mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$. In other words, we set

$$\det(1 - T\,\mathrm{Frob}_q \mid \mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)) = \prod_\lambda (1 - \lambda T)^{\mu_\lambda}. \qquad (1\text{-}3\text{-}1)$$

For $e \geq 1$, let $\mu_{\lambda,e} \in \mathbb{Z}_{\geq 0}$ denote the number of $e \times e$ Jordan blocks with eigenvalue λ in the Jordan normal form of Frob_q acting on $\mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \bar{\mathbb{Q}}_\ell)$. Then $\mu_\lambda = \sum_{e \geq 1} e\mu_{\lambda,e}$.

Corollary 1.4. *Let X be a proper, equidimensional scheme over $\mathbb{F}_q$. In the above notation, $\mu_{\lambda,e} = \mu_{q^n/\lambda,e}$. Moreover, $\mu_{\sqrt{q^n},e}$ and $\mu_{-\sqrt{q^n},e}$ are even for $n + e$ even. In particular, $\mu_\lambda = \mu_{q^n/\lambda}$ and, for n odd, $\mu_{\sqrt{q^n}}$ and $\mu_{-\sqrt{q^n}}$ are even.*

The last statement of Corollary 1.4 implies that, for n odd,

$$\det(\mathrm{Frob}_q \mid \mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)) = q^{nb_n/2},$$

$$\det(1 - T\,\mathrm{Frob}_q \mid \mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)) = q^{nb_n/2} T^{b_n} \det(1 - q^{-n}T^{-1}\mathrm{Frob}_q \mid \mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)),$$

where $b_n = \dim \mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$. It also implies that $\dim \mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) = \sum_\lambda \mu_\lambda$ is even.

Remark 1.5. Some special cases of the last statement of Corollary 1.4 were previously known.

(1) Gabber's theorem on the independence of ℓ for intersection cohomology [Fujiwara 2002, Theorem 1] states that (1-3-1) belongs to $\mathbb{Z}[T]$ and is independent of ℓ. The fact that (1-3-1) belongs to $\mathbb{Q}[T]$ implies $\mu_\lambda = \mu_{\lambda'}$, for λ and λ' in the same $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbit. In particular, $\mu_\lambda = \mu_{q^n/\lambda}$, and, if q is *not* a square and n is odd, $\mu_{\sqrt{q^n}} = \mu_{-\sqrt{q^n}}$, so that $\dim \mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) = \sum_\lambda \mu_\lambda$ is even in this case.

(2) For X proper smooth, the fact that $\mu_{\sqrt{q^n}}$ and $\mu_{-\sqrt{q^n}}$ are even for n odd follows from a theorem of Suh [2012, Theorem 3.3.1].

Remark 1.6. The first two statements of Corollary 1.4 are consistent with the conjectural semisimplicity of the Frobenius action on $\mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ (namely, $\mu_{\lambda,e} = 0$ for $e \geq 2$), which would follow from the standard conjectures. To see this implication, let $X' \to X$ be a surjective generically finite morphism such that X' is projective

smooth over $\mathbb{F}_q$, which exists by de Jong's alterations [1996, Theorem 4.1]. Then $\mathrm{IH}^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ as a $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-module is a direct summand of $\mathrm{H}^n((X')_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$.[1] The semisimplicity of the Frobenius action on $\mathrm{H}^n((X')_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ would follow from the Lefschetz type standard conjecture for X' and the Hodge type standard conjecture for $X' \times X'$ [Kleiman 1994, Theorem 5.6(2)].

To prove Theorem 1.1, we may assume that k is finitely generated over its prime field. We will keep this assumption in the rest of the Introduction. This includes notably the case of a number field. We deduce Theorem 1.1 from a relative result with coefficients. In the case where k is a finite field, the coefficients are pure perverse sheaves. In the general case, we apply the formalism of pure *horizontal* perverse sheaves of Annette Huber [1997], as extended by Sophie Morel [2012]. Since the proofs are the same in the two cases, we recommend readers not familiar with horizontal perverse sheaves to concentrate on the case of a finite field and to ignore the word "horizontal". Unless otherwise stated, we will only consider the middle perversity. We let $\bar{\mathbb{Q}}_\ell$ denote the algebraic closure of $\mathbb{Q}_\ell$.

Definition 1.7. Let X be a scheme of finite type over k and let $A \in \mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell)$ be a horizontal perverse sheaf on X, pure of weight w. We say that A is *orthogonal* if there exists a symmetric perfect pairing $A \otimes A \to K_X(-w)$. We say that A is *symplectic* if there exists an alternating perfect pairing $A \otimes A \to K_X(-w)$.

Here $K_X = \mathrm{R}a_X^! \bar{\mathbb{Q}}_\ell$ is the dualizing complex on X, where $a_X : X \to \mathrm{Spec}(k)$ is the structural morphism.

Theorem 1.8 (special case of Theorem 5.1.5). *Let $f : X \to Y$ be a proper morphism of schemes of finite type over k and let $A \in \mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell)$ be an orthogonal (resp. symplectic) pure horizontal perverse sheaf on X. Then*

$$\mathrm{R}f_*A \simeq \bigoplus_n ({}^p\mathrm{R}^n f_*A)[-n], \qquad (1\text{-}8\text{-}1)$$

and ${}^p\mathrm{R}^n f_*A$ is orthogonal (resp. symplectic) for n even and symplectic (resp. orthogonal) for n odd.

Recall that the Beilinson–Bernstein–Deligne–Gabber decomposition theorem [Beilinson et al. 1982, Théorème 5.4.5] implies that (1-8-1) holds after base change to the algebraic closure $\bar{k}$ of k.

Theorem 1.1 follows from Theorem 1.8 applied to the morphism $a_X : X \to \mathrm{Spec}(k)$. Even if one is only interested in Theorem 1.1, our proof leads one to consider the relative situation of Theorem 1.8.

Next we state results for operations that do not necessarily preserve pure (horizontal) complexes. For a scheme X of finite type over k, we let $\mathrm{K}_{\mathrm{orth}}(X, \bar{\mathbb{Q}}_\ell)$

---

[1]This argument is also used in Gabber's proof of the integrality of (1-3-1).

denote the subgroup of the Grothendieck group $K(X, \bar{\mathbb{Q}}_\ell)$ of $D_c^b(X, \bar{\mathbb{Q}}_\ell)$ generated by orthogonal pure horizontal perverse sheaves of even weights and symplectic pure horizontal perverse sheaves of odd weights.

Theorem 1.9 (special case of Theorem 5.2.2). *Grothendieck's six operations preserve* K_{orth}.

Note that the preservation of K_{orth} by each of the six operations is nontrivial. The crucial case turns out to be the preservation by the "extension by zero" functor $j_!$ for certain open immersions j (Proposition 4.3.1).

As Michel Gros points out, one may compare these theorems to Morihiko Saito's theory [1990] of mixed Hodge modules. By definition, a mixed Hodge module admits a weight filtration for which the graded pieces are *polarizable* pure Hodge modules. One may compare Definition 1.7 to polarizable pure Hodge modules.

Let us state a consequence of Theorem 1.9 on Galois action on cohomology in the case where $k = \mathbb{F}_q$ is a finite field. Let X be a scheme of finite type over $\mathbb{F}_q$. The eigenvalues of Frob_q acting on $H^*(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ are q-Weil integers[2] of integral weights. We let $m_\lambda \in \mathbb{Z}$ denote the multiplicity of the eigenvalue λ. In other words, we set

$$\prod_n \det(1 - T \, \mathrm{Frob}_q \mid H^n(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell))^{(-1)^n} = \prod_\lambda (1 - \lambda T)^{m_\lambda}. \qquad (1\text{-}9\text{-}1)$$

Applying the theorem to $(a_X)_*$, where $a_X : X \to \mathrm{Spec}(\mathbb{F}_q)$, we obtain the following.

Corollary 1.10. *Let X be a scheme of finite type over $\mathbb{F}_q$. In the above notation, $m_\lambda = m_{q^w/\lambda}$ for every q-Weil integer λ of weight w, and, for w odd, $m_{\sqrt{q^w}}$ and $m_{-\sqrt{q^w}}$ are even. In particular, for w odd, $\sum_\lambda m_\lambda$ (where λ runs through q-Weil integers of weight w), the dimension of the weight-w part of $H^*(X_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell)$, is even.*

Theorem 1.9 also implies analogues of Corollary 1.10 for compactly supported cohomology $H_c^*(X, \mathbb{Q}_\ell)$, and, if X is equidimensional, intersection cohomology $IH^*(X, \mathbb{Q}_\ell)$ and compactly supported intersection cohomology $IH_c^*(X, \mathbb{Q}_\ell)$. In the case of $H_c^*(X, \mathbb{Q}_\ell)$, the analogue of (1-9-1) is the inverse of the zeta function, and the analogue of Corollary 1.10 was established by Suh [2012, Theorem 3.3.1] using rigid cohomology.

Remark 1.11. Some special cases of Corollary 1.10 were previously known. By Gabber's theorem on the independence of ℓ [Fujiwara 2002, Theorem 2], (1-9-1) belongs to $\mathbb{Q}(T)$ and is independent of ℓ. The fact that (1-9-1) belongs to $\mathbb{Q}(T)$ implies that $m_\lambda = m_{\lambda'}$, for λ and λ' in the same $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbit. In particular, $m_\lambda = m_{q^w/\lambda}$ for every q-Weil integer λ of weight w, and, if q is *not* a square and w is odd, $m_{\sqrt{q^w}} = m_{-\sqrt{q^w}}$ so that $\sum_\lambda m_\lambda$ (where λ runs through q-Weil integers of weight w) is even in this case.

---

[2]The integrality is a special case of [Zheng 2008, Variante 5.1].

One ingredient in the proof of Theorem 1.9 is de Jong's alterations. Note that, even for a finite étale cover $f : X \to Y$, one cannot recover the parity of an object on Y from the parity of its pullback to X. More precisely, for an element A in the Grothendieck group of mixed horizontal perverse sheaves on Y such that $f^*A \in K_{orth}$, we do not have $A \in K_{orth}$ in general. We use equivariant alterations to compensate for this loss of information. In order to better deal with the equivariant situation, we will work systematically with Deligne–Mumford stacks in the main text. We note however that the proofs of Theorems 1.1 and 1.8 (and the corollaries to Theorem 1.1) do not depend on stacks, and readers only interested in these results may, in the corresponding portions of the text (Sections 2, 3 and 5.1), assume every stack to be a scheme.

The paper is organized as follows. In Section 2, we study symmetry of complexes and perverse sheaves over a general field. In Section 3, we study symmetry and decomposition of pure complexes over a finite field and prove Theorem 1.8 in this case. In Section 4, we study symmetry in Grothendieck groups over a finite field and prove Theorem 1.9 in this case. In Section 5, we study symmetry of horizontal complexes over a general field finitely generated over its prime field and finish the proof of the theorems. In the Appendix, we collect some general symmetry properties in categories with additional structures, which are used in the main body of the paper.

Conventions. Unless otherwise indicated, X, Y, etc., will denote Deligne–Mumford stacks *of finite presentation* (i.e., of finite type and quasiseparated) over a base field k; this rules out stacks such as $B\mathbb{Z}$. We recall that, for schemes, being of finite presentation over k is the same as being of finite type over k.

We let ℓ denote a prime number invertible in k, and we let $D_c^b(X, \bar{\mathbb{Q}}_\ell)$ denote the derived category of $\bar{\mathbb{Q}}_\ell$-complexes on X. We refer the reader to [Zheng 2015b] for the construction of $D_c^b(X, \bar{\mathbb{Q}}_\ell)$ and of Grothendieck's six operations. We denote by $a_X : X \to \operatorname{Spec}(k)$ the structural morphism, by $K_X := Ra_X^!\bar{\mathbb{Q}}_\ell$ the dualizing complex on X, and by D_X the dualizing functor $D_{K_X} := R\mathcal{H}om(-, K_X)$.

As mentioned above, we will only consider the middle perversity unless otherwise stated. We let $\operatorname{Perv}(X, \bar{\mathbb{Q}}_\ell) \subseteq D_c^b(X, \bar{\mathbb{Q}}_\ell)$ denote the full subcategory of perverse $\bar{\mathbb{Q}}_\ell$-sheaves on X. For a separated quasifinite morphism $f : X \to Y$, the middle extension functor $f_{!*} : \operatorname{Perv}(X, \bar{\mathbb{Q}}_\ell) \to \operatorname{Perv}(Y, \bar{\mathbb{Q}}_\ell)$ is the image of the support-forgetting morphism ${}^p\mathcal{H}^0 f_! \to {}^p\mathcal{H}^0 Rf_*$.

Throughout the article, we let σ and σ' represent elements of $\{\pm 1\}$.

2. Symmetry of complexes and perverse sheaves

In this section, we study symmetry properties of $\bar{\mathbb{Q}}_\ell$-complexes, namely objects of $D_c^b(X, \bar{\mathbb{Q}}_\ell)$, over an arbitrary field k. In Section 2.1, we define σ-self-dual complexes and we study their behavior under operations that commute with duality. In

Section 2.2, we analyze σ-self-dual semisimple perverse sheaves. In this generality none of the results is difficult, but they will be used quite often in the sequel.

2.1. Symmetry of complexes. The tensor product endows $\mathrm{D}^b_c(X, \bar{\mathbb{Q}}_\ell)$ with the structure of a closed symmetric monoidal structure. The definition below only makes use of the symmetry constraint $c_{AB} : A \otimes B \xrightarrow{\sim} B \otimes A$ and the internal mapping object $\mathrm{R}\mathscr{H}om$.

Definition 2.1.1 (σ-self-dual complexes). Let $A, C \in \mathrm{D}^b_c(X, \bar{\mathbb{Q}}_\ell)$. We say that A is *1-self-dual with respect to C* (resp. -1-*self-dual with respect to C*) if there exists a pairing $A \otimes A \to C$ that is

- *symmetric* (resp. *alternating*), in the sense that the diagram

$$A \otimes A \xrightarrow{\quad c_{AA} \quad} A \otimes A$$
$$\searrow \qquad \swarrow$$
$$C \tag{2-1-1}$$

  commutes (resp. anticommutes), and

- *perfect*, in the sense that the pairing induces an isomorphism $A \xrightarrow{\sim} D_C A :=$ $\mathrm{R}\mathscr{H}om(A, C)$.

We say that A is *self-dual with respect to C* if there exists an isomorphism $A \xrightarrow{\sim} D_C A$.

The symmetry of the pairing $A \otimes A \to C$ can also be expressed in terms of the induced morphism $f : A \to D_C A$. In fact, the diagram (2-1-1) σ-commutes if and only if the diagram

$$A \xrightarrow{\quad f \quad} D_C A$$
$$\underset{\mathrm{ev}}{\searrow} \qquad \underset{D_C f}{\nearrow}$$
$$D_C D_C A$$

σ-commutes (Lemma A.4.2).

Remark 2.1.2. Similarly one can define self-dual and σ-self-dual E_λ-complexes, where E_λ is any algebraic extension of $\mathbb{Q}_\ell$. Note that, for $A, C \in \mathrm{D}^b_c(X, E_\lambda)$, A is self-dual (resp. σ-self-dual) with respect to C if and only if $A \otimes_{E_\lambda} \bar{\mathbb{Q}}_\ell$ satisfies the same property with respect to $C \otimes_{E_\lambda} \bar{\mathbb{Q}}_\ell$. Indeed, the "only if" part is obvious. To see the "if" part, consider $U = \mathbf{Isom}(A_{\bar{k}}, D_C A_{\bar{k}})$ as in Lemma 2.1.3 below. Here $A_{\bar{k}}$ denotes the pullback of A to $X_{\bar{k}}$. Recall that rational points form a Zariski dense subset of any affine space over an infinite field. If $A \otimes_{E_\lambda} \bar{\mathbb{Q}}_\ell$ is self-dual (resp. σ-self-dual) with respect to $C \otimes_{E_\lambda} \bar{\mathbb{Q}}_\ell$, then $U \cap V$ is nonempty, and hence has an E_λ-point. Here $V \subseteq \mathbf{Hom}(A_{\bar{k}}, D_C A_{\bar{k}})$ is represented by the E_λ-vector subspace,

image of morphisms (resp. σ-symmetric morphisms) $A \to D_C A$. For the above reason, we will work almost exclusively with $\bar{\mathbb{Q}}_\ell$-complexes.

Lemma 2.1.3. *Let $A, B \in D_c^b(X, E_\lambda)$ satisfy $\dim_{E_\lambda} \operatorname{Hom}(A, B) < \infty$. Then there exists a Zariski open subscheme $U = \mathbf{Isom}(A, B)$ of the affine space $\mathbf{Hom}(A, B)$ over E_λ represented by the E_λ-vector space $\operatorname{Hom}(A, B)$ such that, for any algebraic extension E'_λ of E_λ, the subset $U(E'_\lambda)$ is the set of isomorphisms $A \otimes_{E_\lambda} E'_\lambda \xrightarrow{\sim} B \otimes_{E_\lambda} E'_\lambda$.*

Proof. Assume $A, B \in D^{[a,b]}$. Choose a stratification of X by connected, geometrically unibranch substacks such that the restrictions of $\mathscr{H}^n A$ and $\mathscr{H}^n B$ to each stratum are lisse sheaves. Choose a geometric point x in each stratum. Then a morphism $f : A \otimes_{E_\lambda} E'_\lambda \to B \otimes_{E_\lambda} E'_\lambda$ is an isomorphism if and only if $\mathscr{H}^n f_x$ is for every $n \in [a, b]$ and every x in the finite collection. Then $\mathbf{Isom}(A, B)$ is the intersection of the pullbacks of the open subsets $\mathbf{Isom}(\mathscr{H}^n A_x, \mathscr{H}^n B_x) \subseteq \mathbf{Hom}(\mathscr{H}^n A_x, \mathscr{H}^n B_x)$. $\square$

We will mostly be interested only in duality with respect to Tate twists $K_X(-w)$, $w \in \mathbb{Z}$, of the dualizing complex $K_X = Ra_X^! \bar{\mathbb{Q}}_\ell$. In this case, the evaluation morphism $A \to D_{K_X(-w)} D_{K_X(-w)} A$ is an isomorphism. The functor $D_{K_X(-w)}$ preserves perverse sheaves. We will sometimes write K for K_X when no confusion arises.

In the rest of this subsection, we study the behavior of σ-self-dual complexes under operations that commute with the dualizing functors (up to shift and twist). The results are mostly formal, but for completeness we provide a proof for each result, based on general facts on symmetry in categories collected in the Appendix. Readers willing to accept results may skip the proofs.

Most of the proofs consist of showing that the natural isomorphism representing the commutation of the functor in question with duality is symmetric in the sense of Definition A.3.3. It then follows from Lemma A.3.9 that the functor in question preserves σ-self-dual objects.

Remark 2.1.4 (preservation of σ-self-dual complexes). Let $f : X \to Y$ be a morphism. Let $w, w' \in \mathbb{Z}$.

(1) For $n \in \mathbb{Z}$, Tate twist $A \mapsto A(n)$ carries $\bar{\mathbb{Q}}_\ell$-complexes σ-self-dual with respect to C to $\bar{\mathbb{Q}}_\ell$-complexes σ-self-dual with respect to $C(2n)$; the shift functor $A \mapsto A[n]$ carries $\bar{\mathbb{Q}}_\ell$-complexes σ-self-dual with respect to C to $\bar{\mathbb{Q}}_\ell$-complexes $(-1)^n \sigma$-self-dual with respect to $C[2n]$.

This follows from Lemma A.5.6.

(2) D_X carries $\bar{\mathbb{Q}}_\ell$-complexes σ-self-dual with respect to $K_X(-w)$ to $\bar{\mathbb{Q}}_\ell$-complexes σ-self-dual with respect to $K_X(w)$.

Since $D_X A \simeq (D_{K_X(-w)} A)(w)$, the assertion follows from (1).

(3) Assume that f is proper. Then $Rf_* : D_c^b(X, \bar{\mathbb{Q}}_\ell) \to D_c^b(Y, \bar{\mathbb{Q}}_\ell)$ preserves σ-self-dual objects with respect to $K(-w)$. In other words, Rf_* carries $\bar{\mathbb{Q}}_\ell$-complexes

σ-self-dual with respect to $K_X(-w)$ to $\bar{\mathbb{Q}}_\ell$-complexes σ-self-dual with respect to $K_Y(-w)$.

Since $\mathrm{R}f_*$ is a right-lax symmetric functor (Definition A.1.5), the morphism $\mathrm{R}f_*D_X \to D_{\mathrm{R}f_*K_X}\mathrm{R}f_*$ is symmetric by Construction A.4.6. Composing with the adjunction map $\mathrm{R}f_*K_X \simeq \mathrm{R}f_!K_X \to K_Y$, we obtain a symmetric isomorphism $\mathrm{R}f_*D_X \xrightarrow{\sim} D_Y\mathrm{R}f_*$.

(4) Assume that f is a closed immersion, and let $A \in \mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell)$. Then A is σ-self-dual with respect to $K_X(-w)$ if and only if f_*A is σ-self-dual with respect to $K_Y(-w)$.

Since the functor f_* is fully faithful in this case, the assertion follows from the proof of (3) above and Lemma A.3.9.

(5) Assume that f is an open immersion and let $A \in \mathrm{Perv}(X, \bar{\mathbb{Q}}_\ell)$ be a perverse sheaf. Then A is σ-self-dual with respect to $K_X(-w)$ if and only if $f_{!*}A$ is σ-self-dual with respect to $K_Y(-w)$.

Since $f_!$ is a symmetric functor, the morphism $f_!D_X \to D_{f_!K_X}f_!$ is symmetric by Construction A.4.6. It follows that the composite map in the commutative square

$$
\begin{array}{ccc}
f_!D_X & \xrightarrow{\ \alpha\ } & \mathrm{R}f_*D_X \\
\downarrow & & \simeq \Big\downarrow \beta \\
D_{f_!K_X}f_! & \longrightarrow & D_Y f_!
\end{array}
$$

is symmetric. Here the lower horizontal map is given by the adjunction map $f_!K_X \to K_Y$. Moreover, we have a commutative square

$$
\begin{array}{ccc}
f_{!*}D_X & \xrightarrow[\sim]{\ \gamma\ } & D_Y f_{!*} \\
\downarrow & & \downarrow \\
\mathrm{R}^p\mathrm{R}^0 f_*D_X & \xrightarrow[\sim]{{}^p\mathcal{H}^0\beta} & D_Y\,{}^p\mathrm{R}^0 f_!
\end{array}
$$

By Lemma A.3.10, γ is symmetric. Since the functor $f_{!*}$ is fully faithful by Lemma 2.1.5 below, it suffices to apply Lemma A.3.9. The "if" part also follows from (8) below.

(6) Let $A \in \mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell)$ be σ-self-dual with respect to $K_X(-w)$ and let $B \in \mathrm{D}_c^b(X', \bar{\mathbb{Q}}_\ell)$ be σ'-self-dual with respect to $K_{X'}(-w')$. Then the exterior tensor product $A \boxtimes B$ in $\mathrm{D}_c^b(X \times X', \bar{\mathbb{Q}}_\ell)$ is $\sigma\sigma'$-self-dual with respect to $K_{X\times X'}(-w - w')$.

Since $-\boxtimes-$ is a symmetric monoidal functor, the Künneth isomorphism (see [Grothendieck 1977, Equation (1.7.6), Proposition 2.3])

$$
D_X(-) \boxtimes D_{X'}(-) \xrightarrow{\sim} D_{K_X \boxtimes K_{X'}}(-\boxtimes-) \simeq D_{X\times X'}(-\boxtimes-)
$$

is symmetric by Construction A.4.6.

(7) If f is smooth, purely of dimension d, then $f^*[d]$ carries $\bar{\mathbb{Q}}_\ell$-complexes σ-self-dual with respect to $K_Y(-w)$ to $\bar{\mathbb{Q}}_\ell$-complexes $(-1)^d\sigma$-self-dual with respect to $K_X(-d-w)$.

Since f^* is a symmetric monoidal functor, the isomorphism

$$f^*T^d D_Y \xrightarrow{\sim} D_{f^*K_Y[2d]} f^*T^d \simeq D_{K_X(-d)} f^*T^d$$

is $(-1)^d$-symmetric by Construction A.4.6 and Remark A.5.10.

(8) If X and Y are regular, purely of dimension d and e, respectively, then $f^*[d-e]\colon$ $D^b_{\text{lisse}}(Y, \bar{\mathbb{Q}}_\ell) \to D^b_{\text{lisse}}(X, \bar{\mathbb{Q}}_\ell)$ carries $\bar{\mathbb{Q}}_\ell$-complexes σ-self-dual with respect to $K_Y(-w)$ to $\bar{\mathbb{Q}}_\ell$-complexes $(-1)^{d-e}\sigma$-self-dual with respect to $K_X(-(d-e)-w)$. Here D^b_{lisse} denotes the full subcategory of D^b_c consisting of complexes with lisse cohomology sheaves.

Let $r = d - e$. As in (7), the natural transformation

$$f^*T^r D_Y \to D_{f^*K_Y[2r]} f^*T^r \simeq D_{K_X(-r)} f^*T^r$$

is $(-1)^r$-symmetric. For $A \in D^b_c(Y, \bar{\mathbb{Q}}_\ell)$, this natural transformation can be computed as

$$f^*T^r D_Y A \simeq f^*T^r D_{K_Y(-r)} A \otimes R f^! \bar{\mathbb{Q}}_\ell \xrightarrow{\alpha} R f^! D_{K_Y(-r)} T^r A \simeq D_{K_X(-r)} f^*T^r A.$$

For $A \in D^b_{\text{lisse}}$, α is an isomorphism.

Similar results hold for self-dual $\bar{\mathbb{Q}}_\ell$-complexes.

Lemma 2.1.5. *Let $j\colon U \to X$ be an immersion. Then the functor $j_{!*}\colon \text{Perv}(U, \bar{\mathbb{Q}}_\ell) \to \text{Perv}(X, \bar{\mathbb{Q}}_\ell)$ is fully faithful.*

Proof. Let A and B be perverse $\bar{\mathbb{Q}}_\ell$-sheaves on U, and let $\alpha : \text{Hom}(A, B) \to \text{Hom}(j_{!*}A, j_{!*}B)$ be the map induced by $j_{!*}$. As the composite map

$$\text{Hom}(A,B) \xrightarrow{\alpha} \text{Hom}(j_{!*}A, j_{!*}B) \xrightarrow{\beta} \text{Hom}({}^p\mathscr{H}^0 j_! A, {}^p\mathscr{H}^0 R j_* B) \simeq \text{Hom}(j_! A, R j_* B)$$

is an isomorphism and β is an injection, α is an isomorphism. $\qquad\square$

Example 2.1.6. Assume that X is equidimensional. We define the *intersection complex* of X by $\text{IC}_X = j_{!*}(\mathbb{Q}_\ell[d])$, where $j : U \to X$ is a dominant open immersion such that U_{red} is regular and d equals $\dim X$. Then by parts (5) and (7) of Remark 2.1.4, IC_X is $(-1)^d$-self-dual with respect to $K_X(-d)$.

Although we do not need it, let us mention the following stability of σ-self-dual complexes under nearby cycles.

Remark 2.1.7. Let S be the spectrum of a Henselian discrete valuation ring, of generic point η and closed point s, on which ℓ is invertible. Let $\mathfrak{X}$ be a Deligne–Mumford stack of finite presentation over S. Then the nearby cycle functor

$\mathrm{R}\Psi : \mathrm{D}_c^b(\mathfrak{X}_\eta, \bar{\mathbb{Q}}_\ell) \to \mathrm{D}_c^b(\mathfrak{X}_s \times_s \eta, \bar{\mathbb{Q}}_\ell)$ preserves σ-self-dual objects with respect to $K(-w)$.

Indeed, $\mathrm{R}\Psi$ is a right-lax symmetric monoidal functor. Hence, by Construction A.4.6, the composite $\mathrm{R}\Psi D_{\mathfrak{X}_\eta} \to D_{\mathrm{R}\Psi K \mathfrak{X}_s} \mathrm{R}\Psi \to D_{\mathfrak{X}_s} \mathrm{R}\Psi$, which is a natural isomorphism (see [Illusie 1994, Théorème 4.2]), is symmetric.

Remark 2.1.4(6) can be applied to the exterior tensor power functor $(-)^{\boxtimes m}$: $\mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{D}_c^b(X^m, \bar{\mathbb{Q}}_\ell)$, $m \geq 0$. We now discuss a refinement

$$\mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{D}_c^b([X^m/\mathfrak{S}_m], \bar{\mathbb{Q}}_\ell), \quad A \mapsto A^{\boxtimes m}, \qquad (2\text{-}1\text{-}2)$$

given by permutation. Readers not interested in this refinement may skip this part as it will not be used in the proofs of the results mentioned in the Introduction.

We briefly recall one way to define the symmetric product stack $[X^m/\mathfrak{S}_m]$. For every k-scheme S, the groupoid $[X^m/\mathfrak{S}_m](S)$ is the groupoid of pairs (T, x), where T is a finite étale cover of S of degree m and x is an object of $X(T)$, with isomorphisms of pairs defined in the obvious way.

Remark 2.1.8. The functor (2-1-2) carries complexes σ-self-dual with respect to $K_X(-w)$ to complexes σ^m-self-dual with respect to $K_{[X^m/\mathfrak{S}_m]}(-mw)$.

Indeed, $(-)^{\boxtimes m}$ is a symmetric monoidal functor. Hence, the isomorphism

$$(D_X(-))^{\boxtimes m} \xrightarrow{\sim} D_{K_X^{\boxtimes m}}((-)^{\boxtimes m}) \simeq D_{[X^m/\mathfrak{S}_m]}((-)^{\boxtimes m})$$

is symmetric by Construction A.4.6.

2.2. *Symmetry of perverse sheaves.*

In this subsection, we study σ-self-dual perverse sheaves. We first prove a two-out-of-three property, which will play an important role in later sections. We then discuss a trichotomy for indecomposable perverse $\bar{\mathbb{Q}}_\ell$-sheaves. From this we deduce a criterion for semisimple perverse $\bar{\mathbb{Q}}_\ell$-sheaves to be σ-self-dual in terms of multiplicities of simple factors.

Proposition 2.2.1 (two-out-of-three). *Let A be a perverse $\bar{\mathbb{Q}}_\ell$-sheaf satisfying $A \simeq A' \oplus A''$. If A and A' are σ-self-dual with respect to $K_X(-w)$, then so is A''.*

Proof. We write D for $D_{K_X(-w)}$ and let $f : A \xrightarrow{\sim} DA$ and $g' : A' \xrightarrow{\sim} DA'$ be σ-symmetric isomorphisms. We let $f' : A' \to DA'$ denote the restriction of f to A', namely the composite

$$A' \xrightarrow{i} A \xrightarrow{f}_{\sim} DA \xrightarrow{Di} DA',$$

where $i : A' \to A$ is the inclusion. Let $g : A \to DA$ be the direct sum of g' with the zero map $A'' \to DA''$. These are σ-symmetric morphisms. Consider linear combinations $h_{a,b} = af + bg$ and $h'_{a,b} = af' + bg'$, where $a, b \in \bar{\mathbb{Q}}_\ell$. By Lemma 2.1.3, there are only finitely many values of $(a : b)$ for which $h_{a,b}$ is not an isomorphism. The same holds for $h'_{a,b}$. Therefore, there exist $a, b \in \bar{\mathbb{Q}}_\ell$ such that

$h_{a,b}$ and $h'_{a,b}$ are isomorphisms. Consider the orthogonal complement of A' in A with respect to $h_{a,b}$:

$$B = \mathrm{Ker}(A \xrightarrow[\sim]{h_{a,b}} DA \xrightarrow{Di} DA').$$

Then $h_{a,b}$ induces a σ-symmetric isomorphism $B \xrightarrow{\sim} DB$. Moreover, $A \simeq A' \oplus B$, so that $B \simeq A''$. Here we used the Krull–Schmidt theorem [Atiyah 1956, Theorem 1] and the fact that perverse sheaves have finite lengths. □

Remark 2.2.2. The two-out-of-three property also holds more trivially for self-dual complexes. In fact, if we have decompositions of perverse $\bar{\mathbb{Q}}_\ell$-sheaves $A \simeq A' \oplus A''$ and $B \simeq B' \oplus B''$ such that $A \simeq D_X B(-w)$ and $A' \simeq D_X B'(-w)$, then we have $A'' \simeq D_X B''(-w)$ by the Krull–Schmidt theorem.

Proposition 2.2.3 (trichotomy). *Let A be an indecomposable perverse $\bar{\mathbb{Q}}_\ell$-sheaf on X. Then exactly one of the following occurs*:

- *A is 1-self-dual with respect to $K_X(-w)$;*
- *A is -1-self-dual with respect to $K_X(-w)$;*
- *A is not self-dual with respect to $K_X(-w)$.*

This follows from general facts (Lemma A.2.7 and Remark A.2.8) applied to the category of perverse $\bar{\mathbb{Q}}_\ell$-sheaves.

Remark 2.2.4. In the case of a simple perverse $\bar{\mathbb{Q}}_\ell$-sheaf, the proof can be somewhat simplified with the help of Schur's lemma. This case is analogous to a standard result on complex representations of finite or compact groups [Serre 1998, Section 13.2, Proposition 38; Bröcker and tom Dieck 1995, Proposition II.6.5].

Remark 2.2.5. An indecomposable perverse E_λ-sheaf on X, self-dual with respect to $K_X(-w)$, is either 1-self-dual or -1-self-dual, by Lemma A.2.7 and Remark A.2.8. Note that a simple perverse E_λ-sheaf can be 1-self-dual and -1-self-dual with respect to $K_X(-w)$ at the same time.

Corollary 2.2.6. *Let $A \simeq \bigoplus_B B^{n_B}$ be a semisimple perverse $\bar{\mathbb{Q}}_\ell$-sheaf on X, where B runs through isomorphism classes of simple perverse $\bar{\mathbb{Q}}_\ell$-sheaves on X. Then A is σ-self-dual with respect to $K_X(-w)$ if and only if the following conditions hold*:

(1) *$n_B = n_{(D_X B)(-w)}$ for B not self-dual with respect to $K_X(-w)$;*

(2) *n_B is even for B that are $-\sigma$-self-dual with respect to $K_X(-w)$.*

Moreover, A is self-dual with respect to $K_X(-w)$ if and only if (1) holds.

In particular, if B and B' are respectively 1-self-dual and -1-self-dual simple perverse sheaves on X, then $B \oplus B'$ is self-dual but neither 1-self-dual nor -1-self-dual.

Proof. It is clear that (1) is equivalent to the condition that A is self-dual. If (1) and (2) hold, then A is σ-self-dual by Proposition 2.2.3 and the fact that $B \oplus (D_X B)(-w)$ is σ-self-dual with respect to $K_X(-w)$ for all B (Remark A.2.6(2)). It remains to show that if A is σ-self-dual, then (2) holds. Let B be $-\sigma$-self-dual. As $B^{\oplus n_B} \simeq B \otimes V$ is σ-self-dual, where $V = \bar{\mathbb{Q}}_\ell^{\oplus n_B}$, the isomorphism

$$\mathrm{Hom}(B \otimes V, D_X(B \otimes V)(-w))$$
$$\simeq \mathrm{Hom}(B, (D_X B)(-w)) \otimes \mathrm{Hom}(V, V^*) \simeq \mathrm{Hom}(V, V^*)$$

provides a skew-symmetric $n_B \times n_B$ matrix with entries in $\bar{\mathbb{Q}}_\ell$, which implies that n_B is even. More formally, we can apply the second part of Lemma A.3.9 to the fully faithful functor $F : V \mapsto B \otimes V$ from the category of finite-dimensional $\bar{\mathbb{Q}}_\ell$-vector spaces to $D_c^b(X, \bar{\mathbb{Q}}_\ell)$. The natural isomorphism $FD \xrightarrow{\sim} D_{K_X(-w)} F$ is $-\sigma$-self-dual. $\square$

Remark 2.2.7. The semisimplification of a σ-self-dual perverse sheaf is σ-self-dual by Lemma A.2.9. The converse does not hold. See Example 3.1.5 below.

We will need to consider more generally geometrically semisimple perverse sheaves, namely perverse sheaves whose pullbacks to $X_{\bar{k}}$ are semisimple. Part (1) of the following lemma extends [Beilinson et al. 1982, Corollaire 5.3.11] for pure perverse sheaves.

Lemma 2.2.8. *Let A be a geometrically semisimple perverse $\bar{\mathbb{Q}}_\ell$-sheaf on X.*

(1) *Let $i : Y \to X$ be a closed immersion with complementary open immersion $j : U \to X$. Then A admits a unique decomposition $A \simeq j_{!*} j^* A \oplus i_* B$, where B is a perverse sheaf on Y. Moreover, we have $B \simeq {}^p\mathcal{H}^0 i^* A \simeq {}^p R^0 i^! A$.*

(2) *A admits a unique decomposition $A \simeq \bigoplus_V A_V$, where V runs through irreducible closed substacks of X, and the support of each indecomposable direct summand of the perverse sheaf A_V is V.*

Assume additionally that A is indecomposable. Then, by part (1) of the lemma, we have $j_{!*} j^* A \simeq A$ if U intersects with the support of A (and $j^* A = 0$ otherwise). Moreover, the support of A is irreducible, and A is isomorphic to $f_{!*}(\mathcal{F}[d])$ for some immersion $f : W \to X$, with W regular irreducible of dimension d, and some lisse $\bar{\mathbb{Q}}_\ell$-sheaf $\mathcal{F}$ on V.

Proof. (1) The proof is identical to that of [Beilinson et al. 1982, Corollaire 5.3.11]. The uniqueness of the decomposition is clear. For existence, it suffices to check that

- the adjunction map ${}^p\mathcal{H}^0 j_! j^* A \to A$ factorizes through the quotient $j_{!*} j^* A$ of ${}^p\mathcal{H}^0 j_! j^* A$, and the adjunction map $A \to {}^p R^0 j_* j^* A$ factorizes through the subobject $j_{!*} j^* A$ of ${}^p R^0 j_* j^* A$;

- the composite of the adjunction maps $i_* {}^p\mathrm{R}^0 i^! A \to A \to i_* {}^p\mathcal{H}^0 i^* A$ is an isomorphism;

and these maps provide a decomposition of A. These statements can be easily checked over $\bar{k}$.

(2) Again the uniqueness is clear. The existence follows from the fact that the support of every indecomposable direct summand of A is irreducible. $\square$

Remark 2.2.9. In Lemma 2.2.8, A is σ-self-dual with respect to $K_X(-w)$ if and only if each direct summand A_V in the support decomposition is σ-self-dual with respect to $K_X(-w)$.

As an application, we show that for geometrically semisimple perverse sheaves the property of being σ-self-dual is local for the Zariski topology. This Zariski local nature will be useful in Section 4.

Proposition 2.2.10. Let $(X_\alpha)_{\alpha \in I}$ be a Zariski open covering of X, and let A and B be geometrically semisimple perverse $\bar{\mathbb{Q}}_\ell$-sheaves on X. Then $A \simeq (D_X B)(-w)$ if and only if $A \mid X_\alpha \simeq (D_{X_\alpha} B \mid X_\alpha)(-w)$ for every $\alpha \in I$. Moreover, A is σ-self-dual with respect to $K_X(-w)$ if and only if $A \mid X_\alpha$ is so with respect to $K_{X_\alpha}(-w)$ for every $\alpha \in I$.

Proof. We prove the second assertion, the proof of the first assertion being simpler. It suffices to show the "if" part. Let $j_\alpha : X_\alpha \to X$. By parts (5) and (8) of Remark 2.1.4, $j_{\alpha!*} j_\alpha^* A$ is σ-self-dual. Since $j_{\alpha!*} j_\alpha^* A \simeq \bigoplus_V A_V$, where V satisfies $V \cap X_\alpha \neq \varnothing$, we conclude that each A_V is σ-self-dual.

Alternatively we may apply Lemma 2.2.11 below. Indeed, by quasicompactness, we may assume that I is finite. For $J \subseteq I$ nonempty, $j_{J!*} j_J^* A$ is σ-self-dual. Thus the same holds for $A \simeq j_{\varnothing!*} j_\varnothing^* A$ by the two-out-of-three property. $\square$

Lemma 2.2.11. Let $(X_\alpha)_{\alpha \in I}$ be a finite Zariski open covering of X, and let A be a geometrically semisimple perverse $\bar{\mathbb{Q}}_\ell$-sheaf on X. Then

$$\bigoplus_{\substack{J \subseteq I \\ \#J \text{ even}}} j_{J!*} j_J^* A \simeq \bigoplus_{\substack{J \subseteq I \\ \#J \text{ odd}}} j_{J!*} j_J^* A,$$

where $j_J : \bigcap_{\alpha \in J} X_\alpha \to X$ is the open immersion.

Proof. We may assume that A is indecomposable. Then both sides are direct sums of copies of A and the multiplicities are equal:

$$\sum_{\substack{0 \le i \le m \\ i \text{ even}}} \binom{m}{i} = \sum_{\substack{0 \le i \le m \\ i \text{ odd}}} \binom{m}{i}.$$

Here $m \ge 1$ is the number of indices $\alpha \in I$ such that the support of A intersects with X_α. $\square$

3. Symmetry and decomposition of pure complexes

In this section, we study symmetry of pure perverse sheaves and, more generally, of pure complexes that decompose into shifts of perverse sheaves. We first work over a finite field. In Section 3.1, we analyze σ-self-dual pure perverse sheaves and give a criterion in terms of multiplicities of factors. In Section 3.2, we study the behavior of such perverse sheaves under operations that preserve purity. The main result of this section is the preservation of a certain class of complexes under derived proper direct image (Theorem 3.2.3), which implies the finite field case of Theorem 1.8. Such preservation results constitute the starting point of the analysis in Section 4 of the effects of more general operations in the mixed case. In Section 3.3, we work over a separably closed base field and we prove preservation results for certain semisimple complexes, by reducing to the finite field case.

3.1. *Symmetry of pure perverse sheaves over a finite field.* In this subsection and the next, we work over a finite field $k = \mathbb{F}_q$. Recall that X, Y, etc., denote Deligne–Mumford stacks of finite presentation over $\mathbb{F}_q$. Let $\iota : \bar{\mathbb{Q}}_\ell \to \mathbb{C}$ be an embedding.

In this subsection, we study σ-self-dual ι-pure perverse sheaves. We give a criterion for ι-pure perverse sheaves to be σ-self-dual in terms of multiplicities of factors.

For $n \geq 1$, let E_n be the sheaf on $\mathrm{Spec}(\mathbb{F}_q)$ of stalk $(\bar{\mathbb{Q}}_\ell)^n = \bigoplus_{i=1}^{n} \bar{\mathbb{Q}}_\ell e_i$ on which Frobenius $F = \mathrm{Frob}_q$ acts unipotently with one Jordan block: $F e_1 = e_1$ and $F e_i = e_i + e_{i-1}$ for $i > 1$. Recall that any indecomposable ι-pure perverse sheaf A on X is isomorphic to a perverse sheaf of the form $B \otimes a_X^* E_n$, where B is a simple perverse sheaf on X, $n \geq 1$, and where $a_X : X \to \mathrm{Spec}(\mathbb{F}_q)$.

Proposition 3.1.1. *Let $w \in \mathbb{Z}$, and let A be a perverse $\bar{\mathbb{Q}}_\ell$-sheaf on X, isomorphic to $\bigoplus_B (B \otimes a_X^* E_n)^{m_{B,n}}$, where B runs over simple perverse $\bar{\mathbb{Q}}_\ell$-sheaves on X. Then A is σ-self-dual with respect to $K_X(-w)$ if and only if the following conditions hold:*

(1) $m_{B,n} = m_{(D_X B)(-w),n}$ *for B not self-dual with respect to $K_X(-w)$;*

(2) $m_{B,n}$ *is even for B σ-self-dual with respect to $K_X(-w)$ and n even;*

(3) $m_{B,n}$ *is even for B $-\sigma$-self-dual with respect to $K_X(-w)$ and n odd.*

Moreover, A is self-dual with respect to $K_X(-w)$ if and only if (1) holds.

Proof. The equivalence between (1) and the condition that A is self-dual follows from the isomorphism $D_X(B \otimes a_X^* E_n) \simeq D_X B \otimes a_X^* E_n$. For the "if" part of the σ-self-dual case, note that $C \oplus D_X C(-w)$ is σ-self dual with respect to $K_X(-w)$, so that, by the trichotomy in Proposition 2.2.3, it suffices to show that $B \otimes a_X^* E_n$ is σ'-self-dual (resp. $-\sigma'$-self-dual) for B σ'-self-dual and n odd (resp. even). For the "only if" part, we reduce to the case where $m_{B,n} = 0$ for all B except for one σ'-self-dual B. For both parts, consider the functor $F = B \otimes a_X^* - : \mathrm{Perv}(\mathrm{Spec}(\mathbb{F}_q), \bar{\mathbb{Q}}_\ell) \to \mathrm{Perv}(X, \bar{\mathbb{Q}}_\ell)$, which is fully faithful by Lemma 3.1.2 below. The natural isomorphism $F D_{\mathrm{Spec}(\mathbb{F}_q)} \simeq$

$D_{K_X(-w)}F$ is σ'-symmetric. By Lemma A.3.8, we are then reduced to the case where $X = \mathrm{Spec}(\mathbb{F}_q)$ and $B = (\bar{\mathbb{Q}}_\ell)_X$, which follows from Lemma 3.1.3 below. $\square$

Lemma 3.1.2. *Let B be a simple perverse $\bar{\mathbb{Q}}_\ell$-sheaf on X. Then the functor $B \otimes a_X^* -$ is fully faithful. In other words, for $\bar{\mathbb{Q}}_\ell$-sheaves E and E' on $\mathrm{Spec}(\mathbb{F}_q)$, the map $\alpha : \mathrm{Hom}(E, E') \to \mathrm{Hom}(B \otimes a_X^* E, B \otimes a_X^* E')$ is an isomorphism.*

Proof. We have $B \simeq j_{!*}(\mathscr{F}[d])$, where $j : U \to X$ is an immersion, with U_{red} connected regular, purely of dimension d, and where $\mathscr{F}$ is a simple lisse $\bar{\mathbb{Q}}_\ell$-sheaf on U. We have $B \otimes a_X^* E \simeq j_{!*}((\mathscr{F} \otimes a_U^* E)[d])$. The map α is the composite

$$\mathrm{Hom}(E, E') \xrightarrow{\beta} \mathrm{Hom}(\mathscr{F} \otimes a_U^* E, \mathscr{F} \otimes a_U^* E') \xrightarrow{\gamma} \mathrm{Hom}(B \otimes a_X^* E, B \otimes a_X^* E'),$$

where γ is an isomorphism by Lemma 2.1.5. The map β is obviously injective. To show that β is an isomorphism, we may assume that $E = E_n$, $E' = E_m$. Since the socle of $\mathscr{F} \otimes a_U^* E_m$ is $\mathscr{F}$,

$$\mathrm{Hom}(\mathscr{F}, \mathscr{F}) \simeq \mathrm{Hom}(\mathscr{F}, \mathscr{F} \otimes a_U^* E_m)$$

is one-dimensional. Dually, since the cosocle of $\mathscr{F} \otimes a_U^* E_n$ is $\mathscr{F}$,

$$\mathrm{Hom}(\mathscr{F} \otimes a_U^* E_n, \mathscr{F}) \simeq \mathrm{Hom}(\mathscr{F}, \mathscr{F})$$

is one-dimensional. Thus

$$\dim \mathrm{Hom}(\mathscr{F} \otimes a_U^* E_n, \mathscr{F} \otimes a_U^* E_m) \leq \min\{n, m\} = \dim \mathrm{Hom}(E_n, E_m).$$

It follows that β is an isomorphism. $\square$

Lemma 3.1.3. *Let L be a field of characteristic $\neq 2$, and let $N_n \in \mathrm{M}_{n \times n}(L)$ be the matrix defined by $(N_n)_{i,j} = 1$ for $i = j - 1$ and $(N_n)_{i,j} = 0$ otherwise. Let $m_1, \ldots, m_l \geq 0$ be integers, and let*

$$N := N(m_1, \ldots, m_l) := \mathrm{diag}(N_1, \ldots, N_1, \ldots, N_l, \ldots, N_l),$$

where each N_n is repeated m_n times. Then there exists an invertible symmetric (resp. invertible skew-symmetric) matrix A such that $AN = -N^T A$ if and only if m_n is even for n even (resp. m_n is even for n odd).

For L of characteristic 0, the equality is equivalent to $\exp(N)^T A \exp(N) = A$.

Proof. We denote the entries of A by $a_{n,c,i}^{n',c',i'}$, where

$$1 \leq n, n' \leq l, \quad 1 \leq c \leq m_n, \quad 1 \leq c' \leq m_{n'}, \quad 1 \leq i \leq n, \quad 1 \leq i' \leq n'.$$

Then we have $AN = -N^T A$ if and only if $a_{n,c,i}^{n',c',i'} = -a_{n,c,i-1}^{n',c',i'+1}$ for $1 < i \leq n$, $1 \leq i' < n'$ and $a_{n,c,i}^{n',c',i'} = 0$ for $i + i' \leq \max\{n, n'\}$. Let A_n be the $n \times n$ matrix given by $(A_n)_{ij} = (-1)^i$ for $i + j = n + 1$ and $(A_n)_{ij} = 0$ otherwise. For $N = N_n$, n odd (resp. even), we can take $A = A_n$. For $N = \mathrm{diag}(N_n, N_n)$, n even (resp. odd), we

can take $A = \begin{pmatrix} 0 & A_n \\ -A_n & 0 \end{pmatrix}$. The "if" part follows. The "only if" part follows from the case $\sigma = -1$ of Proposition A.6.8, because P_{1-n} is $(-1)^{1-n}$-self-dual (resp. $(-1)^n$-self-dual) and $\dim P_{1-n}$ equals m_n. Let us give a more elementary proof of the "only if" part by induction on l. For $l = 1$, the assertion is void (resp. A defines a nondegenerate alternating bilinear form on an m_1-dimensional vector space, which implies that m_1 is even). For $l \geq 2$, consider the $m_l \times m_l$ submatrices $B = \left(a^{l,c',l}_{l,c,1}\right)_{c,c'}$, $C = \left(a^{l,c',1}_{l,c,l}\right)_{c,c'}$ of A. Let A' be the matrix obtained from A by removing the rows and columns in A that contain entries of B or C. Note that for $i' < l$ we have $a^{n',c',i'}_{l,c,1} = 0$, and for $i < l$ we have $a^{l,c',1}_{n,c,i} = 0$. Thus, up to reordering the indices, we have

$$A = \begin{pmatrix} A' & 0 & B' \\ 0 & 0 & B \\ C' & C & D \end{pmatrix}.$$

It follows that $B^T = \sigma'C = (-1)^{l-1}\sigma'B$, where $\sigma' = 1$ (resp. $\sigma' = -1$), and that B is invertible, so that m_l is even for l even (resp. l odd). Moreover, A' is invertible symmetric (resp. invertible skew-symmetric) and $A'N' = -N'^T A'$, where $N' = N(m_1, \ldots, m_{l-3}, m_{l-2} + m_l, m_{l-1})$ ($N' = N(m_1)$ for $l = 2$). The assertion then follows from the induction hypothesis. $\square$

Example 3.1.4. Let A and A' be sheaves on $X = \operatorname{Spec}(\mathbb{F}_q)$ and let $w \in \mathbb{Z}$. For $n \geq 1$ and $\lambda \in \bar{\mathbb{Q}}_\ell^\times$, we let $\mu_{\lambda,n}$ and $\mu'_{\lambda,n}$ denote the number of $n \times n$ Jordan blocks of eigenvalue λ in the Jordan normal forms of the Frobenius Frob_q acting on $A_{\bar{\mathbb{F}}_q}$ and $(A')_{\bar{\mathbb{F}}_q}$, respectively. Then:

- $A \simeq (D_X A')(-w)$ if and only if $\mu_{\lambda,n} = \mu'_{q^w/\lambda,n}$ for all $n \geq 1$ and all λ. In particular, A is self-dual with respect to $\bar{\mathbb{Q}}_\ell(-w)$ if and only if $\mu_{\lambda,n} = \mu_{q^w/\lambda,n}$ for all $n \geq 1$ and all λ. Note that the last condition trivially holds for $\lambda = \pm q^{w/2}$.

- A is 1-self-dual (resp. -1-self-dual) with respect to $\bar{\mathbb{Q}}_\ell(-w)$ if and only if it is self-dual with respect to $\bar{\mathbb{Q}}_\ell(-w)$ and $\mu_{q^{w/2},n}$, $\mu_{-q^{w/2},n}$ are even for n even (resp. n odd).

Example 3.1.5. Let B be a simple perverse sheaf ι-pure of weight w, not self-dual with respect to $K_X(-w)$. Then $A = B^{\oplus 2} \oplus ((D_X B)(-w) \otimes a_X^* E_2)$ is not self-dual, but the semisimplification of A is both 1-self-dual and -1-self-dual.

Remark 3.1.6. (1) An ι-pure complex self-dual with respect to $K_X(-w)$ is necessarily of weight w.

(2) Every simple perverse $\bar{\mathbb{Q}}_\ell$-sheaf is ι-pure by a theorem of Lafforgue [2002, Corollaire VII.8] (with a gap filled by Deligne [2012, Théorème 1.6]; see [Sun 2012b, Remark 2.8.1] for the case of stacks).

(3) The two-out-of-three property (Proposition 2.2.1) in the case of ι-pure perverse sheaves also follows from the criterion of Proposition 3.1.1.

(4) Since ι-pure perverse sheaves are geometrically semisimple, for such perverse sheaves the property of being self-dual (resp. σ-self-dual) is local for the Zariski topology by Proposition 2.2.10.

3.2. *Symmetry and decomposition of pure complexes over a finite field.* In this subsection, we study the behavior of σ-self-dual ι-pure perverse sheaves under operations that preserve purity. The main goal is to prove the finite field case of Theorem 1.8 on derived proper direct image of σ-self-dual ι-pure perverse sheaves. The behavior of σ-self-dual complexes has already been described in Section 2.1. The focus of this subsection is on decomposition and on the self-duality of individual perverse cohomology sheaves. To state our results, it is convenient to introduce the following terminology.

Definition 3.2.1 (split complexes). We say that a complex of $\bar{\mathbb{Q}}_\ell$-sheaves A is *split* if it is a direct sum of shifts of perverse sheaves, or, in other words, if $A \simeq \bigoplus_i ({}^p\mathscr{H}^i A)[-i]$.

Definition 3.2.2 ($\mathrm{D}^w_{\iota,\sigma}$). Let $w \in \mathbb{Z}$. Denote by $\mathrm{D}^w_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{Ob}(\mathrm{D}^b_c(X, \bar{\mathbb{Q}}_\ell))$ (resp. $\mathrm{D}^w_{\iota,\mathrm{sd}}(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{Ob}(\mathrm{D}^b_c(X, \bar{\mathbb{Q}}_\ell))$) the subset consisting of split ι-pure complexes A of weight w such that ${}^p\mathscr{H}^i A$ is $(-1)^{w+i}\sigma$-self-dual (resp. self-dual) with respect to $K_X(-w-i)$ for all i. Denote by $\mathrm{D}^w_{\iota,\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{Ob}(\mathrm{D}^b_c(X, \bar{\mathbb{Q}}_\ell) \times \mathrm{D}^b_c(X, \bar{\mathbb{Q}}_\ell))$ the subset consisting of pairs (A, B) of split ι-pure complexes of weight w such that ${}^p\mathscr{H}^i A$ is isomorphic to $(D_X {}^p\mathscr{H}^i B)(-w-i)$ for all i.

By definition, we have $\mathrm{D}^w_{\iota,\mathrm{sd}}(X, \bar{\mathbb{Q}}_\ell) = \Delta^{-1}(\mathrm{D}^w_{\iota,\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell))$, where $\Delta : \mathrm{D}^b_c(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{D}^b_c(X, \bar{\mathbb{Q}}_\ell) \times \mathrm{D}^b_c(X, \bar{\mathbb{Q}}_\ell)$ is the diagonal embedding.

Since in this subsection we will only consider operations that preserve purity, the factor $(-1)^w$ in the definition above is fixed, hence not essential. We include this factor here to make the definition compatible with the mixed case studied in Section 4, where the factor is essential (see Definition 4.2.1).

The main result of this section is the following preservation result under proper direct image, which clearly implies the finite field case of Theorem 1.8.

Theorem 3.2.3. *Let $f : X \to Y$ be a proper morphism of Deligne–Mumford stacks of finite presentation over $\mathbb{F}_q$, where Y has finite inertia. Then $\mathrm{R}f_*$ preserves $\mathrm{D}^w_{\iota,\sigma}$ and $\mathrm{D}^w_{\iota,\mathrm{d}}$. In other words, for $A \in \mathrm{D}^w_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$ we have $\mathrm{R}f_*A \in \mathrm{D}^w_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell)$, and for $(A, B) \in \mathrm{D}^w_{\iota,\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell)$ we have $(\mathrm{R}f_*A, \mathrm{R}f_*B) \in \mathrm{D}^w_{\iota,\mathrm{d}}$.*

The preservation of $\mathrm{D}^w_{\iota,\mathrm{d}}$ has the following two consequences, obtained respectively by considering the diagonal embedding and the first factor.

Corollary 3.2.4. *Let $f : X \to Y$ be a proper morphism, where Y has finite inertia. Then $\mathrm{R}f_*$ preserves $\mathrm{D}^w_{\iota,\mathrm{sd}}$.*

Corollary 3.2.5. *Let $f : X \to Y$ be a proper morphism, where Y has finite inertia. Then $\mathrm{R}f_*$ preserves split ι-pure complexes of weight w. In other words, if A is a split ι-pure complex of weight w on X, then $\mathrm{R}f_*A$ is a split ι-pure complex of weight w on Y.*

Corollary 3.2.5 clearly extends to the case where $w \in \mathbb{R}$. Recall that the Beilinson–Bernstein–Deligne–Gabber decomposition theorem [Beilinson et al. 1982, Théorème 5.4.5] ([Sun 2012a, Theorem 1.2] for the case of stacks) implies that the pullback of $\mathrm{R}f_*A$ (or any ι-pure complex on Y) to $Y \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q$ is split.

Remark 3.2.6. For $w \in \mathbb{Z}$, let $\mathrm{D}_{\iota,\mathrm{spl}}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell)$ be the full subcategory consisting of split ι-pure complexes of weight w. Consider the twisted dualizing functor $\bar{D}_{\iota,X}^w : \mathrm{D}_{\iota,\mathrm{spl}}^w(X, \bar{\mathbb{Q}}_\ell)^{\mathrm{op}} \to \mathrm{D}_{\iota,\mathrm{spl}}^w(X, \bar{\mathbb{Q}}_\ell)$ that carries each complex A to $\bigoplus_i (D_X{}^p\mathscr{H}^iA)(-w-i)[-i]$. Then $\mathrm{D}_{\iota,\mathrm{d}}^w$ is the collection of pairs $(A, \bar{D}_{\iota,X}^wA)$. Thus the preservation of $\mathrm{D}_{\iota,\mathrm{d}}^w$ by $\mathrm{R}f_*$ is equivalent to the preservation of $\mathrm{D}_{\iota,\mathrm{spl}}^w$ and the existence of an isomorphism $\mathrm{R}f_*\bar{D}_{\iota,X}^wA \simeq \bar{D}_{\iota,X}^w\mathrm{R}f_*A$ for every object A of $\mathrm{D}_{\iota,\mathrm{spl}}^w(X, \bar{\mathbb{Q}}_\ell)$. Our proof of Theorem 3.2.3 relies on the two-out-of-three property, and the resulting isomorphism is not necessarily functorial in A. Thus our proof does *not* provide a natural isomorphism between the functors $\mathrm{R}f_*\bar{D}_{\iota,X}^w$ and $\bar{D}_{\iota,X}^w\mathrm{R}f_*$.

Let us first recall that the following operations preserve ι-pure complexes [Beilinson et al. 1982, Stabilités 5.1.14, Corollaire 5.4.3] ([Sun 2012a] for the case of stacks). The proof makes use of the fact that these operations commute with duality (up to shift and twist).

Remark 3.2.7 (preservation of ι-pure complexes). Let $f : X \to Y$ be a morphism, and let $w, w' \in \mathbb{R}$.

(1) For $A \in \mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell)$ ι-pure of weight w, $A(n)$ is ι-pure of weight $w - 2n$ and $A[n]$ is ι-pure of weight $w + n$ for $n \in \mathbb{Z}$.

(2) $A \in \mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell)$ is ι-pure of weight w if and only if $D_X A$ is ι-pure of weight $-w$.

(3) If f is an open immersion, the functor $f_{!*}$ preserves ι-pure perverse sheaves of weight w.

(4) Assume that f is smooth. Then f^* preserves ι-pure complexes of weight w. Moreover, if f is surjective, then $A \in \mathrm{D}_c^b(Y, \bar{\mathbb{Q}}_\ell)$ is ι-pure of weight w if and only if f^*A is so.

(5) Assume that X and Y are regular. Then f^* preserves ι-pure complexes of weight w in $\mathrm{D}_{\mathrm{lisse}}^b$. Moreover, if f is surjective, then $A \in \mathrm{D}_{\mathrm{lisse}}^b(Y, \bar{\mathbb{Q}}_\ell)$ is ι-pure of weight w if and only if f^*A is so.

(6) For $A \in \mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell)$ ι-pure of weight w and $A' \in \mathrm{D}_c^b(X', \bar{\mathbb{Q}}_\ell)$ ι-pure of weight w', $A \boxtimes A' \in \mathrm{D}_c^b(X \times X', \bar{\mathbb{Q}}_\ell)$ is ι-pure of weight $w + w'$.

(7) $A \in D_c^b(X, \bar{\mathbb{Q}}_\ell)$ is ι-pure of weight w if and only if $A^{\boxtimes m} \in D_c^b([X^m/\mathfrak{S}_m], \bar{\mathbb{Q}}_\ell)$ is ι-pure of weight mw, where $m \geq 1$.

(8) If f is a proper morphism, $\mathrm{R}f_*$ preserves ι-pure complexes of weight w.

(9) Assume that f is a closed immersion and let $A \in D_c^b(X, \bar{\mathbb{Q}}_\ell)$. Then A is ι-pure of weight w if and only if f_*A is so.

Recall that these operations also preserve σ-self-dual complexes (Remark 2.1.4). With the exception of derived proper direct image, the operations also preserve perversity (up to shift). Hence, they also preserve $D_{\iota,\sigma}^w$, up to modification of w and σ. The details are given below. The case of $(-)^{\boxtimes m}$ requires some additional arguments and will be given in Proposition 3.2.14 later.

Remark 3.2.8 (preservation of $D_{\iota,\sigma}^w$, easy part). Let $f : X \to Y$ be a morphism, and let $w, w' \in \mathbb{Z}$.

(1) If $A \in D_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$, then $A[n] \in D_{\iota,\sigma}^{w+n}(X, \bar{\mathbb{Q}}_\ell)$ and $A(n) \in D_{\iota,\sigma}^{w-2n}(X, \bar{\mathbb{Q}}_\ell)$ for $n \in \mathbb{Z}$.

(2) D_X carries $D_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$ to $D_{\iota,\sigma}^{-w}(X, \bar{\mathbb{Q}}_\ell)$.

(3) Assume that X is regular and let $\mathscr{F}$ be a lisse $\bar{\mathbb{Q}}_\ell$-sheaf on X, punctually ι-pure of weight w. Then there exists a nondegenerate σ-symmetric pairing $\mathscr{F} \otimes \mathscr{F} \to \bar{\mathbb{Q}}_\ell(-w)$ if and only if $\mathscr{F}$ belongs to $D_{\iota,(-1)^w\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$.

(4) If f is smooth, then f^* preserves $D_{\iota,\sigma}^w$.

(5) If X and Y are regular, then f^* preserves $D_{\iota,\sigma}^w \cap D_{\mathrm{lisse}}^b$.

(6) The functor $- \boxtimes -$ carries $D_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell) \times D_{\iota,\sigma'}^{w'}(X', \bar{\mathbb{Q}}_\ell)$ to $D_{\iota,\sigma\sigma'}^{w+w'}(X \times X', \bar{\mathbb{Q}}_\ell)$.

(7) Assume that f is a closed immersion and let $A \in D_c^b(X, \bar{\mathbb{Q}}_\ell)$. Then we have $A \in D_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$ if and only if $f_*A \in D_{\iota,\sigma}^w(Y, \bar{\mathbb{Q}}_\ell)$.

(8) Assume that f is an open immersion and let $A \in \mathrm{Perv}(X, \bar{\mathbb{Q}}_\ell)$. Then we have $A \in D_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$ if and only if $f_{!*}A \in D_{\iota,\sigma}^w(Y, \bar{\mathbb{Q}}_\ell)$.

Similar properties hold for $D_{\iota,\mathrm{d}}^w$.

Next we transcribe the two-out-of-three property (Proposition 2.2.1) established earlier in terms of $D_{\iota,\sigma}^w$.

Remark 3.2.9. If $A, A', A'' \in D_c^b(X, \bar{\mathbb{Q}}_\ell)$ satisfy $A \simeq A' \oplus A''$ and two of the three complexes are in $D_{\iota,\sigma}^w$, then so is the third one. A similar property holds for $D_{\iota,\mathrm{d}}$.

Note that the proper direct image $\mathrm{R}f_*$ does not preserve perversity and in general there seems to be no canonical way to produce pairings on the perverse cohomology sheaves $^p\mathrm{R}^i f_*A$ from pairings on A. In the case of projective direct image, the relative hard Lefschetz theorem provides such pairings. Let us first fix some terminology on projective morphisms of Deligne–Mumford stacks.

Definition 3.2.10. Let $f : X \to Y$ be a quasicompact schematic morphism of Deligne–Mumford stacks. We say that an invertible sheaf $\mathscr{L}$ on X is *f-ample* if, for one (or, equivalently, for every) étale surjective morphism $g : Y' \to Y$ where Y' is a scheme, $h^*\mathscr{L}$ is f'-ample [Grothendieck 1961, Définition 4.6.1]. Here h and f' are as shown in the following Cartesian square:

$$
\begin{CD}
X' @>h>> X \\
@Vf'VV @VVfV \\
Y' @>g>> Y
\end{CD}
$$

We say that a morphism $f : X \to Y$ of Deligne–Mumford stacks is *quasiprojective* if it is schematic, of finite presentation, and if there exists an f-ample invertible sheaf on X. We say that f is *projective* if it is quasiprojective and proper.

The following is an immediate extension of the case of schemes [Beilinson et al. 1982, Théorème 5.4.10].

Proposition 3.2.11 (relative hard Lefschetz). *Let $f : X \to Y$ be a projective morphism of Deligne–Mumford stacks of finite presentation over $\mathbb{F}_q$. Let $\eta \in H^2(X, \bar{\mathbb{Q}}_\ell(1))$ be the first Chern class of an f-ample invertible sheaf on X. Let A be an ι-pure perverse sheaf on X. Then, for $i \geq 0$, the morphism*

$$
{}^p R^{-i} f_*(\eta^i \otimes \mathrm{id}_A) : {}^p R^{-i} f_* A \to {}^p R^i f_* A(i)
$$

is an isomorphism.

By Deligne's decomposition theorem [1994], the proposition implies that $R f_* A$ is split.

Proposition 3.2.12. *Let $f : X \to Y$ be a projective morphism, and let $w \in \mathbb{Z}$. Then $R f_*$ preserves $D_{\iota,\sigma}^w$ and $D_{\iota,\mathrm{d}}^w$.*

Proof. We prove the case of $D_{\iota,\sigma}^w$, the case of $D_{\iota,\mathrm{d}}^w$ being simpler. It suffices to show that, for every $(-1)^w \sigma$-self-dual ι-pure perverse sheaf A of weight w, $R f_* A$ belongs to $D_{\iota,\sigma}^w$. Given a $(-1)^w \sigma$-symmetric isomorphism $A \xrightarrow{\sim} (D_X A)(-w)$, the isomorphism

$$
{}^p R^{-i} f_* A \xrightarrow{\sim} {}^p R^{-i} f_*(D_X A)(-w) \underset{\eta^i}{\xrightarrow{\sim}} {}^p R^i f_*(D_X A)(i-w) \xrightarrow{\sim} (D_Y\, {}^p R^{-i} f_* A)(i-w)
$$

corresponding to the pairing obtained from

$$
R f_* A[-i] \otimes R f_* A[-i] \to R f_*(A \otimes A)[-2i]
$$
$$
\to R f_* K_X(-w)[-2i] \xrightarrow{\eta^i} R f_* K_X(i-w) \to K_Y(i-w)
$$

is $(-1)^{w+i} \sigma$-symmetric by Lemma A.5.11. $\qquad\square$

Proof of Theorem 3.2.3. We will prove the case of $D^w_{\iota,\sigma}$. The case of $D^w_{\iota,\mathrm{d}}$ is similar.

Consider the diagram

$$
\begin{array}{ccc}
X & \xrightarrow{\ f_1\ } & Y \times_{\bar{Y}} \bar{X} \longrightarrow Y \\
& & \downarrow \qquad\qquad \downarrow \\
& & \bar{X} \xrightarrow{\ \bar{f}\ } \bar{Y}
\end{array}
$$

in which $\bar{f}$ is the morphism of coarse moduli spaces (they exist by the Keel–Mori theorem [1997]) associated to f. Since f_1 is proper and quasifinite, $\mathrm{R}f_{1*}$ is t-exact for the perverse t-structures, and by Remarks 3.2.7(8) and 2.1.4(3) we see that the theorem holds for f_1. Thus we may assume that f is representable. We proceed by induction on the dimension of X. Let $A \in D^w_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$; we may assume that A is perverse. Applying Chow's lemma [Raynaud and Gruson 1971, Corollaire I.5.7.13] to the proper morphism $\bar{f}$ of algebraic spaces, we obtain a projective birational morphism $\bar{g} : \bar{X}' \to \bar{X}$ such that $\bar{f}\bar{g} : \bar{X}' \to \bar{Y}$ is projective. Let $g : X' \to X$ be the base change of $\bar{g}$. Let U be a dense open substack of X such that g induces an isomorphism $g^{-1}(U) \xrightarrow{\sim} U$. Let j and j' be the open immersions, as shown in the commutative diagram

$$
\begin{array}{ccc}
& & X' \\
& \nearrow^{j'} & \downarrow g \\
U & \xrightarrow{\ j\ } & X
\end{array}
$$

By [Beilinson et al. 1982, Corollaire 5.3.11] (see also Lemma 2.2.8), we have

$$
A \simeq j_{!*}j^*A \oplus B,
$$

where $B \in \mathrm{Perv}(X, \bar{\mathbb{Q}}_\ell)$ is supported on $X \backslash U$. By parts (4) and (8) of Remark 3.2.8, we have $j_{!*}j^*A \in D^w_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$. By the two-out-of-three property, $B \in D^w_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$. Since g is projective, by Proposition 3.2.12 we have $\mathrm{R}g_* j'_{!*}j^*A \in D^w_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$, so

$$
\mathrm{R}g_* j'_{!*}j^*A \simeq j_{!*}j^*A \oplus C,
$$

where $C \in D^w_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$ is supported on $X \backslash U$. Now by applying $\mathrm{R}f_*$ to $A \oplus C \simeq \mathrm{R}g_* j'_{!*}j^*A \oplus B$, we obtain

$$
\mathrm{R}f_*A \oplus \mathrm{R}f_*C \simeq \mathrm{R}f_*\mathrm{R}g_* j'_{!*}j^*A \oplus \mathrm{R}f_*B.
$$

By the induction hypothesis, $\mathrm{R}f_*B$ and $\mathrm{R}f_*C$ belong to $D^w_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell)$. As fg is projective, by Proposition 3.2.12 we have $\mathrm{R}(fg)_* j'_{!*}j^*A \in D^w_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell)$. It then follows from the two-out-of-three property that $\mathrm{R}f_*A$ belongs to $D^w_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell)$. $\qquad\square$

Remark 3.2.13 (Gabber). In the case $Y = \mathrm{Spec}(\mathbb{F}_q)$, the proof of Theorem 3.2.3 still makes use of the relative hard Lefschetz theorem (applied to the morphism g).

With the help of a refined Chow's lemma, it is possible to prove this case of Theorem 3.2.3 using only the absolute hard Lefschetz theorem, at least in the case of schemes.

The following is a preservation result for the exterior tensor power functor $(-)^{\boxtimes m}$. Unlike the functors listed in Remark 3.2.8, $(-)^{\boxtimes m}$ is not additive and the reduction to the case of perverse sheaves is not trivial.

Proposition 3.2.14. *Let A be an ι-mixed $\bar{\mathbb{Q}}_\ell$-complex of integral weights on X such that, for all $n, w \in \mathbb{Z}$, $\mathrm{gr}_w^W \, {}^p\mathcal{H}^n A$ is $(-1)^w \sigma$-self-dual with respect to $K_X(-w)$. Then $\mathrm{gr}_w^W \, {}^p\mathcal{H}^n (A^{\boxtimes m})$ is $(-1)^w \sigma^m$-self-dual with respect to $K_{[X^m/\mathfrak{S}_m]}(-w)$ for all $n, w \in \mathbb{Z}$. Here W denotes the ι-weight filtrations. In particular, the functor $(-)^{\boxtimes m}$ carries $\mathrm{D}_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$ to $\mathrm{D}_{\iota,\sigma^m}^{mw}([X^m/\mathfrak{S}_m], \bar{\mathbb{Q}}_\ell)$.*

Similar results hold for $\mathrm{D}_{\iota,\mathrm{d}}$.

Proof. Let $A^n = {}^p\mathcal{H}^n A$. Then $\tau \in \mathfrak{S}_m$ acts on X^m by $(x_1, \ldots, x_m) \mapsto (x_{\tau(1)}, \ldots, x_{\tau(m)})$. By the Künneth formula,

$$ {}^p\mathcal{H}^n (A^{\boxtimes m}) \simeq \bigoplus_{n_1 + \cdots + n_m = n} A^{n_1} \boxtimes \cdots \boxtimes A^{n_m}, $$

where τ acts on the right-hand side by $\prod_{i<j, \tau(i)>\tau(j)} (-1)^{n_i n_j}$ times the canonical isomorphism

$$ \tau^* (A^{n_{\tau(1)}} \boxtimes \cdots \boxtimes A^{n_{\tau(m)}}) \xrightarrow{\sim} A^{n_1} \boxtimes \cdots \boxtimes A^{n_m}. $$

Note that $W_w \, {}^p\mathcal{H}^n (A^{\boxtimes m}) \subseteq {}^p\mathcal{H}^n (A^{\boxtimes m})$ is the perverse subsheaf given by

$$ \sum_{\substack{n_1 + \cdots + n_m = n \\ w_1 + \cdots + w_m = w}} W_{w_1} A^{n_1} \boxtimes \cdots \boxtimes W_{w_m} A^{n_m}. $$

So

$$ \mathrm{gr}_w^W \, {}^p\mathcal{H}^n (A^{\boxtimes m}) \simeq \bigoplus_{\substack{n_1 + \cdots + n_m = n \\ w_1 + \cdots + w_m = w}} \mathrm{gr}_{w_1}^W A^{n_1} \boxtimes \cdots \boxtimes \mathrm{gr}_{w_1}^W A^{n_m}. $$

Thus the $(-1)^{w_i} \sigma$-symmetric isomorphisms

$$ \mathrm{gr}_{w_i}^W A^{n_i} \xrightarrow{\sim} (D_X \, \mathrm{gr}_{w_i}^W A^{n_i})(-w_i) $$

induce a $(-1)^w \sigma^m$-symmetric isomorphism

$$ \mathrm{gr}_w^W \, {}^p\mathcal{H}^n (A^{\boxtimes m}) \xrightarrow{\sim} (D_{X^m} \, \mathrm{gr}_w^W \, {}^p\mathcal{H}^n (A^{\boxtimes m}))(-w), $$

compatible with the actions of $\mathfrak{S}_m$. $\square$

We conclude this subsection with a symmetry criterion in terms of traces of squares of Frobenius, an analogue of the Frobenius–Schur indicator theorem in representation theory (see [Serre 1998, Section 13.2, Proposition 39; Bröcker and tom

Dieck 1995, Proposition II.6.8]). This criterion will be used to show a result on the independence of ℓ of symmetry (Corollary 4.2.14). We refer the reader to [Katz 2005, Theorem 1.9.6] for a related criterion on the symmetry of the geometric monodromy. For a groupoid $\mathscr{C}$, we let $|\mathscr{C}|$ denote the set of isomorphism classes of its objects.

Proposition 3.2.15. *Let X be a Deligne–Mumford stack of finite presentation over $\mathbb{F}_q$, connected and geometrically unibranch of dimension d. Let $\mathscr{F}$ be a semisimple lisse $\bar{\mathbb{Q}}_\ell$-sheaf on X, punctually ι-pure of weight $w \in \mathbb{Z}$. Consider the series*

$$L^{(2)}(T) = \exp\left(\sum_{m \geq 1} \sum_{x \in |X(\mathbb{F}_{q^m})|} \frac{\iota \operatorname{tr}(\operatorname{Frob}_x^2 \mid \mathscr{F}_{\bar{x}})}{\# \operatorname{Aut}(x)} \frac{T^m}{m} \right),$$

where $\bar{x}$ denotes a geometric point above x, and where $\operatorname{Frob}_x = \operatorname{Frob}_{q^m}$. Then the series $L^{(2)}(T)$ converges absolutely for $|T| < q^{-w-d}$ and extends to a rational function satisfying

$$\begin{aligned}
-\operatorname{ord}_{T=q^{-w-d}} & L^{(2)}(T) \\
&= \dim \operatorname{H}^0(X, (\operatorname{Sym}^2(\mathscr{F}^\vee))(-w)) - \dim \operatorname{H}^0(X, (\wedge^2(\mathscr{F}^\vee))(-w)).
\end{aligned}$$

In particular, if $\mathscr{F}$ is simple and σ-self-dual (resp. not self-dual) with respect to $\bar{\mathbb{Q}}_\ell(-w)$, then

$$-\operatorname{ord}_{T=q^{-w-d}} L^{(2)}(T) = \sigma \quad (\text{resp.} = 0).$$

Proof. For $x \in X(\mathbb{F}_{q^m})$,

$$\operatorname{tr}(\operatorname{Frob}_x^2 \mid \mathscr{F}_{\bar{x}}) = \operatorname{tr}(\operatorname{Frob}_x \mid \operatorname{Sym}^2 \mathscr{F}_{\bar{x}}) - \operatorname{tr}(\operatorname{Frob}_x \mid \wedge^2 \mathscr{F}_{\bar{x}}).$$

Thus $L^{(2)}(T) = L_\iota(X, \operatorname{Sym}^2 \mathscr{F}, T)/L_\iota(X, \wedge^2 \mathscr{F}, T)$ (see [Sun 2012b, Definition 4.1] for the definition of the L-series $L_\iota(X, -, T)$). Note that $\mathscr{F} \otimes \mathscr{F}$ is lisse punctually ι-pure of weight $2w$, and semisimple by a theorem of Chevalley [1955, Chapitre IV, Proposition 5.2]. The same holds for $\operatorname{Sym}^2 \mathscr{F}$ and $\wedge^2 \mathscr{F}$. For $\mathscr{G}$ lisse punctually ι-pure of weight $2w$ on X, the series $L_\iota(X, \mathscr{G}, T)$ converges absolutely for $|T| < q^{-w-d}$ and extends to a rational function

$$\iota \prod_i \det(1 - T \operatorname{Frob}_q \mid \operatorname{H}_c^i(X_{\bar{\mathbb{F}}_q}, \mathscr{G}))^{(-1)^{i+1}}$$

by [Sun 2012b, Theorem 4.2]. Only the factor $i = 2d$ may contribute to poles on the circle $|T| = q^{-w-d}$, by [Sun 2012b, Theorem 1.4]. For every dense open substack U of X such that U_{red} is regular, we have

$$\operatorname{H}_c^{2d}(X_{\bar{\mathbb{F}}_q}, \mathscr{G}) \simeq \operatorname{H}^0(U_{\bar{\mathbb{F}}_q}, \mathscr{G}^\vee)^\vee(-d) \simeq \operatorname{H}^0(X_{\bar{\mathbb{F}}_q}, \mathscr{G}^\vee)^\vee(-d).$$

Here in the second assertion we used the hypothesis on X, which implies that the homomorphism $\pi_1(U) \to \pi_1(X)$ is surjective. Therefore,

$$- \operatorname{ord}_{T=q^{-w-d}} L_\iota(X, \mathscr{G}, T) = \dim \operatorname{H}^0(X, \mathscr{G}^\vee(-w))$$

for $\mathscr{G}$ semisimple. $\qquad\square$

3.3. *Variant: semisimple complexes over a separably closed field.* In this subsection, let k be a separably closed field. We establish variants over k of results of Section 3.2. The main result is a preservation result under proper direct image (Theorem 3.3.7). We also include an example of Gabber (Remark 3.3.13) showcasing the difference in parity of Betti numbers between zero and positive characteristics.

One key point in Section 3.2 is the relative hard Lefschetz theorem for pure perverse sheaves. If k has characteristic zero, a conjecture of Kashiwara states that all semisimple perverse sheaves satisfy relative hard Lefschetz. Kashiwara's conjecture was proved by Drinfeld [2001] assuming de Jong's conjecture for infinitely many primes ℓ, which was later proved by Gaitsgory [2007] for $\ell > 2$.

Drinfeld's proof uses the techniques of reduction from k to finite fields in [Beilinson et al. 1982, Section 6]. The reduction holds, in fact, without restriction on the characteristic of k and provides a class of semisimple perverse sheaves over k for which the relative hard Lefschetz theorem holds. Let us briefly recall the reduction. Let X be a Deligne–Mumford stack of finite presentation over k. There exist a subring $R \subseteq k$ of finite type over $\mathbb{Z}[1/\ell]$ and a Deligne–Mumford stack X_R of finite presentation over $\operatorname{Spec}(R)$ such that $X \simeq X_R \otimes_R k$. For extra data $(\mathscr{T}, \mathscr{L})$ on X, we have an equivalence [Beilinson et al. 1982, 6.1.10]

$$\operatorname{D}^b_{\mathscr{T}, \mathscr{L}}(X, \bar{\mathbb{Q}}_\ell) \xrightarrow{\sim} \operatorname{D}^b_{\mathscr{T}, \mathscr{L}}(X_s, \bar{\mathbb{Q}}_\ell) \tag{3-3-1}$$

for every geometric point s above a closed point of $\operatorname{Spec}(R)$, provided that R is big enough (relative to the data $(\mathscr{T}, \mathscr{L})$). Here X_s denotes the base change of X_R by $s \to \operatorname{Spec}(R)$. Note that s is the spectrum of an algebraic closure of a finite field. Each $A \in \operatorname{D}^b_c(X, \bar{\mathbb{Q}}_\ell)$ is contained in $\operatorname{D}^b_{\mathscr{T}, \mathscr{L}}(X, \bar{\mathbb{Q}}_\ell)$ for some $(\mathscr{T}, \mathscr{L})$.

Definition 3.3.1 (admissible semisimple complexes). Let A be a semisimple perverse $\bar{\mathbb{Q}}_\ell$-sheaf on X. If k is an algebraic closure of a finite field, we say that A is *admissible* if there exists a Deligne–Mumford stack X_0 of finite presentation over a finite subfield k_0 of k, an isomorphism $X \simeq X_0 \otimes_{k_0} k$, and a perverse $\bar{\mathbb{Q}}_\ell$-sheaf A_0 on X_0 such that A is isomorphic to the pullback of A_0. More generally, if k has characteristic > 0, we say that A is *admissible* if the images of A under the equivalences (3-3-1), for all geometric points s over a closed point of $\operatorname{Spec}(R)$, are admissible, for some R big enough. If k has characteristic zero, we adopt the convention that every semisimple perverse $\bar{\mathbb{Q}}_\ell$-sheaf is admissible.

We say that a complex $B \in D_c^b(X, \bar{\mathbb{Q}}_\ell)$ is *admissible semisimple* if we have $B \simeq \bigoplus_i ({}^p\mathcal{H}^i B)[-i]$ and if, for each i, the i-th perverse cohomology sheaf ${}^p\mathcal{H}^i B$ is admissible semisimple.

Remark 3.3.2. In the case where k is the algebraic closure of a finite field k_0, for X_0 as above, the pullback of an ι-pure complex on X_0 to X is admissible semisimple by the decomposition theorems [Beilinson et al. 1982, Théorèmes 5.3.8, 5.4.5] ([Sun 2012a] for the case of stacks). Conversely, if a semisimple perverse $\bar{\mathbb{Q}}_\ell$-sheaf A on X is the pullback of A_0 on X_0 as above, then we may take A_0 to be pure (of weight 0, for example) by Lafforgue's theorem [2002, Corollaire VII.8], mentioned in Remark 3.1.6(2).

Remark 3.3.3. Following [Beilinson et al. 1982, 6.2.4], we say that a simple perverse $\bar{\mathbb{Q}}_\ell$-sheaf on X is *of geometric origin* if it belongs to the class of simple perverse $\bar{\mathbb{Q}}_\ell$-sheaves generated from the constant sheaf $\bar{\mathbb{Q}}_\ell$ on $\mathrm{Spec}(k)$ by taking composition factors of perverse cohomology sheaves under the six operations. By [Beilinson et al. 1982, Lemme 6.2.6] (suitably extended), simple perverse $\bar{\mathbb{Q}}_\ell$-sheaves of geometric origin are admissible.

The operations that preserve purity also preserve admissible semisimple complexes. The details are given below.

Remark 3.3.4 (preservation of admissible semisimple complexes). Let $f : X \to Y$ be a morphism.

- The full subcategory of D_c^b consisting of objects A such that the composition factors of ${}^p\mathcal{H}^i A$ are admissible for all i is stable under the operations Rf_*, $Rf_!$, f^*, $Rf^!$, $\otimes$, $R\mathcal{H}om$, and $(-)^{\boxtimes m}$.

- $D_X : D_c^b(X, \bar{\mathbb{Q}}_\ell)^{\mathrm{op}} \to D_c^b(X, \bar{\mathbb{Q}}_\ell)$ preserves admissible semisimple complexes.

- If f is an open immersion, $f_{!*}$ preserves admissible semisimple perverse sheaves.

- Assume that f is a closed immersion and let $A \in D_c^b(X, \bar{\mathbb{Q}}_\ell)$. Then A is admissible semisimple if and only if $f_* A$ is admissible semisimple.

- If f is smooth, f^* preserves admissible semisimple complexes.

- If X and Y are regular, f^* preserves admissible semisimple complexes in D_{lisse}^b.

- The functors
$$- \boxtimes - : D_c^b(X, \bar{\mathbb{Q}}_\ell) \times D_c^b(X', \bar{\mathbb{Q}}_\ell) \to D_c^b(X \times X', \bar{\mathbb{Q}}_\ell),$$
$$(-)^{\boxtimes m} : D_c^b(X, \bar{\mathbb{Q}}_\ell) \to D_c^b([X^m/\mathfrak{S}_m], \bar{\mathbb{Q}}_\ell), \quad m \geq 0,$$
preserve admissible semisimple complexes.

- If f is a proper morphism, Rf_* preserves admissible semisimple complexes.

These properties reduce to the corresponding properties for pure complexes over a finite field (Remark 3.2.7). Since the equivalences (3-3-1) are compatible with these operations, this reduction is clear in positive characteristic. The reduction in characteristic zero is more involved. The case of $R f_*$ is done in [Drinfeld 2001] and the other cases can be done similarly.

Definition 3.3.5 (D_σ). We let

$$D_\sigma(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{Ob}(D_c^b(X, \bar{\mathbb{Q}}_\ell)) \quad \left(\text{resp. } D_{\mathrm{sd}}(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{Ob}(D_c^b(X, \bar{\mathbb{Q}}_\ell))\right)$$

be the subset consisting of admissible semisimple complexes A such that $^p\mathscr{H}^i A$ is $(-1)^i \sigma$-self-dual (resp. self-dual) with respect to K_X, for all i. We denote by $D_{\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{Ob}(D_c^b(X, \bar{\mathbb{Q}}_\ell) \times D_c^b(X, \bar{\mathbb{Q}}_\ell))$ the subset consisting of pairs (A, B) such that both A and B are admissible semisimple, and such that $^p\mathscr{H}^i A$ is isomorphic to $D_X {}^p\mathscr{H}^i B$.

By definition, we have $D_{\mathrm{sd}}(X, \bar{\mathbb{Q}}_\ell) = \Delta^{-1}(D_{\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell))$, where $\Delta : D_c^b(X, \bar{\mathbb{Q}}_\ell) \to D_c^b(X, \bar{\mathbb{Q}}_\ell) \times D_c^b(X, \bar{\mathbb{Q}}_\ell)$ is the diagonal embedding.

Example 3.3.6. For $X = \mathrm{Spec}(k)$, every object A of $D_c^b(X, \bar{\mathbb{Q}}_\ell)$ is admissible semisimple and belongs to $D_{\mathrm{sd}}(X, \bar{\mathbb{Q}}_\ell)$. Let $d_i = \dim \mathscr{H}^i(A)$. Then:

- A is 1-self-dual with respect to $\bar{\mathbb{Q}}_\ell$ if and only if it is self-dual with respect to $\bar{\mathbb{Q}}_\ell$, namely if $d_i = d_{-i}$ for all i. (Recall that in general self-dual objects are not necessarily 1-self-dual.)

- A is -1-self-dual with respect to $\bar{\mathbb{Q}}_\ell$ if and only if d_i equals d_{-i} for all i and d_0 is even.

- $A \in D_1(X, \bar{\mathbb{Q}}_\ell)$ if and only if d_i is even for i odd.

- $A \in D_{-1}(X, \bar{\mathbb{Q}}_\ell)$ if and only if d_i is even for i even.

- For $A, B \in D_c^b(X, \bar{\mathbb{Q}}_\ell)$, we have $(A, B) \in D_{\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell)$ if and only if $A \simeq B$.

The main result of this subsection is the following.

Theorem 3.3.7. *Let $f : X \to Y$ be a proper morphism of Deligne–Mumford stacks of finite presentation over k, where Y has finite inertia. Then $R f_*$ preserves D_σ and D_{d}.*

Corollary 3.3.8. *Let $f : X \to Y$ be a proper morphism, where Y has finite inertia. Then $R f_*$ preserves D_{sd}.*

The strategy for proving Theorem 3.3.7 is the same as for Theorem 3.2.3. Let us recall that the operations listed in Remark 3.3.4 that preserve admissible semisimple complexes also preserve σ-self-dual complexes (Remark 2.1.4). With the exception of proper direct image $R f_*$, they also preserve perversity, hence they preserve D_σ. The details are given below.

Remark 3.3.9 (preservation of D_σ, easy part). Let $f : X \to Y$ be a morphism, and let $n \in \mathbb{Z}$.

(1) If $A \in D_\sigma(X, \bar{\mathbb{Q}}_\ell)$, then $A[n] \in D_{(-1)^n \sigma}(X, \bar{\mathbb{Q}}_\ell)$.

(2) D_X preserves $D_\sigma(X, \bar{\mathbb{Q}}_\ell)$.

(3) Assume that X is regular and let $\mathscr{F}$ be a lisse $\bar{\mathbb{Q}}_\ell$-sheaf on X, admissible semisimple. Then there exists a nondegenerate σ-symmetric pairing $\mathscr{F} \otimes \mathscr{F} \to \bar{\mathbb{Q}}_\ell$ if and only if $\mathscr{F}$ belongs to $D_\sigma(X, \bar{\mathbb{Q}}_\ell)$.

(4) If f is smooth, then f^* preserves D_σ.

(5) If X and Y are regular, then f^* preserves $D_\sigma \cap D_{\mathrm{lisse}}^b$.

(6) Assume that f is a closed immersion and let $A \in D_c^b(X, \bar{\mathbb{Q}}_\ell)$. Then we have $A \in D_\sigma(X, \bar{\mathbb{Q}}_\ell)$ if and only if $f_* A \in D_\sigma(Y, \bar{\mathbb{Q}}_\ell)$.

(7) The exterior tensor product functors induce functors

$$- \boxtimes - : D_\sigma(X, \bar{\mathbb{Q}}_\ell) \times D_{\sigma'}(X', \bar{\mathbb{Q}}_\ell) \to D_{\sigma\sigma'}(X \times X', \bar{\mathbb{Q}}_\ell),$$

$$(-)^{\boxtimes m} : D_\sigma(X, \bar{\mathbb{Q}}_\ell) \to D_{\sigma^m}([X^m/\mathfrak{S}_m], \bar{\mathbb{Q}}_\ell), \quad m \geq 0.$$

For $(-)^{\boxtimes m}$, the reduction to perverse sheaves is nontrivial and is similar to Proposition 3.2.14.

Similar properties hold for D_d.

By Proposition 2.2.1, the two-out-of-three property holds for D_σ and D_d.

We state a relative hard Lefschetz theorem over an arbitrary field F in which ℓ is invertible.

Proposition 3.3.10 (relative hard Lefschetz). *Let $f : X \to Y$ be a projective morphism of Deligne–Mumford stacks of finite presentation over F. Let $\eta \in H^2(X, \bar{\mathbb{Q}}_\ell(1))$ be the first Chern class of an f-ample invertible sheaf on X. Let A be a perverse $\bar{\mathbb{Q}}_\ell$-sheaf on X whose pullback to $X \otimes_F \bar{F}$ is admissible semisimple. Then, for $i \geq 0$, the morphism*

$$^p\mathscr{H}^{-i}(\eta^i \otimes \mathrm{id}_A) : {}^p R^{-i} f_* A \to {}^p R^i f_* A(i)$$

is an isomorphism.

That the morphism is an isomorphism can be checked on $X \otimes_F \bar{F}$. Thus we are reduced to the case where $F = k$ is separably closed. As mentioned earlier, the relative hard Lefschetz theorem in this case is obtained by reduction to the finite field case (Proposition 3.2.11).

Combining Proposition 3.3.10 with Lemma A.5.11, we obtain the following preservation result under projective direct image.

Proposition 3.3.11. *Let $f : X \to Y$ be a projective morphism (over k). Then $R f_*$ preserves D_σ and D_d.*

The proof of Theorem 3.2.3 can now be repeated verbatim to prove Theorem 3.3.7.

Over an arbitrary field F in which ℓ is invertible, we may exploit the relative hard Lefschetz theorem to get analogues for split complexes that are geometrically semisimple.

Proposition 3.3.12. *Let $f : X \to Y$ be a proper morphism of separated Deligne–Mumford stacks of finite type over F. Assume that X is regular. Let $\mathscr{F}$ be a lisse $\bar{\mathbb{Q}}_\ell$-sheaf on X, whose pullback to $X_{\bar{F}}$ is admissible semisimple. Then we have $\mathrm{R}f_*\mathscr{F} \simeq \bigoplus_i ({}^p\mathrm{R}^i f_*\mathscr{F})[-i]$.*

Proof. By [Laumon and Moret-Bailly 2000, Théorème 16.6], there exists a finite surjective morphism $g_1 : X' \to X$ where X' is a scheme. Up to replacing X' by its normalization, we may assume that X' is normal. By de Jong's alterations [1996, Theorem 4.1], there exists a proper surjective morphism $g_2 : X'' \to X'$, generically finite, such that X'' is regular and quasiprojective over k. Let $g = g_1 g_2 : X'' \to X$. By the relative hard Lefschetz theorem (Proposition 3.3.10) and Deligne's decomposition theorem [1994], we have

$$\mathrm{R}(fg)_* g^* \mathscr{F} \simeq \bigoplus_i ({}^p\mathrm{R}^i (fg)_* g^* \mathscr{F})[-i].$$

Note that $g^*\mathscr{F} \simeq g^*\mathscr{F} \otimes \mathrm{R}g^!\bar{\mathbb{Q}}_\ell \simeq \mathrm{R}g^!\mathscr{F}$. Consider the composite

$$\alpha : \mathscr{F} \to \mathrm{R}g_* g^* \mathscr{F} \simeq \mathrm{R}g_! \mathrm{R}g^! \mathscr{F} \to \mathscr{F}$$

of the adjunction morphisms. Since α is generically multiplication by the degree of g, it is an isomorphism. It follows that $\mathscr{F}$ is a direct summand of $\mathrm{R}g_* g^*\mathscr{F}$, so that $\mathrm{R}f_*\mathscr{F}$ is a direct summand of $\mathrm{R}(fg)_* g^*\mathscr{F}$. $\qquad\square$

Remark 3.3.13 (Gabber). Let X be a proper smooth algebraic space over k and let $\mathscr{F}$ be a lisse $\bar{\mathbb{Q}}_\ell$-sheaf on X with finite monodromy, -1-self-dual with respect to $\bar{\mathbb{Q}}_\ell$. Then $\mathscr{F}$ is admissible semisimple (since each simple factor is of geometric origin), and $\mathscr{F}$ belongs to D_{-1}. By Theorem 3.3.7, $b_n(\mathscr{F}) := \dim \mathrm{H}^n(X, \mathscr{F})$ is even for n even.

If k has characteristic 0, then $b_n(\mathscr{F})$ is even for all n. To see this, we may assume $k = \mathbb{C}$, X connected, and $\mathscr{F}$ simple. Let G be the monodromy group of $\mathscr{F}$ and let $f : Y \to X$ be the corresponding Galois étale cover. Then

$$\mathrm{H}^n(X, \mathscr{F}) \simeq \mathrm{H}^n(Y, f^*\mathscr{F})^G \simeq (\mathrm{H}^n(Y, \bar{\mathbb{Q}}_\ell) \otimes_{\bar{\mathbb{Q}}_\ell} V)^G,$$

where V is the representation of G corresponding to $\mathscr{F}$. Thus $b_n(\mathscr{F})$ is the multiplicity of $V^\vee$ in the representation $\mathrm{H}^n(Y, \bar{\mathbb{Q}}_\ell)$ of G. Since the complex representation $\mathrm{H}^n(Y(\mathbb{C}), \mathbb{C})$ of G has a real structure $\mathrm{H}^n(Y(\mathbb{C}), \mathbb{R})$, it admits a G-invariant nondegenerate symmetric bilinear form. In other words, it is 1-self-dual. The same holds for $\mathrm{H}^n(Y, \bar{\mathbb{Q}}_\ell)$. Therefore, the multiplicity of $V^\vee$, which is -1-self-dual, is

necessarily even (see [Serre 1998, Section 13.2, Theorem 31; Bröcker and tom Dieck 1995, Proposition II.6.6 (i)–(iii)]).

By contrast, if k has characteristic 2 or 3, then $b_n(\mathscr{F})$ may be odd for n odd, as shown by the following counterexample. Let E be a supersingular elliptic curve over k and let G be its automorphism group. Let $X' \to X$ be a finite étale cover of connected projective smooth curves over k of Galois group G, which exists by [Pacheco and Stevenson 2000, Theorem 7.4], as explained in [Partsch 2013, Section 3]. Let $f : Y = (X' \times E)/G \to X$ be the projection, where G acts diagonally on $X' \times E$. Then $\mathscr{F} = \mathrm{R}^1 f_* \overline{\mathbb{Q}}_\ell$ is a -1-self-dual simple lisse sheaf of rank 2 on X, of monodromy G. Note that $f^* \mathscr{F}$ is a -1-self-dual simple lisse sheaf on Y of monodromy G, since $\pi_1(Y)$ maps onto $\pi_1(X)$. We claim that $b_1(f^* \mathscr{F})$ and $b_1(\mathscr{F})$ are not of the same parity. Indeed, consider the Leray spectral sequence for $(f, f^* \mathscr{F})$:

$$E_2^{pq} = \mathrm{H}^p(X, \mathrm{R}^q f_* f^* \mathscr{F}) \Rightarrow \mathrm{H}^{p+q}(Y, f^* \mathscr{F}).$$

By the projection formula,

$$f_* f^* \mathscr{F} \simeq f_* \overline{\mathbb{Q}}_\ell \otimes \mathscr{F} \simeq \mathscr{F}, \quad \mathrm{R}^1 f_* f^* \mathscr{F} \simeq \mathrm{R}^1 f_* \overline{\mathbb{Q}}_\ell \otimes \mathscr{F} = \mathscr{F} \otimes \mathscr{F},$$

so we have an exact sequence

$$0 \to \mathrm{H}^1(X, \mathscr{F}) \to \mathrm{H}^1(Y, f^* \mathscr{F}) \to \mathrm{H}^0(X, \mathscr{F} \otimes \mathscr{F}) \to E_2^{20} = 0.$$

Since $\dim \mathrm{H}^0(X, \mathscr{F} \otimes \mathscr{F}) = 1$, we get $b_1(f^* \mathscr{F}) = b_1(\mathscr{F}) + 1$. (That the Leray spectral sequence degenerates at E_2 also follows from a general theorem of Deligne [1968].) By the Grothendieck–Ogg–Shafarevich formula, $b_1(\mathscr{F}) = (2g - 2)\, \mathrm{rk}(\mathscr{F}) = 4g - 4$ is even, where g is the genus of X. It follows that $b_1(f^* \mathscr{F}) = 4g - 3$ is odd.

4. Symmetry in Grothendieck groups

In Section 3, we studied the behavior of σ-self-dual pure perverse sheaves under operations that preserve purity. Mixed Hodge theory suggests that one may expect results for more general operations in the mixed case. This section confirms such expectations in a weak sense, by working in Grothendieck groups. We work over a finite field $k = \mathbb{F}_q$. In Section 4.1, we review operations on Grothendieck groups. In Section 4.2, we define certain subgroups of the Grothendieck groups and state the main result of this section (Theorem 4.2.5), which says that these subgroups are preserved by Grothendieck's six operations, and which contains the finite field case of Theorem 1.9. The proof is a bit involved and is given in Section 4.3.

4.1. *Operations on Grothendieck groups.* In this subsection, we review Grothendieck groups and operations on them. The six operations are easily defined. The

action of the middle extension functor $f_{!*}$ on Grothendieck groups is more subtle, and we justify our definition with the help of purity.

Construction 4.1.1 (six operations on Grothendieck groups). Let X be a Deligne–Mumford stack of finite presentation over a field. We let $K(X, \bar{\mathbb{Q}}_\ell)$ denote the Grothendieck group of $D_c^b(X, \bar{\mathbb{Q}}_\ell)$, which is a free abelian group generated by the isomorphism classes of simple perverse $\bar{\mathbb{Q}}_\ell$-sheaves. For an object A of $D_c^b(X, \bar{\mathbb{Q}}_\ell)$, we let $[A]$ denote its class in $K(X, \bar{\mathbb{Q}}_\ell)$. The usual operations on derived categories induce maps between Grothendieck groups. More precisely, for a morphism $f : X \to Y$ of Deligne–Mumford stacks of finite presentation over a field, we have $\mathbb{Z}$-(bi)linear maps

$$- \boxtimes - : K(X, \bar{\mathbb{Q}}_\ell) \times K(Y, \bar{\mathbb{Q}}_\ell) \to K(X \times Y, \bar{\mathbb{Q}}_\ell),$$

$$- \otimes -, \mathcal{H}om(-, -) : K(X, \bar{\mathbb{Q}}_\ell) \times K(X, \bar{\mathbb{Q}}_\ell) \to K(X, \bar{\mathbb{Q}}_\ell),$$

$$D_X : K(X, \bar{\mathbb{Q}}_\ell) \to K(X, \bar{\mathbb{Q}}_\ell),$$

$$f^*, f^! : K(Y, \bar{\mathbb{Q}}_\ell) \to K(X, \bar{\mathbb{Q}}_\ell),$$

$$f_*, f_! : K(X, \bar{\mathbb{Q}}_\ell) \to K(Y, \bar{\mathbb{Q}}_\ell).$$

The tensor product $(- \otimes -)$ endows $K(X, \bar{\mathbb{Q}}_\ell)$ with a ring structure. The map f^* is a ring homomorphism.

The Grothendieck ring is equipped with the structure of a λ-ring as follows. Readers not interested in this structure may skip this part as it is not used in the proof of the theorems in the Introduction. For $m \geq 0$, we have a map

$$(-)^{\boxtimes m} : K(X, \bar{\mathbb{Q}}_\ell) \to K([X^m/\mathfrak{S}_m], \bar{\mathbb{Q}}_\ell),$$

which preserves multiplication and satisfies $(n[A])^{\boxtimes m} = n^m[A]^{\boxtimes m}$ (with the convention $0^0 = 1$) for $n \geq 0$ and $(-[A])^{\boxtimes m} = (-1)^m[\mathscr{S}] \otimes [A]^{\boxtimes m}$, where $\mathscr{S}$ is the lisse sheaf of rank 1 on $[X^m/\mathfrak{S}_m]$ given by the sign character $\mathfrak{S}_m \to \bar{\mathbb{Q}}_\ell^\times$. The maps $\lambda^m : K(X, \bar{\mathbb{Q}}_\ell) \to K(X, \bar{\mathbb{Q}}_\ell)$ given by $\lambda^m(x) = (-1)^m p_* \Delta^*(-x)^{\boxtimes m}$, where $\Delta : X \times B\mathfrak{S}_m \to [X^m/\mathfrak{S}_m]$ is the diagonal morphism and $p : X \times B\mathfrak{S}_m \to X$ is the projection, endow $K(X, \bar{\mathbb{Q}}_\ell)$ with the structure of a special λ-ring. The map f^* is a λ-ring homomorphism. We refer the reader to [Grothendieck 1958, Section 4] and [Atiyah and Tall 1969] for the definitions of special λ-ring and λ-ring homomorphism.

Remark 4.1.2. For a separated quasifinite morphism $f : X \to Y$, the functor $f_{!*} : \mathrm{Perv}(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{Perv}(Y, \bar{\mathbb{Q}}_\ell)$ is *not exact* in general. There exists a unique homomorphism $f_{!*} : K(X, \bar{\mathbb{Q}}_\ell) \to K(Y, \bar{\mathbb{Q}}_\ell)$ such that $f_{!*}[A] = [f_{!*}A]$ for A perverse *semisimple*. As we shall see in Lemma 4.1.8, over a finite field this identity also holds for A pure perverse.

We note the following consequence of Lemma 2.2.11 (applied to semisimple perverse sheaves).

Lemma 4.1.3. *Let $(X_\alpha)_{\alpha \in I}$ be a finite Zariski open covering of X. Let $A \in \mathrm{K}(X, \bar{\mathbb{Q}}_\ell)$. Then*

$$\sum_{\substack{J \subseteq I \\ \#J \text{ even}}} j_{J!*} j_J^* A = \sum_{\substack{J \subseteq I \\ \#J \text{ odd}}} j_{J!*} j_J^* A,$$

where $j_J : \bigcap_{\alpha \in J} X_\alpha \to X$ is the open immersion.

In the rest of this section we work over a finite field $k = \mathbb{F}_q$. We first recall the following injectivity, which will be used in the proof of Corollary 4.2.10.

Lemma 4.1.4. *The homomorphism $\mathrm{K}(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{Map}\left(\coprod_{m \geq 1} |X(\mathbb{F}_{q^m})|, \bar{\mathbb{Q}}_\ell\right)$ sending A to $x \mapsto \mathrm{tr}(\mathrm{Frob}_x \mid A_{\bar{x}})$ is injective.*

As in [Laumon 1987, Théorème 1.1.2], this injectivity follows from Chebotarev's density theorem [Serre 1965, Theorem 7], which extends to the case of Deligne–Mumford stacks as follows.

Lemma 4.1.5. *Let $Y \to X$ be a Galois étale cover of irreducible Deligne–Mumford stacks of dimension d of finite presentation over $\mathbb{F}_q$, and let G be the Galois group. Let $R \subseteq G$ be a subset stable under conjugation. Then*

$$\lim_{T \to (q^{-d})^-} \sum_{m \geq 1} \sum_x \frac{1}{\#\mathrm{Aut}(x)} \frac{T^m}{m} \bigg/ \log \frac{1}{T - q^{-d}} = \#R/\#G,$$

where x runs through isomorphism classes of $X(\mathbb{F}_{q^m})$ such that the image F_x of Frob_x in G (well-defined up to conjugation) lies in R.

Proof. For a character $\chi : G \to \bar{\mathbb{Q}}_\ell$ of a $\bar{\mathbb{Q}}_\ell$-representation of G, consider the L-series

$$L(X, \iota\chi, T) = L_\iota(X, \mathscr{F}_\chi, T) = \exp\left(\sum_{m \geq 1} \sum_{x \in |X(\mathbb{F}_{q^m})|} \frac{\iota\chi(F_x)}{\#\mathrm{Aut}(x)} \frac{T^m}{m}\right)$$

associated to the corresponding lisse $\bar{\mathbb{Q}}_\ell$-sheaf $\mathscr{F}_\chi$ on X [Sun 2012b, Definition 4.1]. The series $L(X, \iota\chi, T)$ converges absolutely for $|T| < q^{-d}$ and extends, by [Sun 2012b, Theorem 4.2], to a rational function

$$\iota \prod_i \det(1 - T \, \mathrm{Frob}_q \mid \mathrm{H}_c^i(X_{\bar{\mathbb{F}}_q}, \mathscr{F}_\chi))^{(-1)^{i+1}}.$$

As $\mathrm{H}_c^{2d}(X_{\bar{\mathbb{F}}_q}, \mathscr{F}_\chi) \simeq \mathrm{H}^0(U_{\bar{\mathbb{F}}_q}, \mathscr{F}_\chi^\vee)^\vee(-d)$ for a dense open substack U of X such that U_{red} is regular, $-\mathrm{ord}_{T=q^{-d}} L(X, \iota\chi, T) = \dim \mathrm{H}^0(U, \mathscr{F}_\chi^\vee)$ is the multiplicity of the identity character in χ, so that

$$\lim_{T \to (q^{-d})^-} \sum_{m \geq 1} \sum_{x \in |X(\mathbb{F}_{q^m})|} \frac{\iota\chi(F_x)}{\#\mathrm{Aut}(x)} \frac{T^m}{m} \bigg/ \log \frac{1}{T - q^{-d}} = \sum_{g \in G} \iota\chi(g)/\#G.$$

This equality extends to an arbitrary class function $\chi : G \to \bar{\mathbb{Q}}_\ell$. It then suffices to take χ to be the characteristic function of R. □

Next we discuss purity.

Notation 4.1.6. For $w \in \mathbb{R}$, we let $\mathrm{K}_\iota^w(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{K}(X, \bar{\mathbb{Q}}_\ell)$ denote the subgroup generated by perverse sheaves ι-pure of weight w on X. We set $\mathrm{K}_\iota^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell) := \bigoplus_{w \in \mathbb{Z}} \mathrm{K}_\iota^w(X, \bar{\mathbb{Q}}_\ell)$.

The group $\mathrm{K}_\iota^w(X, \bar{\mathbb{Q}}_\ell)$ is a free abelian group generated by the isomorphism classes of simple perverse sheaves ι-pure of weight w on X. We also have $\bigoplus_{w \in \mathbb{R}} \mathrm{K}_\iota^w(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{K}(X, \bar{\mathbb{Q}}_\ell)$, and the λ-subring $\mathrm{K}_\iota^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{K}(X, \bar{\mathbb{Q}}_\ell)$ is stable under Grothendieck's six operations and duality. For $w \in \mathbb{Z}$, the group $\mathrm{K}^w(X, \bar{\mathbb{Q}}_\ell) := \bigcap_\iota \mathrm{K}_\iota^w(X, \bar{\mathbb{Q}}_\ell)$ is a free abelian group generated by the isomorphism classes of perverse sheaves pure of weight w on X.

Remark 4.1.7. In fact, we have $\bigoplus_{w \in \mathbb{R}} \mathrm{K}_\iota^w(X, \bar{\mathbb{Q}}_\ell) = \mathrm{K}(X, \bar{\mathbb{Q}}_\ell)$, as every $\bar{\mathbb{Q}}_\ell$-sheaf on X is ι-mixed by Lafforgue's theorem [2002, Corollaire VII.8], mentioned in Remark 3.1.6(2).

For a subset $I \subseteq \mathbb{R}$, we let $\mathrm{Perv}_\iota^I(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{Perv}(X, \bar{\mathbb{Q}}_\ell)$ denote the full subcategory of perverse sheaves ι-mixed of weights contained in I. Lemmas 4.1.8 and 4.1.9 below, which justify the definition of the map $f_{!*}$ in Remark 4.1.2, are taken from [Zheng 2005, Lemme 2.9, Corollaire 2.10].

Lemma 4.1.8. *Let $f : X \to Y$ be a separated quasifinite morphism. For $w \in \mathbb{R}$, the functor*

$$f_{!*} : \mathrm{Perv}_\iota^{\{w, w+1\}}(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{Perv}_\iota^{\{w, w+1\}}(Y, \bar{\mathbb{Q}}_\ell)$$

is exact. In particular, $f_{!*}[A] = [f_{!*}A]$ for $A \in \mathrm{Perv}_\iota^{\{w, w+1\}}(X, \bar{\mathbb{Q}}_\ell)$.

Proof. As the assertion is local for the étale topology on Y and trivial for f proper quasifinite, we may assume that f is an open immersion. Let $i : Z \to Y$ be the closed immersion complementary to f. We proceed by induction on the dimension d of Z. Let $0 \to A_1 \to A_2 \to A_3 \to 0$ be a short exact sequence in $\mathrm{Perv}_\iota^{\{w, w+1\}}(X, \bar{\mathbb{Q}}_\ell)$. As in Gabber's proof of his theorem on the independence on ℓ for middle extensions [Fujiwara 2002, Theorem 3], up to shrinking Z, we may assume that Z is smooth equidimensional and that $\mathcal{H}^n i^* \mathrm{R} f_* A_j$ is lisse for every j and every n. It follows that the distinguished triangle

$$i_* \mathrm{R} i^! f_{!*} A_j \to f_{!*} A_j \to \mathrm{R} f_* A_j \to$$

induces isomorphisms $f_{!*} A_j \xrightarrow{\sim} {}^P\tau^{\leq -d-1} \mathrm{R} f_* A_j$ and ${}^P\tau^{\geq -d} \mathrm{R} f_* A_j \xrightarrow{\sim} i_* \mathrm{R} i^! f_{!*} A_j[1]$ for every j. Here P denotes the t-structure obtained by gluing $(\mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell), 0)$ and the canonical t-structure on $\mathrm{D}_c^b(Z, \bar{\mathbb{Q}}_\ell)$. Thus ${}^P\mathrm{R}^{-d-1} f_* A_j \simeq i_* \mathcal{H}^{-d-1} i^* f_{!*} A_j$ has punctual ι-weights $\leq w - d$, while ${}^P\mathrm{R}^{-d} f_* A_j \simeq i_* \mathcal{H}^{-d+1} \mathrm{R} i^! f_{!*} A_j$ has punctual

ι-weights $\geq w - d + 1$. Therefore, the morphism ${}^P\mathrm{R}^{-d-1}f_*A_3 \to {}^P\mathrm{R}^{-d}f_*A_1$ is zero. Applying Lemma 4.1.9 below, we get a distinguished triangle

$$ {}^P\tau^{\leq -d-1}\mathrm{R}f_*A_1 \to {}^P\tau^{\leq -d-1}\mathrm{R}f_*A_2 \to {}^P\tau^{\leq -d-1}\mathrm{R}f_*A_3 \to . $$

Taking perverse cohomology sheaves, we get the exactness of the sequence

$$ 0 \to f_{!*}A_1 \to f_{!*}A_2 \to f_{!*}A_3 \to 0. \qquad \Box $$

Lemma 4.1.9. *Let P be a t-structure on a triangulated category $\mathscr{D}$ and let $A \xrightarrow{a} B \xrightarrow{b} C \xrightarrow{c} A[1]$ be a distinguished triangle such that ${}^P\mathrm{H}^0c : {}^P\mathrm{H}^0C \to {}^P\mathrm{H}^1A$ is zero. Then there exists a unique nine-diagram of the form*

$$ (4\text{-}1\text{-}1) $$

in which the columns are the canonical distinguished triangles.

By a *nine-diagram* in a triangulated category (see Proposition 1.1.11 of [Beilinson et al. 1982]), we mean a diagram

$$
\begin{array}{ccccccc}
A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & A[1] \\
\downarrow & & \downarrow & & \downarrow & & \vdots \\
A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & A'[1] \\
\downarrow & & \downarrow & & \downarrow & & \vdots \\
A'' & \longrightarrow & B'' & \longrightarrow & C'' & \longrightarrow & A''[1] \\
\downarrow & & \downarrow & & \downarrow & - & \vdots \\
A[1] & \dashrightarrow & B[1] & \dashrightarrow & C[1] & \dashrightarrow & A[2]
\end{array}
$$

in which the square marked with "$-$" is anticommutative and all other squares are commutative, the dashed arrows are induced from the solid ones by translation, and the rows and columns in solid arrows are distinguished triangles.

Proof. First note that vcu is the image of $^P\mathrm{H}^0 c$ under the isomorphism

$$\mathrm{Hom}(^P\mathrm{H}^0 C, {}^P\mathrm{H}^1 A) \xrightarrow{\sim} \mathrm{Hom}(^P\tau^{\leq 0}C, (^P\tau^{\geq 1}A)[1]).$$

Hence $vcu = 0$. Moreover, $\mathrm{Hom}(^P\tau^{\leq 0}C, {}^P\tau^{\geq 1}A) = 0$. Thus by [Beilinson et al. 1982, Proposition 1.1.9], there exist a unique c_0 making $(*)$ commutative and a unique c_1 making $(**)$ commutative. This proves the uniqueness of (4-1-1). It remains to show that (4-1-1) thus constructed is a nine-diagram. To do this, we extend the upper left square of (4-1-1) into a nine-diagram

$$(4\text{-}1\text{-}2)$$

$$
\begin{array}{ccccccc}
^P\tau^{\leq 0}A & \xrightarrow{^P\tau^{\leq 0}a} & ^P\tau^{\leq 0}B & \longrightarrow & C_0 & \longrightarrow & (^P\tau^{\leq 0}A)[1] \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
A & \xrightarrow{a} & B & \xrightarrow{b} & C & \xrightarrow{c} & A[1] \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle(***)} & & \downarrow \\
^P\tau^{\geq 1}A & \xrightarrow{^P\tau^{\geq 1}a} & ^P\tau^{\geq 1}B & \longrightarrow & C_1 & \longrightarrow & (^P\tau^{\geq 1}A)[1] \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
(^P\tau^{\leq 0}A)[1] & \xrightarrow{(^P\tau^{\leq 0}a)[1]} & (^P\tau^{\leq 0}B)[1] & \longrightarrow & C_0[1] & \longrightarrow & (^P\tau^{\leq 0}A)[2]
\end{array}
$$

By the first and third rows of (4-1-2), $C_0 \in {}^P\mathscr{D}^{\leq 0}$ and $C_1 \in {}^P\mathscr{D}^{\geq 0}$. Taking $^P\mathrm{H}^0$ of $(***)$, we obtain a commutative diagram

$$
\begin{array}{ccc}
^P\mathrm{H}^0 C & \xrightarrow{\ 0\ } & ^P\mathrm{H}^1 A \\
{\scriptstyle e}\downarrow & & \| \\
^P\mathrm{H}^0 C_1 & \xrightarrow{\ d\ } & ^P\mathrm{H}^1 A
\end{array}
$$

in which e is an epimorphism and d is a monomorphism. Thus $^P\mathrm{H}^0 C_1 = 0$, so that $C_1 \in {}^P\mathscr{D}^{\geq 1}$. Further applying [Beilinson et al. 1982, Proposition 1.1.9], we may identify (4-1-2) with (4-1-1). $\qquad\square$

4.2. *Statement and consequences of main result.* In this subsection, we define a subgroup $\mathrm{K}_{\iota,\sigma}$ of the Grothendieck group and state its preservation by Grothendieck's six operations, given in Theorem 4.2.5 which contains the finite field case of Theorem 1.9. We then give a number of consequences and discuss the relationship with the independence of ℓ and Laumon's theorem on Euler characteristics.

Definition 4.2.1 ($\mathrm{K}_{\iota,\sigma}$)**.** We define $\mathrm{K}_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{K}_\iota^w(X, \bar{\mathbb{Q}}_\ell)$ (resp. $\mathrm{K}_{\iota,\mathrm{sd}}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{K}_\iota^w(X, \bar{\mathbb{Q}}_\ell)$), for $w \in \mathbb{Z}$, to be the subgroup generated by $[B]$, for B perverse, ι-pure

of weight w, and $(-1)^w \sigma$-self-dual (resp. self-dual) with respect to $K_X(-w)$. We set

$$K_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell) = \bigoplus_{w \in \mathbb{Z}} K_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell) \quad \left(\text{resp. } K_{\iota,\mathrm{sd}}(X, \bar{\mathbb{Q}}_\ell) = \bigoplus_{w \in \mathbb{Z}} K_{\iota,\mathrm{sd}}^w(X, \bar{\mathbb{Q}}_\ell)\right).$$

We define the *twisted dualizing map*

$$\bar{D}_{\iota,X} : K_\iota^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell) \to K_\iota^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell)$$

to be the direct sum of the group automorphisms $\bar{D}_{\iota,X}^w : K_\iota^w(X, \bar{\mathbb{Q}}_\ell) \to K_\iota^w(X, \bar{\mathbb{Q}}_\ell)$ sending $[A]$ to $[(D_X A)(-w)]$. We let $K_{\iota,\mathrm{d}}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq K_\iota^w(X, \bar{\mathbb{Q}}_\ell)^2$ denote the graph of $\bar{D}_{\iota,X}^w$. We set

$$K_{\iota,\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell) = \bigoplus_{w \in \mathbb{Z}} K_{\iota,\mathrm{d}}^w(X, \bar{\mathbb{Q}}_\ell).$$

Note that $\bar{D}_{\iota,X} \bar{D}_{\iota,X} = \mathrm{id}$, and that $K_{\iota,\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell) \subseteq K_\iota^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell)^2$ is the graph of $\bar{D}_{\iota,X}$.

Example 4.2.2. For $X = \mathrm{Spec}(\mathbb{F}_q)$, an element $A \in K(X, \bar{\mathbb{Q}}_\ell)$ is determined by the determinant

$$P(A, T) := \det(1 - T \,\mathrm{Frob}_q \mid A_{\bar{\mathbb{F}}_q}) \in \bar{\mathbb{Q}}_\ell(T).$$

Assume $A \in K_\iota^w(X, \bar{\mathbb{Q}}_\ell)$, $w \in \mathbb{Z}$. For $\lambda \in \bar{\mathbb{Q}}_\ell$ satisfying $|\iota(\lambda)| = q^{w/2}$, we let m_λ and m_λ' denote the order at $T = 1/\lambda$ of $P(A, T)$ and $P(\bar{D}_{\iota,X} A, T)$, respectively. We then have $m_\lambda = m_{q^w/\lambda}'$; in other words,

$$\iota P(A, T) = \bar{\iota} P(\bar{D}_{\iota,X} A, T). \tag{4-2-1}$$

We also have $K_{\iota,(-1)^{w+1}}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq K_{\iota,(-1)^w}^w(X, \bar{\mathbb{Q}}_\ell) = K_{\iota,\mathrm{sd}}^w(X, \bar{\mathbb{Q}}_\ell)$. The following conditions are equivalent:

(1) $A \in K_{\iota,(-1)^w}^w(X, \bar{\mathbb{Q}}_\ell) = K_{\iota,\mathrm{sd}}^w(X, \bar{\mathbb{Q}}_\ell)$;

(2) $m_\lambda = m_{q^w/\lambda}$ for all λ;

(3) $\iota P(A, T) \in \mathbb{R}(T)$.

Furthermore, the following conditions are equivalent:

(1) $A \in K_{\iota,(-1)^{w+1}}^w(X, \bar{\mathbb{Q}}_\ell)$;

(2) $m_{q^{w/2}}, m_{-q^{w/2}}$ are even, and we have $m_\lambda = m_{q^w/\lambda}$ for all λ;

(3) the rank $b = \sum_\lambda m_\lambda \in \mathbb{Z}$ of A is even, and we have $\iota P(A, T) \in \mathbb{R}(T)$ and $\det(\mathrm{Frob}_q \mid A_{\bar{\mathbb{F}}_q}) = q^{wb/2}$.

Remark 4.2.3. Let $w \in \mathbb{Z}$.

(1) By definition, $K_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell) \subseteq K(X, \bar{\mathbb{Q}}_\ell)$ (resp. $K_{\iota,\mathrm{sd}}(X, \bar{\mathbb{Q}}_\ell) \subseteq K(X, \bar{\mathbb{Q}}_\ell)$) is generated by the image of $D_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$ (resp. $D_{\iota,\mathrm{sd}}^w(X, \bar{\mathbb{Q}}_\ell)$), from Definition 3.2.2. Moreover, $K_{\iota,\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell) \subseteq K(X, \bar{\mathbb{Q}}_\ell)^2$ is generated by the image of $D_{\iota,\mathrm{d}}^w(X, \bar{\mathbb{Q}}_\ell)$.

(2) By Remark 2.2.7, in the definition of $K^w_{\iota,\sigma}$, one may restrict to semisimple perverse sheaves. This also holds for $K^w_{\iota,sd}$. Thus $K^w_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$ (resp. $K^w_{\iota,sd}(X, \bar{\mathbb{Q}}_\ell)$) is generated by $[A] + [(D_X A)(-w)]$ for A simple perverse ι-pure of weight w, and $[B]$ for B simple perverse ι-pure of weight w and $(-1)^w \sigma$-self-dual (resp. self-dual) with respect to $K_X(-w)$.

(3) By Proposition 2.2.3, we have $K^w_{\iota,sd}(X, \bar{\mathbb{Q}}_\ell) = K^w_{\iota,1}(X, \bar{\mathbb{Q}}_\ell) + K^w_{\iota,-1}(X, \bar{\mathbb{Q}}_\ell)$.

(4) $K_{\iota,d}(X, \bar{\mathbb{Q}}_\ell)$ is generated by $([B], [(D_X A)(-w)])$ for B simple perverse ι-pure of weight w. Thus $K_{\iota,sd}(X, \bar{\mathbb{Q}}_\ell) = \Delta^{-1}(K_{\iota,d}(X, \bar{\mathbb{Q}}_\ell))$, where $\Delta \colon K^{\mathbb{Z}}_\iota(X, \bar{\mathbb{Q}}_\ell) \to K^{\mathbb{Z}}_\iota(X, \bar{\mathbb{Q}}_\ell)^2$ is the diagonal embedding. In other words, for $A \in K^{\mathbb{Z}}_\iota(X, \bar{\mathbb{Q}}_\ell)$, A belongs to $K_{\iota,sd}(X, \bar{\mathbb{Q}}_\ell)$ if and only if $A = \bar{D}_{\iota,X} A$.

(5) For $A \in K^{\mathbb{Z}}_\iota(X, \bar{\mathbb{Q}}_\ell)$ and $n \in \mathbb{Z}$, we have $\bar{D}_{\iota,X}(A(n)) = (\bar{D}_{\iota,X} A)(n)$. For $A \in K^w_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$, we have $A(n) \in K^{w-2n}_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$.

(6) Let A be a perverse sheaf on X, ι-pure of weight w. By Corollary 2.2.6, $[A] \in K^w_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$ if and only if the semisimplification of A is $(-1)^w \sigma$-self-dual with respect to $K_X(-w)$. Similar results hold for $K_{\iota,sd}$ and $K_{\iota,d}$.

Remark 4.2.4. Although we do not need it in the sequel, let us give two more descriptions of $K^w_{\iota,\sigma}$. In our definition of $K^w_{\iota,\sigma}$, we consider self-dual perverse sheaves B only and do not take the bilinear form $B \simeq D_X B(-w)$ as part of the data. Alternatively, we can also include the form and consider the Grothendieck group GS of symmetric spaces in $\mathrm{Perv}^{\{w\}}_\iota$ (equipped with the duality $D_X(-w)$ and the evaluation map modified by a factor of $(-1)^w \sigma$). The Grothendieck–Witt group GW is a quotient of GS, equipped with a homomorphism $\mathrm{GW} \to K^w_\iota$. We refer the reader to [Quebbemann et al. 1979, page 280; Schlichting 2010, Section 2.2] for the definition of the Grothendieck–Witt group of an abelian category with duality (generalizing Quillen's definition [1971, Section 5.1] for representations). In our situation, the canonical maps

$$\mathrm{GS} \to \mathrm{GW} \to K^w_{\iota,\sigma}$$

are isomorphisms. In fact, by definition, $K^w_{\iota,\sigma}$ is the image of GW. Moreover, since we work over the algebraically closed field $\bar{\mathbb{Q}}_\ell$, symmetric spaces with isomorphic underlying objects are isometric [Quebbemann et al. 1979, Applications 3.4(3)].

We now consider preservation of $K_{\iota,\sigma}$ and $K_{\iota,d}$ by cohomological operations. The preservation of $K_{\iota,d}$ is equivalent to the commutation with the twisted dualizing map $\bar{D}_\iota$. The main result of this section is the following generalization of Theorem 1.9.

Theorem 4.2.5. *Let* $f \colon X \to Y$ *be a morphism between Deligne–Mumford stacks of finite inertia and finite presentation over* $\mathbb{F}_q$. *Then Grothendieck's six operations*

induce maps

$$- \otimes -, \mathscr{H}om(-, -) : \mathrm{K}_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell) \times \mathrm{K}_{\iota,\sigma'}(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{K}_{\iota,\sigma\sigma'}(X, \bar{\mathbb{Q}}_\ell),$$

$$f^*, f^! : \mathrm{K}_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell) \to \mathrm{K}_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell),$$

$$f_*, f_! : \mathrm{K}_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{K}_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell).$$

Moreover, Grothendieck's six operations on $\mathrm{K}_\iota^{\mathbb{Z}}$ *commute with the twisted dualizing map* $\bar{D}_\iota$.

The proof will be given in the next section. We now make a list of pure cases in which the preservation has already been established. Most items of the list below follow from Remark 3.2.8.

Remark 4.2.6 (preservation of $\mathrm{K}_{\iota,\sigma}$, pure cases). Let $f : X \to Y$ be a morphism, and let $w, w' \in \mathbb{Z}$.

(1) D_X carries $\mathrm{K}_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$ to $\mathrm{K}_{\iota,\sigma}^{-w}(X, \bar{\mathbb{Q}}_\ell)$.

(2) If f is smooth, then f^* preserves $\mathrm{K}_{\iota,\sigma}^w$.

(3) If f is an open immersion, then $f_{!*}$ preserves $\mathrm{K}_{\iota,\sigma}^w$.

(4) The functor $- \boxtimes -$ carries $\mathrm{K}_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell) \times \mathrm{K}_{\iota,\sigma'}^{w'}(X', \bar{\mathbb{Q}}_\ell)$ to $\mathrm{K}_{\iota,\sigma\sigma'}^{w+w'}(X \times X', \bar{\mathbb{Q}}_\ell)$, and the functor $(-)^{\boxtimes m}$, $m \geq 0$, carries $\mathrm{K}_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$ to $\mathrm{K}_{\iota,\sigma^m}^{mw}([X^m/\mathfrak{S}_m], \bar{\mathbb{Q}}_\ell)$. For the latter we use Proposition 3.2.14.

(5) Assume that f is a closed immersion and let $A \in \mathrm{K}(X, \bar{\mathbb{Q}}_\ell)$. Then we have $A \in \mathrm{K}_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$ if and only if $f_* A \in \mathrm{K}_{\iota,\sigma}^w(Y, \bar{\mathbb{Q}}_\ell)$.

(6) Assume that f is proper. If f is projective or Y has finite inertia, then f_* preserves $\mathrm{K}_{\iota,\sigma}^w$, by Proposition 3.2.12 and Theorem 3.2.3.

Similar properties hold for $\mathrm{K}_{\iota,\mathrm{d}}$.

The Zariski local nature of $\mathrm{K}_{\iota,\sigma}^w$ will be used in the proof of Theorem 4.2.5. It follows from the Zariski local nature of σ-self-dual perverse sheaves (Proposition 2.2.1). It also follows from Remark 4.2.6(3) and Lemma 4.1.3.

Remark 4.2.7 (Zariski local nature). Let $(X_\alpha)_{\alpha \in I}$ be a Zariski open covering of X and let $A \in \mathrm{K}(X, \bar{\mathbb{Q}}_\ell)$. Then $A \in \mathrm{K}_{\iota,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$ if and only if $A \mid X_\alpha \in \mathrm{K}_{\iota,\sigma}^w(X_\alpha, \bar{\mathbb{Q}}_\ell)$ for every α. The same holds for $\mathrm{K}_{\iota,\mathrm{d}}$.

We now turn to consequences of Theorem 4.2.5. The ring part of the next two corollaries follows from the two assertions of Theorem 4.2.5 applied to a_X^* (recall $a_X : X \to \mathrm{Spec}(\mathbb{F}_q)$) and $- \otimes -$. For the λ-ring part, we apply Remark 4.2.6(4) to the map $(-)^{\boxtimes m}$ and Theorem 4.2.5 to the maps Δ^* and p_* in the definition of λ^m in Construction 4.1.1.

Corollary 4.2.8. *Assume that X has finite inertia. Then $\mathrm{K}_{\iota,1}(X, \bar{\mathbb{Q}}_\ell)$ is a λ-subring of $\mathrm{K}(X, \bar{\mathbb{Q}}_\ell)$. In particular, $\mathrm{K}_{\iota,1}(X, \bar{\mathbb{Q}}_\ell)$ contains the class $[\bar{\mathbb{Q}}_\ell]$ of the constant sheaf $\bar{\mathbb{Q}}_\ell$ on X.*

Corollary 4.2.9. *Assume that X has finite inertia. Then $\bar{D}_{\iota,X} : \mathrm{K}_{\iota}^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{K}_{\iota}^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell)$ is a λ-ring homomorphism. In particular, $\bar{D}_{\iota,X}[\bar{\mathbb{Q}}_\ell] = [\bar{\mathbb{Q}}_\ell]$.*

Another consequence of Theorem 4.2.5 is the following pointwise characterization of $\mathrm{K}_{\iota,\mathrm{d}}$ and $\mathrm{K}_{\iota,\mathrm{sd}}$. We let $\mathrm{K}_{\iota,\bar{\iota}}(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{K}(X, \bar{\mathbb{Q}}_\ell)^2$ (resp. $\mathrm{K}_{\iota,\mathbb{R}}(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{K}(X, \bar{\mathbb{Q}}_\ell)$) denote the subgroup consisting of elements (A, A') (resp. A) such that, for every morphism $x : \mathrm{Spec}(\mathbb{F}_{q^m}) \to X$ and every geometric point $\bar{x}$ above x, we have

$$\iota \, \mathrm{tr}(\mathrm{Frob}_x, A_{\bar{x}}) = \bar{\iota} \, \mathrm{tr}(\mathrm{Frob}_x, A'_{\bar{x}}) \quad (\text{resp. } \iota \, \mathrm{tr}(\mathrm{Frob}_x, A_{\bar{x}}) \in \mathbb{R}).$$

The notation $\mathrm{K}_{\iota,\bar{\iota}}$ and $\mathrm{K}_{\iota,\mathbb{R}}$ will only be used in Corollary 4.2.10 and Remark 4.2.11.

Corollary 4.2.10. *Assume that X has finite inertia. Let $A \in \mathrm{K}_{\iota}^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell)$. Then for every $m \geq 1$, every morphism $x : \mathrm{Spec}(\mathbb{F}_{q^m}) \to X$, and every geometric point $\bar{x}$ above x, we have*

$$\iota \, \mathrm{tr}(\mathrm{Frob}_x, A_{\bar{x}}) = \bar{\iota} \, \mathrm{tr}(\mathrm{Frob}_x, (\bar{D}_{\iota,X} A)_{\bar{x}}). \qquad (4\text{-}2\text{-}2)$$

Moreover, $\mathrm{K}_{\iota,\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell) = \mathrm{K}_{\iota,\bar{\iota}}(X, \bar{\mathbb{Q}}_\ell) \cap \mathrm{K}_{\iota}^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell)^2$. In particular, $\mathrm{K}_{\iota,\mathrm{sd}}(X, \bar{\mathbb{Q}}_\ell) = \mathrm{K}_{\iota,\mathbb{R}} \cap \mathrm{K}_{\iota}^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell)$.

Proof. By the second assertion of Theorem 4.2.5 applied to x^*, we see that $\bar{D}_{\iota,\mathrm{Spec}(\mathbb{F}_{q^m})} x^* A = x^* \bar{D}_{\iota,X} A$. Therefore, (4-2-1) in Example 4.2.2 implies (4-2-2). It follows that $\mathrm{K}_{\iota,\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{K}_{\iota,\bar{\iota}}(X, \bar{\mathbb{Q}}_\ell) \cap \mathrm{K}_{\iota}^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell)^2$. The inclusion in the other direction follows from the injectivity of the homomorphism $\mathrm{K}(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{Map}\left(\coprod_{m \geq 1} |X(\mathbb{F}_{q^m})|, \bar{\mathbb{Q}}_\ell\right)$ (Lemma 4.1.4). The last assertion of Corollary 4.2.10 follows from the second one. $\square$

Remark 4.2.11. Corollary 4.2.10 also follows from [Katz 2005, Parts (1) and (4) of Lemma 1.8.1], which in turn follow from Gabber's theorem on the independence of ℓ for middle extensions [Fujiwara 2002, Theorem 3]. By Gabber's theorem on the independence of ℓ for Grothendieck's six operations [Fujiwara 2002, Theorem 2] (see [Zheng 2009, 3.2] for a different proof and [Zheng 2009, Proposition 5.8] for the case of stacks), $\mathrm{K}_{\iota,\bar{\iota}}$ and $\mathrm{K}_{\iota,\mathbb{R}}$ in Corollary 4.2.10 are stable under the six operations. Thus the second assertion of Theorem 4.2.5 follows from Gabber's theorems on the independence of ℓ. We will not use Gabber's theorems on the independence of ℓ in our proof of Theorem 4.2.5.

Remark 4.2.12. The pointwise characterization of $\mathrm{K}_{\iota,\mathrm{sd}}$ in Corollary 4.2.10 does not extend to $\mathrm{K}_{\iota,\sigma}$. For instance, if X is regular and geometrically connected and if $f : E \to X$ is a family of elliptic curves with nonconstant j-invariant, then $\mathscr{F} = \mathrm{R}^1 f_* \bar{\mathbb{Q}}_\ell$ is a geometrically simple lisse $\bar{\mathbb{Q}}_\ell$-sheaf on X by [Deligne 1980,

Lemme 3.5.5]. Thus we have $[\mathscr{F}] \in \mathrm{K}^1_{\iota,1}(X, \bar{\mathbb{Q}}_\ell) \backslash \mathrm{K}^1_{\iota,-1}(X, \bar{\mathbb{Q}}_\ell)$, but, for every closed point x of X, we have $[\mathscr{F}_x] \in \mathrm{K}^1_{\iota,1}(x, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{K}^1_{\iota,-1}(x, \bar{\mathbb{Q}}_\ell)$.

Remark 4.2.13. Let $f : X \to Y$ be as in Theorem 4.2.5 and let $\mathrm{I}(Y, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{K}(Y, \bar{\mathbb{Q}}_\ell)$ be the ideal generated by $[\bar{\mathbb{Q}}_\ell(1)] - [\bar{\mathbb{Q}}_\ell]$. A theorem of Laumon [1981] ([Illusie and Zheng 2013, Theorem 3.2] for the case of Deligne–Mumford stacks) states that $f_* \equiv f_!$ modulo $\mathrm{I}(Y, \bar{\mathbb{Q}}_\ell)$. This is equivalent to the congruence $D_Y f_* \equiv f_* D_X$ (and to $D_Y f_! \equiv f_! D_X$) modulo $\mathrm{I}(Y, \bar{\mathbb{Q}}_\ell)$. Thus the second assertion of Theorem 4.2.5 can be seen as a refinement of Laumon's theorem.

In the case of $\mathrm{K}_{\iota,\sigma}$, we have the following result on the independence of (ℓ, ι). Let $\ell' \neq q$ be a prime number and let $\iota' : \bar{\mathbb{Q}}_{\ell'} \to \mathscr{C}$ be an embedding.

Corollary 4.2.14. *Assume that X has finite inertia. Let $A \in \mathrm{K}^{\mathbb{Z}}_\iota(X, \bar{\mathbb{Q}}_\ell)$ and let $A' \in \mathrm{K}^{\mathbb{Z}}_{\iota'}(X, \bar{\mathbb{Q}}_{\ell'})$. Assume that A and A' are compatible in the sense that, for every morphism $x : \mathrm{Spec}(\mathbb{F}_{q^m}) \to X$ and every geometric point $\bar{x}$ above x, we have*

$$\iota \operatorname{tr}(\mathrm{Frob}_x, A_{\bar{x}}) = \iota' \operatorname{tr}(\mathrm{Frob}_x, A'_{\bar{x}}).$$

Then A belongs to $\mathrm{K}_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$ if and only if A' belongs to $\mathrm{K}_{\iota',\sigma}(X, \bar{\mathbb{Q}}_{\ell'})$.

Proof. Let $(X_\alpha)_{\alpha \in I}$ be a stratification of X. Then we have $A = \sum_{\alpha \in I} j_{\alpha!} j_\alpha^* A$ and $A' = \sum_{\alpha \in I} j_{\alpha!} j_\alpha^* A'$, where $j_\alpha : X_\alpha \to X$ is the immersion. Thus, by Theorem 4.2.5, up to replacing X by a stratum, we may assume that X is regular and A belongs to the subgroup generated by lisse $\bar{\mathbb{Q}}_\ell$-sheaves, that is, $A = \sum_{\mathscr{F}} n_{\mathscr{F}} [\mathscr{F}]$, where $\mathscr{F}$ runs over isomorphism classes of simple lisse $\bar{\mathbb{Q}}_\ell$-sheaves. For each $\mathscr{F}$ appearing in the decomposition, let $\mathscr{F}'$ be the companion of $\mathscr{F}$ [Drinfeld 2012] ([Zheng 2015a] for the case of stacks), namely the simple lisse Weil $\bar{\mathbb{Q}}_{\ell'}$-sheaf such that

$$\iota \operatorname{tr}(\mathrm{Frob}_x, \mathscr{F}_{\bar{x}}) = \iota' \operatorname{tr}(\mathrm{Frob}_x, \mathscr{F}'_{\bar{x}})$$

for all x and $\bar{x}$ as above. Since $A' = \sum_{\mathscr{F}} n_{\mathscr{F}} [\mathscr{F}']$, each $\mathscr{F}'$ is an honest $\bar{\mathbb{Q}}_{\ell'}$-sheaf. By Corollary 4.2.10, we have $(\bar{D}\mathscr{F})' = \bar{D}(\mathscr{F}')$. Therefore, we may assume that $A = [\mathscr{F}]$ and $A' = [\mathscr{F}']$. In this case, the assertion follows from the symmetry criterion in terms of squares of Frobenius (Proposition 3.2.15). $\square$

4.3. *Proof of main result.* The situation of Theorem 4.2.5 is quite different from that of Gabber's theorem on the independence of ℓ [Fujiwara 2002, Theorem 2]. In Gabber's theorem, the preservation by $- \otimes -$ and f^* is trivial and the preservation by $f_!$ follows from the Grothendieck trace formula. The key point of Gabber's theorem is thus the preservation by D_X. The preservation by middle extensions [Fujiwara 2002, Theorem 3] follows from the preservation by the six operations. In Theorem 4.2.5, the stability under each of the six operations is nontrivial, but the preservation by D_X and middle extensions is easy. To prove Theorem 4.2.5, we

will first deduce that $f_!$ preserves $K_{\iota,\sigma}$ and $K_{\iota,d}$ in an important special case from the preservation by middle extensions.

Proposition 4.3.1. *Let X be a regular Deligne–Mumford stack of finite presentation over $\mathbb{F}_q$ and let $D = \sum_{\alpha \in I} D_\alpha$ be a strict normal crossing divisor, with D_α regular. Assume that there exists a finite étale morphism $f : Y \to X$ such that $f^{-1}(D_\alpha)$ is defined globally by $t_\alpha \in \Gamma(Y, \mathscr{O}_Y)$ for all $\alpha \in I$. Let $\mathscr{F}$ be a lisse $\bar{\mathbb{Q}}_\ell$-sheaf on $U = X - D$, tamely ramified along D. Assume that $[\mathscr{F}] \in K_\iota^{\mathbb{Z}}(U, \bar{\mathbb{Q}}_\ell)$. Then $\bar{D}_{\iota,X}[j_!\mathscr{F}] = j_! \bar{D}_{\iota,U}[\mathscr{F}]$ and, if $[\mathscr{F}] \in K_{\iota,\sigma}(U, \bar{\mathbb{Q}}_\ell)$, $[j_!\mathscr{F}]$ belongs to $K_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$, where $j : U \to X$ is the open immersion.*

Proof. We will prove the case of $K_{\iota,\sigma}$. The case of $K_{\iota,d}$ is similar.

We may assume that f is a Galois étale cover of group G. Note that, for $g \in G$, we have $g t_\alpha = u t_\alpha$ for some root of unity u in k. We apply the construction of [Deligne 1980, 1.7.9] to our setting as follows. For $J \subseteq I$, let $U_J = X - \bigcup_{\beta \in I - J} D_\beta$ and let $D_J^* = \bigcap_{\beta \in J} D_\beta \cap U_J$. For a locally constant constructible sheaf of sets $\mathscr{G}$ on U, tamely ramified along D, there exists an integer n invertible in k such that $f^{-1}\mathscr{G}$ extends to $\mathscr{G}'$ on the cover $(f^{-1}U_J)[t_\alpha^{1/n}]_{\alpha \in J}$ of $f^{-1}U_J$. We let $(f^{-1}\mathscr{G})[f^{-1}D_J^*]$ denote the restriction of $\mathscr{G}'$ to D_J^*, which is locally constant constructible and equipped with an action of a central extension G_J of G by μ_n^J, compatible with the action of G on $f^{-1}D_J^*$. Extending this construction to $\bar{\mathbb{Q}}_\ell$-sheaves by taking limits, we obtain a lisse $\bar{\mathbb{Q}}_\ell$-sheaf $(f^*\mathscr{F})[f^{-1}D_J^*]$ on $f^{-1}D_J^*$ endowed with an action of a central extension of G by $\hat{\mathbb{Z}}_L^J(1)$, compatible with the action of G on $f^{-1}D_J^*$. Here L denotes the set of primes invertible in k.

Let us first show that, for all $J \subseteq I$, we have $[j_J^* R j_* \mathscr{F}] \in K_{\iota,\sigma}(D_J^*, \bar{\mathbb{Q}}_\ell)$, where $j_J : D_J^* \to X$ is the immersion. We proceed by induction on $\#J$. The assertion is trivial for J empty, as $j_\varnothing = j$. For J nonempty, choose $\beta \in J$. Consider the diagram with Cartesian square

$$
\begin{array}{ccc}
 & & D_J^* \\
 & & \downarrow {\scriptstyle j'_{\beta, J'}} \\
D_{\{\beta\}}^* & \xrightarrow{\ j'_\beta\ } & D_\beta \\
{\scriptstyle i'_\beta} \downarrow & {\scriptstyle j_{\{\beta\}}} \searrow & \downarrow {\scriptstyle i_\beta} \\
U \xrightarrow{\ j^\beta\ } & U_\beta \xrightarrow{\ j_\beta\ } & X
\end{array}
$$

in which $U_\beta = X - \bigcup_{\alpha \in I - \{\beta\}} D_\alpha$, $D_{\{\beta\}} = D_\beta \cap U_\beta$, and $J' = J - \{\beta\}$. By [Zheng 2008, Lemme 3.7] (or by direct computation using [Deligne 1980, 1.7.9]), the base change morphism

$$i_\beta^* R j_* \mathscr{F} \to R j'_{\beta *} i_\beta'^* R j_*^\beta \mathscr{F}$$

is an isomorphism, so that

$$j_J^* R j_* \mathcal{F} \simeq (j'_{\beta,J'})^* i_\beta^* R j_* \mathcal{F} \simeq (j'_{\beta,J'})^* R j'_{\beta*} i_\beta^{\prime*} R j_*^\beta \mathcal{F}.$$

Since $\#J' < \#J$, by the induction hypothesis applied to j'_β and J', it suffices to show that the class of $i_\beta^{\prime*} R j_*^\beta \mathcal{F} \simeq j_{\{\beta\}}^* R j_* \mathcal{F}$ is in $K_{\iota,\sigma}(D_{\{\beta\}}^*, \bar{\mathbb{Q}}_\ell)$. For this, we may assume $\mathcal{F}$ ι-pure of weight $w \in \mathbb{Z}$. Let $H_\beta < \hat{\mathbb{Z}}_L(1)^{\{\beta\}} < G_{\{\beta\}}$ be an open subgroup whose action on $V = (f^*\mathcal{F})[f^{-1}D_{\{\beta\}}^*]$ is unipotent. Let $N : V(1) \to V$ be the logarithm of this action and let M be the monodromy filtration on V. We have $j_{\{\beta\}}^* R j_* \in D^{[0,1]}$,

$$j_{\{\beta\}}^* j_* \mathcal{F} \simeq (\mathrm{Ker}(N)(-1))^{G_{\{\beta\}}/H_\beta},$$

$$j_{\{\beta\}}^* R^1 j_* \mathcal{F} \simeq (\mathrm{Coker}(N))^{G_{\{\beta\}}/H_\beta}(-1),$$

$$\mathrm{gr}_i^M (\mathrm{Ker}(N)(-1)) \simeq \begin{cases} P_i(V,N) & i \le 0, \\ 0 & i > 0, \end{cases}$$

$$\mathrm{gr}_i^M (\mathrm{Coker}(N)) \simeq \begin{cases} P_{-i}(V,N)(-i) & i \ge 0, \\ 0 & i < 0. \end{cases}$$

By [Deligne 1980, Corollaire 1.8.7, Remarque 1.8.8], $P_i(V,N)$ is pure of weight $w + i$ for $i \le 0$. Moreover, $P_i(V,N)$ is $(-1)^{w+i}\sigma$-self-dual by Proposition A.6.8. It follows that $[j_{\{\beta\}}^* j_* \mathcal{F}], [j_{\{\beta\}}^* R^1 j_* \mathcal{F}] \in K_{\iota,\sigma}$.

Next we show that, if $\mathcal{F}$ is ι-pure of weight $w \in \mathbb{Z}$, then, for all $n \ge 0$ and $J \subseteq I$, we have $[j_J^* R j_{n*} j_{!*}^n \mathcal{F}] \in K_{\iota,\sigma}(D_J^*, \bar{\mathbb{Q}}_\ell)$. Here $U \xrightarrow{j^n} U_n \xrightarrow{j_n} X$ are immersions, where $U_n = X - \bigcup_{K \subseteq I, \#K \ge n} D_K^*$ and $j_{!*}^n \mathcal{F} := (j_{!*}^n (\mathcal{F}[d]))[-d]$, where $d = \dim(X)$ (a function on $\pi_0(X)$). The proof is similar to Gabber's proof of the independence of ℓ for middle extensions [Fujiwara 2002, Theorem 3]. We proceed by induction on n. For $n = 0$, we have $U_0 = U$ and the assertion is shown in the preceding paragraph. For $n \ge 1$, consider the immersions

$$U_n - U_{n-1} \xrightarrow{i_n} U_n \xleftarrow{j_{n-1}^n} U_{n-1}$$

and the distinguished triangle

$$i_{n*} R i_n^! j_{!*}^n \mathcal{F} \to j_{!*}^n \mathcal{F} \to R(j_{n-1}^n)_* j_{!*}^{n-1} \mathcal{F} \to .$$

The second and third arrows induce isomorphisms $j_{!*}^n \mathcal{F} \xrightarrow{\sim} \tau^{\le n-1} R(j_{n-1}^n)_* j_{!*}^{n-1} \mathcal{F}$ and $\tau^{\ge n} R(j_{n-1}^n)_* j_{!*}^{n-1} \mathcal{F} \xrightarrow{\sim} i_{n*} R i_n^! j_{!*}^n \mathcal{F}[1]$. By the induction hypothesis, the left-hand side of

$$[i_n^* R(j_{n-1}^n)_* j_{!*}^{n-1} \mathcal{F}] = [i_n^* j_{!*}^n \mathcal{F}] - [R i_n^! j_{!*}^n \mathcal{F}]$$

belongs to $K_{\iota,\sigma}$. The first term of the right-hand side belongs to $\bigoplus_{w' \le w+n-1} K_\iota^{w'}$ and the second term belongs to $\bigoplus_{w' \ge w+n+1} K_\iota^{w'}$. It follows that both terms belong

to $K_{\iota,\sigma}$. Thus, by the preceding paragraph, $[j_J^* R(j_n i_n)_* R i_n^! j_{!*}^n \mathscr{F}] \in K_{\iota,\sigma}$. Moreover, by the induction hypothesis, $[j_J^* R(j_{n-1})_* j_{!*}^{n-1} \mathscr{F}] \in K_{\iota,\sigma}$. Therefore, we have $[j_J^* R j_{n*} j_{!*}^n \mathscr{F}] = [j_J^* R(j_n i_n)_* R i_n^! j_{!*}^n \mathscr{F}] + [j_J^* R(j_{n-1})_* j_{!*}^{n-1} \mathscr{F}] \in K_{\iota,\sigma}$.

Taking $n = 1 + \#I$ so that $U_n = X$ in the preceding paragraph, we get that $[j_J^* j_{!*} \mathscr{F}] \in K_{\iota,\sigma}(D_J^*, \bar{\mathbb{Q}}_\ell)$, for $\mathscr{F}$ ι-pure and $J \subseteq I$. Here $j_{!*} \mathscr{F} := (j_{!*}(\mathscr{F}[d]))[-d]$.

Finally, we show the proposition by induction on $\#I$. The assertion is trivial for I empty. For I nonempty, we may assume $\mathscr{F}$ ι-pure. We have

$$[j_{!*} \mathscr{F}] = [j_! \mathscr{F}] + \sum_{\varnothing \neq J \subseteq I} [j_{J!} j_J^* j_{!*} \mathscr{F}].$$

By the preceding paragraph and the induction hypothesis, for $\varnothing \neq J \subseteq I$, we have $[j_{J!} j_J^* j_{!*} \mathscr{F}] \in K_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$. Moreover, $[j_{!*} \mathscr{F}] \in K_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$. It follows that $[j_! \mathscr{F}] \in K_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$. $\square$

Lemma 4.3.2. *Let X be a Noetherian Deligne–Mumford stack with separated diagonal. Then there exist a finite group G and a G-equivariant dominant open immersion $V \to W$ of schemes such that the induced morphism $[V/G] \to [W/G]$ fits into a commutative diagram*

$$
\begin{array}{ccc}
[V/G] & \longrightarrow & [W/G] \\
 & \searrow{\scriptstyle j} & \downarrow{\scriptstyle f} \\
 & & X
\end{array}
$$

in which j is an open immersion and f is quasifinite, proper, and surjective.

Proof. By [Laumon and Moret-Bailly 2000, 16.6.3], there exists a finite group G acting on a scheme V that fits into a Cartesian square

$$
\begin{array}{ccc}
V & \longrightarrow & Z \\
\downarrow & & \downarrow{\scriptstyle g} \\
[V/G] & \xrightarrow{\ j\ } & X
\end{array}
$$

in which Z is a scheme, g is finite surjective, and j is a dense open immersion. It then suffices to take W to be the schematic closure of V in $(Z/X)^G$ (fiber product over X of copies of Z indexed by G) endowed with the action of G by permutation of factors. $\square$

Proof of Theorem 4.2.5. We will prove the preservation of $K_{\iota,\sigma}$. The commutation with $\bar{D}_\iota$ is similar.

(1) Let us first show the case of $f_!$ for an open immersion f. Since Y has finite inertia, there exists a Zariski open covering (Y_α) of Y with Y_α separated. By the Zariski local nature of $K_{\iota,\sigma}$ (Remark 4.2.7), we may assume Y separated. We may assume f dominant.

We proceed by induction on $d = \dim X$. For $d < 0$ (i.e., $X = \varnothing$), the assertion is trivial. For $d \geq 0$, let $A \in \mathrm{K}_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$. Note that if $A' \in \mathrm{K}(X, \bar{\mathbb{Q}}_\ell)$ is such that the support of $A - A'$ has dimension $< d$, then, by the induction hypothesis, to show $f_! A \in \mathrm{K}_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell)$, it suffices to show $A' \in \mathrm{K}_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$ and $f_! A' \in \mathrm{K}_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell)$. This applies in particular to $A' = j_! j^* A$, where $j : U \to X$ is a dominant open immersion. In this case $f_! A' = (fj)_! j^* A$. This allows us to shrink X.

Applying Lemma 4.3.2 to Y, we obtain a finite group G, a G-equivariant dominant open immersion of schemes $V \to W$, and a commutative diagram

$$
\begin{array}{ccc}
[V/G] & \longrightarrow & [W/G] \\
& \searrow & \downarrow{\scriptstyle p} \\
& & Y
\end{array}
$$

in which p is proper quasifinite surjective, and the oblique arrow is an open immersion. Let $j : U \to X$, where $U = X \cap [V/G] = [V'/G]$. By the remark above, it suffices to show that $j_!$ and $(fj)_!$ preserve $\mathrm{K}_{\iota,\sigma}$. In the case of $j_!$, up to replacing Y by X and p by its restriction to X, we are reduced to the case of $(fj)_!$. Since $(fj)_! = f'_! p_*$, where $f' : U \to [W/G]$, we are reduced to the case of $f'_!$. Thus, changing notation, we are reduced to the case of $f_!$, where $f : X = [V/G] \to [W/G] = Y$ is given by a G-equivariant open immersion of schemes $V \to W$.

The reduction of this case to the case where V is the complement of a G-strict normal crossing divisor of W is similar to parts of [Zheng 2009, Section 3]. We may assume V reduced. Shrinking V, we may assume V normal and $A = [\mathscr{F}]$, where $\mathscr{F} = \mathscr{F}_{\mathscr{O}} \otimes_{\mathscr{O}} \bar{\mathbb{Q}}_\ell$, where $\mathscr{F}_{\mathscr{O}}$ is a lisse $\mathscr{O}$-sheaf and $\mathscr{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_\ell$. Applying [Zheng 2009, Lemme 3.5], we obtain a G-stable dense open subscheme U of V and an equivariant morphism $(u, \alpha) : (U', G') \to (U, G)$, where α is surjective and u is a Galois étale cover of group $\mathrm{Ker}(\alpha)$ trivializing $\mathscr{F}_{\mathscr{O}}/\mathfrak{m}\mathscr{F}_{\mathscr{O}}$, where $\mathfrak{m}$ is the maximal ideal of $\mathscr{O}$. By Nagata compactification, this can be completed into a commutative diagram

$$
\begin{array}{ccc}
(U', G') & \xrightarrow{(f', \mathrm{id})} & (W', G') \\
{\scriptstyle (u,\alpha)}\downarrow & & \downarrow{\scriptstyle (w,\alpha)} \\
(U, G) & \longrightarrow & (W, G)
\end{array}
$$

in which w is proper and f' is an open immersion. Since $[u/\alpha]$ is an isomorphism and Remark 4.2.6(6) applies to $[w/\alpha]_*$, shrinking X and changing notation, we are reduced to the case where $\mathscr{F}_{\mathscr{O}}/\mathfrak{m}\mathscr{F}_{\mathscr{O}}$ is constant on every connected component. We may assume W reduced. Let k' be a finite extension of k such that the irreducible components of $W \otimes_k k'$ are geometrically irreducible. Up to replacing W by $W \otimes_k k'$ and G by $G \times \mathrm{Gal}(k'/k)$, we may assume that the irreducible components

of W are geometrically irreducible and that there exists a G-equivariant morphism $W \to \mathrm{Spec}(k')$. Shrinking V, we may assume V regular. Moreover, we may assume that G acts transitively on $\pi_0(V)$. Let V_0 be an irreducible component of V and let G_0 be the decomposition group. Then f can be decomposed as $X \simeq [V_0/G_0] \to [W/G_0] \xrightarrow{g} [W/G] = Y$, where g is finite. Changing notation, we may assume V irreducible. Up to replacing W by the closure of V, we may assume W irreducible, thus geometrically irreducible.

Applying Gabber's refinement [Zheng 2009, Lemme 3.8] (see also [Vidal 2004, 4.4]) of de Jong's alterations [1997], we obtain a diagram with Cartesian square

$$
\begin{array}{ccc}
(U', G') \longrightarrow (V', G') \longrightarrow (W', G') \\
\quad\quad\quad\quad\quad {\scriptstyle (v,\alpha)}\Big\downarrow \quad\quad\quad\quad {\scriptstyle (w,\alpha)}\Big\downarrow \\
\quad\quad\quad\quad\quad (V, G) \longrightarrow (W, G)
\end{array}
$$

in which (w, α) is a Galois alteration, W' is regular quasiprojective over k, and U' is the complement of a G'-strict normal crossing divisor of W'. As $\mathscr{F}$ is lisse and $[V/G]$, $[V'/G']$ are regular, $A' = [v/\alpha]^*A$ belongs to $\mathrm{K}_{\iota,\sigma}([V'/G'], \bar{\mathbb{Q}}_\ell)$, so that $[v/\alpha]_*A$ belongs to $\mathrm{K}_{\iota,\sigma}([V/G], \bar{\mathbb{Q}}_\ell)$. Moreover, the support of $A - [v/\alpha]_*A'$ has dimension $< d$. Thus it suffices to show that $f_![v/\alpha]_*A' = [w/\alpha]_*f_!'A'$ belongs to $\mathrm{K}_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell)$, where $f' : [W'/G'] \to [V'/G']$. Let $j' : [U'/G'] \to [V'/G']$. It suffices to show that $j_!'j'^*A'$ and $(f'j')_!j'^*A'$ belong to $\mathrm{K}_{\iota,\sigma}$. Changing notation, we are reduced to showing $f_![\mathscr{F}] \in \mathrm{K}_{\iota,\sigma}([W/G], \bar{\mathbb{Q}}_\ell)$ for $f : [V/G] \to [W/G]$, where V is the complement of a G-strict normal crossing divisor D of a regular quasiprojective scheme W over k and $\mathscr{F}$ is a lisse sheaf on $[V/G]$ tame along D such that $[\mathscr{F}] \in \mathrm{K}_{\iota,\sigma}([V/G], \bar{\mathbb{Q}}_\ell)$.

Note that W admits a Zariski open covering by G-stable affine schemes. Thus, by the Zariski local nature of $\mathrm{K}_{\iota,\sigma}$ (Remark 4.2.7), we may assume W affine. In this case, the assertion is a special case of Proposition 4.3.1. This finishes the proof of the case of $f_!$ for f an open immersion.

(2) Next we establish the general case of $f_!$. Let $(X_\alpha)_{\alpha \in I}$ be a Zariski open covering of X with X_α separated. For $J \subseteq I$, let $j_J : \bigcap_{\beta \in J} X_\beta \to X$ be the open immersion. Let $A \in \mathrm{K}_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$. Then, by Lemma 4.1.3, $A = \sum_{\varnothing \neq J \subseteq I} (-1)^{1+\#J} j_{J!}j_J^*A$. Thus we may assume X separated. Applying Nagata compactification [Conrad et al. 2012] to the morphism $\bar{X} \to \bar{Y}$ of coarse spaces, we obtain a diagram with Cartesian squares

$$
\begin{array}{ccccc}
X & \xrightarrow{f_1} & \bar{X} \times_{\bar{Y}} Y & \xrightarrow{f_2} & \bar{Z} \times_{\bar{Y}} Y & \xrightarrow{f_3} & Y \\
\Big\downarrow & & \Big\downarrow & & \Big\downarrow \\
\bar{X} & \xrightarrow{\quad g_2 \quad} & \bar{Z} & \xrightarrow{\quad g_3 \quad} & \bar{Y}
\end{array}
$$

in which f_1 is proper and quasifinite, g_2 is an open immersion, and g_3 is proper. Thus $f_! = f_{3*}f_{2!}f_{1*}$ preserves $K_{\iota,\sigma}$.

The case of $f_* = D_Y f_! D_X$ follows immediately.

(3) Next we establish the case of f^*. The argument is similar to the deduction of the congruence $f^* \equiv f^!$ modulo $I(X, \bar{\mathbb{Q}}_\ell)$ [Zheng 2015b, Corollary 9.5] from Laumon's theorem, mentioned in Remark 4.2.13. Let $B \in K_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell)$. If f is a closed immersion, then $B = j_! j^* B + f_* f^* B$, where j is the complementary open immersion. It follows that $f_* f^* B \in K_{\iota,\sigma}(Y, \bar{\mathbb{Q}}_\ell)$, so that $f^* B \in K_{\iota,\sigma}$. In the general case, let $(Y_\alpha)_{\alpha \in I}$ be a stratification of Y such that each Y_α is the quotient stack of an affine scheme by a finite group action. For each α, form the Cartesian square

$$
\begin{array}{ccc}
X_\alpha & \xrightarrow{j'_\alpha} & X \\
\scriptstyle f_\alpha \downarrow & & \downarrow \scriptstyle f \\
Y_\alpha & \xrightarrow{j_\alpha} & Y
\end{array}
$$

Then $f^* B = \sum_{\alpha \in I} f^* j_{\alpha!} j_\alpha^* B = \sum_{\alpha \in I} j'_{\alpha!} f_\alpha^* j_\alpha^* B$. Thus we may assume $Y = [Y'/H]$, where Y' is an affine scheme endowed with an action of a finite group H. Similarly, we may assume $X = [X'/G]$, where X' is an affine scheme endowed with an action of a finite group G. Up to changing X' and G, we may further assume that $f = [f'/\gamma]$, for $(f, \gamma) : (X', G) \to (Y', H)$, by [Zheng 2009, Proposition 5.1]. In this case f' can be decomposed into G-equivariant morphisms $X' \xrightarrow{i} Z' \xrightarrow{p} Y'$ where i is a closed immersion and p is an affine space. Thus $f^* \simeq [i/\mathrm{id}]^*[p/\gamma]^*$ preserves $K_{\iota,\sigma}$.

The assertions for the other operations follow immediately: $f^! = D_X f^* D_Y$, $- \otimes - = \Delta_X^*(- \boxtimes -)$, $\mathscr{H}om(-, -) = D(- \otimes D-)$. $\square$

5. Variant: horizontal complexes

In this section, let k be a field finitely generated over its prime field. This includes, notably, the case of a number field. Many results in previous sections over finite fields can be generalized to Annette Huber's horizontal complexes [1997], as extended by Sophie Morel [2012], over k. In Section 5.1, after briefly reviewing horizontal complexes, we discuss symmetry and decomposition of pure horizontal complexes and prove analogues of results of Section 3.2. In Section 5.2, we discuss symmetry in Grothendieck groups of horizontal complexes and give analogues of results of Section 4. This section stems from a suggestion of Takeshi Saito.

5.1. *Symmetry and decomposition of pure horizontal complexes.* Let X be a Deligne–Mumford stack of finite presentation over k. Huber [1997] (see also [Morel 2012]) defines a triangulated category $D_h^b(X, \bar{\mathbb{Q}}_\ell)$ of horizontal complexes. For a finite extension Λ of $\mathbb{Z}_\ell$, $D_h^b(X, \Lambda)$ is the 2-colimit of the categories $D_c^b(X_R, \Lambda)$,

indexed by triples (R, X_R, u), where $R \subseteq k$ is a subring of finite type over $\mathbb{Z}[1/\ell]$ such that $k = \mathrm{Frac}(R)$, X_R is a Deligne–Mumford stack of finite presentation over $\mathrm{Spec}(R)$, and $u : X \to X_R \otimes_R k$ is an isomorphism. We may restrict to R regular and X_R flat over $\mathrm{Spec}(R)$. We have Grothendieck's six operations on $\mathrm{D}_h^b(X, \Lambda)$.

The triangulated category $\mathrm{D}_h^b(X, \bar{\mathbb{Q}}_\ell)$ is equipped with a canonical t-structure and a perverse t-structure. We let $\mathrm{Sh}_h(X, \bar{\mathbb{Q}}_\ell)$ and $\mathrm{Perv}_h(X, \bar{\mathbb{Q}}_\ell)$ denote the respective hearts. The pullback functors via $X \to X_R$ induce a conservative functor $\eta^* : \mathrm{D}_h^b(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell)$ t-exact for the canonical t-structures and the perverse t-structures, and compatible with the six operations. Moreover, η^* induces *fully faithful* exact functors $\mathrm{Sh}_h(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{Sh}(X, \bar{\mathbb{Q}}_\ell)$ and $\mathrm{Perv}_h(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{Perv}(X, \bar{\mathbb{Q}}_\ell)$ [Morel 2012, Propositions 2.3 and 2.5]. Every object of $\mathrm{Perv}_h(X, \bar{\mathbb{Q}}_\ell)$ has finite length.

Remark 5.1.1. The functor $\eta^* : \mathrm{Perv}_h(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{Perv}(X, \bar{\mathbb{Q}}_\ell)$ preserves indecomposable objects. By the description of simple objects, the functor also preserves simple objects. Thus, via the functor, $\mathrm{Perv}_h(X, \bar{\mathbb{Q}}_\ell)$ can be identified with a full subcategory of $\mathrm{Perv}(X, \bar{\mathbb{Q}}_\ell)$ stable under subquotients. The subcategory is *not* stable under extensions in general.

By restricting to closed points of $\mathrm{Spec}(R[1/\ell])$, we get a theory of weights for horizontal complexes. Weight filtration does not always exist, but this will not be a problem for us. The analogue of Remark 3.2.7 for the preservation of pure complexes holds. Moreover, the analogues of [Beilinson et al. 1982, Théorèmes 5.3.8 and 5.4.5] hold for the decomposition of the pullbacks of pure horizontal complexes to $\bar{k}$. In other words, the functor

$$\bar{\eta}^* : \mathrm{D}_h^b(X, \bar{\mathbb{Q}}_\ell) \xrightarrow{\eta^*} \mathrm{D}_c^b(X, \bar{\mathbb{Q}}_\ell) \to \mathrm{D}_c^b(X_{\bar{k}}, \bar{\mathbb{Q}}_\ell)$$

obtained by composing η^* with the pullback functor carries pure complexes to admissible semisimple complexes (Definition 3.3.1). Indeed, both theorems follow from [Beilinson et al. 1982, Proposition 5.1.15(iii)], which has the following analogue, despite the fact that the analogue of [Beilinson et al. 1982, Proposition 5.1.15(ii)] does not hold in general.

Proposition 5.1.2. *Let* $K, L \in \mathrm{D}_h^b(X, \bar{\mathbb{Q}}_\ell)$, *with* K *mixed of weights* $\leq w$ *and* L *mixed of weights* $\geq w$. *Then* $\mathrm{Ext}^i(\bar{\eta}^* K, \bar{\eta}^* L)^{\mathrm{Gal}(\bar{k}/k)} = 0$ *for* $i > 0$. *In particular, the map* $\mathrm{Ext}^i(\eta^* K, \eta^* L) \to \mathrm{Ext}^i(\bar{\eta}^* K, \bar{\eta}^* L)$ *is zero.*

Proof. The second assertion follows from the first one, as the map factors through $E^i := \mathrm{Ext}^i(\bar{\eta}^* K, \bar{\eta}^* L)^{\mathrm{Gal}(\bar{k}/k)}$. For the first assertion, consider the horizontal complex $\mathscr{E} = \mathrm{R}a_{X*}\mathrm{R}\mathscr{H}om(K, L)$ on $\mathrm{Spec}(k)$, which has weight ≥ 0. Therefore, $E^i \simeq \Gamma(\mathrm{Spec}(k), \mathscr{H}^i \mathscr{E}) = 0$ for $i > 0$. $\qquad \square$

As pure horizontal perverse sheaves are geometrically semisimple, Lemma 2.2.8 on the support decomposition applies (see [Beilinson et al. 1982, Corollaire 5.3.11]).

The general preservation properties of σ-self-dual complexes listed in Remark 2.1.4 still hold for D_h^b. The two-out-of-three property (Proposition 2.2.1) holds for σ-self-dual horizontal perverse sheaves. The trichotomy for indecomposable horizontal perverse sheaves (Proposition 2.2.3) also holds.

We say that a horizontal complex of $\bar{\mathbb{Q}}_\ell$-sheaves A is *split* if it is a direct sum of shifts of horizontal perverse sheaves, or, in other words, if $A \simeq \bigoplus_i ({}^p\mathcal{H}^i A)[-i]$. Definition 3.2.2 can be repeated as follows.

Definition 5.1.3 ($D_{h,\sigma}^w$). Let $w \in \mathbb{Z}$. We denote by $D_{h,\sigma}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{Ob}(D_h^b(X, \bar{\mathbb{Q}}_\ell))$ (resp. $D_{h,\mathrm{sd}}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{Ob}(D_c^b(X, \bar{\mathbb{Q}}_\ell))$) the subset consisting of split pure horizontal complexes A of weight w such that ${}^p\mathcal{H}^i A$ is $(-1)^{w+i}\sigma$-self-dual (resp. self-dual) with respect to $K_X(-w-i)$ for all i. We denote by $D_{h,\mathrm{d}}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq \mathrm{Ob}(D_h^b(X, \bar{\mathbb{Q}}_\ell) \times D_h^b(X, \bar{\mathbb{Q}}_\ell))$ the subset consisting of pairs (A, B) of split pure horizontal complexes of weight w such that ${}^p\mathcal{H}^i A$ is isomorphic to $(D_X \,{}^p\mathcal{H}^i B)(-w-i)$ for all i.

The analogue of Remark 3.2.8 holds for the preservation of $D_{h,\sigma}^w$ and $D_{h,\mathrm{d}}^w$. The two-out-of-three property, an analogue of Remark 3.2.9, also holds for $D_{h,\sigma}^w$ and $D_{h,\mathrm{d}}^w$. We have the following analogue of Proposition 3.2.14, which holds with the same proof as before, and a similar result for $D_{h,\mathrm{d}}^w$.

Proposition 5.1.4. *Let $m \geq 0$. Let A be a mixed horizontal complex on X such that, for all $n \in \mathbb{Z}$, ${}^p\mathcal{H}^n A$ admits a weight filtration W, and such that $\mathrm{gr}_w^W \,{}^p\mathcal{H}^n A$ is $(-1)^w\sigma$-self-dual with respect to $K_X(-w)$ for all $w \in \mathbb{Z}$. Then, for all $n \in \mathbb{Z}$, ${}^p\mathcal{H}^n(A^{\boxtimes m})$ admits a weight filtration W, and $\mathrm{gr}_w^W \,{}^p\mathcal{H}^n(A^{\boxtimes m})$ is $(-1)^w\sigma^m$-self-dual with respect to $K_{[X^m/\mathfrak{S}_m]}(-mw)$ for all $w \in \mathbb{Z}$. Moreover, the functor $(-)^{\boxtimes m}$ carries $D_{h,\sigma}^w(X, \bar{\mathbb{Q}}_\ell)$ to $D_{h,\sigma^m}^{mw}([X^m/\mathfrak{S}_m], \bar{\mathbb{Q}}_\ell)$.*

We have the following analogues of Theorem 3.2.3 and Corollary 3.2.5, which hold with the same proofs as before.

Theorem 5.1.5. *Let $f : X \to Y$ be a proper morphism of Deligne–Mumford stacks of finite presentation over k. Assume that Y has finite inertia. Then Rf_* preserves $D_{h,\sigma}^w$ and $D_{h,\mathrm{d}}^w$.*

Corollary 5.1.6. *Assume that Y has finite inertia. Then Rf_* preserves split pure complexes of weight w.*

The analogue of Corollary 3.2.4 also holds for $D_{h,\mathrm{sd}}^b$.

Theorem 1.8 is a special case of Theorem 5.1.5. Applying it to a_X, we obtain Theorem 1.1. Indeed, as we remarked in the Introduction, in Theorem 1.1 we may assume that k is finitely generated over its prime field. The horizontal perverse sheaf IC_X, pure of weight d, is $(-1)^d$-self-dual with respect to $K_X(-d)$ by Example 2.1.6, so $\mathrm{IC}_X[-d] \in D_{h,1}^0$, hence $Ra_{X*}\,\mathrm{IC}_X[-d] \in D_{h,1}^0$ by Theorem 1.8, which proves Theorem 1.1.

5.2. *Symmetry in Grothendieck groups of horizontal complexes.* We let X be a Deligne–Mumford stack of finite presentation over k, and we let $K_h(X, \bar{\mathbb{Q}}_\ell)$ denote the Grothendieck group of $D_h^b(X, \bar{\mathbb{Q}}_\ell)$, which is a free abelian group generated by the isomorphism classes of simple horizontal perverse $\bar{\mathbb{Q}}_\ell$-sheaves. The functor η^* induces an injection $K_h(X, \bar{\mathbb{Q}}_\ell) \to K(X, \bar{\mathbb{Q}}_\ell)$, which identifies $K_h(X, \bar{\mathbb{Q}}_\ell)$ with a λ-subring of $K(X, \bar{\mathbb{Q}}_\ell)$. The operations on Grothendieck groups in Construction 4.1.1 and Remark 4.1.2 induce operations on K_h.

For $w \in \mathbb{Z}$, we let $K_h^w(X, \bar{\mathbb{Q}}_\ell) \subseteq K_h(X, \bar{\mathbb{Q}}_\ell)$ denote the subgroup generated by pure horizontal perverse sheaves of weight w on X, and we let $K_h^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell) = \bigoplus_{w \in \mathbb{Z}} K_h^w(X, \bar{\mathbb{Q}}_\ell) \subseteq K_h(X, \bar{\mathbb{Q}}_\ell)$. The analogue of Lemma 4.1.8 holds, which further justifies the definition of the map $f_{!*}$ in Remark 4.1.2.

We repeat Definition 4.2.1 as follows.

Definition 5.2.1 ($K_{h,\sigma}$). We let $K_{h,\sigma}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq K_h^w(X, \bar{\mathbb{Q}}_\ell)$ (resp. $K_{h,\mathrm{sd}}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq K_h^w(X, \bar{\mathbb{Q}}_\ell)$), for $w \in \mathbb{Z}$, be the subgroup generated by $[B]$, for B perverse, ι-pure of weight w, and $(-1)^w \sigma$-self-dual (resp. self-dual) with respect to $K_X(-w)$. We set

$$K_{h,\sigma}(X, \bar{\mathbb{Q}}_\ell) = \bigoplus_{w \in \mathbb{Z}} K_{h,\sigma}^w(X, \bar{\mathbb{Q}}_\ell) \quad \left(\text{resp. } K_{\iota,\mathrm{sd}}(X, \bar{\mathbb{Q}}_\ell) = \bigoplus_{w \in \mathbb{Z}} K_{h,\mathrm{sd}}^w(X, \bar{\mathbb{Q}}_\ell) \right).$$

We define the *twisted dualizing map*

$$\bar{D}_{h,X} : K_h^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell) \to K_h^{\mathbb{Z}}(X, \bar{\mathbb{Q}}_\ell)$$

to be the direct sum of the group automorphisms $\bar{D}_{h,X}^w : K_h^w(X, \bar{\mathbb{Q}}_\ell) \to K_h^w(X, \bar{\mathbb{Q}}_\ell)$ sending $[A]$ to $[(D_X A)(-w)]$. We let $K_{h,\mathrm{d}}^w(X, \bar{\mathbb{Q}}_\ell) \subseteq K_h^w(X, \bar{\mathbb{Q}}_\ell)^2$ denote the graph of $\bar{D}_{h,X}^w$ and set

$$K_{h,\mathrm{d}}(X, \bar{\mathbb{Q}}_\ell) = \bigoplus_{n \in \mathbb{Z}} K_{h,\mathrm{d}}^w(X, \bar{\mathbb{Q}}_\ell).$$

The subgroup $K_{\mathrm{orth}}(X, \bar{\mathbb{Q}}_\ell)$ in the Introduction is $K_{h,1}(X, \bar{\mathbb{Q}}_\ell)$. If k is a finite field, $K_{h,\sigma}(X, \bar{\mathbb{Q}}_\ell)$ is the intersection $\bigcap_\iota K_{\iota,\sigma}(X, \bar{\mathbb{Q}}_\ell)$ of the subgroups $K_{\iota,\sigma}$ of Definition 4.2.1, where ι runs over embeddings $\bar{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$.

The analogue of Remark 4.2.3 holds for the definition of $K_{h,\sigma}$, $K_{h,\mathrm{sd}}$, and $K_{h,\mathrm{d}}$. The analogues of Remarks 4.2.6 and 4.2.7 hold for the preservation and Zariski local nature of $K_{h,\sigma}$ and $K_{h,\mathrm{d}}$ with the same proofs.

The following analogue of Theorem 4.2.5 holds with the same proof. In particular, the analogue of Proposition 4.3.1 holds.

Theorem 5.2.2. *Let X and Y be Deligne–Mumford stacks of finite inertia and finite presentation over k and let $f : X \to Y$ be a morphism. Then Grothendieck's six*

operations induce maps

$$- \otimes -, \mathscr{H}om(-,-) : K_{h,\sigma}(X, \bar{\mathbb{Q}}_\ell) \times K_{h,\sigma'}(X, \bar{\mathbb{Q}}_\ell) \to K_{h,\sigma\sigma'}(X, \bar{\mathbb{Q}}_\ell),$$

$$f^*, f^! : K_{h,\sigma}(Y, \bar{\mathbb{Q}}_\ell) \to K_{h,\sigma}(X, \bar{\mathbb{Q}}_\ell),$$

$$f_*, f_! : K_{h,\sigma}(X, \bar{\mathbb{Q}}_\ell) \to K_{h,\sigma}(Y, \bar{\mathbb{Q}}_\ell).$$

Moreover, *Grothendieck's six operations on* $K_h^{\mathbb{Z}}$ *commute with the twisted dualizing map* $\bar{D}_h$.

The analogues of Corollaries 4.2.8 and 4.2.9 hold. The relationship with Laumon's theorem (Remark 4.2.13) also holds.

Theorem 1.9 is a special case of Theorem 5.2.2.

Appendix: Symmetry and duality in categories

In the appendix, we collect some general symmetry properties in categories with additional structures. The tensor product equips the derived category of ℓ-adic sheaves with a symmetric structure. We discuss symmetry of pairings in symmetric categories in Section A.1. The category of perverse sheaves is not stable under tensor product, but is equipped with a duality functor. We study symmetry in categories with duality in Sections A.2 and A.3. We discuss the relation of the two points of view in Section A.4. We then study the effects of translation on symmetry in Section A.5; these results are applied in the main text to the Lefschetz pairing. In Section A.6, we study symmetry of primitive parts under a nilpotent operator; these results are applied in the main text to the monodromy operator. The results of the appendix are formal but are used in the main text. The presentation here is influenced by [Quebbemann et al. 1979], [Riou 2014, Section 12], and [Schlichting 2010]. Recall that $\sigma, \sigma' \in \{\pm 1\}$.

A.1. *Symmetric categories.* In this subsection, we discuss symmetry of pairings in symmetric categories.

Definition A.1.1 (symmetric category). A *symmetric category* is a category $\mathscr{C}$ endowed with a bifunctor $- \otimes - : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$ and a natural isomorphism (called the *symmetry constraint*) $c_{AB} : A \otimes B \to B \otimes A$, for objects A and B of $\mathscr{C}$, satisfying $c_{AB}^{-1} = c_{BA}$. We say that the symmetric category $\mathscr{C}$ is *closed* if for every object A of $\mathscr{D}$, the functor $- \otimes A : \mathscr{C} \to \mathscr{C}$ admits a right adjoint, which we denote by $\mathscr{H}om(A, -)$.

In our applications, we mostly encounter symmetric *monoidal* categories (see, for example, [Mac Lane 1998, Section VII.7] for the definition), but the associativity and unital constraints are mostly irrelevant to the results of this article.

To deal with signs, we need the following additive variant of Definition A.1.1.

Definition A.1.2. A *symmetric additive category* is a symmetric category $(\mathscr{D}, \otimes)$ such that $\mathscr{D}$ is an additive category and $-\otimes- : \mathscr{D} \times \mathscr{D} \to \mathscr{D}$ is an additive bifunctor (namely, a bifunctor additive in each variable). A *closed symmetric additive category* is a closed symmetric category $(\mathscr{D}, \otimes)$ such that $\mathscr{D}$ is an additive category.

A closed symmetric additive category is necessarily a symmetric additive category and the internal Hom functor $\mathscr{Hom}(-, -) : \mathscr{D}^{\mathrm{op}} \times \mathscr{D} \to \mathscr{D}$ is an additive bifunctor.

Definition A.1.3. Let $(\mathscr{C}, \otimes, c)$ be a symmetric category. Assume that $\mathscr{C}$ is an additive category if $\sigma = -1$. Let A, B, K be objects of $\mathscr{C}$.

(1) We define the *transpose* of a pairing $g : B \otimes A \to K$ to be the composite

$$g^T : A \otimes B \xrightarrow{c} B \otimes A \xrightarrow{g} K.$$

We call σg^T the *σ-transpose* of g.

(2) We say that a pairing $f : A \otimes A \to K$ is *σ-symmetric* if $f = \sigma f^T$.

We have $(g^T)^T = g$. We will often say "symmetric" instead of "1-symmetric".

Note that, for a pair of pairings $f : A \otimes B \to K$ and $g : B \otimes A \to K$ in a symmetric additive category, $(2f, 2g)$ is a sum of a pair of 1-transposes and a pair of -1-transposes:

$$(2f, 2g) = (f + g^T, g + f^T) + (f - g^T, g - f^T).$$

Remark A.1.4. Let $(\mathscr{C}, \otimes, c)$ be a symmetric category such that $\mathscr{C}$ is an additive category. Then $(\mathscr{C}, \otimes, -c)$ is another symmetric category. The -1-transpose in $(\mathscr{C}, \otimes, c)$ of a pairing $g : A \otimes B \to K$ is the transpose in $(\mathscr{C}, \otimes, -c)$ of g.

Next we consider effects of functors on symmetry.

Definition A.1.5. Let $\mathscr{C}$ and $\mathscr{D}$ be symmetric categories. A *right-lax symmetric functor* (resp. *symmetric functor*) from $\mathscr{C}$ to $\mathscr{D}$ is a functor $G : \mathscr{C} \to \mathscr{D}$ endowed with a natural transformation (resp. natural isomorphism) of functors $\mathscr{C} \times \mathscr{C} \to \mathscr{D}$ given by morphisms $G(A) \otimes G(B) \to G(A \otimes B)$ in $\mathscr{D}$ for objects A, B of $\mathscr{C}$, such that the following diagram commutes:

$$
\begin{array}{ccc}
G(A) \otimes G(B) & \longrightarrow & G(A \otimes B) \\
{\scriptstyle c_{GA,GB}} \downarrow & & \downarrow {\scriptstyle G(c_{A,B})} \\
G(B) \otimes G(A) & \longrightarrow & G(B \otimes A)
\end{array}
$$

Between symmetric monoidal categories, one has the notions of symmetric monoidal functors and lax symmetric monoidal functors, which are compatible with the associativity constraints and unital constraints. In our applications we will need to consider symmetric functors between symmetric monoidal categories that are *not* symmetric monoidal functors. For example, if f is an open immersion,

then $f_!$ is a symmetric functor compatible with the associativity constraint, but not compatible with the unital constraints except in trivial cases. Again we emphasize that the compatibility with the associativity and unital constraints is irrelevant to the results in this article.

Example A.1.6. Let $\mathscr{C}$ and $\mathscr{D}$ be symmetric categories. Let $F : \mathscr{C} \to \mathscr{D}$ be a functor admitting a right adjoint $G : \mathscr{D} \to \mathscr{C}$. Then every symmetric structure on F induces a right-lax symmetric structure on G, given by the morphism $G(A) \otimes G(B) \to G(A \otimes B)$ adjoint to

$$F(G(A) \otimes G(B)) \xrightarrow{\sim} F(G(A)) \otimes F(G(B)) \to A \otimes B.$$

This construction extends to *left-lax* symmetric structures on F and provides a bijection between left-lax symmetric structures on F and right-lax symmetric structures on G. Since we do not need this extension, we omit the details.

Example A.1.7. Let $\mathscr{C}$ be a symmetric *monoidal* category. Then $\mathscr{C} \times \mathscr{C}$ is a symmetric monoidal category and the functor $- \otimes - : \mathscr{C} \times \mathscr{C} \to \mathscr{C}$ is a symmetric monoidal functor and, in particular, a symmetric functor. The symmetric structure of the functor is given by the isomorphisms $(A \otimes A') \otimes (B \otimes B') \xrightarrow{\sim} (A \otimes B) \otimes (A' \otimes B')$ for objects A, A', B, B' of $\mathscr{C}$.

Construction A.1.8. Let $\mathscr{C}$ and $\mathscr{D}$ be symmetric categories and let $G : \mathscr{C} \to \mathscr{D}$ be a right-lax symmetric functor. Let A, B, K be objects of $\mathscr{C}$. A pairing $A \otimes B \to K$ induces a pairing $G(A) \otimes G(B) \to G(A \otimes B) \to G(K)$.

The following lemma follows immediately from the definitions.

Lemma A.1.9. *Let $\mathscr{C}$ and $\mathscr{D}$ be symmetric categories and let $G : \mathscr{C} \to \mathscr{D}$ be a right-lax symmetric functor. Let A, B, K be objects of $\mathscr{C}$. Let $A \otimes B \to K$ and $B \otimes A \to K$ be transposes of each other. Then the induced pairings $GA \otimes GB \to GK$ and $GB \otimes GA \to GK$ are transposes of each other.*

A.2. *Categories with duality.* In this subsection, we study symmetry in categories with duality.

Definition A.2.1 (duality). Let $\mathscr{C}$ be a category. A *duality* on $\mathscr{C}$ is a functor $D : \mathscr{D}^{\mathrm{op}} \to \mathscr{D}$ endowed with a natural transformation $\mathrm{ev} : \mathrm{id}_{\mathscr{C}} \to DD$ such that the composite $D \xrightarrow{\mathrm{ev}D} DDD \xrightarrow{D\mathrm{ev}} D$ is isomorphic to id_D. The duality (D, ev) is said to be *strong* if ev is a natural isomorphism.

We are mostly interested in strong dualities in the main text. However, for the proofs of many results on strong dualities, it is necessary to consider general dualities (for example, the duality $D_{\mathrm{R}f_*K_X}$ in the proof of Remark 2.1.4(3) is not strong in general). Our terminology here is consistent with [Schlichting 2010, Definition 3.1]. Some authors refer to a strong duality simply as "duality" [Quebbemann et al. 1979].

The underlying functor of a strong duality is an equivalence of categories. If $\mathscr{C}$ is an additive category, we say that a duality on $\mathscr{C}$ is *additive* if the underlying functor is additive. By an *additive category with duality*, we mean an additive category equipped with an additive duality.

A basic example of duality is provided by the internal Hom functor in a closed symmetric category. We will discuss this in detail in Section A.4. By analogy with this case, we sometimes refer to morphisms $B \to DA$ in a category with duality as *forms*. We have the following notion of symmetry for forms.

Definition A.2.2 (symmetry of forms). Let $(\mathscr{C}, D, \mathrm{ev})$ be a category with duality for $\sigma = 1$ (resp. additive category with duality for $\sigma = -1$) and let A, B be objects of $\mathscr{D}$.

(1) We define the *transpose* of a morphism $g : B \to DA$ to be the composite
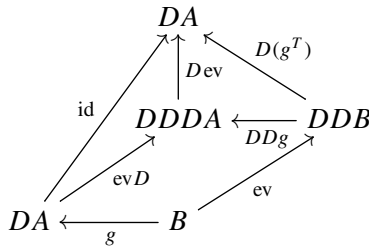
$$A \xrightarrow{\ \mathrm{ev}\ } DDA \xrightarrow{\ Dg\ } DB.$$

  We call σg^T the *σ-transpose* of g.

(2) We say that a morphism $f : A \to DA$ is *σ-symmetric* if $f = \sigma f^T$.

Again we will often say "symmetric" instead of "1-symmetric". The terminology above is justified by the following lemma.

Lemma A.2.3. *We have $(g^T)^T = g$. The map $\mathrm{Hom}_{\mathscr{C}}(B, DA) \to \mathrm{Hom}_{\mathscr{C}}(A, DB)$ carrying g to g^T is a bijection.*

Proof. The first assertion follows from the commutativity of the diagram

For the second assertion, note that the map carrying $h : A \to DB$ to h^T is the inverse of the map $g \mapsto g^T$, by the first assertion. □

Remark A.2.4. If $(\mathscr{C}, D, \mathrm{ev})$ is an additive category with duality, then $(\mathscr{C}, D, -\mathrm{ev})$ is another additive category with duality. The -1-transpose in $(\mathscr{C}, D, \mathrm{ev})$ of a morphism $g : B \to DA$ is the transpose in $(\mathscr{C}, D, -\mathrm{ev})$ of g. This allows us in the sequel to omit the -1-symmetric case in many results without loss of generality.

We will be especially interested in objects A that admit isomorphisms $A \xrightarrow{\sim} DA$.

Definition A.2.5. Let $(\mathscr{C}, D, \mathrm{ev})$ be a category with duality and A an object of $\mathscr{C}$.

(1) We say that A is *self-dual* if there exists an isomorphism $A \xrightarrow{\sim} DA$.

(2) Assume that $(\mathscr{C}, D, \mathrm{ev})$ is an additive category with duality if $\sigma = -1$. We say that A is σ-*self-dual* if there exists a σ-symmetric isomorphism $A \xrightarrow{\sim} DA$.

We warn the reader that being 1-self-dual is more restrictive than being self-dual. If A is 1-self-dual or -1-self-dual, then $\mathrm{ev} : A \to DDA$ is an isomorphism.

Remark A.2.6. Let $(\mathscr{C}, D, \mathrm{ev})$ be an additive category with duality.

(1) The classes of self-dual objects and σ-self-dual objects of $\mathscr{D}$ are stable under finite products.

(2) If A is an object of $\mathscr{D}$ such that $\mathrm{ev} : A \to DDA$ is an isomorphism, then $A \oplus DA$ is 1-self-dual and -1-self-dual. In fact, the isomorphism $A \oplus DA \xrightarrow{\sigma \, \mathrm{ev} \oplus \mathrm{id}} DDA \oplus DA \simeq D(A \oplus DA)$ is σ-symmetric.

(3) Some self-dual objects are neither 1-self-dual nor -1-self-dual (Corollary 2.2.6).

We close this subsection with a couple of lemmas on σ-self-dual objects. They are used in Section 2.2 but not in the rest of this appendix.

A σ-symmetric isomorphism $f : A \xrightarrow{\sim} DA$ induces an involution on $\mathrm{End}(A)$ carrying $g \in \mathrm{End}(A)$ to $f^{-1}(Dg)f$. If $\mathscr{C}$ is a k-linear category and D is a k-linear functor, then the involution is k-linear.

Lemma A.2.7. *Let* $(\mathscr{C}, D, \mathrm{ev})$ *be an additive category with duality. Let A be an object of $\mathscr{D}$ such that $R = \mathrm{End}(A)$ is a local ring and 2 is invertible in R.*

(1) *If A is self-dual with respect to D, then A is 1-self-dual or -1-self-dual with respect to D.*

(2) *If A is both 1-self-dual and -1-self-dual with respect to D, then every symmetric (resp. -1-symmetric) isomorphism $f : A \to DA$ induces a nontrivial involution on the residue division ring of R.*

This is essentially [Quebbemann et al. 1979, Proposition 2.5]. We recall the proof in our notation. It will be apparent from the proof that the additional assumption in [Quebbemann et al. 1979] that D is a strong duality is not used.

Proof. (1) Since $A \simeq DA$, we have $\mathrm{End}(A) \simeq \mathrm{Hom}(A, DA)$. The image $M \subseteq \mathrm{Hom}(A, DA)$ of the maximal ideal of $R = \mathrm{End}(A)$ is the complement of the set of isomorphisms. For any $f \in \mathrm{Hom}(A, DA)$, we have $2f = (f + f^T) + (f - f^T)$, where $f + f^T$ is symmetric and $f - f^T$ is -1-symmetric. If f is an isomorphism, then $2f$ is an isomorphism, so that either $f + f^T$ or $f - f^T$ is an isomorphism.

(2) Let $g : A \to DA$ be a -1-symmetric (resp. symmetric) isomorphism. Then $h = f^{-1}g$ is a unit of R whose image under the involution induced by f is $-h$. Thus the involution is nontrivial on the residue field of R. $\square$

Remark A.2.8. (1) If $\mathscr{C}$ is an abelian category and A is an indecomposable object of finite length, then $\mathrm{End}(A)$ is a local ring [Atiyah 1956, Lemma 7].

(2) Let k be a separably closed field of characteristic $\neq 2$. Assume that $\mathscr{C}$ is a k-linear category, D is a k-linear functor, and $R = \text{End}(A)$ is a finite k-algebra. Then any k-linear involution on R is trivial on the residue field. It follows then from Lemma A.2.7 that exactly one of the following holds: A is 1-self-dual; A is -1-self-dual; A is not self-dual.

Lemma A.2.9. *Let (D, ev) be a **strong** duality on an abelian category $\mathscr{C}$. Let A be a σ-self-dual object of finite length. Then the semisimplification A^{ss} of A is σ-self-dual.*

Note that by assumption D is an equivalence of categories, hence an exact functor.

Proof. We fix a σ-symmetric isomorphism $f : A \to DA$. For any subobject N of A, we let $N^\perp$ denote the kernel of the morphism $A \xrightarrow{f} DA \to DN$. Then we have $A/N^\perp \simeq DN$, so that $N^{\text{ss}} \oplus (A/N^\perp)^{\text{ss}}$ is σ-self-dual by Remark A.2.6. If N is totally isotropic, namely $N \subseteq N^\perp$, then f induces a σ-symmetric isomorphism $N^\perp/N \xrightarrow{\sim} D(N^\perp/N)$ (see [Quebbemann et al. 1979, Lemma 5.2]). Now let N be a maximal totally isotropic subobject of A. By [Quebbemann et al. 1979, Theorem 6.12], $N^\perp/N$ is semisimple. Therefore, $A^{\text{ss}} \simeq N^{\text{ss}} \oplus (A/N^\perp)^{\text{ss}} \oplus N^\perp/N$ is σ-self-dual. $\square$

A.3. *Duality and functors.*

In this subsection, we study symmetry of functors between categories with duality.

Given categories with duality $(\mathscr{C}, D_{\mathscr{C}}, \text{ev})$ and $(\mathscr{D}, D_{\mathscr{D}}, \text{ev})$, and functors $F, G : \mathscr{C} \to \mathscr{D}$, we sometimes refer to natural transformations $GD_{\mathscr{C}} \to D_{\mathscr{D}}F$ as *form transformations*. If $\mathscr{C}$ is the category with one object $*$ and one morphism id, and if we identify functors $\{*\} \to \mathscr{D}$ with objects of $\mathscr{D}$, then a form transformation is simply a form in $\mathscr{D}$. Form transformations are composed as follows.

Construction A.3.1. Let $(\mathscr{B}, D_{\mathscr{B}}, \text{ev})$, $(\mathscr{C}, D_{\mathscr{C}}, \text{ev})$, and $(\mathscr{D}, D_{\mathscr{D}}, \text{ev})$ be categories with duality. Let $F, G : \mathscr{C} \to \mathscr{D}$ and $F', G' : \mathscr{B} \to \mathscr{C}$ be functors. Let $\alpha : FD_{\mathscr{C}} \to D_{\mathscr{D}}G$ and $\alpha' : F'D_{\mathscr{B}} \to D_{\mathscr{C}}G'$ be natural transformations. We define the *composite* of α and α' to be

$$\alpha\alpha' : FF'D_{\mathscr{B}} \xrightarrow{F\alpha'} FD_{\mathscr{C}}G' \xrightarrow{\alpha G'} D_{\mathscr{D}}GG'.$$

As the name suggests, form transformations act on forms. This can be seen as the case $\mathscr{B} = \{*\}$ of the preceding construction, as follows.

Construction A.3.2. Let $(\mathscr{C}, D_{\mathscr{C}}, \text{ev})$ and $(\mathscr{D}, D_{\mathscr{D}}, \text{ev})$ be categories with duality. Let $F, G : \mathscr{C} \to \mathscr{D}$ be functors and let $\alpha : FD_{\mathscr{C}} \to D_{\mathscr{D}}G$ be a natural transformation. Let A, B be objects of $\mathscr{C}$ and let $f : A \to D_{\mathscr{C}}B$ be a morphism in $\mathscr{C}$. The action of α on f is the composite

$$\alpha f : FA \xrightarrow{Ff} FD_{\mathscr{C}}B \xrightarrow{\alpha_B} D_{\mathscr{D}}GB.$$

We have the following notion of symmetry for form transformations.

Definition A.3.3 (symmetry of form transformations). Let $(\mathscr{C}, D_\mathscr{C}, \mathrm{ev})$, $(\mathscr{D}, D_\mathscr{D}, \mathrm{ev})$ be categories with duality. Let $F, G : \mathscr{C} \to \mathscr{D}$ be functors. Assume that $(\mathscr{D}, D_\mathscr{D}, \mathrm{ev})$ is an additive category with duality if $\sigma = -1$.

(1) We define the *transpose* of a natural transformation $\beta : GD_\mathscr{C} \to D_\mathscr{D}F$ to be the composite

$$\beta^T : FD_\mathscr{C} \xrightarrow{\mathrm{ev}FD_\mathscr{C}} D_\mathscr{D}D_\mathscr{D}FD_\mathscr{C} \xrightarrow{D_\mathscr{D}\beta D_\mathscr{C}} D_\mathscr{D}GD_\mathscr{C}D_\mathscr{C} \xrightarrow{D_\mathscr{D}G\mathrm{ev}} D_\mathscr{D}G.$$

We call $\sigma\beta^T$ the σ-transpose of β.

(2) We say that a natural transformation $\alpha : FD_\mathscr{C} \to D_\mathscr{D}F$ is *σ-symmetric* if $\alpha = \sigma\alpha^T$.

Again we will often say "symmetric" instead of "1-symmetric". The terminology above is justified by the following easy lemma.

Lemma A.3.4. *We have $(\beta^T)^T = \beta$. The map* $\mathrm{Nat}(GD_\mathscr{C}, D_\mathscr{D}F) \to \mathrm{Nat}(FD_\mathscr{C}, D_\mathscr{D}G)$ *carrying β to β^T is a bijection.*

The transpose $\alpha = \beta^T$ is uniquely characterized by the commutativity of the diagram

$$
\begin{array}{ccc}
F & \xrightarrow{F\mathrm{ev}} & FD_\mathscr{C}D_\mathscr{C} \\
{\scriptstyle \mathrm{ev}F}\downarrow & & \downarrow{\scriptstyle \alpha D_\mathscr{C}} \\
D_\mathscr{D}D_\mathscr{D}F & \xrightarrow{D_\mathscr{D}\beta} & D_\mathscr{D}GD_\mathscr{C}
\end{array}
\tag{A-3-1}
$$

If $\mathscr{C} = \{*\}$, Definition A.3.3 reduces to Definition A.2.2.

Remark A.3.5. A more direct analogue of Definition A.2.2(1) for functors is as follows. Let $\mathscr{C}$ be a category and let $(\mathscr{D}, D_\mathscr{D}, \mathrm{ev})$ be a category with duality. Let $G : \mathscr{C} \to \mathscr{D}$ and $H : \mathscr{C} \to \mathscr{D}^{\mathrm{op}}$ be functors. Then the map $\mathrm{Nat}(G, D_\mathscr{D}H) \to \mathrm{Nat}(H, D_\mathscr{D}G)$ carrying $\gamma : G \to D_\mathscr{D}H$ to $\gamma^* : H \xrightarrow{\mathrm{ev}H} D_\mathscr{D}D_\mathscr{D}H \xrightarrow{D_\mathscr{D}\gamma} D_\mathscr{D}G$ is a bijection. Indeed, γ is a collection $(\gamma_A : GA \to D_\mathscr{D}HA)_A$ of forms in $\mathscr{D}$ and γ^* is characterized by $(\gamma^*)_A = (\gamma_A)^T$ for all objects A of $\mathscr{C}$, so that $(\gamma^*)^* = \gamma$. As one of the referee points out, this operation does not lead to a notion of symmetry, since G and H do not have the same variance.

Remark A.3.6. In the situation of Definition A.3.3, we have a bijection

$$\mathrm{Nat}(GD_\mathscr{C}, D_\mathscr{D}F) \xrightarrow{\sim} \mathrm{Nat}(F, D_\mathscr{D}GD_\mathscr{C}) \tag{A-3-2}$$

carrying β to β^*. Note that β^* is the composite $F \xrightarrow{F\mathrm{ev}} FD_\mathscr{C}D_\mathscr{C} \xrightarrow{\beta^T D_\mathscr{C}} D_\mathscr{D}GD_\mathscr{C}$, and β^T is the composite $FD_\mathscr{C} \xrightarrow{\beta^* D_\mathscr{C}} D_\mathscr{D}GD_\mathscr{C}D_\mathscr{C} \xrightarrow{D_\mathscr{D}G\mathrm{ev}} D_\mathscr{D}G$.

If we equip the functor category $\mathrm{Fun}(\mathscr{C}, \mathscr{D})$ with the duality carrying G to $D_\mathscr{D}GD_\mathscr{C}$ and the evaluation transformation given by $G \xrightarrow{\mathrm{ev}G\mathrm{ev}} D_\mathscr{D}D_\mathscr{D}GD_\mathscr{C}D_\mathscr{C}$, then natural transformations $F \to D_\mathscr{D}GD_\mathscr{C}$ are forms in this category with duality, and

Definition A.3.3 of transposes of forms applies. Definition A.3.3 is compatible with Definition A.2.2 via the bijection (A-3-2) in the sense that we have $(\beta^*)^T = (\beta^T)^*$.

Composition of form transformations is compatible with transposition.

Lemma A.3.7. *Let* $(\mathcal{B}, D_\mathcal{B}, \mathrm{ev})$, $(\mathcal{C}, D_\mathcal{C}, \mathrm{ev})$, $(\mathcal{D}, D_\mathcal{D}, \mathrm{ev})$ *be categories with duality. Let* $F, G : \mathcal{C} \to \mathcal{D}$ *and* $F', G' : \mathcal{B} \to \mathcal{C}$ *be functors. Let* $\alpha : FD_\mathcal{C} \to D_\mathcal{D}G$ *and* $\alpha' : F'D_\mathcal{B} \to D_\mathcal{C}G'$ *be natural transformations and let* $\alpha\alpha' : FF'D_\mathcal{B} \to D_\mathcal{D}GG'$ *be the composite. Then* $(\alpha\alpha')^T = \alpha^T\alpha'^T$.

Proof. In the diagram

all inner cells commute. It follows that the outer hexagon commutes. □

Taking $\mathcal{B} = \{*\}$, we obtain the following compatibility of transposition with the action of form transformations.

Lemma A.3.8. *Let* $(\mathcal{C}, D_\mathcal{C}, \mathrm{ev})$ *and* $(\mathcal{D}, D_\mathcal{D}, \mathrm{ev})$ *be categories with duality. Let* $F, G : \mathcal{C} \to \mathcal{D}$ *be functors equipped with a natural transformation* $\alpha : FD_\mathcal{C} \to D_\mathcal{D}G$. *Let* $f : A \to D_\mathcal{C}B$ *be a morphism in* $\mathcal{C}$. *Then* $(\alpha f)^T = \alpha^T f^T$.

The following consequence of Lemma A.3.8 is used many times in Section 2.

Lemma A.3.9. *Let* $(\mathcal{C}, D_\mathcal{C}, \mathrm{ev})$ *and* $(\mathcal{D}, D_\mathcal{D}, \mathrm{ev})$ *be categories with duality, and let* $F : \mathcal{C} \to \mathcal{D}$ *be a functor endowed with a symmetric natural* **isomorphism** $\alpha : FD_\mathcal{C} \xrightarrow{\sim} D_\mathcal{D}F$.

(1) *F carries 1-self-dual objects of $\mathcal{C}$ to 1-self-dual objects of $\mathcal{D}$.*

(2) *If F is fully faithful, then the converse holds: any object A of $\mathcal{C}$ such that FA is 1-self-dual is 1-self-dual.*

Proof. For (1), let $f : A \xrightarrow{\sim} D_\mathcal{C}A$ be a symmetric isomorphism. By Lemma A.3.8, αf is symmetric. The assertion follows from the fact that αf is an isomorphism. For (2), let $g : FA \xrightarrow{\sim} D_\mathcal{D}FA$ be a symmetric isomorphism. Since F is fully faithful, there exists a unique morphism $f : A \to D_\mathcal{C}A$ such that $\alpha f = g$. Note that f is an isomorphism. Since $\alpha f^T = g$, we have $f^T = f$. □

The following lemma is used in Section 2.1 to show the symmetry of the middle extension functor.

Lemma A.3.10. *Let* $(\mathscr{C}, D_{\mathscr{C}}, \mathrm{ev})$ *and* $(\mathscr{D}, D_{\mathscr{D}}, \mathrm{ev})$ *be categories with duality. Assume that* $\mathscr{D}$ *is an abelian category and that* $D_{\mathscr{D}}$ *carries epimorphisms in* $\mathscr{D}$ *to monomorphisms. Let* $E, G : \mathscr{C} \to \mathscr{D}$ *be functors endowed with natural transformations* $\alpha : E \to G$ *and* $\beta : GD_{\mathscr{C}} \to D_{\mathscr{D}}E$ *such that the composite* $ED_{\mathscr{C}} \xrightarrow{\alpha D_{\mathscr{C}}} GD_{\mathscr{C}} \xrightarrow{\beta} D_{\mathscr{D}}E$ *is symmetric and such that the image functor* $F : \mathscr{C} \to \mathscr{D}$ *of* α *fits into a commutative diagram*

$$
\begin{array}{ccc}
FD_{\mathscr{C}} & \xrightarrow{\ \gamma\ } & D_{\mathscr{D}}F \\
\downarrow & & \downarrow \\
GD_{\mathscr{C}} & \xrightarrow{\ \beta\ } & D_{\mathscr{D}}E
\end{array}
$$

Then the natural transformation $\gamma : FD_{\mathscr{C}} \to D_{\mathscr{D}}F$ *is symmetric.*

Proof. In fact, in the diagram

the outer square commutes by the symmetry of $\beta\alpha$ and all inner cells except the inner square commute. It follows that the inner square commutes. □

We conclude this subsection with another example of form transformation, which will be used to handle the sign of the Lefschetz pairing (see Lemma A.5.11). We refer to [Kashiwara and Schapira 2006, Remark 10.1.10(ii)] for the convention on distinguished triangles in the opposite category of a triangulated category.

Lemma A.3.11. *Let* $\mathscr{D}$ *be a triangulated category equipped with a t-structure P. Let* $(D, \mathrm{ev}) : \mathscr{D}^{\mathrm{op}} \to \mathscr{D}$ *be a duality on the underlying category of* $\mathscr{D}$*. Assume that D underlies a **right t-exact** triangulated functor. We consider* $\tau = {}^{P}\tau^{\geq a}$ *and* $\tau' = {}^{P}\tau^{\leq -a}$ *as functors* $\mathscr{D} \to \mathscr{D}$*. Then the form transformations* $\tau D \to D\tau'$ *and* $\tau'D \to D\tau$ *induced by the diagrams*

$$
\tau D \to \tau D\tau' \xleftarrow{\ \sim\ } D\tau', \tag{A-3-3}
$$

$$
\tau'D \xleftarrow{\ \sim\ } \tau'D\tau \to D\tau \tag{A-3-4}
$$

are transposes of each other.

The second arrow in (A-3-3) is an isomorphism by the assumption that D carries $^P\tau^{\leq -a}$ to $^P\tau^{\geq -a}$. To see that the first arrow in (A-3-4) is an isomorphism, consider, for any object A of $\mathscr{D}$, the distinguished triangle

$$D^P\tau^{\geq a} A \xrightarrow{f} DA \to D^P\tau^{\leq a-1} A \to .$$

By assumption, $D^P\tau^{\leq a-1} A$ is in $^P\mathscr{D}^{\geq 1-a}$. Thus, by Lemma 4.1.9, $^P\tau^{\leq -a} f$ is an isomorphism.

Proof. The commutativity of (A-3-1) follows from the commutativity of the diagram
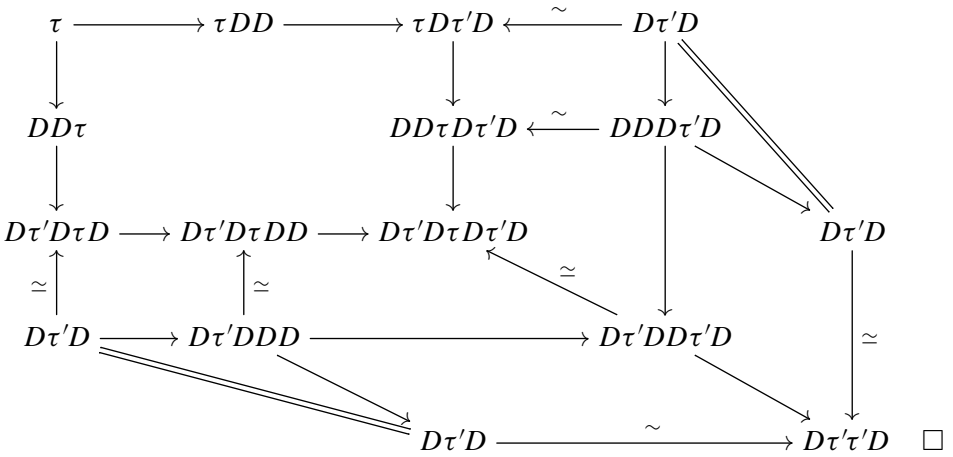
Remark A.3.12. For any truncation functor $\tau = {}^P\tau^{[a,b]}$ with dual truncation functor $\tau' = {}^P\tau^{[-b,-a]}$, combining the two form transformations in the lemma, we obtain a form transformation $\gamma_\tau : \tau D \to D\tau'$ whose transpose is γ'_τ. The form transformation γ_τ is an isomorphism if D is *t-exact*.

A.4. *Duality in closed symmetric categories.* In this subsection, we study dualities given by internal Hom functors in closed symmetric categories. Let $(\mathscr{C}, \otimes, c)$ be a closed symmetric category (Definition A.1.1).

Construction A.4.1. Let K be an object of $\mathscr{C}$, and let D_K denote the functor $\mathscr{H}om(-, K) : \mathscr{D}^{\mathrm{op}} \to \mathscr{D}$. For an object A, the composite

$$A \otimes D_K A \xrightarrow{c} D_K A \otimes A \xrightarrow{\mathrm{adj}} K,$$

where adj denotes the adjunction morphism, corresponds by adjunction to a morphism $A \to D_K D_K A$. This defines a natural transformation $\mathrm{ev} : \mathrm{id}_\mathscr{D} \to D_K D_K$, which makes D_K a duality on $\mathscr{D}$. The latter follows by adjunction from the commutativity

of the diagram

$$
\begin{array}{ccc}
D_K A \otimes D_K D_K A & \xrightarrow{\ c\ } & D_K D_K A \otimes D_K A \\
{\scriptstyle \mathrm{id}\,\otimes\mathrm{ev}}\big\uparrow & & \big\uparrow{\scriptstyle \mathrm{ev}\otimes\mathrm{id}} \\
D_K A \otimes A & \xrightarrow{\ c\ } & A \otimes D_K A
\end{array}
$$

with diagonal morphisms adj to K.

We defined transposes of pairings in symmetric categories (Definition A.2.2) and in categories with duality (Definition A.1.3). The two definitions are compatible via the above construction, by the following lemma.

Lemma A.4.2. *Let A, B, K be objects of $\mathscr{C}$, and set $D = D_K$. Then the following diagram commutes*:

$$
\begin{array}{ccc}
\mathrm{Hom}(B \otimes A, K) & \xrightarrow{\ -\circ c\ } & \mathrm{Hom}(A \otimes B, K) \\
{\scriptstyle \simeq}\big\downarrow & & \big\downarrow{\scriptstyle \simeq} \\
\mathrm{Hom}(B, DA) \xrightarrow{\ D\ } \mathrm{Hom}(DDA, DB) & \xrightarrow{-\circ\mathrm{ev}(A)} & \mathrm{Hom}(A, DB)
\end{array}
$$

Proof. Let $f \in \mathrm{Hom}(B, DA)$. The two images of f in $\mathrm{Hom}(A \otimes B, K)$ are the two composite morphisms in the commutative diagram

$$
\begin{array}{ccc}
A \otimes B & \xrightarrow{\ c\ } & B \otimes A \\
{\scriptstyle \mathrm{id}\,\otimes f}\big\downarrow & & \big\downarrow{\scriptstyle f\otimes\mathrm{id}} \\
A \otimes DA & \xrightarrow{\ c\ } DA \otimes A & \xrightarrow{\ \mathrm{adj}\ } K
\end{array}
\qquad \square
$$

Following Definition A.2.5, we say A is *self-dual* with respect to K if $A \simeq D_K A$. We say A is *σ-self-dual* with respect to K if there exists a σ-symmetric isomorphism $A \xrightarrow{\sim} D_K A$, or, in other words, if there exists a σ-symmetric pairing $A \otimes A \to K$ that is *perfect* in the sense that it induces an isomorphism $A \xrightarrow{\sim} D_K A$.

Definition A.4.3. A *dualizing object* of $\mathscr{C}$ is an object K of $\mathscr{C}$ such that the evaluation transformation $\mathrm{ev} : \mathrm{id}_{\mathscr{C}} \to D_K D_K$ is a natural isomorphism, or, in other words, such that (D_K, ev) is a strong duality.

Remark A.4.4. Let $\mathscr{B}$ be a closed symmetric *monoidal* category and let K be an object of $\mathscr{B}$. The associativity constraint induces an isomorphism $\mathscr{H}om(A, D_K B) \simeq D_K(A \otimes B)$ for objects A, B of $\mathscr{D}$. In particular, if K is a dualizing object, then $\mathscr{H}om(A, B) \simeq \mathscr{H}om(A, D_K D_K B) \simeq D_K(A \otimes D_K B)$.

We close this subsection by constructing two symmetric form transformations.

Construction A.4.5. For a morphism $f : K \to L$ of $\mathscr{C}$, the natural transformation $D_f : \mathrm{id}_{\mathscr{C}}\, D_K \to D_L\, \mathrm{id}_{\mathscr{C}}$ is symmetric. This follows from the commutativity of the diagram

$$
\begin{array}{ccccc}
A \otimes D_K A & \xrightarrow{\;c\;} & D_K A \otimes A & \xrightarrow{\;\mathrm{adj}\;} & K \\
{\scriptstyle \mathrm{id}\,\otimes D_f}\big\downarrow & & {\scriptstyle D_f\otimes\mathrm{id}}\big\downarrow & & \big\downarrow{\scriptstyle f} \\
A \otimes D_L A & \xrightarrow{\;c\;} & D_L A \otimes A & \xrightarrow{\;\mathrm{adj}\;} & L
\end{array}
$$

The action of D_f on forms (Construction A.3.2) carries $A \otimes B \to K$ to the composite $A \otimes B \to K \xrightarrow{f} L$.

Construction A.4.6. Let $\mathscr{C}$ and $\mathscr{D}$ be closed symmetric categories and let $G : \mathscr{C} \to \mathscr{D}$ be a right-lax symmetric functor (Definition A.1.5). For objects A, K of $\mathscr{C}$, consider the morphism

$$
G\mathscr{H}om(A, K) \xrightarrow{\;\mathrm{adj}\;} \mathscr{H}om(GA, G\mathscr{H}om(A, K) \otimes GA)
$$
$$
\to \mathscr{H}om(GA, G(\mathscr{H}om(A, K) \otimes A)) \xrightarrow{\;\mathrm{adj}\;} \mathscr{H}om(GA, GK).
$$

This induces a symmetric natural transformation $G D_K \to D_{GK} G$ (see [Riou 2014, Théorème 12.2.5]), whose action on forms carries $A \otimes B \to K$ to the pairing $GA \otimes GB \to GK$ of Construction A.1.8.

A.5. *Symmetry and translation.* The derived category of ℓ-adic sheaves is equipped with a shift functor $A \mapsto A[1]$ and the Tate twist functor $A \mapsto A(1)$. In this subsection, we study the effects of such translation functors on symmetry. Lemma A.5.11 is used in the main text to handle the symmetry of the Lefschetz pairing.

Recall that a *category with translation* [Kashiwara and Schapira 2006, Definition 10.1.1(i)] is a category $\mathscr{D}$ equipped with an equivalence of categories $T : \mathscr{D} \to \mathscr{D}$. We let $T^{-1} : \mathscr{D} \to \mathscr{D}$ denote a quasi-inverse of T. For an integer n, we will often write $[n]$ for T^n. Recall that a *functor of categories of translation* [Kashiwara and Schapira 2006, Definition 10.1.1(ii)] $(\mathscr{D}, T) \to (\mathscr{D}', T')$ is a functor $F : \mathscr{D} \to \mathscr{D}'$ endowed with a natural isomorphism $\eta : FT \xrightarrow{\sim} T'F$. Recall that a *morphism of functors of categories with translation* $(F, \eta) \to (G, \xi)$ is a natural transformation $\alpha : F \to G$ of functors such that the following diagram commutes:

$$
\begin{array}{ccc}
FT & \xrightarrow[\sim]{\;\eta\;} & T'F \\
{\scriptstyle \alpha T}\big\downarrow & & \big\downarrow{\scriptstyle T'\alpha} \\
GT & \xrightarrow[\sim]{\;\xi\;} & T'G
\end{array}
$$

Our first goal is to define duality on categories with translation, a variant of
Definition A.2.1. We endow $\mathscr{D}^{\mathrm{op}}$ with the translation functor $(T^{\mathrm{op}})^{-1} : \mathscr{D}^{\mathrm{op}} \to \mathscr{D}^{\mathrm{op}}$.
We endow $F^{\mathrm{op}} : \mathscr{A}^{\mathrm{op}} \to \mathscr{A}'^{\mathrm{op}}$ with the isomorphism $F^{\mathrm{op}}(T^{\mathrm{op}})^{-1} \xrightarrow{\sim} (T'^{\mathrm{op}})^{-1} F^{\mathrm{op}}$
induced by

$$\eta^{\mathrm{op}} : T'^{\mathrm{op}} F^{\mathrm{op}} \xrightarrow{\sim} F^{\mathrm{op}} T^{\mathrm{op}}.$$

Definition A.5.1 (duality on a category with translation). Let $(\mathscr{D}, T)$ be a category
with translation. A *duality on* $(\mathscr{D}, T)$ is a functor of categories with translation
$(D, \eta) : (\mathscr{D}^{\mathrm{op}}, (T^{\mathrm{op}})^{-1}) \to (\mathscr{D}, T)$ endowed with a structure of duality on the
underlying functor $D : \mathscr{D}^{\mathrm{op}} \to \mathscr{D}$ such that $\mathrm{ev} : \mathrm{id}_{\mathscr{D}} \to D D^{\mathrm{op}}$ is a morphism of
functors of categories with translation. This means that the diagram

$$
\begin{array}{ccc}
T & \xrightarrow{\ \mathrm{ev}\ } & D D^{\mathrm{op}} T \\
{\scriptstyle \mathrm{ev}} \downarrow & & \downarrow {\scriptstyle D(T^{\mathrm{op}})^{-1} \eta^{\mathrm{op}} T} \\
T D D^{\mathrm{op}} & \xleftarrow{\ \eta D^{\mathrm{op}}\ } & D(T^{\mathrm{op}})^{-1} D^{\mathrm{op}}
\end{array}
$$

commutes. In other words, the isomorphisms $\eta^{-1} : TD \xrightarrow{\sim} D(T^{\mathrm{op}})^{-1}$ and $T^{-1}\eta T^{\mathrm{op}} :$
$T^{-1} D \xrightarrow{\sim} D T^{\mathrm{op}}$ are *transposes* of each other in the sense of Definition A.3.3.

The above definitions have obvious additive variants. An *additive category with
translation* is defined to be a category with translation whose underlying category
is additive. For additive categories with translation $\mathscr{D}$ and $\mathscr{D}'$, a *functor of additive
categories with translation* $\mathscr{D} \to \mathscr{D}'$ is defined to be a functor of categories with
translation whose underlying functor is additive. An *additive duality* on an additive
category with translation is a duality on the category with translation such that the
underlying functor is additive.

As in the case without translation, a basic example of dualities on categories
with translation is provided by closed symmetric categories with translation (see
Construction A.5.9 below). Our next goal is to define symmetric categories with
translation, a variant of Definition A.1.1. Note that in the example of ℓ-adic sheaves,
the shift and twist functors differ in signs with regard to tensor products. To deal
with the two cases simultaneously, we let $\epsilon = \pm 1$. The case $\epsilon = -1$ of the following
definition corresponds to [Kashiwara and Schapira 2006, Definition 10.1.1(v)]. For
a more general notion, see [Verdier 1996, Définition I.1.4.4].

Definition A.5.2. Let $\mathscr{D}$, $\mathscr{D}'$, $\mathscr{D}''$ be additive categories with translation. An
ϵ-*bifunctor of additive categories with translation* $F : \mathscr{D} \times \mathscr{D}' \to \mathscr{D}''$ is an additive
bifunctor endowed with functorial isomorphisms $F(A[1], B) \simeq F(A, B)[1]$ and
$F(A, B[1]) \simeq F(A, B)[1]$ for objects A of $\mathscr{D}$ and B of $\mathscr{D}'$, such that the following

diagram ϵ-commutes:

$$
\begin{array}{ccc}
F(A[1], B[1]) & \xrightarrow{\ \sim\ } & F(A, B[1])[1] \\
\simeq \downarrow & & \downarrow \simeq \\
F(A[1], B)[1] & \xrightarrow{\ \sim\ } & F(A, B)[2]
\end{array}
$$

Therefore, the following diagram ϵ^{mn}-commutes:

$$
\begin{array}{ccc}
F(X[m], Y[n]) & \xrightarrow{\ \sim\ } & F(X, Y[n])[m] \\
\simeq \downarrow & & \downarrow \simeq \\
F(X[m], Y)[n] & \xrightarrow{\ \sim\ } & F(X, Y)[m+n]
\end{array}
$$

Definition A.5.3 (symmetric category with translation). An ϵ-*symmetric additive category with translation* is an additive category with translation $\mathscr{D}$ endowed with a symmetric structure $\otimes$ and a structure of an additive ϵ-bifunctor of categories with translation on $- \otimes - : \mathscr{D} \times \mathscr{D} \to \mathscr{D}$, such that the symmetry constraint, when restricted to each variable, is a morphism of functors of categories with translation $\mathscr{D} \to \mathscr{D}$. We say that an ϵ-symmetric additive category with translation is *closed* if its underlying symmetric category is closed.

For $\epsilon = 1$, Definitions A.5.2 and A.5.3 make sense without assuming that the categories in question are additive.

Example A.5.4. Let $\mathscr{C}$ be a symmetric *monoidal* category and let X be a *dualizable* object of $\mathscr{C}$, that is, there exists an object B of $\mathscr{C}$ such that $A \otimes B \simeq \mathbf{1}$. Then $- \otimes A$ endows $\mathscr{C}$ with the structure of a 1-symmetric category with translation. This applies in particular to the Tate twist functor on the abelian category of perverse $\bar{\mathbb{Q}}_\ell$-sheaves.

Example A.5.5. The derived category of any commutatively ringed topos is a closed -1-symmetric additive category with translation. Similarly, the derived category of $\bar{\mathbb{Q}}_\ell$-sheaves is a closed -1-symmetric additive category with translation.

Let $\mathscr{D}$ be an ϵ-symmetric additive category with translation.

Lemma A.5.6. *The diagram*

$$
\begin{array}{ccccc}
A[m] \otimes B[n] & \xrightarrow{\ \sim\ } & (A \otimes B[n])[m] & \xrightarrow{\ \sim\ } & (A \otimes B)[m+n] \\
c \downarrow \simeq & & & & \simeq \downarrow c[m+n] \\
B[n] \otimes A[m] & \xrightarrow{\ \sim\ } & (B \otimes A[m])[n] & \xrightarrow{\ \sim\ } & (B \otimes A)[m+n]
\end{array}
$$

ϵ^{mn}-*commutes for all objects A, B of $\mathscr{D}$ and all integers m, n. Here c denotes the symmetry constraint.*

Proof. In the diagram

$$A[m] \otimes B[n] \xrightarrow{\ \sim\ } (A \otimes B[n])[m] \xrightarrow{\ \sim\ } (A \otimes B)[m+n]$$

the upper squares commute by functoriality, and the lower triangle ϵ^{mn}-commutes by the definition of ϵ-bifunctor of additive categories with translation. □

Construction A.5.7. Let A, B, K be objects of $\mathscr{D}$. A pairing $A \otimes B \to K$ induces a pairing

$$(A[m]) \otimes (B[n]) \simeq (A \otimes B[n])[m] \simeq (A \otimes B)[m+n] \to K[m+n].$$

Lemma A.5.6 implies the following.

Lemma A.5.8. *Let A, B, K be objects of $\mathscr{D}$. Let $A \otimes B \to K$ and $B \otimes A \to K$ be two pairings that are σ-transposes of each other. Then the induced pairings $(A[m]) \otimes (B[n]) \to K[m+n]$ and $(B[n]) \otimes (A[m]) \to K[m+n]$ are $\epsilon^{mn}\sigma$-transposes of each other.*

Let $\mathscr{D}$ be a *closed ϵ-symmetric* additive category with translation.

Construction A.5.9. Consider the isomorphisms

$$\alpha_n : \mathscr{H}om(A[-n], B) \xrightarrow{\sim} \mathscr{H}om(A, B)[n],$$
$$\beta_n : \mathscr{H}om(A, B[n]) \xrightarrow{\sim} \mathscr{H}om(A, B)[n],$$

given by the isomorphisms

$$\mathrm{Hom}(C, \mathscr{H}om(A[-n], B)) \simeq \mathrm{Hom}(C \otimes A[-n], B) \simeq \mathrm{Hom}((C \otimes A)[-n], B),$$
$$\mathrm{Hom}(C, \mathscr{H}om(A, B[n])) \simeq \mathrm{Hom}(C \otimes A, B[n]) \simeq \mathrm{Hom}((C \otimes A)[-n], B),$$

and

$$\mathrm{Hom}((C \otimes A)[-n], B) \simeq \mathrm{Hom}(C[-n] \otimes A, B)$$
$$\simeq \mathrm{Hom}(C[-n], \mathscr{H}om(A, B)) \simeq \mathrm{Hom}(C, \mathscr{H}om(A, B)[n])$$

for objects A, B, C of $\mathscr{D}$. We have $\alpha_m \alpha_n = \epsilon^{mn} \alpha_{m+n}$, $\beta_m \beta_n = \beta_{mn}$, $\alpha_m \beta_n = \epsilon^{mn} \beta_n \alpha_m$. We endow $\mathscr{H}om(-, -) : \mathscr{D}^{\mathrm{op}} \times \mathscr{D} \to \mathscr{D}$ with the structure of an ϵ-bifunctor of additive categories with translation given by $\epsilon\alpha_1$ and β_1.[3] Let $\tilde{\alpha}_n = (\epsilon\alpha_1)^n = \epsilon^{n(n+1)/2}\alpha_n$.

---

[3]The sign convention is adopted only for concreteness. Our results do not depend on the convention.

In particular, $D_A : \mathscr{D}^{\mathrm{op}} \to \mathscr{D}$ is endowed with the structure of a functor of additive categories with translation, which, together with $\mathrm{ev} : \mathrm{id}_{\mathscr{D}} \to D_A D_A^{\mathrm{op}}$, defines an additive duality on the additive category with translation (see [Calmès and Hornbostel 2009, Proposition 3.2.1]).

Remark A.5.10. Construction A.5.7 corresponds to the construction that sends $f : A \to D_K B$ to $\epsilon^{n(n-1)/2}$ times the morphism

$$A[m] \xrightarrow{f[m]} (D_K B)[m] \xrightarrow[\sim]{\tilde{\alpha}_{-n}} D_K(B[n])[m+n] \xrightarrow{\beta_{m+n}^{-1}} D_{K[m+n]}(B[n]),$$

where $\tilde{\alpha}$ and β are as in Construction A.5.9. In fact, the following diagram $\epsilon^{n(n-1)/2}$-commutes:

$$
\begin{array}{ccc}
\mathrm{Hom}(A[m] \otimes B[n], K[m+n]) \xrightarrow{\sim} \mathrm{Hom}((A \otimes B[n])[m], K[m+n]) & \\
\simeq \downarrow \qquad\qquad\qquad\qquad\qquad\qquad \downarrow \simeq & \\
\mathrm{Hom}(A[m], D_{K[m+n]}(B[n])) \quad \mathrm{Hom}((A \otimes B)[m+n], K[m+n]) \xrightarrow{\sim} \mathrm{Hom}(A \otimes B, K) & \\
\simeq \downarrow \tilde{\alpha}_{-n} \qquad\qquad\qquad\qquad\qquad\qquad\qquad \downarrow \simeq & \\
\mathrm{Hom}(A[m], D_K(B[n])[m+n]) \xrightarrow[\sim]{\beta_{m+n}^{-1}} \mathrm{Hom}(A[m], D_K B[m]) \xrightarrow{\sim} \mathrm{Hom}(A, D_K B) &
\end{array}
$$

Thus, Construction A.5.7 corresponds to the form transformation $\gamma_{m,n} : T^m D_K \xrightarrow{\sim} D_{K[m+n]} T^n$, defined to be $\epsilon^{n(n-1)/2}$ times the isomorphism

$$T^m D_K \xrightarrow[\sim]{\tilde{\alpha}_{-n}} T^{m+n} D_K T^n \xrightarrow[\sim]{\beta_{m+n}^{-1}} D_{K[m+n]} T^n$$

given by Construction A.5.9. By the above, the ϵ^{mn}-transpose of $\gamma_{m,n}$ is $\gamma_{n,m}$.

We combine the above discussion on translation with our previous discussion on truncation into the following lemma, which is applied in the proof of Proposition 3.2.12 to the Lefschetz pairing.

Lemma A.5.11. *Let $\mathscr{D}$ be a closed -1-symmetric additive category with translation. Assume that the underlying category with translation is further equipped with a triangulated structure and a t-structure P. Let K and L be objects of $\mathscr{D}$ such that D_L is a right t-exact triangulated functor. For any σ-symmetric pairing $A \otimes A \to K$ and any morphism $\xi : K[2n] \to L$, the pairing ${}^P\mathrm{H}^n A \otimes {}^P\mathrm{H}^n A \to L$ induced by*

$$A[n] \otimes A[n] \xrightarrow{\sim} (A \otimes A)[2n] \to K[2n] \xrightarrow{\xi} L$$

is $(-1)^n \sigma$-symmetric.

In fact, the form transformation ${}^P\mathrm{H}^n D_K \to D_L {}^P\mathrm{H}^n$ given by

$$\tau^{[0,0]} T^n D_K \xrightarrow{\gamma_{n,n}} \tau^{[0,0]} D_{K[2n]} T^n \xrightarrow{D_\xi} \tau^{[0,0]} D_L T^n \xrightarrow{\gamma_\tau} D_L \tau^{[0,0]} T^n$$

is $(-1)^n$-symmetric. Here $\gamma_{n,n}$ and γ_τ are as in Remarks A.5.10 and A.3.12.

Remark A.5.12. Let us mention in passing that Lurie's theory [2014, Chapter 1] of stable ∞-categories provides a nicer framework for symmetric monoidal structures in derived categories. If $(\mathscr{D}, \otimes)$ is a closed symmetric monoidal ∞-category such that the underlying ∞-category $\mathscr{D}$ is stable, then $-\otimes-$ and $\mathscr{H}om(-,-)$ are automatically exact in each variable and the homotopy category of $\mathscr{D}$ is a closed -1-symmetric additive category with translation.

A.6. *Duality and nilpotence.* In this subsection, we study symmetry of primitive parts under a (twisted) nilpotent operator. We formulate the problem in the language of duality on a category with translation introduced in Definition A.5.1. The main result of this subsection is Proposition A.6.8. This is applied in the main text to the logarithm of the monodromy operator associated to a normal crossing divisor to show that Grothendieck's six operations preserve K_{orth} (see the proof of Proposition 4.3.1).

Let $(\mathscr{A}, T)$ be an additive category with translation. In this subsection, we denote $T^n A$ by $A(n)$ instead of $A[n]$. Our first goal is to define a category of objects with nilpotent operators and record its relation with duality.

Construction A.6.1. Consider the additive category $\mathrm{Nil}(\mathscr{A}, T)$ of pairs (A, N) of an object A of $\mathscr{A}$ and a morphism $N : A(1) \to A$ which is nilpotent in the sense that there exists an integer $d \geq 0$ such that

$$N^d := N \circ N(1) \circ \cdots \circ N(d-1) : A(d) \to A$$

is the zero morphism. A morphism $(A, N) \to (A', N')$ is a morphism $f : A \to A'$ of $\mathscr{A}$ satisfying $N'f(1) = fN$.

There are two ways to identify $\mathrm{Nil}(\mathscr{A}, T)^{\mathrm{op}}$ and $\mathrm{Nil}(\mathscr{A}^{\mathrm{op}}, (T^{\mathrm{op}})^{-1})$, which differ by a sign. We fix $\sigma = \pm 1$ and consider the isomorphism of categories

$$E_{\mathscr{A}} = E_{(\mathscr{A}, T), \sigma} : \mathrm{Nil}(\mathscr{A}, T)^{\mathrm{op}} \to \mathrm{Nil}(\mathscr{A}^{\mathrm{op}}, (T^{\mathrm{op}})^{-1})$$

sending $(A, N : A(1) \to A)$ to $(A, \sigma N(-1) : A \to A(-1))$. The composite

$$\mathrm{Nil}(\mathscr{A}, T) \xrightarrow{E_{\mathscr{A}}^{\mathrm{op}}} \mathrm{Nil}(\mathscr{A}^{\mathrm{op}}, (T^{\mathrm{op}})^{-1})^{\mathrm{op}} \xrightarrow{E_{\mathscr{A}^{\mathrm{op}}}} \mathrm{Nil}(\mathscr{A}, T)$$

equals the identity. The duality we put on $\mathrm{Nil}(\mathscr{A}, T)$ will depend on the choice of σ. In the main text we take $\sigma = -1$.

Let $F : (\mathscr{A}, T) \to (\mathscr{A}', T')$ be a functor of additive categories with translation. Then F induces an additive functor $\mathrm{Nil}_F : \mathrm{Nil}(\mathscr{A}, T) \to \mathrm{Nil}(\mathscr{A}', T')$ carrying $(A, N : TA \to A)$ to $(FA, T'FA \simeq FTA \xrightarrow{FN} FA)$ and $f : (A, N) \to (A', N')$ to Ff. Let $\gamma : F \to F'$ be a morphism of functors of categories with translation. Then γ induces a natural transformation $\mathrm{Nil}_\gamma : \mathrm{Nil}_F \to \mathrm{Nil}_{F'}$, which is a natural isomorphism if γ is an isomorphism.

The following diagrams commute:

$$
\begin{array}{ccc}
\operatorname{Nil}(\mathscr{A}, T)^{\mathrm{op}} & \xrightarrow{\operatorname{Nil}_F^{\mathrm{op}}} & \operatorname{Nil}(\mathscr{A}', T')^{\mathrm{op}} \\
\scriptstyle E_{\mathscr{A}} \big\downarrow & & \big\downarrow \scriptstyle E_{\mathscr{A}'} \\
\operatorname{Nil}(\mathscr{A}^{\mathrm{op}}, (T^{\mathrm{op}})^{-1}) & \xrightarrow{\operatorname{Nil}_{F^{\mathrm{op}}}} & \operatorname{Nil}(\mathscr{A}'^{\mathrm{op}}, (T'^{\mathrm{op}})^{-1})
\end{array}
\qquad
\begin{array}{ccc}
E_{\mathscr{A}'} \operatorname{Nil}_{F'}^{\mathrm{op}} & \xrightarrow{\operatorname{Nil}_\gamma^{\mathrm{op}}} & E_{\mathscr{A}'} \operatorname{Nil}_F^{\mathrm{op}} \\
\big\| & & \big\| \\
\operatorname{Nil}_{F^{\mathrm{op}}} E_{\mathscr{A}'} & \xrightarrow{\operatorname{Nil}_{\gamma^{\mathrm{op}}}} & \operatorname{Nil}_{F^{\mathrm{op}}} E_{\mathscr{A}}.
\end{array}
$$

Construction A.6.2. Let $D : (\mathscr{A}^{\mathrm{op}}, (T^{\mathrm{op}})^{-1}) \to (\mathscr{A}, T)$ be an additive duality on the additive category with translation (see the comment following Definition A.5.1). Consider the functor $D_{\operatorname{Nil}(\mathscr{A}, T)}$, composite of

$$
\operatorname{Nil}(\mathscr{A}, T)^{\mathrm{op}} \xrightarrow[\sim]{E_{\mathscr{A}}} \operatorname{Nil}(\mathscr{A}^{\mathrm{op}}, (T^{\mathrm{op}})^{-1}) \xrightarrow{\operatorname{Nil}_D} \operatorname{Nil}(\mathscr{A}, T),
$$

and the natural transformation

$$
\operatorname{id}_{\operatorname{Nil}(\mathscr{A}, T)} \xrightarrow{\operatorname{Nil}_{\mathrm{ev}}} \operatorname{Nil}_D \operatorname{Nil}_{D^{\mathrm{op}}} = \operatorname{Nil}_D \operatorname{Nil}_{D^{\mathrm{op}}} E_{\mathscr{A}^{\mathrm{op}}} E_{\mathscr{A}}^{\mathrm{op}}
$$
$$
= \operatorname{Nil}_D E_{\mathscr{A}} \operatorname{Nil}_D^{\mathrm{op}} E_{\mathscr{A}}^{\mathrm{op}} = D_{\operatorname{Nil}(\mathscr{A}, T)} D_{\operatorname{Nil}(\mathscr{A}, T)}^{\mathrm{op}}.
$$

These define an additive duality on the additive category $\operatorname{Nil}(\mathscr{A}, T)$, which is strong if D is strong on $\mathscr{A}$.

In the rest of this section, let $(\mathscr{A}, T)$ be an *abelian category with translation*, namely an additive category with translation whose underlying category $\mathscr{A}$ is abelian. Our next goal is to review the decomposition into primitive parts. The following is a variant of [Deligne 1980, Proposition 1.6.1, 1.6.14], with essentially the same proof.

Lemma A.6.3. *Let (A, N) be an object of $\operatorname{Nil}(\mathscr{A}, T)$. Then there exists a unique finite increasing filtration M of A satisfying $N M_j(1) \subseteq M_{j-2}$ and such that N^k induces an isomorphism $\operatorname{gr}_k^M A(k) \xrightarrow{\sim} \operatorname{gr}_{-k}^M A$, for $k \geq 0$.*

Proof. Let $d \geq 0$ be an integer such that $N^{d+1} = 0$. We proceed by induction on d. We have $M_d = A$ and $M_{-d-1} = 0$. For $d > 0$, we have $M_{d-1} = \operatorname{Ker}(N^d)(-d)$ and $M_{-d} = \operatorname{Im}(N^d)$. We have $N^d = 0$ on $\operatorname{Ker}(N^d)(-d) / \operatorname{Im}(N^d)$. Let M' be the corresponding filtration given by the induction hypothesis. Then, for $-d \leq i \leq d-1$, M_i is the inverse image in $\operatorname{Ker}(N^d)(-d)$ of $M_i' \subseteq \operatorname{Ker}(N^d)(-d) / \operatorname{Im}(N^d)$. $\square$

The following is an immediate consequence of the construction of the filtration M.

Lemma A.6.4. *Let $f : (A, N) \to (A', N')$ be a morphism of $\operatorname{Nil}(\mathscr{A}, T)$. Then f is compatible with the corresponding filtrations. More precisely, if M and M' denote the corresponding filtrations, then $f(M_j) \subseteq M_j'$.*

For $i \leq 0$, let $P_i(A, N) = \operatorname{Ker}(N : \operatorname{gr}_i^M A(1) \to \operatorname{gr}_{i-2}^M A)(-1)$. The inclusion $\operatorname{Ker}(N)(-1) \subseteq A$ induces an isomorphism $\operatorname{gr}_i^M(\operatorname{Ker}(N)(-1)) \xrightarrow{\sim} P_i(A, N)$. We

thus obtain functors

$$P_i = P_{i,\mathscr{A}} : \mathrm{Nil}(\mathscr{A}, T) \to \mathscr{A}.$$

For all j, we have

$$\mathrm{gr}_j^M A \simeq \bigoplus_{\substack{k \geq |j| \\ k \equiv j \ (\mathrm{mod}\ 2)}} P_{-k}(A, N)\left(-\tfrac{j+k}{2}\right).$$

We now proceed to define form transformations on the primitive part functors. Let (A, N) be an object of $\mathrm{Nil}(\mathscr{A}, T)$. If $M = M(A, N)$ and $M^* = M(E_{\mathscr{A}}(A, N))$, then we have the following short exact sequence in $\mathscr{A}$:

$$0 \to M_{-j-1} \to A \to M_j^* \to 0.$$

Thus $\mathrm{gr}_{-j}^M A$ can be identified with $\mathrm{gr}_j^{M^*} A$. Moreover, $N^{-i} : \mathrm{gr}_{-i}^M A(-i) \xrightarrow{\sim} \mathrm{gr}_i^M A$ induces an isomorphism in $\mathscr{A}$

$$\alpha_{\mathscr{A}}(A, N) : P_{i,\mathscr{A}^{\mathrm{op}}}(E_{\mathscr{A}}(A, N))(-i) \simeq \mathrm{gr}_{-i}^M(\mathrm{Coker}(N))(-i)$$
$$\xrightarrow{\sim} \mathrm{gr}_i^M(\mathrm{Ker}(N)(-1)) \simeq P_{i,\mathscr{A}}(A, N).$$

This defines a natural isomorphism of functors $\alpha_{\mathscr{A}} : P_{i,\mathscr{A}}^{\mathrm{op}} \xrightarrow{\sim} (T^{\mathrm{op}})^{-i} P_{i,\mathscr{A}^{\mathrm{op}}} E_{\mathscr{A}}$. By definition, we have the following.

Lemma A.6.5. *The isomorphism* $T^{-i} P_{i,\mathscr{A}^{\mathrm{op}}}^{\mathrm{op}} E_{\mathscr{A}}^{\mathrm{op}} \xrightarrow[\sim]{\alpha_{\mathscr{A}^{\mathrm{op}}}} P_{i,\mathscr{A}} E_{\mathscr{A}^{\mathrm{op}}} E_{\mathscr{A}}^{\mathrm{op}} = P_{i,\mathscr{A}}$ *is* $\sigma^i \alpha_{\mathscr{A}}^{\mathrm{op}}$.

Let $(\mathscr{A}, T)$, $(\mathscr{A}', T')$ be abelian categories with translation and let $F : (\mathscr{A}, T) \to (\mathscr{A}', T')$ be a functor of categories with translation such that the underlying functor $\mathscr{A} \to \mathscr{A}'$ is *exact*. Let (A, N) be an object of $(\mathscr{A}, T)$ and let $M = M(A, N)$, $M' = M(\mathrm{Nil}_F(A, N))$. The exactness of F allows us to identify $F(M_j A)$ as a subobject of FA, and under this identification we have $F(M_j A) = M_j'(FA)$. We have an obvious natural isomorphism $\beta_F : P_{i,\mathscr{A}'} \mathrm{Nil}_F \xrightarrow{\sim} F P_{i,\mathscr{A}}$. The following functoriality of β is obvious.

Lemma A.6.6. *Let* $F, F' : (\mathscr{A}, T) \to (\mathscr{A}', T')$ *be functors of categories with translation such that the underlying functors are exact, and let* $\gamma : F \to F'$ *be a morphism of functors of categories with translation. Then the following diagram commutes*:

$$\begin{array}{ccc}
P_{i,\mathscr{A}'} \mathrm{Nil}_F & \xrightarrow[\sim]{\beta_F} & F P_{i,\mathscr{A}} \\
{\scriptstyle \mathrm{Nil}_\gamma} \downarrow & & \downarrow {\scriptstyle \gamma} \\
P_{i,\mathscr{A}'} \mathrm{Nil}_{F'} & \xrightarrow[\sim]{\beta_{F'}} & F' P_{i,\mathscr{A}}
\end{array}$$

By construction, the isomorphisms α and β have the following compatibility.

Lemma A.6.7. *The following diagram commutes*:

$$
\begin{array}{ccccc}
(T'^{\mathrm{op}})^{-i}\, F^{\mathrm{op}}\, P_{i,\mathscr{A}^{\mathrm{op}}}\, E_{\mathscr{A}} & \xleftarrow{\ \sim\ } & F^{\mathrm{op}}(T^{\mathrm{op}})^{-i}\, P_{i,\mathscr{A}^{\mathrm{op}}}\, E_{\mathscr{A}} & \xleftarrow{\ \alpha_{\mathscr{A}}\ }_{\sim} & F^{\mathrm{op}}\, P^{\mathrm{op}}_{i,\mathscr{A}} \\[4pt]
\beta_{F^{\mathrm{op}}}\big\uparrow \simeq & & & & \simeq\big\downarrow \beta^{\mathrm{op}}_{F} \\[4pt]
(T'^{\mathrm{op}})^{-i}\, P_{i,\mathscr{A}'^{\mathrm{op}}}\, \mathrm{Nil}_{F^{\mathrm{op}}}\, E_{\mathscr{A}} & = = & (T'^{\mathrm{op}})^{-i}\, P_{i,\mathscr{A}'^{\mathrm{op}}}\, E_{\mathscr{A}'}\, \mathrm{Nil}^{\mathrm{op}}_{F} & \xleftarrow{\ \alpha_{\mathscr{A}'}\ }_{\sim} & P^{\mathrm{op}}_{\mathscr{A}'}\, \mathrm{Nil}^{\mathrm{op}}_{F}
\end{array}
$$

The following is the main result of this subsection.

Proposition A.6.8. *Let* $(\mathscr{A}, T)$ *be an abelian category with translation and let* $D : (\mathscr{A}^{\mathrm{op}}, (T^{\mathrm{op}})^{-1}) \to (\mathscr{A}, T)$ *be a duality such that the underlying functor* $\mathscr{A}^{\mathrm{op}} \to \mathscr{A}$ *is exact. Then, for* $i \le 0$, *the composite isomorphism*

$$
P_{i,\mathscr{A}}\, D_{\mathrm{Nil}(\mathscr{A},T)} = P_{i,\mathscr{A}}\, \mathrm{Nil}_{D}\, E_{\mathscr{A}} \xrightarrow[\ \sim\ ]{\ \beta_{D}\ } DP_{i,\mathscr{A}^{\mathrm{op}}} E_{\mathscr{A}} \xrightarrow[\ \sim\ ]{\ \alpha_{\mathscr{A}}^{-1}\ } (D(T^{\mathrm{op}})^{i}) P^{\mathrm{op}}_{i,\mathscr{A}}
$$

is σ^{i}-*symmetric*.

Note that $T^{-i}D \simeq D(T^{\mathrm{op}})^{i} : \mathscr{A}^{\mathrm{op}} \to \mathscr{A}$ endowed with the natural transformation $\mathrm{id}_{\mathscr{A}} \xrightarrow{\ \mathrm{ev}\ } DD^{\mathrm{op}} \simeq (D(T^{\mathrm{op}})^{i})(T^{-i}D)^{\mathrm{op}}$ is a duality on $\mathscr{A}$. By the proposition, $P_{i,\mathscr{A}}$ carries σ'-self-dual objects of $\mathrm{Nil}(\mathscr{A}, T)$ to $\sigma^{i}\sigma'$-self-dual objects of $\mathscr{A}$.

Proof. In the diagram

the triangle σ^{i}-commutes by Lemma A.6.5, the upper-left inner cell commutes by Lemma A.6.6, the lower-right inner cell commutes by Lemma A.6.7, and the other inner cells trivially commute. $\qquad\square$

Acknowledgements

References

[Atiyah 1956] M. F. Atiyah, "On the Krull–Schmidt theorem with application to sheaves", *Bull. Soc. Math. France* **84** (1956), 307–317. MR 19,172b Zbl 0072.18101

[Atiyah and Tall 1969] M. F. Atiyah and D. O. Tall, "Group representations, λ-rings and the *J*-homomorphism", *Topology* **8** (1969), 253–297. MR 39 #5702 Zbl 0159.53301

[Beilinson et al. 1982] A. A. Beilinson, J. Bernstein, and P. Deligne, "Faisceaux pervers", pp. 5–171 in *Analyse et topologie sur les espaces singuliers, I* (Luminy, 1981), Astérisque **100**, Société Mathématique de France, Paris, 1982. MR 86g:32015 Zbl 0536.14011

[Bröcker and tom Dieck 1995] T. Bröcker and T. tom Dieck, *Representations of compact Lie groups*, Graduate Texts in Mathematics **98**, Springer, New York, NY, 1995. MR 97i:22005 Zbl 0874.22001

[Calmès and Hornbostel 2009] B. Calmès and J. Hornbostel, "Tensor-triangulated categories and dualities", *Theory Appl. Categ.* **22**:6 (2009), 136–200. MR 2010k:18008 Zbl 1178.18005

[Chevalley 1955] C. Chevalley, *Théorie des groupes de Lie, III: Théorèmes généraux sur les algèbres de Lie*, Actualités Scientifiques et Industrielles **1226**, Hermann, Paris, 1955. MR 16,901a Zbl 0186.33104

[Conrad et al. 2012] B. Conrad, M. Lieblich, and M. Olsson, "Nagata compactification for algebraic spaces", *J. Inst. Math. Jussieu* **11**:4 (2012), 747–814. MR 2979821 Zbl 1255.14003

[Deligne 1968] P. Deligne, "Théorème de Lefschetz et critères de dégénérescence de suites spectrales", *Inst. Hautes Études Sci. Publ. Math.* **35** (1968), 107–126. MR 39 #5582 Zbl 0159.22501

[Deligne 1980] P. Deligne, "La conjecture de Weil, II", *Inst. Hautes Études Sci. Publ. Math.* **52** (1980), 137–252. MR 83c:14017 Zbl 0456.14014

[Deligne 1994] P. Deligne, "Décompositions dans la catégorie dérivée", pp. 115–128 in *Motives* (Seattle, WA, 1991), edited by U. Jannsen et al., Proceedings of Symposia in Pure Mathematics **55**, American Mathematical Society, Providence, RI, 1994. MR 95h:18013 Zbl 0809.18008

[Deligne 2012] P. Deligne, "Finitude de l'extension de ℚ engendrée par des traces de Frobenius, en caractéristique finie", *Mosc. Math. J.* **12**:3 (2012), 497–514. MR 3024820 Zbl 1260.14022

[Drinfeld 2001] V. Drinfeld, "On a conjecture of Kashiwara", *Math. Res. Lett.* **8**:5-6 (2001), 713–728. MR 2003c:14022 Zbl 1079.14509

[Drinfeld 2012] V. Drinfeld, "On a conjecture of Deligne", *Mosc. Math. J.* **12**:3 (2012), 515–542. MR 3024821 Zbl 1271.14028

[Fujiwara 2002] K. Fujiwara, "Independence of *l* for intersection cohomology (after Gabber)", pp. 145–151 in *Algebraic geometry 2000, Azumino* (Nagano, 2000), edited by S. Usui et al., Advanced Studies in Pure Mathematics **36**, Mathematical Society of Japan, Tokyo, 2002. MR 2004c:14038 Zbl 1057.14029

[Gaitsgory 2007] D. Gaitsgory, "On de Jong's conjecture", *Israel J. Math.* **157** (2007), 155–191. MR 2008j:14021 Zbl 1123.11020

[Grothendieck 1958] A. Grothendieck, "La théorie des classes de Chern", *Bull. Soc. Math. France* **86** (1958), 137–154. MR 22 #6818 Zbl 0091.33201

[Grothendieck 1961] A. Grothendieck, "Éléments de géométrie algébrique, II: Étude globale élémentaire de quelques classes de morphismes", *Inst. Hautes Études Sci. Publ. Math.* **8** (1961), 5–222. MR 36 #177b Zbl 0118.36206

[Grothendieck 1977] A. Grothendieck, "Formule de Lefschetz", exposé III, rédigé par L. Illusie, pp. 73–137 in *Séminaire de Géometrie Algébrique du Bois-Marie* (*SGA 5*)*: cohomologie l-adique et fonctions L* (Bures-sur-Yvette, 1965–1966), edited by L. Illusie, Lecture Notes in Mathematics **589**, Springer, Berlin, 1977. MR 58 #10907 Zbl 0355.14004

[Huber 1997] A. Huber, "Mixed perverse sheaves for schemes over number fields", *Compos. Math.* **108**:1 (1997), 107–121. MR 98k:14024 Zbl 0882.14006

[Illusie 1994] L. Illusie, "Autour du théorème de monodromie locale", pp. 9–57 in *Périodes p-adiques* (Bures-sur-Yvette, 1988), edited by J.-M. Fontaine, Astérisque **223**, Société Mathématique de France, Paris, 1994. MR 95k:14032 Zbl 0837.14013

[Illusie and Zheng 2013] L. Illusie and W. Zheng, "Odds and ends on finite group actions and traces", *Int. Math. Res. Not.* **2013**:1 (2013), 1–62. MR 3041694 Zbl 06132684

[de Jong 1996] A. J. de Jong, "Smoothness, semi-stability and alterations", *Inst. Hautes Études Sci. Publ. Math.* **83** (1996), 51–93. MR 98e:14011 Zbl 0916.14005

[de Jong 1997] A. J. de Jong, "Families of curves and alterations", *Ann. Inst. Fourier* (*Grenoble*) **47**:2 (1997), 599–621. MR 98f:14019 Zbl 0868.14012

[Kashiwara and Schapira 2006] M. Kashiwara and P. Schapira, *Categories and sheaves*, Grundlehren der Mathematischen Wissenschaften **332**, Springer, Berlin, 2006. MR 2006k:18001 Zbl 1118.18001

[Katz 2005] N. M. Katz, *Moments, monodromy, and perversity: a Diophantine perspective*, Annals of Mathematics Studies **159**, Princeton University Press, 2005. MR 2006j:14020 Zbl 1079.14025

[Keel and Mori 1997] S. Keel and S. Mori, "Quotients by groupoids", *Ann. of Math.* (2) **145**:1 (1997), 193–213. MR 97m:14014 Zbl 0881.14018

[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**, American Mathematical Society, Providence, RI, 1994. MR 95k:14010 Zbl 0820.14006

[Lafforgue 2002] L. Lafforgue, "Chtoucas de Drinfeld et correspondance de Langlands", *Invent. Math.* **147**:1 (2002), 1–241. MR 2002m:11039 Zbl 1038.11075

[Laumon 1981] G. Laumon, "Comparaison de caractéristiques d'Euler–Poincaré en cohomologie *l*-adique", *C. R. Acad. Sci. Paris Sér. I Math.* **292**:3 (1981), 209–212. MR 82e:14030 Zbl 0468.14005

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

[Laumon and Moret-Bailly 2000] G. Laumon and L. Moret-Bailly, *Champs algébriques*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **39**, Springer, Berlin, 2000. MR 2001f:14006 Zbl 0945.14005

[Lurie 2014] J. Lurie, "Higher algebra", preprint, 2014, available at http://www.math.harvard.edu/~lurie/papers/higheralgebra.pdf.

[Mac Lane 1998] S. Mac Lane, *Categories for the working mathematician*, 2nd ed., Graduate Texts in Mathematics **5**, Springer, New York, NY, 1998. MR 2001j:18001 Zbl 0906.18001

[Morel 2012] S. Morel, "Complexes mixtes sur un schéma de type fini sur ℚ", preprint, 2012, available at http://web.math.princeton.edu/~smorel/sur_Q.pdf.

[Pacheco and Stevenson 2000] A. Pacheco and K. F. Stevenson, "Finite quotients of the algebraic fundamental group of projective curves in positive characteristic", *Pacific J. Math.* **192**:1 (2000), 143–158. MR 2000k:14023 Zbl 0951.14016

[Partsch 2013] H. Partsch, "Deformations of elliptic fiber bundles in positive characteristic", *Nagoya Math. J.* **211** (2013), 79–108. MR 3079280 Zbl 1274.14044

[Quebbemann et al. 1979] H.-G. Quebbemann, W. Scharlau, and M. Schulte, "Quadratic and Hermitian forms in additive and abelian categories", *J. Algebra* **59**:2 (1979), 264–289. MR 82d:18015 Zbl 0412.18016

[Quillen 1971] D. Quillen, "The Adams conjecture", *Topology* **10** (1971), 67–80. MR 43 #5525 Zbl 0219.55013

[Raynaud and Gruson 1971] M. Raynaud and L. Gruson, "Critères de platitude et de projectivité: techniques de «platification» d'un module", *Invent. Math.* **13**:1 (1971), 1–89. MR 46 #7219 Zbl 0227.14010

[Riou 2014] J. Riou, "Dualité", exposé XVII, pp. 351–453 in *Travaux de Gabber sur l'uniformisation locale et la cohomologie étale des schémas quasi-excellents* (Palaiseau, 2006–2008), edited by L. Illusie et al., Astérisque **363-364**, Société Mathématique de France, Paris, 2014. MR 3329787 Zbl 1320.14032

[Saito 1990] M. Saito, "Mixed Hodge modules", *Publ. Res. Inst. Math. Sci.* **26**:2 (1990), 221–333. MR 91m:14014 Zbl 0727.14004

[Schlichting 2010] M. Schlichting, "Hermitian *K*-theory of exact categories", *J. K-Theory* **5**:1 (2010), 105–165. MR 2011b:19007 Zbl 05690542

[Serre 1965] J.-P. Serre, "Zeta and *L* functions", pp. 82–92 in *Arithmetical algebraic geometry* (Purdue, IN, 1963), edited by O. F. G. Schilling, Harper & Row, New York, NY, 1965. MR 33 #2606 Zbl 0171.19602

[Serre 1998] J.-P. Serre, *Représentations linéaires des groupes finis*, 5th ed., Hermann, Paris, 1998. 2nd ed., 1971, translated as *Linear representations of finite groups*, Graduate Texts in Mathematics **42**, Springer, New York, 1977. MR 80f:20001 Zbl 0926.20003

[Suh 2012] J. Suh, "Symmetry and parity in Frobenius action on cohomology", *Compos. Math.* **148**:1 (2012), 295–303. MR 2881317 Zbl 1258.14023

[Sun 2012a] S. Sun, "Decomposition theorem for perverse sheaves on Artin stacks over finite fields", *Duke Math. J.* **161**:12 (2012), 2297–2310. MR 2972459 Zbl 1312.14057

[Sun 2012b] S. Sun, "*L*-series of Artin stacks over finite fields", *Algebra Number Theory* **6**:1 (2012), 47–122. MR 2950161 Zbl 06064705

[Verdier 1996] J.-L. Verdier, *Des catégories dérivées des catégories abéliennes*, edited by G. Maltsiniotis, Astérisque **239**, Société Mathématique de France, Paris, 1996. MR 98c:18007 Zbl 0882.18010

[Vidal 2004] I. Vidal, "Théorie de Brauer et conducteur de Swan", *J. Algebraic Geom.* **13**:2 (2004), 349–391. MR 2005m:14030 Zbl 1070.14020

[Zheng 2005] W. Zheng, "Théorème de Gabber d'indépendance de *l*", Master's thesis, Université Paris-Sud, Orsay, 2005, available at http://159.226.47.28/~zheng/memoire.pdf.

[Zheng 2008] W. Zheng, "Sur la cohomologie des faisceaux *l*-adiques entiers sur les corps locaux", *Bull. Soc. Math. France* **136**:3 (2008), 465–503. MR 2009d:14015 Zbl 1216.14016

[Zheng 2009] W. Zheng, "Sur l'indépendance de *l* en cohomologie *l*-adique sur les corps locaux", *Ann. Sci. Éc. Norm. Supér.* (4) **42**:2 (2009), 291–334. MR 2010i:14032 Zbl 1203.14023

[Zheng 2015a] W. Zheng, "Companions on Artin stacks", preprint, 2015. arXiv 1512.08929

[Zheng 2015b] W. Zheng, "Six operations and Lefschetz–Verdier formula for Deligne–Mumford stacks", *Sci. China Math.* **58**:3 (2015), 565–632. MR 3319927 Zbl 06430227

shsun@math.tsinghua.edu.cn   *Yau Mathematical Sciences Center, Tsinghua University, Jinchunyuan West Building, Beijing, 100084, China*

wzheng@math.ac.cn   *Morningside Center of Mathematics, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Zhongguancun Donglu 55, Beijing, 100190, China*

Generalized Heegner cycles at Eisenstein primes and the Katz *p*-adic *L-function*

Daniel Kriz

We consider normalized newforms $f \in S_k(\Gamma_0(N), \varepsilon_f)$ whose nonconstant term Fourier coefficients are congruent to those of an Eisenstein series modulo some prime ideal above a rational prime p. In this situation, we establish a congruence between the anticyclotomic p-adic L-function of Bertolini, Darmon, and Prasanna and the Katz two-variable p-adic L-function. From this we derive congruences between images under the p-adic Abel–Jacobi map of certain generalized Heegner cycles attached to f and special values of the Katz p-adic L-function.

Our results apply to newforms associated with elliptic curves $E/\mathbb{Q}$ whose mod-p Galois representations $E[p]$ are reducible at a good prime p. As a consequence, we show the following: if K is an imaginary quadratic field satisfying the Heegner hypothesis with respect to E and in which p splits, and if the bad primes of E satisfy certain congruence conditions mod p and p does not divide certain Bernoulli numbers, then the Heegner point $P_E(K)$ is nontorsion, implying, in particular, that $\mathrm{rank}_{\mathbb{Z}} E(K) = 1$. From this we show that if E is semistable with reducible mod-3 Galois representation, then a positive proportion of real quadratic twists of E have rank 1 and a positive proportion of imaginary quadratic twists of E have rank 0.

1. Notation and conventions

Throughout the paper, let us fix the following notational conventions.

For $m, n \in \mathbb{Z}$, let (m, n) denote the greatest common divisor of m and n, and let $\mathrm{lcm}(m, n)$ denote the least common multiple. We let $\ell \parallel N$ indicate that ℓ strictly divides N. We let $\Phi : \mathbb{Z} \to \mathbb{Z}$ denote the Euler totient function. Given an extension of number fields L/K and an integral ideal $\mathfrak{a}$ of $\mathcal{O}_L$, let $\mathrm{Nm}_{L/K} \mathfrak{a}$ denote the relative ideal norm of $\mathfrak{a}$ and let $|\mathfrak{a}|$ denote the smallest positive rational integer in $\mathfrak{a}$. For ideals $\mathfrak{a}, \mathfrak{b}$, we let $(\mathfrak{a}, \mathfrak{b})$ denote the greatest common ideal divisor and $\mathrm{lcm}(\mathfrak{a}, \mathfrak{b})$ the least common ideal multiple. For a place v of a number field, let Frob_v denote the *arithmetic Frobenius* attached to v, i.e., the Frobenius element which is sent to v under the (inverse of the) Artin reciprocity map.

Throughout, we will fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. All number fields in our discussion will be viewed as being embedded in $\overline{\mathbb{Q}}$. For each rational prime p, we will fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and let $\mathbb{C}_p$ denote the topological closure of $\overline{\mathbb{Q}}_p$. We fix an embedding $i_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ as well as an embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ for each p. We also fix field identifications $i : \mathbb{C} \xrightarrow{\sim} \mathbb{C}_p$ for each p. (We will use the same symbol i for all p, as the underlying p will be clear from context.)

Let K denote a general number field. Let $\mathbb{A}_K$ and $\mathbb{A}_K^\times$ denote the adèles and idèles over K, respectively, and let $\mathbb{A}_{K,f}$ and $\mathbb{A}_{K,f}^\times$ denote the finite adèles and idèles, respectively. For a Hecke character $\chi : \mathbb{A}_K^\times \to \mathbb{C}^\times$, let $\mathfrak{f}(\chi) \subset \mathcal{O}_K$ denote the conductor of χ. As usual, if $\mathfrak{a} \subset \mathcal{O}_K$ is an integral ideal with $(\mathfrak{a}, \mathfrak{f}(\chi)) \neq 1$, then we set $\chi(\mathfrak{a}) = 0$.

Given a Dirichlet (i.e., finite order) character ψ over a number field K of conductor $\mathfrak{f} \subset \mathcal{O}_K$, we will identify ψ with its associated finite order Hecke character on idèles, taking the following convention: for $x \in (\mathcal{O}/\mathfrak{f})^\times$,

$$\psi(x \bmod \mathfrak{f}) = \prod_{v \nmid \mathfrak{f}} \psi_v(x) = \prod_{v \mid \mathfrak{f}} \psi_v^{-1}(x),$$

where, in the first product, v runs over all places of E which do not divide $\mathfrak{f}$. When $K = \mathbb{Q}$, we define the Gauss sum of ψ by

$$\mathfrak{g}(\psi) := \sum_{a \in (\mathbb{Z}/\mathfrak{f}\mathbb{Z})^\times} \psi(a) e^{2\pi i (a/|\mathfrak{f}|)}.$$

For a finite prime ℓ, we define the Gauss sum of the local character $\psi_\ell : \mathbb{Q}_\ell^\times \to \mathbb{C}^\times$ similarly: letting $|\mathfrak{f}| = \prod_\ell \ell^{e_\ell}$, we set

$$\mathfrak{g}_\ell(\psi) := \psi_\ell(\ell^{e_\ell}) \sum_{a \in (\mathbb{Z}_\ell/\ell^{e_\ell}\mathbb{Z}_\ell)^\times} \psi_\ell^{-1}(a) e^{2\pi i \{a/\ell^{e_\ell}\}_\ell},$$

where $\{x\}_\ell$ denotes the ℓ-fractional part of $x \in \mathbb{Z}_\ell$. Thus

$$\prod_{\ell \mid \mathfrak{f}} \mathfrak{g}_\ell(\psi) = \mathfrak{g}(\psi) \prod_{\ell \mid \mathfrak{f}} \psi_\ell(|\mathfrak{f}|) = \mathfrak{g}(\psi) \prod_{\ell \nmid \mathfrak{f}} \psi_\ell^{-1}(|\mathfrak{f}|) = \mathfrak{g}(\psi).$$

Let $\mathbb{N}_\mathbb{Q} : \mathbb{A}_\mathbb{Q} \to \mathbb{C}$ denote the adèlic norm, normalized so that $\mathbb{N}_{\mathbb{Q},\infty}$ equals $|\cdot|_\infty$ (the usual archimedean absolute value). Then, for any number field K, let $\mathrm{Nm}_{K/\mathbb{Q}} : \mathbb{A}_K \to \mathbb{A}_\mathbb{Q}$ denote the norm homomorphism (which induces the ideal norm recalled above), and set $\mathbb{N}_K := \mathbb{N}_\mathbb{Q} \circ \mathrm{Nm}_{K/\mathbb{Q}}$. Note that when K is imaginary quadratic, $\mathbb{N}_K : \mathbb{A}_K^\times \to \mathbb{C}^\times$ is an algebraic Hecke character of infinity type $(-1, -1)$. For any Hecke character $\chi : \mathbb{A}_K^\times \to \mathbb{C}^\times$, let

$$\chi_j := \chi \mathbb{N}_K^{-j}.$$

Using the fixed isomorphism $i : \mathbb{C} \xrightarrow{\sim} \mathbb{C}_p$ and the Artin isomorphism, we can view $\mathbb{N}_K^{-1}$ as a character $\mathbb{N}_K^{-1} : \mathrm{Gal}(\bar{K}/K) \to \mathbb{Z}_p^\times$. Then any $x \in \mathbb{Z}_p^\times$ can be uniquely written as $\omega(x) \cdot \langle x \rangle$, where $\omega(x) \in \mu_{2(p-1)}$ and $\langle x \rangle \in 1 + 2p\mathbb{Z}_p$. We then define the *Teichmüller character* $\omega : \mathrm{Gal}(\bar{K}/K) \to \mu_{2(p-1)}$ by $\omega_K(a) := \omega(\mathbb{N}_K^{-1}(a))$. For simplicity, we will let $\omega_\mathbb{Q} = \omega$. Given an extension of number fields K/L and a Hecke character ϕ over L, we will let $\phi_{/K} := \phi \circ \mathrm{Nm}_{K/L}$; note that, viewing ϕ as a character $\mathrm{Gal}(\bar{L}/L) \to \mathbb{C}^\times$, this corresponds to restriction to the subgroup $\mathrm{Gal}(\bar{K}/K)$.

For a quadratic field $K/\mathbb{Q}$ with $K = \mathbb{Q}(\sqrt{D})$, where D is a squarefree integer, we recall that the fundamental discriminant of K is given by

$$D_K = \begin{cases} D & \text{if } D \equiv 1 \pmod 4, \\ 4D & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

For quadratic K, let ε_K be the associated Dirichlet character of conductor D_K; conversely, for a quadratic Dirichlet character χ, let K_χ be the associated imaginary quadratic field. Given two quadratic fields $L = \mathbb{Q}(\sqrt{D})$ and $K = \mathbb{Q}(\sqrt{D'})$, we will let $L \cdot K$ denote the quadratic field $\mathbb{Q}(\sqrt{DD'})$. Unless otherwise noted, all Dirichlet characters over $\mathbb{Q}$ are taken to be *primitive*, and so are uniquely identified with finite order Hecke characters over $\mathbb{Q}$ under the arithmetic normalization described above. Given Dirichlet characters ψ_1, ψ_2 over $\mathbb{Q}$, we define $\psi_1 \psi_2$ to be the *primitive* Dirichlet character equal to $\psi_1(a)\psi_2(a)$ for $a \in \left(\mathbb{Z}/\mathrm{lcm}(\mathfrak{f}(\psi_1), \mathfrak{f}(\psi_2))\right)^\times$ (and indeed this equality holds for the associated Hecke characters). In particular, for quadratic L and K as above, we have $\varepsilon_{L \cdot K} = \varepsilon_L \varepsilon_K$.

Given a normalized newform $f \in S_k(\Gamma_1(N))$, let $a_n(f)$ denote the n-th Fourier coefficient of f (i.e., the n-th coefficient of the q-expansion at ∞); when f is obvious from context, we will often abbreviate $a_n(f)$ to a_n. Moreover, when f is defined over $\mathbb{Q}$ and thus associated with an elliptic curve $E/\mathbb{Q}$, we will sometimes write $a_n(E) = a_n(f)$. Let E_f denote the finite extension of $\mathbb{Q}$ generated by the

Fourier coefficients $a_n(f)$. Given a Hecke character χ, let E_χ denote the finite extension of $\mathbb{Q}$ generated by its values. Set $E_{f,\chi} = E_f E_\chi$.

For $s \in \mathbb{C}$, let $\Re(s)$ and $\Im(s)$ denote the real and imaginary parts of s, respectively. We let $\mathcal{H}^+ := \{s \in \mathbb{C} : \Im(s) > 0\}$.

2. Introduction

The study of Heegner points has provided some of the greatest insights into the Birch and Swinnerton-Dyer conjecture. In particular, given an elliptic curve $E/\mathbb{Q}$ and an imaginary quadratic field K satisfying a suitable *Heegner hypothesis* with respect to E, the nontriviality of the Heegner point $P_E(K) \in E(K) \otimes \mathbb{Q}$ introduced in Section 3.4 implies, via the descent argument of [Kolyvagin 1990], that $\mathrm{rank}_{\mathbb{Z}} E(K) = 1$. Our main result establishes, for elliptic curves E with $E[p]$ a reducible Galois representation at a good prime p, a congruence mod p between the formal logarithm of the Heegner point and a special value of the Katz p-adic L-function with certain Euler factors removed. Using Gross's factorization [1980] of the Katz p-adic L-function on the cyclotomic line, we can then find an explicit congruence between the formal logarithm of the Heegner point and a quantity involving certain Bernoulli numbers and (inverses of) Euler factors at primes of bad reduction. Thus we derive an explicit criterion (involving Bernoulli numbers) for the nontriviality of $P_E(K) \in E(K) \otimes \mathbb{Q}$ in certain families of E.

Our results also have higher-dimensional applications, namely in computing with algebraic cycle classes in Chow groups of motives attached to newforms. Suppose N is a positive integer and K is an imaginary quadratic field satisfying the Heegner hypothesis with respect to N, suppose $f = \sum_{n \geq 1} a_n q^n$ is a weight-$k \geq 2$ level-N normalized newform whose Fourier coefficients are congruent to those of an Eisenstein series outside the constant term modulo some prime ideal above p, and suppose χ is an algebraic Hecke character over K central critical with respect to f. We consider the Rankin–Selberg motive $M_{f,\chi^{-1}} := M_{f/K} \otimes M_{\chi^{-1}}$, defined over K, associated with (f, χ), where M_f is the motive associated with f (see [Scholl 1990]), $M_{f/K}$ is its base change to K, and M_χ is the motive associated with χ (see [Deninger 1990]). For convenience of notation, we will formulate our discussion with respect to

$$M_{(f,\chi^{-1})/F} = M_{f/F} \otimes M_{(\chi^{-1})/F},$$

where F/K is some large enough abelian extension in "situation (S)" as described on page 314, and $f_{/F}$ and $\chi_{/F}$ are the corresponding base extensions to F. In fact, one may recover $M_{\chi^{-1}}$ as a direct factor of the Grothendieck restriction of $M_{(\chi^{-1})/F}$; see [Deninger 1990] or [Geisser 1997]. Indeed, we have a factorization

$$M_{(f,\chi^{-1})/F} = \bigoplus_{\chi_0 : \mathrm{Gal}(F/K) \to \mathbb{C}^\times} M_{f,\chi^{-1}\chi_0}.$$

Under certain conditions guaranteeing that the value of $L(\pi_f \times \pi_{\chi^{-1}}, s) = L(M_{f,\chi^{-1}}, s)$ (and thus also that of $L((\pi_f \times \pi_{\chi^{-1}})_{/F}, s) = L(M_{(f,\chi^{-1})_{/F}}, s))$ will vanish at the central point of the functional equation, we seek to construct algebraic cycle classes in the Chow group associated with $M_{(f,\chi^{-1})_{/F}}$, thus providing evidence for the Beilinson–Bloch conjecture for Chow motives associated with $(f, \chi)_{/F}$. Natural candidates for representatives of such classes are *generalized Heegner cycles* (in the sense of [Bertolini et al. 2013]), generated by algebraic cycles on a suitable *generalized Kuga–Sato variety* which arise from graphs of isogenies between products of CM curves. Under the above hypotheses, our main theorem provides a criterion for a generalized Heegner cycle class associated with (f, χ), with χ in a certain infinity type range, to be nontrivial, namely that an associated special value of the Katz p-adic L-function (with certain Euler factors removed) is not (too) divisible by p. One may thus use special value formulas of p-adic L-functions in order to get explicit p-nondivisibility criteria for the nontriviality of Heegner cycle classes. In our main corollary, we explicitly address the case when Gross's factorization theorem can be applied, which corresponds precisely with the case when the relevant generalized Heegner cycle arises from a *classical* Heegner cycle (see Remark 8).

2.1. Chow motives. To make our discussion more precise, let us briefly recall some definitions pertaining to Chow motives. Let X be a nonsingular variety over a number field F. An *algebraic cycle* of X is a formal sum of subvarieties of X. We let $\mathrm{CH}^j(X)$ denote the group generated by algebraic cycles of X of codimension j modulo rational equivalence. Call $\mathrm{CH}^j(X)$ the *j-th Chow group of X*, and call $\mathrm{CH}(X) := \bigoplus_{0 \le j \le \dim X} \mathrm{CH}^j(X)$ the *Chow group of X*. For varieties X, Y over F, call $\mathrm{Corr}^d(X, Y) := \mathrm{CH}^{\dim Y + d}(X \times_F Y)$ the *group of (degree-d) correspondences from X to Y*. The group $\mathrm{Corr}(X, X) := \bigoplus_{0 \le d \le \dim X} \mathrm{Corr}^d(X, X)$ has a ring structure defined by *composition of correspondences*: given $g \in \mathrm{Corr}^{d_1}(X, Y)$ and $h \in \mathrm{Corr}^{d_2}(Y, Z)$, we define

$$h \circ g := \pi_{13,*}(\pi_{12}^*(g).\pi_{23}^*(h)) \in \mathrm{Corr}^{d_1+d_2}(X, Z),$$

where $\pi_{12}, \pi_{13}, \pi_{23} : X \times_F Y \times_F Z \to X \times_F Y, X \times_F Z, Y \times_F Z$ are the canonical projections, and "." denotes the Chow intersection pairing. We call $\mathrm{Corr}(X, X)$ the *ring of correspondences on X*. For any number field E, let $\mathrm{Corr}^d(X, Y)_E := \mathrm{Corr}^d(X, Y) \otimes_{\mathbb{Z}} E$. A *Chow motive over F with coefficients in E* is a triple (X, e, m) consisting of a nonsingular variety X over F, an idempotent $e \in \mathrm{Corr}^0(X, X)_E$, and an integer m. Define the *category of Chow motives* $\mathcal{M}_{F,E}$ whose objects consist of Chow motives over F with coefficients in E, and with morphisms given by

$$\mathrm{Hom}_{\mathcal{M}_{F,E}}((X, e, m), (Y, f, n)) := f \circ \mathrm{Corr}^{n-m}(X, Y)_{\mathbb{Q}} \circ e.$$

Define the *category of Grothendieck motives* $\mathcal{M}_{F,E}^{\mathrm{hom}}$ with objects being cycles of X modulo (motivic) homological equivalence, and with morphisms defined in the same way as above. Note that since rational equivalence is stronger than homological equivalence, there is a natural functor

$$\mathcal{M}_{F,E} \to \mathcal{M}_{F,E}^{\mathrm{hom}}.$$

Let $\mathrm{CH}^j(X)_0$ denote the subgroup of $\mathrm{CH}^j(X)$ consisting of null-homological cycles.

2.2. The Beilinson–Bloch conjecture for Rankin–Selberg motives. Now let K be an imaginary quadratic field, and let H denote the Hilbert class field over K. Fix $f \in S_k(\Gamma_0(N), \varepsilon_f)$, where $k \geq 2$, and let $r := k-2$. Let χ be a Hecke character over K of infinity type $(r-j, j)$ which is central critical with respect to f, and where $0 \leq j \leq r$. Suppose also that every prime $\ell \mid N$ splits in K, i.e., K satisfies the Heegner hypothesis with respect to N. Then we can choose an ideal $\mathfrak{N}$ of $\mathcal{O}_K$ with $\mathcal{O}_K/\mathfrak{N} = \mathbb{Z}/N$. Assume also that $\mathfrak{f}(\chi) \mid \mathfrak{N}$.

The ambient motive in our setup will be $M := (X_r, \epsilon_X, 0) \in \mathcal{M}_{F, E_{f,\chi}}$, where F, to be fixed later, is some large enough abelian extension of K containing H, and ϵ_X is some projector in the ring of correspondences on X which has induced actions on the various cohomological realizations of M via the corresponding cycle class maps. (The projector ϵ_X essentially picks out the part of the cohomology of X_r which comes from the Galois representations attached to pairs $(f, \chi)_{/F}$.) Here the underlying $((2r+1)$-dimensional) variety is the *generalized Kuga–Sato variety* $X_r := W_r \times A^r$, defined over H, where A is a fixed CM elliptic curve of $\mathcal{O}_K$-type (i.e., with $\mathrm{End}_H(A) = \mathcal{O}_K$) and $W_r := \mathcal{E}^r$ (the *classical Kuga–Sato variety*) is the (canonical desingularization of the) r-fold fiber product of copies of the universal elliptic curve $\mathcal{E}$ with $\Gamma_1(N)$-level structure over the (compactified) modular curve $X_1(N) := \overline{Y_1(N)}$ (and thus is defined over $\mathbb{Q}$). This is well-defined in the case where the cusps of $Y_1(N)$ are *regular* in the sense of [Diamond and Shurman 2005, Section 3.2], which holds in particular when $N > 4$. The fibers of $X_r \to X_1(N)$, outside of the cusps of $X_1(N)$, are of the form $E^r \times A^r$ where E varies over elliptic curves.

The motive M_f is given by the triple $(W_r, \epsilon_f, 0)$ for some projector in the ring of correspondences on W_r which picks out the f-isotypic component of the cohomology of W_r under the Hecke action; in particular, this Chow motive is defined over $\mathbb{Q}$, with coefficients in E_f. For an extension $F/\mathbb{Q}$, we let $M_{f/F}$ denote the base change to F. The definition of the motive $M_{(\chi^{-1})/F}$ is slightly more subtle. Let F/K be an abelian extension such that $\chi_A^{r-j} \bar{\chi}_A^j = \chi_{/F}$, where $\chi_A : \mathbb{A}_F^\times \to K^\times$ is the Hecke character associated with the CM elliptic curve A having infinity type $(1, \ldots, 1, 0, \ldots, 0)$ (with the first $[F:K]$ places corresponding to the embeddings $F \hookrightarrow \overline{\mathbb{Q}}$ preserving our fixed embedding $K \hookrightarrow \overline{\mathbb{Q}}$, and the next $[F:K]$ places to their complex conjugates). We then say F is in "situation (S)".

(Such an F always exists; see [Deninger 1990, Proposition 1.3.1].) We have a motive $M_{(\chi^{-1})/F} := (A^r, \epsilon_{\chi/F}, 0) \in \mathcal{M}_{F, E_\chi}$ for some suitable projector $\epsilon_{\chi/F}$ picking out the $\chi/F = \chi_A^{r-j} \bar{\chi}_A^j$-isotypic component of the cohomology of A^r under the Galois action.

Let $H_\mathfrak{N}$ be the field over which the individual points of $A[\mathfrak{N}]$ are defined. We will henceforth take and fix an abelian extension F/K large enough so that it contains $H_\mathfrak{N}$ and is in situation (S). (Note that this is possible since $H_\mathfrak{N}$ is an abelian extension of K.) The Rankin–Selberg motive

$$M_{(f, \chi^{-1})/F} := M_{f/F} \otimes M_{(\chi^{-1})/F} = (W_r, \epsilon_{f/F}, 0) \otimes (A^r, \epsilon_{\chi/F}, 0) = (X_r, \epsilon_{(f, \chi)/F}, 0)$$

is a submotive of M (in fact, it is the $(f, \chi)_{/F}$-isotypic component $\epsilon_{(f, \chi)/F} M$), and the Beilinson–Bloch conjecture predicts that

$$\begin{aligned}
\dim_{E_{f,\chi}} \epsilon_{(f,\chi)/F} \, \mathrm{CH}^{r+1}(X_r)_{0, E_{f,\chi}}(F) &= \mathrm{ord}_{s=r+1} \, L(H^{2r+1}_{\text{ét}}(M_{(f,\chi^{-1})/F}), s) \\
&= \mathrm{ord}_{s=r+1} \, L(\epsilon_{(f,\chi)/F} H^{2r+1}_{\text{ét}}(M), s) \\
&= \mathrm{ord}_{s=r+1} \, L((V_{f/K} \otimes \chi^{-1})_{/F}(r+1), s) \\
&= \mathrm{ord}_{s=0} \, L((V_{f/K} \otimes \chi^{-1})_{/F}, s) \\
&= \mathrm{ord}_{s=0} \, L(V_{f/K} \otimes \chi^{-1} \otimes \mathrm{Ind}_F^K 1, s) \\
&= \mathrm{ord}_{s=0} \prod_{\substack{\chi_0: \\ \mathrm{Gal}(F/K) \to \mathbb{C}^\times}} L(V_{f/K} \otimes (\chi^{-1}\chi_0), s) \\
&= \mathrm{ord}_{s=\frac{1}{2}} \prod_{\substack{\chi_0: \\ \mathrm{Gal}(F/K) \to \mathbb{C}^\times}} L(\pi_f \times \pi_{\chi^{-1}\chi_0}, s).
\end{aligned}$$

Here $\epsilon_{(f,\chi)/F}$ is the projector corresponding to the $(f, \chi)_{/F}$-isotypic component of the cohomology of X_r under the Hecke and Galois actions, V_f is the 2-dimensional (unique semisimple) $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-representation associated with f, $V_{f/K}$ is its restriction to $\mathrm{Gal}(\bar{K}/K)$, and π_f, $\pi_{\chi^{-1}}$ are the automorphic representations (over K) associated with f and $\theta_{\chi^{-1}}$ under the unitary normalizations.

Under the Heegner hypothesis, we have $L\big(\pi_f \times \pi_{\chi^{-1}}, \frac{1}{2}\big) = 0$, and so the Beilinson–Bloch conjecture predicts that

$$\dim_{E_{f,\chi}} \epsilon_{(f,\chi)/F} \, \mathrm{CH}^{r+1}(X_r)_{0, E_{f,\chi}}(F) \geq 1.$$

Thus we should be able to find a null-homologous cycle class with nonvanishing $\epsilon_{(f,\chi)/F}$-isotypic component in the above Chow group. To this end, we can use the p-adic Waldspurger formula of Bertolini, Darmon, and Prasanna [Bertolini et al. 2013] to consider images under the p-adic Abel–Jacobi map of *generalized Heegner cycles*. Generalized Heegner cycles are, essentially, generated by graphs Γ_φ of isogenies $\varphi : A \to A'$ between CM elliptic curves with $\Gamma_1(N)$-level structure

(i.e., such that $\ker(\varphi) \cap A[\mathfrak{N}] = 0$). We can then view the graph Γ_φ inside X_r:

$$\Gamma_\varphi \subset A^r \times (A')^r \subset A^r \times W_r = X_r.$$

We define the associated *generalized Heegner cycle* associated with (φ, A) as

$$\Delta_\varphi := \epsilon_X \Gamma_\varphi \in \mathrm{CH}^{r+1}(X_r)_{0, E_{f,\chi}}(F).$$

(See Section 3.3 for a precise definition.) It is also a fact that $\epsilon_X H^{2r+2}(X_r, \mathbb{Q}) = 0$, and so Δ_φ is indeed null-homologous. Generalized Heegner cycles are those cycles in $\mathrm{CH}^{r+1}(X_r)_{0, E_{f,\chi}}(F)$ generated by formal $E_{f,\chi}$-linear combinations of Δ_φ for varying φ. The space $\mathrm{CH}(X_r)_{0, E_{f,\chi}}(F)$ has an isotypic decomposition with respect to the action of the Hecke algebra (which is indexed by cuspidal eigenforms) and that of $\mathrm{Gal}(\bar{F}/F)$ (which is indexed by Hecke characters).

Let F_p denote the p-adic completion of F determined by our fixed embedding $i_p : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. We can now apply the p-adic Abel–Jacobi map over F_p to Δ_φ, which is a map

$$\mathrm{AJ}_{F_p} : \mathrm{CH}^{r+1}(X_r)_{0, \mathbb{Q}}(F_p) \to (\mathrm{Fil}^{r+1} \epsilon_X H^{2r+1}_{dR}(X_r/F_p))^\vee$$
$$\cong (S_k(\Gamma_1(N), F_p) \otimes \mathrm{Sym}^r H^1_{dR}(A/F_p))^\vee,$$

where the superscript $\vee$ denotes the F_p-linear dual, and Fil^j denotes the j-th step of the Hodge filtration. A basis of $\epsilon_X H^{2r+1}_{dR}(X_r/F)$ is given by elements of the form $\omega_f \wedge \omega_A^j \eta_A^{r-j}$ for $0 \leq j \leq r$, where

$$\omega_f \in \mathrm{Fil}^{r+1} \epsilon_X H^{r+1}_{dR}(W_r/F) \cong S_k(\Gamma_1(N), F)$$

is associated with $f \in S_k(\Gamma_1(N), F)$, and the $\omega_A^j \eta_A^{r-j}$ form a basis of

$$\mathrm{Fil}^{r+1} \epsilon_X H^r_{dR}(A^r/F) \cong \mathrm{Sym}^r H^1_{dR}(A/F).$$

(Here $\omega_A \in \Omega^1(A/F) = H^{1,0}_{dR}(A/F)$ is a nowhere vanishing differential on A, and $\eta_A \in H^{0,1}_{dR}(A/F)$ is such that $\langle \omega_A, \eta_A \rangle = 1$ under the cup product pairing on de Rham cohomology.)

Bertolini, Darmon, and Prasanna's p-adic Waldspurger formula relates a special value of an anticyclotomic p-adic L-function $\mathcal{L}_p(f, \chi)$ to the Abel–Jacobi image of a certain generalized Heegner cycle Δ, evaluated at the basis element $\omega_f \wedge \omega_A^j \eta_A^{r-j}$. The dual basis element of this latter element is in the $(f, \chi)_{/F}$-isotypic component of $(\mathrm{Fil}^{r+1} \epsilon_X H^{2r+1}_{dR}(X_r/F))^\vee$, and the idempotent $\epsilon_{(f,\chi)/F}$ induces the projection onto this $(f, \chi)_{/F}$-isotypic component. By functoriality of projectors, the nonvanishing of $\mathrm{AJ}_{F_p}(\Delta)$ at $\omega_f \wedge \omega_A^j \eta_A^{r-j}$ shows the nontriviality of $\epsilon_{(f,\chi)/F} \Delta$. Hence, showing the nonvanishing of a special value of Bertolini, Darmon, and Prasanna's p-adic L-function verifies one consequence of the Beilinson–Bloch conjecture for the motive $M_{(f,\chi^{-1})/F} = (X_r, \epsilon_{(f,\chi)/F}, 0)$.

More precisely, nonvanishing of the anticyclotomic p-adic L function $\mathcal{L}_p(f, \chi)$ and functoriality of the action of correspondences on X_r imply

$$
\begin{aligned}
0 &\neq \mathrm{AJ}_{F_p}(\Delta)(\omega_f \wedge \omega_A^j \eta_A^{r-j}) \\
&= \mathrm{AJ}_{F_p}(\Delta)(\epsilon_{(f,\chi)/F}(\omega_f \wedge \omega_A^j \eta_A^{r-j})) \\
&= \mathrm{AJ}_{F_p}(\epsilon_{(f,\chi)/F}\Delta)(\omega_f \wedge \omega_A^j \eta_A^{r-j})
\end{aligned}
$$

and thus $0 \neq \epsilon_{(f,\chi)/F}\Delta \in \epsilon_{(f,\chi)/F}\,\mathrm{CH}^{r+1}(X_r)_{0, E_{f,\chi}}(F)$.

The classical situation $r = 0$ (i.e., $k = 2$) is perhaps instructive. In this case, the underlying generalized Kuga–Sato variety is simply $X_0 = X_1(N)$. Moreover, $\chi : \mathrm{Gal}(F/K) \to \mathbb{C}^\times$ is of finite order, so that $\chi_{/F} = 1$. Therefore, we have $\mathrm{CH}^1(X_1(N))_{0, E_{f,\chi}}(F) = J_1(N)_{E_{f,\chi}}(F)$. The p-adic Abel–Jacobi map

$$
\mathrm{AJ}_{F_p} : J_1(N)_{E_{f,\chi}}(F_p) \to S_k(\Gamma_1(N), F_p)^\vee_{E_{f,\chi}}
$$

is given by $P \mapsto (f \mapsto \log_{\omega_f} P)$, where $\log_{\omega_f}$ is the formal logarithm at p associated with the nonvanishing differential ω_f. Note that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on modular forms (as one may see by letting $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ act on the coefficients of q-expansions), and that this action also preserves eigenspaces of Hecke operators. For a modular form f, let $[f]$ denote its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbit, and let $S_k^{\mathrm{new}}(\Gamma_1(N))$ denote the space of $\Gamma_1(N)$-cuspidal newforms of weight k. Given a normalized newform f, Eichler–Shimura theory attaches to f an abelian variety A_f which arises as a quotient of $J_1(N)$. Let $A_{f,E} := A_f \otimes_{E_f} E$ for any ring E containing E_f. We have an isotypic decomposition of the component of $J_1(N)$ under the Hecke algebra action in the isogeny category,

$$
J_1(N)^{\mathrm{new}} \sim \bigoplus_{\{[f], f \in S_k^{\mathrm{new}}(\Gamma_1(N))\}} A_f \quad,
$$

which implies

$$
J_1(N)^{\mathrm{new}}_{E_{f,\chi}} = \bigoplus_{\{[f], f \in S_k^{\mathrm{new}}(\Gamma_1(N))\}} A_{f, E_{f,\chi}}.
$$

We thus have natural surjections $\Phi_f : J_1(N) \twoheadrightarrow A_f$ (called modular parametrizations) and hence maps $\Phi_f : J_1(N)_{E_{f,\chi}}(F) \twoheadrightarrow A_{f, E_{f,\chi}}(F)$. Let $\chi_0 : \mathrm{Gal}(F/K) \to \mathbb{C}^\times$. Denote by $\Phi_{\chi_0} : A_{f, E_{f,\chi}}(F) \twoheadrightarrow A_{f, E_{f,\chi}}(F)^{\chi_0}$ the projection onto the χ_0-isotypic component under the action of $\mathrm{Gal}(F/K)$, and set $\Phi_{f, \chi_0} = \Phi_{\chi_0} \circ \Phi_f : J_1(N)_{E_{f,\chi}}(F) \twoheadrightarrow A_{f, E_{f,\chi}}(F)^{\chi_0}$. Let ω_{A_f} be the unique invariant differential on the abelian variety A_f/F satisfying $\Phi_f^* \omega_{A_f} = \omega_f$. Generalized Heegner cycles are simply classical Heegner points, i.e., degree-0 divisors $P(\chi_0) \in J_1(N)_{E_{f,\chi}}(F)$ arising from χ_0-twisted $\mathrm{Gal}(F/K)$-traces of CM points on $X_1(N)(F)$. Therefore, $P_f(\chi_0) := \Phi_{f, \chi_0}(P(\chi_0)) \in A_{f, E_{f,\chi}}(F)^{\chi_0}$. Note that, when $\chi_0 = 1$, we have $P_f(1) \in A_{f, E_{f,\chi}}(K)$.

The nonvanishing of the p-adic Abel–Jacobi map implies

$$0 \neq \log_{\omega_f} P(\chi_0) = \log_{\Phi_{f,\chi_0}^* \omega_{A_f}} P(\chi_0) = \log_{\omega_{A_f}} \Phi_{f,\chi_0}(P(\chi_0)) = \log_{\omega_{A_f}} P_f(\chi_0),$$

and so $P_f(\chi_0) \in A_{f,E_{f,\chi}}(F)^{\chi_0}$ is nontrivial. Suppose $\chi_0 = 1$. If $E_f = \mathbb{Q}$, then A_f is an elliptic curve, and $P_f(1) \in A_{f,\mathbb{Q}}(K)$ is nontrivial. By Kolyvagin's theorem [1990], we have $\operatorname{rank}_{\mathbb{Z}} A_f(K) = 1$.

2.3. *Main results.* In the case where $f \in S_k(\Gamma_0(N), \varepsilon_f)$ is a normalized newform with *partial Eisenstein descent* (see Definition 31), i.e., a newform whose Fourier coefficients are congruent to those of an Eisenstein series except possibly at the constant term, we will establish a congruence between Bertolini, Darmon, and Prasanna's anticyclotomic p-adic L-function and the Katz two-variable p-adic L-function which holds wherever the former 1-variable p-adic L-function is defined. A more precise statement is given in our main theorem below. Fix the following assumptions.

Assumptions 1. (1) Let $f \in S_k(\Gamma_0(N), \varepsilon_f)$ be a normalized newform of weight $k \geq 2$ and level $N > 4$.

(2) Let $p \nmid N$ be a rational prime.

(3) Let $K/\mathbb{Q}$ be an imaginary quadratic extension with odd fundamental discriminant $D_K < -4$ and p split in K.

(4) (Heegner hypothesis) For any prime $\ell \mid N$, ℓ is split in $K/\mathbb{Q}$.

Note that assumption (4) guarantees the existence of an integral ideal $\mathfrak{N} \mid N$ of $\mathcal{O}_K$ with

$$\mathcal{O}_K/\mathfrak{N} = \mathbb{Z}/N.$$

Fix such an $\mathfrak{N}$ and write $\mathfrak{N} = \prod_{\ell \mid N} v$ as a product of primes v of $\mathcal{O}_K$ with $v \mid \ell$ for rational primes $\ell \mid N$.

Remark 2. The assumption that $D_K < -4$ is odd is made for calculational convenience in [Bertolini et al. 2013, Remark 4.7] and can most likely be removed. See Liu, Zhang, and Zhang's recent generalization of Bertolini, Darmon, and Prasanna's L-function and their p-adic Waldspurger formula [Liu et al. 2014].

Note that our fixed embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ determines a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ above p. Let $\mathcal{L}_p(f, \chi)$ denote Bertolini, Darmon, and Prasanna's anticyclotomic p-adic L-function described in Section 3.4, and let $L_p(\chi, 0)$ denote the Katz p-adic L-function described in Section 3.5. Let F' and $H_{\mathfrak{N}}$ be the fields defined in Section 3.4, and let $\mathfrak{p}'$ be the prime ideal of $\mathcal{O}_{F'}$ above $\mathfrak{p}$ determined by i_p.

Theorem 3 (main theorem). *Let (f, p, K) be as in Assumptions 1. Suppose f has Eisenstein descent of type $(\psi_1, \psi_2, N_+, N_-, N_0)$ mod $\mathfrak{m}$ (see Definition 31) for*

some integral ideal $\mathfrak{m}$ *of the ring of integers of a p-adic local field M containing* E_f, *and suppose* ψ_1 *and* ψ_2 *are Dirichlet characters over* $\mathbb{Q}$ *with* $\psi_1\psi_2 = \varepsilon_f$. *Let* $\mathfrak{t}$ *be an integral ideal of* $\mathcal{O}_K$ *with* $\mathcal{O}_K/\mathfrak{t} = \mathbb{Z}/\mathfrak{f}(\psi_2)$ *and* $\mathfrak{t} \mid \mathfrak{N}$. *For all* $\chi \in \hat{\Sigma}_{cc}(\mathfrak{N})$ (*see* Section 3.4 *for a precise definition*), *we have the congruence*

$$\mathcal{L}_p(f, \chi) \equiv \psi_1^{-1}(D_K)\left(\frac{|\mathfrak{f}(\psi_2)|^k \chi^{-1}(\bar{\mathfrak{t}})}{4\mathfrak{g}(\psi_2^{-1})(2\pi i)^{k+2j}} \cdot \Xi \cdot L_p(\psi_{1/K}\chi^{-1}, 0)\right)^2 \pmod{\mathfrak{m}\mathcal{O}_{F'_{\mathfrak{p}'}M}},$$

where $k+2j \in \mathbb{Z}/(p-1) \times \mathbb{Z}_p$ *is the signature of* $\chi \in \hat{\Sigma}_{cc}(\mathfrak{N})$ (*see* Definition 23) *and*

$$\Xi = \prod_{\ell \mid N_+}(1 - (\psi_{2/K}\chi^{-1})(\bar{v})\ell^{k-1}) \prod_{\ell \mid N_-}(1 - (\psi_{1/K}\chi^{-1})(\bar{v}))$$
$$\times \prod_{\ell \mid N_0}(1 - (\psi_{2/K}\chi^{-1})(\bar{v})\ell^{k-1})(1 - (\psi_{1/K}\chi^{-1})(\bar{v})).$$

Invoking Bertolini, Darmon, and Prasanna's *p*-adic Waldspurger formula, given as Theorem 25, we can identify the left-hand side of Theorem 3 with a *p*-adic Abel–Jacobi image of a generalized Heegner cycle, and thus derive the following congruence.

Corollary 4. *Suppose* $\chi \in \Sigma_{cc}^{(1)}(\mathfrak{N})$ (*see* Section 3.4 *for a precise definition*) *with infinity type* $(k - 1 - j, 1 + j)$, *where* $0 \le j \le k - 2$. *In the setting of* Theorem 3, *we have, for* $0 \le j \le k - 2$,

$$\Omega_p^{2(k-2-2j)}\left(\frac{1 - \chi^{-1}(\bar{\mathfrak{p}})a_p(f) + \chi^{-2}(\bar{\mathfrak{p}})\varepsilon_f(p)p^{k-1}}{\Gamma(j+1)}\right)^2\left(\mathrm{AJ}_{F'_{\mathfrak{p}'}}(\Delta(\chi \mathbb{N}_K))(\omega_f \wedge \omega_A^j \eta_A^{k-2-j})\right)^2$$
$$\equiv \psi_1^{-1}(D_K)\left(\frac{|\mathfrak{f}(\psi_2)|^k \chi^{-1}(\bar{\mathfrak{t}})}{4\mathfrak{g}(\psi_2^{-1})(2\pi i)^{k-2-2j}} \cdot \Xi \cdot L_p(\psi_{1/K}\chi^{-1}, 0)\right)^2 \pmod{\mathfrak{m}\mathcal{O}_{F'_{\mathfrak{p}'}M}}.$$

Here Ω_p *is the p-adic period defined in* Section 3.4, *and*

$$\Delta(\chi \mathbb{N}_K) := \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi \mathbb{N}_K)^{-1}(\mathfrak{a}) \cdot \Delta_{\varphi_\mathfrak{a}\varphi_0} \in \mathrm{CH}^{k-1}(X_{k-2})_{0, E_\chi}(H_{\mathfrak{N}}),$$

where $\Delta_{\varphi_\mathfrak{a}\varphi_0}$ *is defined as in* Section 3.4.

Remark 5. Corollary 4 can be viewed as providing a new method for verifying a consequence of the Beilinson–Bloch conjecture. In light of the discussion in Section 2.2, we note that for $\chi \in \Sigma_{cc}^{(1)}(\mathfrak{N})$ we have $L\left(\pi_f \times \pi_{\chi^{-1}}, \frac{1}{2}\right) = 0$, which implies $L\left(\pi_f \times \pi_{(\chi^{-1})/F}, \frac{1}{2}\right) = 0$ for any $F/H_{\mathfrak{N}}$ in situation (S). Hence, the Beilinson–Bloch conjecture predicts that $\dim_{E_{f,\chi}} \epsilon_{(f,\chi)/F} \mathrm{CH}^{k-1}(X_{k-2})(F) \ge 1$. Corollary 4 shows that, in the setting where f has Eisenstein descent mod $\mathfrak{m}$, if

$$\Xi \cdot L_p(\psi_{1/K}\chi^{-1}, 0) \not\equiv 0 \pmod{\mathfrak{m}\mathcal{O}_{F'_{\mathfrak{p}'}}},$$

then the generalized Heegner cycle $\Delta(\chi \mathbb{N}_K)$ induces the ostensibly nontrivial algebraic cycle class. We are thus reduced to verifying the p-nondivisibility of the above special values of the Katz p-adic L-function. In Theorem 7 we explicitly evaluate Katz L-values corresponding to *classical* Heegner cycles (see Remark 8) using a theorem of Gross in order to find explicit non-p-divisibility criteria. One might expect to be able to carry out studies of p-nondivisibility for more general Katz L-values in order to establish similar explicit nontriviality criteria for more general Heegner cycles, but we do not do this here.

Suppose that $\varepsilon_f = 1$ and that k is *even*. Note that the anticyclotomic line intersects with the cyclotomic line when $j = k/2 - 1$, in the notation of Corollary 4. For this j, we can take the particular character $\chi = \mathbb{N}_K^{-k/2} \in \Sigma_{cc}^{(1)}(\mathfrak{N})$. Applying Gross's factorization (Theorem 28) of the Katz L-function on the cyclotomic line to the right-hand side of Theorem 3, we get the following explicit congruences between special values of p-adic L-functions. First, fix the following notation for convenience.

Definition 6. Suppose we are given an imaginary quadratic field K. For any Dirichlet character ψ over $\mathbb{Q}$, let

$$\psi_0 := \begin{cases} \psi & \text{if } \psi \text{ even,} \\ \psi \varepsilon_K & \text{if } \psi \text{ odd.} \end{cases}$$

Theorem 7. *In the setting of Theorem 3, specializing to* $\varepsilon_f = 1$, k *even, and* $\psi_1 = \psi_2^{-1} = \psi$,

$$\left(\frac{p^{k/2} - a_p(f) + p^{k/2-1}}{p^{k/2}\Gamma(\frac{k}{2})}\right)^2 \mathrm{AJ}_{F_{\mathfrak{p}'}}\left(\Delta(\mathbb{N}_K^{1-k/2})\right)^2 \left(\omega_f \wedge \omega_A^{k/2-1}\eta_A^{k/2-1}\right)$$

is congruent to

$$\frac{\Xi^2}{4}\left(\frac{1}{k}(1 - \psi^{-1}(p)p^{k/2-1})B_{\frac{k}{2},\psi_0^{-1}\varepsilon_K^{k/2}} \cdot L_p\left(\psi_0(\varepsilon_K\omega)^{1-k/2}, \frac{k}{2}\right)\right)^2 \pmod{\mathfrak{m}\mathcal{O}_{F_{\mathfrak{p}'}M}}$$

if $\psi_0(\varepsilon_K\omega)^{1-k/2} \neq 1$ *or* $k > 2$, *and*

$$\frac{\Xi^2}{4}\left(\frac{p-1}{p}\log_p\bar{\alpha}\right)^2 \pmod{\mathfrak{m}\mathcal{O}_{F_{\mathfrak{p}'}M}}$$

otherwise.

If $\mathfrak{m} = \lambda$, *where* λ *is some prime ideal of* $\mathcal{O}_M$ *above* p, *then more explicitly*

$$\left(\frac{p^{k/2} - a_p(f) + p^{k/2-1}}{p^{k/2}\Gamma(\frac{k}{2})}\right)^2 \mathrm{AJ}_{F_{\mathfrak{p}'}}\left(\Delta_f(\mathbb{N}_K^{1-k/2})\right)^2 \left(\omega_f \wedge \omega_A^{k/2-1}\eta_A^{k/2-1}\right)$$

is congruent to

$$\frac{\Xi^2}{4}\left(\frac{1}{k}(1-\psi^{-1}(p)p^{k/2-1})(1-(\psi\omega^{-k/2})(p))B_{\frac{k}{2},\psi_0^{-1}\varepsilon_K^{k/2}}B_{1,\psi_0\varepsilon_K(\varepsilon_K\omega)^{-k/2}}\right)^2 (\mathrm{mod}\ \lambda\mathcal{O}_{F'_{\mathfrak{p}'},M})$$

if $\psi_0(\varepsilon_K\omega)^{1-k/2} \neq 1,$

$$\frac{\Xi^2}{4}\left(\frac{1}{k}(1-\psi^{-1}(p)p^{k/2-1})B_{\frac{k}{2},\psi_0^{-1}\varepsilon_K^{k/2}} \cdot L_p\left(1,\frac{k}{2}\right)\right)^2 (\mathrm{mod}\ \lambda\mathcal{O}_{F'_{\mathfrak{p}'},M})$$

if $\psi_0(\varepsilon_K\omega)^{1-k/2} = 1,\ k > 2,$ *and*

$$\frac{\Xi^2}{4}\left(\frac{p-1}{p}\log_p\bar{\alpha}\right)^2 (\mathrm{mod}\ \lambda\mathcal{O}_{F'_{\mathfrak{p}'},M})$$

otherwise.

　　Here

$$\Delta(\mathbb{N}_K^{1-k/2}) := \sum_{[\mathfrak{a}]\in\mathrm{Cl}(\mathcal{O}_K)} \mathbb{N}_K^{k/2-1}(\mathfrak{a}) \cdot \Delta_{\varphi_\mathfrak{a}\varphi_0} \in \mathrm{CH}^{k-1}(X_{k-2})_{0,\mathbb{Q}}(H_{\mathfrak{N}}),$$

where $\Delta_{\varphi_\mathfrak{a}\varphi_0}$ *is defined as in [Section 3.4](#),*

$$\Xi = \prod_{\ell\,|\,N_+}\left(1-\frac{\psi^{-1}(\ell)}{\ell^{1-k/2}}\right)\prod_{\ell\,|\,N_-}\left(1-\frac{\psi(\ell)}{\ell^{k/2}}\right)\prod_{\ell\,|\,N_0}\left(1-\frac{\psi^{-1}(\ell)}{\ell^{1-k/2}}\right)\left(1-\frac{\psi(\ell)}{\ell^{k/2}}\right),$$

$\log_p$ *is the Iwasawa p-adic logarithm (i.e., with branch* $\log_p p = 0$*), and* $\bar{\alpha} \in \mathcal{O}_K$ *such that* $(\bar{\alpha}) = \bar{\mathfrak{p}}^{h_K}.$

Remark 8. In the setting of [Theorem 7](#), the generalized Heegner cycle $\Delta(\mathbb{N}_K^{1-k/2})$ can be mapped via a correspondence to a *classical* Heegner cycle arising on the classical Kuga–Sato variety W_{k-2} defined in [Section 2.2](#); see, for example, [Bertolini et al. 2015, Proposition 4.1.1, Theorem 4.1.3]. Therefore, in view of [Remark 5](#), [Theorem 7](#) gives an explicit congruence criterion for showing the nontriviality of a classical Heegner cycle class and thus verifying the aforementioned consequence of the Beilinson–Bloch conjecture.

Remark 9. For any $x \in \bar{\mathfrak{p}}$, we have $\mathrm{ord}_p(x) = 0$, so we can write $x = a + 2\pi$ for $\pi \in \mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}$ and $a \in \mathcal{O}_{K_{\mathfrak{p}}}^\times$. Then $x^{h_K} = a^{h_K} + h_K a^{h_K-1}2\pi + \cdots$, so

$$\mathrm{ord}_p\left(\frac{p-1}{p}\log_p\bar{\alpha}\right) = \mathrm{ord}_p(2h_K).$$

Remark 10. In certain situations, one can use explicit special value formulas to further evaluate the right-hand side of the congruences in [Theorem 7](#). For example,

when $k = 2$ and $\psi_0 \neq 1$, by Leopoldt's formula and the fact that $\varepsilon_K(p) = 1$ since p is split in K, we have

$$L_p(\psi_0, 1) = \left(1 - \frac{\psi(p)}{p}\right) \frac{\mathfrak{g}(\psi_0)}{|\mathfrak{f}(\psi_0)|} \sum_{a=1}^{|\mathfrak{f}(\psi_0)|} \psi_0^{-1}(a) \log_p\left(1 - \exp\left(\frac{2\pi i a}{|\mathfrak{f}(\psi_0)|}\right)\right).$$

Furthermore, Diamond computes explicit formulas for the values of $L_p(\chi, n)$ when n is a positive integer; see [Diamond 1979].

Definition 11. Attached to any normalized newform $f \in S_k(\Gamma_0(N), \varepsilon_f)$ and prime λ above p of a number field M containing E_f is a unique semisimple λ-adic Galois representation $\rho_f : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(M_\lambda)$ (see Section 3.6). Choosing a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-invariant lattice in M_λ^2, one obtains an associated semisimple mod-λ Galois representation $\bar{\rho}_f$ (which turns out to be independent of the choice of lattice). If $p \nmid N$ and if $\bar{\rho}_f$ is reducible, we will see (in Theorem 34) that $N = N_+ N_- N_0$, where $N_+ N_-$ is squarefree and N_0 is squarefull, such that there are Dirichlet characters ψ_1 and ψ_2 over $\mathbb{Q}$ with $\psi_1 \psi_2 = \varepsilon_f$, and where $\ell \mid N_+$ implies $a_\ell \equiv \psi_1(\ell) \pmod{\lambda}$, $\ell \mid N_-$ implies $a_\ell \equiv \psi_2(\ell)\ell^{k-1} \pmod{\lambda}$, and $\ell \mid N_0$ implies $a_\ell \equiv 0 \pmod{\lambda}$. We then say that $\bar{\rho}_f$ is *reducible of type* $(\psi_1, \psi_2, N_+, N_-, N_0)$.

By Theorem 34, we immediately get the following corollary.

Corollary 12. *Let* (f, p, K) *be as in Assumptions 1, and suppose* $\bar{\rho}_f$ *is reducible of type* $(\psi_1, \psi_2, N_+, N_-, N_0)$, *where* $\bar{\rho}_f$ *is the semisimple mod-λ residual representation of* ρ_f *for some prime ideal λ of the ring of integers of a p-adic local field M containing E_f. Then the conclusions of Theorems 3 and 7 hold with* $\mathfrak{m} = \lambda$.

Applying Theorem 7 to the case when k is 2 and f is defined over $\mathbb{Q}$, and is thus associated with an elliptic curve $E/\mathbb{Q}$ of conductor N, we can show the Heegner point $P_E(K)$ is nontorsion when the primes dividing pN satisfy certain congruence conditions and p does not divide certain Bernoulli numbers. First, decompose the conductor $N = N_{\mathrm{split}} N_{\mathrm{nonsplit}} N_{\mathrm{add}}$ into factors such that $\ell \mid N_{\mathrm{split}}$ implies ℓ is of split multiplicative reduction, $\ell \mid N_{\mathrm{nonsplit}}$ implies ℓ is of nonsplit multiplicative reduction, and $\ell \mid N_{\mathrm{add}}$ implies ℓ is of additive reduction.

Theorem 13. *Suppose* $E/\mathbb{Q}$ *is any elliptic curve of conductor N with reducible mod-p Galois representation $E[p]$, or equivalently, $E[p]^{\mathrm{ss}} \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi^{-1}\omega)$, where $p > 2$ is a prime of good reduction for E and ψ is some Dirichlet character with $\mathfrak{f}(\psi)^2 \mid N_{\mathrm{add}}$. Suppose further that*

(1) $\psi(p) \neq 1$,

(2) $N_{\mathrm{split}} = 1$ *(i.e., E has no primes of split multiplicative reduction)*,

(3) $\ell \mid N_{\mathrm{add}}$ *implies either* $\psi(\ell) \neq 1$ *and* $\ell \not\equiv -1 \pmod{p}$, *or* $\psi(\ell) = 0$.

Then, for any imaginary quadratic field K in which p splits, such that K satisfies the Heegner hypothesis with respect to E, and $p \nmid B_{1,\psi_0^{-1}\varepsilon_K} B_{1,\psi_0\omega^{-1}}$, the associated Heegner point $P_E(K) \in E(K)$ (see Section 3.4) *is nontorsion. In particular,* rank$_{\mathbb{Z}} E(K) = 1$.

Remark 14. When ψ is quadratic, the condition $p \nmid B_{1,\psi_0\varepsilon_K}$ of Theorem 13 is equivalent to $p \nmid h_{K_{\psi_0} \cdot K}$. (This follows because $B_{1,\psi_0^{-1}\varepsilon_K} = -2h_{K_{\psi_0} \cdot K}/|\mathcal{O}^{\times}_{K_{\psi_0} \cdot K}|$ by the functional equation and analytic class number formula.)

Remark 15. In light of Theorems 34 and 35, which imply that $a_\ell(E) \equiv \psi(\ell)$ or $\psi^{-1}(\ell)\ell \pmod{p}$ for $\ell \| N$ (i.e., $\ell \mid N_{\text{split}} N_{\text{nonsplit}}$) when $E[p]^{\text{ss}} \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi^{-1}\omega)$, condition (2) can be phrased as

(2)′ for every $\ell \| N$, $\psi(\ell) \equiv -1$ or $-\ell \pmod{p}$.

In terms of local root numbers $w_\ell(E)$, since $w_\ell(E) = -a_\ell(E)$ for $\ell \| N$, conditions (2) and (2)′ can also be viewed as requiring the corresponding local root numbers to all be $+1$.

Remark 16. Theorem 13 (at least partially) recovers a much earlier result of Mazur [1979, Theorem, p. 231], which considers the case $N = \text{prime} \neq p$. In Mazur's setting, we suppose that $E[p]^{\text{ss}} \cong \mathbb{F}_p \oplus \mathbb{F}_p(\omega)$, where $N = \ell \neq p$, let ψ be an *even* quadratic character and choose an imaginary quadratic field K. (In Mazur's notation, we are taking $\chi = \psi\varepsilon_K$ and $K_\chi = K_\psi \cdot K = K_{\psi\varepsilon_K}$.) The case of Mazur's theorem we recover is as follows.

   Suppose (E, p, ψ, K) as above are such that

(1) K satisfies the Heegner hypothesis with respect to $E \otimes \psi$,

(2) p splits in K and $D_K < -4$,

(3) $\psi(p) = -1$,

(4) $p \nmid B_{1,\psi\omega^{-1}}$,

(5) $\text{lcm}(\ell, |\mathfrak{f}(\psi)|^2) > 4$, $\psi(\ell) \neq 1$ and $p \nmid h_{K_\psi \cdot K}$.

Then rank$_{\mathbb{Z}}(E \otimes \psi\varepsilon_K)(\mathbb{Q}) = 0$.

   This follows from Theorem 13 since the latter implies rank$_{\mathbb{Z}}(E \otimes \psi)(K) = 1$, and then rank$_{\mathbb{Z}}(E \otimes \psi\varepsilon_K)(\mathbb{Q}) = 0$ follows from root number considerations (see Proposition 50).

   Assumptions (1)–(4) above are extraneous in the full generality of Mazur's theorem, with (5) being the pertinent hypothesis. These assumptions have the following effects: (1) is part (4) of Assumptions 1 and guarantees that $L((E \otimes \psi)/K, 1) = 0$; (2) is part (3) of Assumptions 1; (3) excludes the possibility of a "trivial zero" from the Kubota–Leopoldt factor $L_p(\psi\varepsilon_K\omega, 0)$, which shows up in the congruence of Theorem 7; (4) essentially controls the Selmer group $\text{Sel}_p((E \otimes \psi)/\mathbb{Q})$ (see Remark 45) so that rank$_{\mathbb{Z}}(E \otimes \psi)(\mathbb{Q}) \leq 1$. Mazur's original statement also allows

for $p \mid \mathfrak{f}(\psi)$, which is ruled out by part (2) of Assumptions 1. We should note, however, that Mazur requires the additional assumptions

(6) $\ell \geq 11$,

(7) p divides the numerator of $\left(\frac{\ell-1}{12}\right)$,

(8) $(p, |\mathfrak{f}(\psi \varepsilon_K)|) \neq (3, 3)$.

Assumption (6) is a technical assumption and is stronger than our assumption $\mathrm{lcm}(\ell, |\mathfrak{f}(\psi)|^2) > 4$ on the level of $E \otimes \psi$, which in turn originates from part (1) of Assumptions 1; (7) means that the newform $f_E \in S_2(\Gamma_0(\ell))$ of E has *full Eisenstein descent* (see Definition 31), and is automatically satisfied when $E[p]$ is reducible and $p > 3$ (see Remark 33); (8) is taken care of by our assumption $D_K < -4$ from part (3) of Assumptions 1.

Perhaps more interesting is the connection between Theorem 13 and the "supplement" to Mazur's theorem, which states that a Heegner point is nontorsion when "$\psi(\ell) \neq 1$" in Assumption (5) above is replaced with "$\psi(\ell) = 1$" (see [Mazur 1979, Theorem, p. 237]). In particular, E satisfies the Heegner hypothesis with respect to both K and $K_\psi \cdot K$, and $E \otimes \psi \varepsilon_K$ has root number -1 so that $P_{E \otimes \psi}(K) \in (E \otimes \psi \varepsilon_K)(\mathbb{Q})$. As is pointed out in [Mazur 1979], under this assumption, the Kubota–Leopoldt factor $L_p(\psi^{-1} \varepsilon_K \omega, 0)$ from Theorem 7 can be related mod p to $(1/p) \frac{d}{ds} L(E, \psi \varepsilon_K, s)_{|s=1}$, itself being related to the p-adic height mod p of

$$P_E(K_\psi \cdot K)^- := P_E(K_\psi \cdot K) - \overline{P_E(K_\psi \cdot K)} \in (E \otimes \psi \varepsilon_K)(\mathbb{Q}).$$

Note that $\psi(\ell) = 1$ places $E \otimes \psi$ outside the scope of Theorem 13, but perhaps this descent result in tandem with Mazur's observation and the mod-p factorization of Theorem 7 suggests an identity (in certain cases) relating the formal logarithm of $P_{E \otimes \psi}(K) \in (E \otimes \psi \varepsilon_K)(\mathbb{Q})$ with the p-adic height of $P_E(K_\psi \cdot K)^- \in (E \otimes \psi \varepsilon_K)(\mathbb{Q})$ times another quantity, perhaps related to the order of $\text{Ш}(E \otimes \psi / \mathbb{Q})[p^\infty]$. A deeper comparison between the results of this paper and Mazur's would be an interesting direction for further investigation.

Remark 17. One of the referees has also pointed out an analogy between Mazur's result and Theorem 13 and the two "reciprocity laws" which Bertolini and Darmon [2005] established in their work on the anticyclotomic Iwasawa main conjecture for elliptic curves. Let $E/\mathbb{Q}$ be an elliptic curve with newform f_E. Mazur's descent result assumes $E \otimes \varepsilon_K$ has root number -1 over $\mathbb{Q}$ and computes the image of $P_E(K)^-$ inside the p-primary part of the component group of the special fiber of a Néron model of E over $\mathbb{Z}_N$. Using an Eisenstein congruence at p, Mazur shows that nonvanishing of this image is equivalent to $p \nmid h_K$, i.e., the p-nondivisibility of a special value of a certain Kubota–Leopoldt p-adic L-function. Bertolini and

Darmon's first reciprocity law also assumes E has root number -1 over K and computes the image inside the p-primary part of the component group of the special fiber of a Néron model over $\mathbb{Z}_{\ell^2}$ of some abelian variety (arising as a quotient of $J_1(N\ell)$ for some prime $\ell \nmid N$ which is inert in K). (Here $\mathbb{Z}_{\ell^2}$ is the unramified quadratic extension of $\mathbb{Z}_\ell$.) Using a level-raising congruence modulo some power of p of f_E with an eigenform g of level $N\ell$ (so that g has root number $+1$ over K), Bertolini and Darmon equate this image (using a Waldspurger-type formula) with a special value of an anticyclotomic p-adic L-function attached to g.

In Theorem 7 applied to E, we assume that E has root number -1 over K and computes the p-adic formal logarithm of $P_E(K)$ modulo some power of p. We then use an Eisenstein congruence at p to equate this with a special value of a Katz p-adic L-function. Bertolini and Darmon's second reciprocity law similarly assumes E has root number -1 over K and computes the image of $P_E(K)$ inside the finite part of some power-of-p-(Bloch–Kato) Selmer group of E. The formal logarithm at p modulo this same power of p in particular maps into this Selmer group. Using another level-raising congruence to an eigenform g of level $N\ell_1\ell_2$ for distinct "admissible" primes $\ell_1, \ell_2 \nmid N$, Bertolini and Darmon again equate this image with a special value of an anticyclotomic p-adic L-function of g. It should be noted that the p-adic Waldspurger formula of Bertolini, Darmon, and Prasanna (Theorem 25) is itself established through exploiting yet another "sign change" congruence, namely by considering congruences with a newform f and its various anticyclotomic twists, considering these twists in a p-adic family, varying the twists through the interpolation region where the global root number is $+1$, and taking a p-adic limit into a region where the root number is -1.

Let us return to the setting of Theorem 13. Considering quadratic twists of E when $E[p]^{\mathrm{ss}} \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi^{-1}\omega)$ (which amounts to varying ψ through quadratic characters), we obtain congruence criteria for the $\mathfrak{f}(\psi)$ which, when satisfied, imply $\mathrm{rank}_{\mathbb{Z}}(E \otimes \psi)(K) = 1$. In Section 5.5, we consider $p = 3$ and use quadratic class number 3-divisibility results to show the following.

Corollary 18. *Suppose $E/\mathbb{Q}$ has reducible mod-3 Galois representation $E[3]$. Then we have*:

(1) *If E is reducible of type $(\psi, \psi^{-1}, N_+, N_-, N_0)$ for some quadratic character ψ, then a positive proportion of quadratic twists of E, ordered by absolute value of discriminant, have rank 0 or 1.*

(2) *If E is semistable, then a positive proportion of real quadratic twists of E, ordered by absolute value of discriminant, have rank 1 and a positive proportion of imaginary quadratic twists of E, likewise ordered, have rank 0.*

Remark 19. For E as in the statement of Corollary 18, explicit lower bounds for these proportions are given in the statement of Theorems 53 and 54, respectively.

One can also use congruence criteria provided by Theorem 13 to find explicit examples of quadratic twists $E \otimes \psi$ with $\mathrm{rank}_{\mathbb{Z}}(E \otimes \psi)(K) = 1$.

Remark 20. Recent work of Harron and Snowden [2015] in particular shows that

$$\lim_{X \to \infty} \frac{N_{\mathbb{Z}/3}(X)}{X^{1/3}} \approx 1.5221,$$

where $N_G(X)$ denotes the number of (isomorphism classes of) elliptic curves E over $\mathbb{Q}$ up to (naive) height X with $E(\mathbb{Q})^{\mathrm{tor}} \cong G$. Corollary 18 applies to all curves with nontrivial rational 3-torsion, and so applies to at least a number of curves on the order of $X^{1/3}$ up to height X.

The organization of this paper is as follows. In Section 3, we review some preliminaries, including definitions pertinent to our discussion and a review of algebraic and p-adic modular forms. In Section 3.4, we recall Bertolini, Darmon, and Prasanna's anticyclotomic p-adic L-function as well as their p-adic Waldspurger formula, which gives the value of the image of a certain generalized Heegner cycle under the p-adic Abel–Jacobi in terms of a special value of their p-adic L-function. In Section 3.5, we recall Katz's p-adic L-function attached to Hecke characters over imaginary quadratic fields K as well as recall Gross's factorization of the L-function on the cyclotomic line. In Section 3.6, we define the notion of a normalized newform f having Eisenstein descent, and relate it to the reducibility of the residual p-adic Galois representation of f.

In Section 4, we prove our main congruence by showing that certain twisted traces over CM points of Maass–Shimura derivatives ∂^j of Eisenstein series represent special values of complex L-functions of Hecke characters. The twisted traces considered in [Bertolini et al. 2013] are exactly of the same kind, with the sole difference being that the Eisenstein series is replaced by a cusp form. Interpolating these twisted traces yields the Katz p-adic L-function and Bertolini, Darmon, and Prasanna's anticyclotomic p-adic L-functions, respectively. When f has partial Eisenstein descent with associated Eisenstein series G, we use the corresponding congruence between the twisted traces of $\partial^j f$ and $\partial^j G$ to derive the congruence between p-adic L-functions.

In Section 5, we apply our congruence formula to the problem of finding nontrivial algebraic cycles whose existence is predicted by the Beilinson–Bloch conjecture. We also give examples of Eisenstein descent, including ways to construct such newforms (see Constructions 38 and 40), and applications of our main theorem to showing nontriviality of algebraic cycle classes. In Section 5.4, we address the particular case of showing nontriviality of generalized Heegner cycles attached to quadratic twists of the Ramanujan Δ function. In Section 5.5, we examine the case of elliptic curves and derive an explicit criterion to show $\mathrm{rank}_{\mathbb{Z}}(E(K)) = 1$ for elliptic curves $E/\mathbb{Q}$ with reducible mod-p Galois representation.

In Section 5.6, we show that when E has reducible mod-3 Galois representation, a positive proportion of quadratic twists of E have rank 0 or 1. These results in certain cases extend those of [Vatsal 1999], who exhibited an infinite family of elliptic curves (namely, those which are semistable with rational 3-torsion), for each member of which a positive proportion of its imaginary quadratic twists have rank 0. Our result gives a larger infinite family of elliptic curves (namely, those which are semistable with reducible mod-3 Galois representation), for each member of which a positive proportion of its imaginary quadratic twists have rank 0 and a positive proportion of its real quadratic twists have rank 1.

3. Preliminaries

In this section, we review some preliminaries relating to Bertolini, Darmon, and Prasanna's and Katz's *p*-adic *L*-functions. Our discussion follows [Bertolini et al. 2013].

3.1. *Algebraic modular forms.* Recall

$$\Gamma_1(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \ (\mathrm{mod}\ N) \right\},$$

$$\Gamma_0(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \ (\mathrm{mod}\ N) \right\},$$

and note that $\Gamma_1(N) \subset \Gamma_0(N)$. From now on, let Γ be $\Gamma_1(N)$ or $\Gamma_0(N)$. For $i = 0, 1$, let $Y_i(N)$ be the associated modular curve whose complex points are in bijection with the Riemann surface $\Gamma_i(N) \backslash \mathcal{H}^+$, and which classifies pairs (E, t) consisting of an elliptic curve E and a $\Gamma_i(N)$-level structure t on E (so $\mathbb{Z}/N \cong t \subset E[N]$ for $i = 0$, and $t \in E[N]$ of exact order N for $i = 1$). Let $X_i(N)$ denote the compactification of $Y_i(N)$. Let $\pi : \mathcal{E} \to Y_1(N)$ denote the universal elliptic curve with $\Gamma_1(N)$-level structure. Throughout the paper, we shall use the interpretation of algebraic modular forms as global sections of powers $\bar{\omega}^k$ of the Hodge bundle $\bar{\omega} := \pi_* \Omega^1_{\mathcal{E}/Y_1(N)}$ of relative differentials $\mathcal{E}/Y_1(N)$ (which we may extend to $X_1(N)$ when $N > 4$), so that an algebraic modular form can be thought of as a function on isomorphism classes of triples $[(E, t, \omega)]$ satisfying base-change compatibility and homogeneity conditions; here E is an elliptic curve, t a Γ-level structure, and ω an invariant differential on E. For details, see [Bertolini et al. 2013, Section 1.1]. Denote by

$$S_k(\Gamma, R) \subset M_k(\Gamma, R) \subset M_k^*(\Gamma, R)$$

the space of weight-k algebraic Γ-cuspforms over a ring R, the space of weight-k algebraic Γ-modular forms, and the space of weight-k weakly holomorphic Γ-modular forms, respectively. (See Section 1.1 of loc. cit. for precise definitions.) We have

similar inclusions for the corresponding spaces considered with nebentypus ε. We will suppress the base ring "R" when it is obvious from context.

Suppose $F \subset \mathbb{C}$ is a field containing the values of a Dirichlet character ε, and suppose $f \in M_k^*(\Gamma_0(N), F, \varepsilon)$. Then we have an associated holomorphic function on $\mathcal{H}^+$ given by

$$f(\tau) := f\left(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau), \frac{1}{N}, 2\pi i dz\right),$$

where dz is the standard differential on $\mathbb{C}/\Lambda$ with period lattice equal to Λ. Note that $f(\tau)$ satisfies the usual weight-k, ϵ-twisted modularity condition for $\Gamma_0(N)$,

$$f(\gamma \cdot \tau) = \varepsilon(d)(c\tau + d)^k f(\tau)$$

for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. The function $f(\tau)$ in fact completely determines the weakly holomorphic modular form $f \in M_k^*(\Gamma_0(N), F, \varepsilon)$.

Denote the space of weight-k nearly holomorphic Γ-modular forms over F and nebentypus ε by $N_k(\Gamma, F, \varepsilon)$. (See Section 1.2 of loc. cit. for precise definitions.) We have the classical *Maass–Shimura* operator $\partial_k : N_k(\Gamma, F, \varepsilon) \to N_{k+2}(\Gamma, F, \varepsilon)$ acting on nearly holomorphic Γ-modular forms by the formula

$$\partial_k f(\tau) := \frac{1}{2\pi i}\left(\frac{d}{d\tau} + \frac{k}{\tau - \bar{\tau}}\right) f(\tau).$$

Note that ∂_k does not preserve holomorphy, but preserves near-holomorphy. We let $\partial_k^j := \partial_{k+2(j-1)} \circ \cdots \circ \partial_k : N_k(\Gamma, F, \varepsilon) \to N_{k+2j}(\Gamma, F, \varepsilon)$, and omit k when it is obvious from context.

3.2. *p-adic modular forms.*

Fix a rational prime p. We will interpret p-adic modular forms analogously to the previous definition of algebraic modular forms, i.e., as global sections of a rigid analytic line bundle over the ordinary locus of $X_i(N)/\mathbb{C}_p$, or equivalently as functions on isomorphism classes of triples $[(E, t, \omega)]$ defined over p-adic rings satisfying certain homogeneity and base-change properties. (For details, see [Bertolini et al. 2013], Section 1.3].)

We have the classical *Atkin–Serre* operator $\theta : M_k^{(p)}(\Gamma, F, \varepsilon) \to M_{k+2}^{(p)}(\Gamma, F, \varepsilon)$ acting on p-adic modular forms, whose effect on q-expansions is given by

$$\theta\left(\sum_{n=0}^{\infty} a_n q^n\right) = q\frac{d}{dq}\sum_{n=0}^{\infty} a_n q^n = \sum_{n=1}^{\infty} n a_n q^n.$$

Now recall our complex and p-adic embeddings $i_\infty : F \hookrightarrow \mathbb{C}$ and $i_p : F \hookrightarrow \mathbb{C}_p$, as well as our field isomorphism $i : \mathbb{C} \xrightarrow{\sim} \mathbb{C}_p$ such that $i_p = i \circ i_\infty$. Let K be an imaginary quadratic field and let H be the Hilbert class field over K. Suppose E/F is a curve with complex multiplication (i.e., such that $\text{End}_H(E)$ is isomorphic to an order of $\mathcal{O}_K$), and let (E, t, ω) be a triple defined over F. Using i_∞ and i_p, we

can view (E, t, ω) as a triple over $\mathbb{C}$ and $\mathbb{C}_p$, respectively. Using i, we can view $f \in M_k^*(\Gamma, F, \varepsilon)$ as an element of $M_k^{(p)}(\Gamma, F, \varepsilon)$ (after possibly rescaling). The following theorem, due to Shimura and Katz, states that the values of $\partial^j f$ and $\theta^j f$ coincide on ordinary CM triples.

Theorem 21 (see [Bertolini et al. 2013, Proposition 1.12]). *Suppose (E, t, ω) is a triple defined over F, where E has complex multiplication by an order of $\mathcal{O}_K$, and assume that E, viewed as an elliptic curve over $\mathcal{O}_{\mathbb{C}_p}$, is ordinary. Suppose $f \in M_k^*(\Gamma, F, \varepsilon)$. Then, for $j \geq 0$, we have:*

(1) $\partial^j f(E, t, \omega) \in i_\infty(F)$.

(2) $\theta^j f(E, t, \omega) \in i_p(F)$.

(3) *Viewing these quantities as elements of F (i.e., identifying $i_\infty(F) \xrightarrow{i_p \circ i_\infty^{-1}} i_p(F)$), we have*
$$\partial^j f(E, t, \omega) = \theta^j f(E, t, \omega).$$

Denote by $\flat$ the "p-depletion" operator on $M_k^{(p)}(\Gamma, F, \varepsilon)$ (see [Bertolini et al. 2013, Section 3.8]), whose action on q-expansions $f(q) = \sum_{n=0}^\infty a_n(f) q^n$ is given by

$$f^\flat(q) = f(q) - a_p(f) f(q^p) + \varepsilon(p) p^{k-1} f(q^{p^2}),$$

so that $a_n(f^\flat) = 0$ for all $n > 0$ with $(n, p) \neq 1$.

3.3. *Isogenies and generalized Heegner cycles.* Recall our assumption that the imaginary quadratic field K satisfies the *Heegner hypothesis* with respect to N:

for all primes $\ell \mid N$, ℓ is split in $K/\mathbb{Q}$.

This condition implies that there exists an integral ideal $\mathfrak{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{N} = \mathbb{Z}/N$. Fix such an $\mathfrak{N}$ and fix a CM elliptic curve A with $\mathrm{End}_H(A) = \mathcal{O}_K$. Let $H_\mathfrak{N}/H$ denote the extension over which the individual $\mathfrak{N}$-torsion points of A are defined, which is an abelian extension of K. A choice of $t_A \in A[\mathfrak{N}]$ of order N determines a $\Gamma_1(N)$-level structure on A defined over any $F/H_\mathfrak{N}$. Fix a choice of t_A once and for all.

Now consider the set

$$\mathrm{Isog}(A) := \{(\varphi, A')\}/\text{Isomorphism},$$

where A' is an elliptic curve and $\varphi : A \to A'$ is an isogeny defined over $\bar{K}$, and two pairs (φ_1, A_1') and (φ_2, A_2') are isomorphic if there is an isomorphism $\iota : A_1' \to A_2'$ over $\bar{K}$ such that $\iota\varphi_1 = \varphi_2$. Let $\mathrm{Isog}^\mathfrak{N}(A) \subset \mathrm{Isog}(A)$ be the subset consisting of isomorphism classes of (φ, A') such that $\ker(\varphi) \cap A[\mathfrak{N}] = \{0\}$. Note that the group $\mathbb{I}^\mathfrak{N}$ of $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{N}$ act on $\mathrm{Isog}^\mathfrak{N}(A)$ via $\mathfrak{a} \star (\varphi, A') = (\varphi_\mathfrak{a}\varphi, A'/A'[\mathfrak{a}])$, where

$$\varphi_\mathfrak{a} : A' \to A'/A'[\mathfrak{a}]$$

is the natural surjection. Given triples (A_1, t_1, ω_1) and (A_2, t_2, ω_2), we define an isogeny from (A_1, t_1, ω_1) to (A_2, t_2, ω_2) to be an isogeny

$$\varphi : A_1 \to A_2 \quad \text{such that} \quad \varphi(t_1) = t_2 \text{ and } \varphi^*(\omega_2) = \omega_1.$$

We have an action of $\mathbb{I}^{\mathfrak{N}}$ on (isomorphism classes of) triples (A', t', ω') with $\text{End}(A') = \mathcal{O}_K$ and $t' \in A'[\mathfrak{N}]$ given by

$$\mathfrak{a} \star (A', t', \omega') = (A'/A'[\mathfrak{a}], \varphi_{\mathfrak{a}}(t'), \omega'_{\mathfrak{a}}), \quad \text{where } \varphi_{\mathfrak{a}}^*(\omega'_{\mathfrak{a}}) = \omega'.$$

Definition 22. Note that a pair $(\varphi, A') \in \text{Isog}^{\mathfrak{N}}(A)$ determines a point $(A', \varphi(t_A)) \in Y_1(N)(H_{\mathfrak{N}}) \subset Y_1(N)(F)$ and, for any integer $r \geq 0$, an embedding $(A')^r \hookrightarrow W_r$. (For the definition of W_r, see Section 2.2.) Using this we view the graph as being embedded in $X_r := W_r \times A^r$:

$$\Gamma_\varphi \subset A^r \times (A')^r \subset A^r \times W_r \cong X_r.$$

We define the *generalized Heegner cycle* associated with (φ, A) as $\Delta_\varphi := \epsilon_X \Gamma_\varphi$, where ϵ_X is the projector defined in [Bertolini et al. 2013, Section 2.2]. Note that Γ_φ is defined over $H_{\mathfrak{N}}$, and thus determines a class in the Chow group $\text{CH}_0^{r+1}(X_r)(H_{\mathfrak{N}})$, as defined in Section 2.2.

3.4. *Bertolini, Darmon, and Prasanna's p-adic L-function and p-adic Waldspurger formula.* Fix a normalized newform $f \in S_k(\Gamma_0(N), \varepsilon_f)$. Given a Hecke character χ of infinity type (j_1, j_2), recall that the central character ε_χ of χ is the finite order character defined by

$$\varepsilon_\chi = \chi_{|\mathbb{A}_\mathbb{Q}^\times} \mathbb{N}_\mathbb{Q}^{j_1+j_2}.$$

We define

$$L(f, \chi^{-1}, 0) := L\big(\pi_f \times \pi_{\chi^{-1}}, s - \tfrac{1}{2}(k - 1 - j_1 - j_2)\big),$$

where π_f and $\pi_{\chi^{-1}}$ are the (unitarily normalized) automorphic representations associated with f and χ, respectively. The Hecke character χ is said to be *central critical with respect to f* if $j_1 + j_2 = k$ and either

(1) $1 \leq j_1, j_2 \leq k - 1$, or

(2) $j_1 \geq k$ and $j_2 \leq 0$,

and if the following condition on the central character of χ is satisfied:

$$\varepsilon_\chi = \varepsilon_f.$$

(Note, since we assume the Heegner hypothesis, this implies that χ is unramified outside of $\mathfrak{f}(\varepsilon_f)$.) Central criticality of χ is equivalent to requiring that $\pi_f \times \pi_{\chi^{-1}}$ is self-dual and that the point of symmetry for the functional equation of $L(f, \chi^{-1}, s)$ is $s = 0$.

For central critical χ with infinity type in range (1) (resp. range (2)) above, the root number satisfies $\epsilon_\infty(f, \chi^{-1}) = -1$ (resp. $\epsilon_\infty(f, \chi^{-1}) = +1$). We henceforth make the auxiliary assumption that

the local root numbers of $L(f, \chi^{-1}, s)$
satisfy $\epsilon_\ell(f, \chi^{-1}) = +1$ at all finite primes ℓ.

This assumption is automatic for $\ell \in S_f = \{\ell : \ell \mid (N, D_K), \ell \nmid \mathfrak{f}(\varepsilon_f)\}$ since we assume the Heegner hypothesis, and thus is automatically satisfied when $(N, D_K) = 1$, as we assume in Assumptions 1. These conditions on the local root numbers of $L(f, \chi^{-1}, s)$ imply that the global root number is $\epsilon(f, \chi^{-1}) = -1$ for χ in infinity type range (1) above, and $\epsilon(f, \chi^{-1}) = +1$ for χ in range (2) above. Thus we have $L(f, \chi^{-1}, 0) = 0$ in range (1) and expect $L(f, \chi^{-1}, 0) \neq 0$ (generically) in range (2).

For any Hecke character ε over $\mathbb{Q}$ of conductor $N_\varepsilon \mid N$, define $\mathfrak{N}_\varepsilon$ to be the unique ideal in $\mathcal{O}_K$ that divides $\mathfrak{N}$ and has norm equal to N_ε. For a Hecke character χ over K, we say that χ is of *finite type* $(\mathfrak{N}, \varepsilon)$ if

$$\chi_{|\hat{\mathcal{O}}_K^\times} = \psi_\varepsilon,$$

where ψ_ε is the composite map

$$\hat{\mathcal{O}}_K^\times \to \prod_{v \mid \mathfrak{N}_\varepsilon} (\mathcal{O}_{K,v}/\mathfrak{N}_\varepsilon \mathcal{O}_{K,v})^\times \cong \prod_{\ell \mid N_\varepsilon} (\mathbb{Z}_\ell/N_\varepsilon \mathbb{Z}_\ell)^\times \xrightarrow{\prod_{\ell \mid N_\varepsilon} \varepsilon_\ell} \mathbb{C}^\times,$$

or equivalently,

$$\hat{\mathcal{O}}_K^\times \to (\hat{\mathcal{O}}_K/\mathfrak{N}_\varepsilon \hat{\mathcal{O}}_K)^\times \cong (\mathcal{O}_K/\mathfrak{N}_{\varepsilon_K} \mathcal{O}_K)^\times \cong (\mathbb{Z}/N_\varepsilon \mathbb{Z})^\times \xrightarrow{\varepsilon^{-1}} \mathbb{C}^\times.$$

Let $\Sigma_{\mathrm{cc}}(\mathfrak{N})$ denote the set of central critical characters of finite type $(\mathfrak{N}, \varepsilon)$ satisfying the above auxiliary condition on local root numbers, with $\mathfrak{f}(\chi) \mid \mathfrak{N}$, and let $\Sigma_{\mathrm{cc}}^{(1)}(\mathfrak{N})$ and $\Sigma_{\mathrm{cc}}^{(2)}(\mathfrak{N})$ denote the subsets of such characters with infinity type $(k + j, -j)$, where $1 - k \leq j \leq -1$ and $j \geq 0$, respectively, so that we have $\Sigma_{\mathrm{cc}}(\mathfrak{N}) = \Sigma_{\mathrm{cc}}^{(1)}(\mathfrak{N}) \sqcup \Sigma_{\mathrm{cc}}^{(2)}(\mathfrak{N})$.

We now define a field F' as follows. Note that $\mathrm{Gal}(H_\mathfrak{N}/H) \cong (\mathbb{Z}/N)^\times$, and let $H_\mathfrak{N}' \subset H_\mathfrak{N}$ be the subfield fixed by $\ker(\varepsilon_f)$. The values $\chi(\mathfrak{a})$ generate a finite extension as χ ranges over $\Sigma_{\mathrm{cc}}^{(2)}(\mathfrak{N})$ and $\mathfrak{a}$ ranges over $\mathbb{A}_{K,f}^\times$. Let F' be the field which is the compositum of this latter extension with E_f and $H_\mathfrak{N}'$, and let $\mathfrak{p}'$ be the prime ideal of $\mathcal{O}_{F'}$ above p determined by our embedding i_p. The set $\Sigma_{\mathrm{cc}}^{(2)}(\mathfrak{N})$ has a natural topology, namely, the topology of uniform convergence induced by the p-adic metric on the completion of F' in $\overline{\mathbb{Q}}_p$, when $\Sigma_{\mathrm{cc}}^{(2)}(\mathfrak{N})$ is viewed as a space of functions on finite idèles prime to p. (See [Bertolini et al. 2013, Section 5.2] for details.) Let $\hat{\Sigma}_{\mathrm{cc}}(\mathfrak{N})$ denote the completion of $\Sigma_{\mathrm{cc}}^{(2)}(\mathfrak{N})$ in this topology. As explained in Section 5.3 of loc. cit., we may view $\Sigma_{\mathrm{cc}}^{(1)}(\mathfrak{N})$ as subset of $\hat{\Sigma}_{\mathrm{cc}}(\mathfrak{N})$.

Definition 23. For a Hecke character over K of infinity type (a, b), we define the *signature* of χ as $a - b \in \mathbb{Z}$. For $\chi \in \Sigma_{cc}^{(2)}(\mathfrak{N})$ of infinity type $(k + j, -j)$, this is $k + 2j$. Given $\chi \in \hat{\Sigma}_{cc}(\mathfrak{N})$, we choose a Cauchy sequence $\{\chi_i\}_{i=1}^{\infty} \subset \Sigma_{cc}^{(2)}(\mathfrak{N})$ converging to χ, where χ_i has infinity type $(k + j_i, -j_i)$. Given $M \in \mathbb{Z}$, there exists an $i(M)$ such that, for all $i_1, i_2 \geq i(M)$, we have $\chi_{i_1}(x) \equiv \chi_{i_2}(x) \pmod{(\mathfrak{p}')^M}$ for all $x \in \mathbb{A}_{K,f}^{\times,p}$. Evaluating on $x \in \mathbb{A}_{K,f}^{\times,p}$ congruent to $1 \pmod{\mathfrak{N}}$, we see that $j_{i_1} \equiv j_{i_2} \pmod{(p-1)p^{M-1}}$. Hence, the Cauchy sequence $\{j_i\}_{i=1}^{\infty} \subset \mathbb{Z}$ converges to an element $j \in \mathbb{Z}/(p-1) \times \mathbb{Z}_p$. Then the signature of χ is $k + 2j \in \mathbb{Z}/(p-1) \times \mathbb{Z}_p$.

The elliptic curve $A_0 = \mathbb{C}/\mathcal{O}_K$ over $\mathbb{C}$ has complex multiplication by $\mathcal{O}_K$, and hence is defined over H. A choice of invariant differential $\omega_0 \in \Omega_{A_0/H}^1$ determines a *complex period* $\Omega_\infty \in \mathbb{C}^\times$ via

$$\omega_0 = \Omega_\infty \cdot 2\pi i \, dz,$$

where z is the standard coordinate on $\mathbb{C}$. We now make the assumption that

$$p \text{ is split in } K/\mathbb{Q},$$

so that in particular $i_p(K) \subset \mathbb{Q}_p$. Let $\mathfrak{p}$ be a prime of K above p. Let $\mathcal{A}_0$ be a good integral model over A_0. The completion of $\mathcal{A}_0$ along its identity section $\hat{\mathcal{A}}_0$ is (non-canonically) isomorphic to $\hat{\mathbb{G}}_m$ over $\mathcal{O}_{\mathbb{C}_p}$. Fix an isomorphism $\iota : \hat{\mathcal{A}}_0 \xrightarrow{\sim} \hat{\mathbb{G}}_m$ (which is equivalent to fixing an isomorphism $\mathcal{A}_0[\mathfrak{p}^\infty] := \varinjlim_n \mathcal{A}_0[\mathfrak{p}^n] \xrightarrow{\sim} \varinjlim_n \mu_{p^n} =: \mu_{p^\infty}$, which is determined up to multiplication by a scalar in $\mathbb{Z}_p^\times$). Let $\omega_{can} := \iota^* \frac{du}{u}$. Now we define a *$p$-adic period* $\Omega_p \in \mathbb{C}_p^\times$ via

$$\omega_0 = \Omega_p \cdot \omega_{can}.$$

Bertolini, Darmon, and Prasanna [Bertolini et al. 2013] define an *anticyclotomic p-adic L-function associated with f and χ*, interpolating a twisted trace over CM triples attached to (f, χ) for $\chi \in \Sigma_{cc}^{(2)}(\mathfrak{N})$. Recall our fixed triple (A, t_A, ω_{can}). Then there is an isogeny $\varphi_0 : A \to A_0$, and we let (A_0, t_0, ω_0) denote the unique triple fitting into an induced isogeny of triples $\varphi_0 : (A, t_A, \omega_{can}) \to (A_0, t_0, \omega_0)$ in the sense of Section 3.3. Henceforth, fix a complex period Ω_∞ and a p-adic period Ω_p associated with ω_0. For $\mathfrak{a} \in \mathbb{I}^{\mathfrak{N}}$, let $\varphi_{\mathfrak{a}} : A_0 \to \mathfrak{a} \star A_0$ be the natural isogeny, so that $(\varphi_{\mathfrak{a}}\varphi_0, A) \in \mathrm{Isog}^{\mathfrak{N}}(A)$.

Theorem 24 [Bertolini et al. 2013, Theorem 5.9]. *Fix a normalized newform f in $S_k(\Gamma_0(N), \varepsilon_f)$. Suppose p is a prime split in $K/\mathbb{Q}$. Let $\{\mathfrak{a}\}$ be a set of representatives of $\mathrm{Cl}(\mathcal{O}_K)$ which are prime to $\mathfrak{N}$. Then there exists a unique continuous function $\hat{\Sigma}_{cc}(\mathfrak{N}) \to \mathbb{C}_p : \chi \mapsto \mathcal{L}_p(f, \chi)$ satisfying*

$$\mathcal{L}_p(f, \chi) = \left(\sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \cdot (\theta^j f)^\flat (\mathfrak{a} \star (A_0, t_0, \omega_{can})) \right)^2$$

for all $\chi \in \Sigma_{cc}^{(2)}(\mathfrak{N})$ of infinity type $(k + j, -j)$ with $j \geq 0$.

Bertolini, Darmon, and Prasanna's *p*-adic Waldspurger formula, which relates the special value of $\mathcal{L}_p(f, \chi)$ at some $\chi \in \Sigma_{cc}^{(1)}(\mathfrak{N}) \subset \hat{\Sigma}_{cc}(\mathfrak{N})$ to the *p*-adic Abel–Jacobi image of a certain generalized Heegner cycle, is the main result of [Bertolini et al. 2013].

Theorem 25 [Bertolini et al. 2013, Theorem 5.13]. *Suppose $\chi \in \Sigma_{cc}^{(1)}(\mathfrak{N})$ has infinity type $(k - 1 - j, 1 + j)$, where $0 \leq j \leq r = k - 2$. Then*

$$\frac{\mathcal{L}_p(f, \chi)}{\Omega_p^{2(r-2j)}} = (1 - \chi^{-1}(\bar{\mathfrak{p}}) a_p(f) + \chi^{-2}(\bar{\mathfrak{p}}) \varepsilon_f(p) p^{k-1})^2$$

$$\times \left(\frac{1}{\Gamma(j+1)} \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi \mathbb{N}_K)^{-1}(\mathfrak{a}) \cdot \mathrm{AJ}_{F'_{\mathfrak{p}'}}(\Delta_{\varphi_\mathfrak{a} \varphi_0})(\omega_f \wedge \omega_A^j \eta_A^{r-j}) \right)^2.$$

Here $\mathrm{AJ}_{F'_{\mathfrak{p}'}}$ is the p-adic Abel–Jacobi map defined in [Bertolini et al. 2013, Section 3.4], *and $\Delta_{\varphi_\mathfrak{a} \varphi_0}$ is the generalized Heegner cycle attached to $(\varphi_\mathfrak{a} \varphi_0, A) \in \mathrm{Isog}^{\mathfrak{N}}(A)$ as defined in Definition 22.*

Suppose χ is a finite order Hecke character on K. We define the Heegner point attached to χ as

$$P(\chi) := \sum_{\sigma \in \mathrm{Gal}(H_\mathfrak{N}/K)} \chi^{-1}(\sigma) \cdot \Delta^\sigma \in J_1(N)(H_\mathfrak{N}) \otimes_{\mathcal{O}_{E_f}} E_{f,\chi},$$

where Δ equals $[(A_0, t, \omega_0)] - (\infty) \in J_1(N)(H_\mathfrak{N})$ and the isomorphism class $[(A_0, t, \omega_0)]$ is viewed as a point in $X_1(N)(H_\mathfrak{N})$. The embedding $i_p : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ allows us to define the formal group logarithm on the formal group by

$$\log_{\omega_f} : \hat{J}_1(N)(\mathfrak{p}' \mathcal{O}_{F'_{\mathfrak{p}'}}) \to \mathbb{C}_p,$$

which we extend to a map

$$\log_{\omega_f} : J_1(N)(F'_{\mathfrak{p}'}) \otimes_{\mathcal{O}_{E_f}} E_{f,\chi} \to \mathbb{C}_p$$

by linearity.

For $k = 2$, we have $\mathrm{AJ}_{F'_{\mathfrak{p}'}}(P(\chi))(\omega_f) = \log_{\omega_f} P(\chi)$. Thus Theorem 25 becomes:

Theorem 26. *Suppose χ is a finite order Hecke character on K with $\chi \mathbb{N}_K \in \Sigma_{cc}^{(1)}(\mathfrak{N})$. Then*

$$\mathcal{L}_p(f, \chi \mathbb{N}_K) = (1 - \chi^{-1}(\bar{\mathfrak{p}}) p^{-1} a_p(f) + \chi^{-2}(\bar{\mathfrak{p}}) \varepsilon_f(p) p^{-1})^2 \log_{\omega_f}^2 P(\chi).$$

3.5. *Katz's p-adic L-function and Gross's factorization on the cyclotomic line.*
We can view any *p*-adic Hecke character $\chi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}_p^\times$ as a Galois character $\chi : \mathrm{Gal}(\bar{K}/K) \to \mathcal{O}_{\mathbb{C}_p}^\times$ via the Artin isomorphism of class field theory. Let $\mathfrak{C}$ be an integral ideal of $\mathcal{O}_K$ which is prime to *p*. Let $K(\mathfrak{C} p^r)$ denote the ray class field

of K of conductor $\mathfrak{C}p^r$ and let $K(\mathfrak{C}p^\infty) = \bigcup_r K(\mathfrak{C}p^r)$. Given a p-adic character χ arising from a type A_0 algebraic Hecke character, denote its complex counterpart by $(\chi)_\infty$. (Throughout this section only, we will make this distinction between complex and p-adic avatars.)

We recall Katz's p-adic L-function for CM fields (applied to our fixed imaginary quadratic field K), as well as Hida and Tilouine's extension [1993] to the case of general auxiliary conductor. Here we use the normalization found in [Gross 1980] (with $\delta = \sqrt{D_K}/2$ and so $\mathfrak{c} = 1$, in the notation of [Katz 1978, Theorem 5.3.0]). Fix a decomposition $\mathfrak{C} = \mathfrak{F}\mathfrak{F}_c\mathfrak{I}$, where $\mathfrak{F}\mathfrak{F}_c$ consists of split primes in K, $\bar{\mathfrak{F}}$ is a subset of $\mathfrak{F}_c$, and $\mathfrak{I}$ consists of inert or ramified primes in K. Recall our fixed identification $i : \mathbb{C} \xrightarrow{\sim} \mathbb{C}_p$, the prime $\mathfrak{p} \mid p$ determining $K \hookrightarrow \bar{\mathbb{Q}}_p$, and the periods Ω_p and Ω_∞ defined in Section 3.4.

Theorem 27 ([Katz 1978]; see also [Hida and Tilouine 1993]). *There exists a unique p-adic analytic function $\chi \mapsto L_p(\chi, 0)$ for $\chi : \mathrm{Gal}(K(\mathfrak{C}p^\infty)/K) \to \mathbb{C}_p^\times$ which satisfies (under our fixed identification $i : \mathbb{C} \xrightarrow{\sim} \mathbb{C}_p$)*

$$L_p(\chi, 0) = 4 \, \mathrm{Local}_{\mathfrak{p}}(\chi)(-1)^{k_1+k_2} \left(\frac{\Omega_p}{\Omega_\infty}\right)^{k_1-k_2} \left(\frac{2\pi i}{\sqrt{D_K}}\right)^{-k_2}$$

$$\times (k_1 - 1)!(1 - \chi(\bar{\mathfrak{p}}))(1 - \check{\chi}(\bar{\mathfrak{p}}))L(\chi, 0) \prod_{v \mid \mathfrak{C}} (1 - \chi(v))$$

for characters χ with infinity type $(-k_1, -k_2)$, where $k_1 \geq 1$ and $k_2 \leq 0$, and such that $\mathfrak{f}(\chi)$ is divisible by all the prime factors of $\mathfrak{F}$. Here $\mathrm{Local}_{\mathfrak{p}}(\chi)$ is a complex scalar associated with our fixed embedding $K \hookrightarrow \bar{\mathbb{Q}}_p$, as in [Katz 1978]. (We have in fact that $\mathrm{Local}_{\mathfrak{p}}(\chi) = 1$ if χ is unramified at $\mathfrak{p}$.)

Recall the dual character $\check{\chi}$ defined by $\check{\chi}(\mathfrak{a}) = \chi^{-1}(\bar{\mathfrak{a}})\mathbb{N}_K(\mathfrak{a})$. The function $L_p(\chi, 0)$ satisfies the functional equation

$$W((\chi)_\infty, \sqrt{D_K})L_p(\check{\chi}, 0) = L_p(\chi, 0),$$

where $W((\chi)_\infty, \delta)$ is given by

$$W((\chi)_\infty, \delta) = \prod_{v \mid \mathfrak{F}} G((\chi)_{\infty,v}^{-1}, \bar{\delta}) \prod_{v \mid \mathfrak{F}_c} G((\chi)_{\infty,\bar{v}}^{-1}, \delta) \prod_{v \mid \mathfrak{I}} G((\chi)_{\infty,v}^{-1}, \delta),$$

$$G((\chi)_{\infty,v}, \delta) = (\chi)_{\infty,v}(\pi_v^{-e}) \sum_{u \in (\mathcal{O}_{K,v}/\pi_v^e \mathcal{O}_{K,v})^\times} (\chi)_{\infty,v}(u)\Psi_{K,v}(-u\pi_v^{-e}\delta^{-1}),$$

e is the exponent of v in $\mathfrak{f}(\chi)$, π_v is a local uniformizer of K_v, and $\Psi_K : \mathbb{A}_K \to \mathbb{C}$ is the standard additive character normalized so that $\Psi_{K,\infty}(x_\infty) = \exp(2\pi i \, \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(x_\infty))$.

Henceforth, set

$$G((\chi)_\infty, \delta) = \prod_{v \mid \mathfrak{F}} G((\chi)_{\infty,v}, \delta).$$

Now define the *p*-adic *L*-function

$$L_p(\chi, s) := L_p(\chi \langle \mathbb{N}_K \rangle^s, 0).$$

Gross gives the following factorization of L_p along the cyclotomic line.

Theorem 28 [Gross 1980]. *In the situation of Theorem 27, suppose that $\mathfrak{F}_c = \bar{\mathfrak{F}}$, $\mathfrak{I} = 1$ and $\mathfrak{C} = f\mathcal{O}_K = \mathfrak{F}\bar{\mathfrak{F}}$, where $f \in \mathbb{Z}_{>0}$. Suppose $\chi : \mathrm{Gal}(K(\mu_{fp^\infty})/\mathbb{Q}) \to \mathbb{C}_p^\times$ is a continuous p-adic Galois character which is trivial on complex conjugation (and so corresponds to an even p-adic Hecke character), and let $\chi_{/K}$ be the restriction of χ to $\mathrm{Gal}(K(\mu_{fp^\infty})/K)$. Then*

$$\frac{\langle f \rangle^s}{\prod_{\ell \mid f} \chi_\ell^{-1}(-\sqrt{D_K})\mathfrak{g}_\ell(\chi)} L_p(\chi_{/K}, s) = L_p(\chi \varepsilon_K \omega, s) L_p(\chi^{-1}, 1 - s)$$

for $s \in \mathbb{Z}_p$, where $f \in \mathbb{Z}_{>0}$ is viewed as $f = \omega(f)\langle f \rangle \in \mu_{2(p-1)} \times (1 + 2p\mathbb{Z}_p) = \mathbb{Z}_p^\times$, and on the right are Kubota–Leopoldt p-adic L-functions for p-adic Hecke characters over $\mathbb{Q}$.

Remark 29. Gross [1980] originally proves Theorem 28 for auxiliary conductor $f = 1$, even though his proof translates *mutatis mutandis* to the case of arbitrary f. The general auxiliary conductor version of the theorem seems to be widely present in the literature, although the author has not been able to locate a complete proof. Thus, for the sake of completeness, we give a proof of Theorem 28, following Gross's method. We will first need a lemma.

Lemma 30. *In the situation of Theorem 27, suppose that $\mathfrak{F}_c = \bar{\mathfrak{F}}$, $\mathfrak{I} = 1$ and $\mathfrak{C} = f\mathcal{O}_K = \mathfrak{F}\bar{\mathfrak{F}}$. Suppose $\chi = \check{\chi} \circ \mathbb{N}_K$ for some Hecke character $\check{\chi}$ over $\mathbb{Q}$. Then*

$$W((\chi)_\infty, \delta) = \frac{G((\chi)_\infty^{-1}, \bar{\delta})}{G((\check{\chi})_\infty^{-1}, -\bar{\delta})}.$$

Proof. Since $\chi = \check{\chi} \circ \mathbb{N}_K$, we have $\chi_v(x) = \chi_{\bar{v}}(\bar{x})$ for any place v of K. For each $v \mid \mathfrak{F}\bar{\mathfrak{F}}$, since $K_v = \mathbb{Q}_\ell$ (where ℓ is the rational prime below v), we can choose representatives $\{u\}$ of $(\mathcal{O}_K/\pi_v^e\mathcal{O}_K)^\times = (\mathbb{Z}/\ell^e\mathbb{Z})^\times$ such that $\bar{u} = u$ and local uniformizers π_v such that $\overline{\pi_v} = \pi_v$. (This is accomplished by replacing π_v with $\pi_v\overline{\pi_v}$ if needed.)

Thus, we have, for any $v \mid \mathfrak{F}$,

$$
\begin{aligned}
G((\check{\chi})_{\infty,v}^{-1}, \delta) \\
&= (\check{\chi})_{\infty,v}^{-1}(\pi_v^{-e}) \sum_{u \in (\mathcal{O}_{K,v}/\pi_v^e \mathcal{O}_{K,v})^\times} (\check{\chi})_{\infty,v}^{-1}(u) \Psi_{K,v}(-u\pi_v^{-e}\delta^{-1}) \\
&= (\mathbb{N}_K)_{\infty,v}^{-1}(\pi_v^{-e})(\chi)_{\infty,\bar{v}}(\overline{\pi_v^{-e}}) \sum_{u \in (\mathcal{O}_{K,v}/\pi_v^e \mathcal{O}_{K,v})^\times} (\mathbb{N}_K)_{\infty,v}^{-1}(u)(\chi)_{\infty,\bar{v}}(\bar{u}) \overline{\Psi_{K,v}(\overline{u\pi_v^{-e}\delta^{-1}})} \\
&= (\mathbb{N}_K)_{\infty,v}^{-1}(\pi_v^{-e})(\chi)_{\infty,v}(\pi_v^{-e}) \overline{\sum_{u \in (\mathcal{O}_{K,v}/\pi_v^e \mathcal{O}_{K,v})^\times} (\chi)_{\infty,v}^{-1}(u) \Psi_{K,v}(u\pi_v^{-e}\overline{\delta^{-1}})} \\
&= (\chi)_{\infty,v}(\pi_v^{-e}) \left(\sum_{u \in (\mathcal{O}_{K,v}/\pi_v^e \mathcal{O}_{K,v})^\times} (\chi)_{\infty,v}^{-1}(u) \Psi_{K,v}(u\pi_v^{-e}\overline{\delta^{-1}}) \right)^{-1} \\
&= \left(G((\chi)_{\infty,v}^{-1}, -\bar{\delta}) \right)^{-1},
\end{aligned}
$$

where in the penultimate equality, we have used the fact that

$$
\left| \sum_{u \in (\mathcal{O}_{K,v}/\pi_v^e \mathcal{O}_{K,v})^\times} (\chi)_{\infty,v}^{-1}(u) \Psi_{K,v}(-u\pi_v^{-e}\overline{\delta^{-1}}) \right|^2 = (\mathbb{N}_K)_{\infty,v}(\pi_v^{-e}).
$$

Now simply note that, by definition of $W((\chi)_\infty, \delta)$ and the above computation,

$$
W((\chi)_\infty, \delta) = \prod_{v \mid \mathfrak{F}} G((\chi)_{\infty,v}^{-1}, \bar{\delta}) \prod_{v \mid \mathfrak{F}} G((\chi)_{\infty,v}^{-1}, \delta) = \frac{G((\chi)_\infty^{-1}, \bar{\delta})}{G((\check{\chi})_\infty^{-1}, -\bar{\delta})}. \qquad \square
$$

Proof of Theorem 28. Interpreting the statement as an assertion about p-adic measures, and proceeding as in [Gross 1980] using Lemma 1.1 of loc. cit., it suffices to prove the theorem at $s = 0$ and when χ is of finite order.

Let χ be unramified at each place dividing D_K. Then $\chi : \mathrm{Gal}(K(\mu_{fp^r})/\mathbb{Q}) \to \mathbb{C}_p^\times$ is an even Dirichlet character, where $fp^r \mathcal{O}_K = \mathfrak{f}(\chi_{/K})$, $(f, p) = 1$ and $fp^r > 1$. Let w_{fp^r} denote the number of roots of unity in $K^\times$ congruent to 1 (mod fp^r), and let $\mathrm{Cl}(fp^r)$ denote the ray class group of $\mathcal{O}_K$ of modulus $fp^r \mathcal{O}_K$. Recall our fixed embeddings $i_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ compatible with the identification $i : \mathbb{C} \xrightarrow{\sim} \mathbb{C}_p$. For $a \in (\mathbb{Z}/fp^r)^\times$, let

$$
C_{fp^r}(a)_\infty = 1 - e^{\frac{-2\pi i a}{fp^r}}, \quad C_{fp^r}(a) = i_\infty^{-1}(C_{fp^r}(a)_\infty), \quad C_{fp^r}(a)_p = i^{-1}(C_{fp^r}(a)_\infty).
$$

Further, let $E_{fp^r}(c)_\infty \in \overline{\mathbb{Q}}^\times \subset \mathbb{C}^\times$ be the "elliptic units" of [Robert 1973], and let

$$
E_{fp^r}(c) = i_\infty^{-1}(E_{fp^r}(c)_\infty), \quad E_{fp^r}(c)_p = i(E_{fp^r}(c)_\infty).
$$

Now, for $a \in (\mathbb{Z}/fp^r)^\times$, choose $c \in \mathrm{Cl}(fp^r)$ so that $\mathrm{Nm}_{K/\mathbb{Q}}(c) \equiv a \pmod{fp^r}$, and let

$$F_{fp^r}(a) = \mathrm{Nm}_{K(fp^r)/K(\mu_{fp^r})}(E_{fp^r}(c)).$$

Finally, for $a \in A = (\mathbb{Z}/fp^r)^\times/\{\pm 1\}$, let

$$F^+(a) = F_{fp^r}(a) F_{fp^r}(-a), \quad C^+(a) = C_{fp^r}(a) C_{fp^r}(-a).$$

Note that in our situation, for any $s \in \mathbb{Z}_p$,

$$G((\chi_{/K}\langle\mathbb{N}_K\rangle^s)_\infty^{-1}, -\sqrt{D_K}) = \prod_{v \mid \mathfrak{F}} G((\chi_{/K}\langle\mathbb{N}_K\rangle^s)_{\infty,v}^{-1}, -\sqrt{D_K})$$

$$= \langle f \rangle^{-s} \prod_{\ell \mid f} \mathfrak{g}_\ell(\chi)\chi_\ell^{-1}(\sqrt{D_K}),$$

where f is viewed as in $\mathbb{Z}_p^\times$. Hence, using the special value formulas from [Katz 1976, Formulas 10.4.9–10.4.12] (suitably modified with respect to the normalization of the *p*-adic *L*-function in [Gross 1980]) we have

$$\frac{1}{\prod_{\ell \mid f} \chi_\ell^{-1}(-\sqrt{D_K})\mathfrak{g}_\ell(\chi)} L_p(\chi_{/K}, 0)$$

$$= \frac{\prod_{\ell \mid f} \chi_\ell(-1)}{G((\chi_{/K})_\infty^{-1}, -\sqrt{D_K})} L_p(\chi_{/K}, 0)$$

$$= -\frac{1}{3fp^r w_{fp^r}}(1 - \chi_{/K}(\bar{\mathfrak{p}}))\left(1 - \frac{\chi_{/K}^{-1}(\mathfrak{p})}{p}\right)\frac{\mathfrak{g}(\chi^{-1})}{fp^r}\sum_{a \in A} \chi(a) \log_p F^+(a)_\mathfrak{p},$$

and

$$L_p(\chi\varepsilon_K\omega, 0) = -(1 - \chi\varepsilon_K(p))B_{1,\chi\varepsilon_K},$$

$$L_p(\chi^{-1}, 1) = -\left(1 - \frac{\chi^{-1}(p)}{p}\right)\frac{\mathfrak{g}(\chi^{-1})}{fp^r}\sum_{a \in A} \chi(a) \log_p C^+(a)_\mathfrak{p}.$$

On the complex side, we have (by Kronecker's second limit formula; see [Stark 1977])

$$L'((\chi_{/K})_\infty, 0) = -\frac{1}{6fp^r w_{fp^r}}\sum_{a \in A}(\chi)_\infty(a) \log F^+(a)_\infty,$$

$$L((\chi)_\infty\varepsilon_K, 0) = -B_{1,(\chi)_\infty\varepsilon_K},$$

$$L((\chi)_\infty^{-1}, 1) = -\frac{\mathfrak{g}((\chi)_\infty^{-1})}{fp^r}\sum_{a \in A}(\chi)_\infty(a) \log C^+(a)_\infty,$$

and thus, by the functional equation, we have

$$L'((\chi)_\infty, 0) = -\frac{1}{2} \sum_{a \in A} (\chi)_\infty(a) \log C^+(a)_\infty,$$

where $\log : \mathbb{R}^\times \to \mathbb{R}$ is the map $x \mapsto \log |x|$. Now we claim that

$$\frac{1}{\prod_{\ell \mid f} \chi_\ell^{-1}(-\sqrt{D_K}) \mathfrak{g}_\ell(\chi)} L_p(\chi_{/K}, 0) = L_p(\chi \varepsilon_K \omega, 0) L_p(\chi^{-1}, 1).$$

Note that

$$(1 - \chi_{/K}(\bar{\mathfrak{p}})) \left(1 - \frac{\chi_{/K}^{-1}(\mathfrak{p})}{p}\right) = (1 - \chi \varepsilon_K(p)) \left(1 - \frac{\chi^{-1}(p)}{p}\right)$$

since $\varepsilon_K(p) = 1$. If this quantity is 0 then the above identity of special values of p-adic L-functions is trivial, so assume this is not the case. By the above formulas, this identity is equivalent to

$$-3 f p^r w_{f p^r} B_{1,\chi \varepsilon_K} \sum_{a \in A} \chi(a) \log_p C^+(a)_p = \sum_{a \in A} \chi(a) \log_p F^+(a)_p.$$

From the complex factorization

$$L((\chi_{/K})_\infty, s) = L((\chi)_\infty \varepsilon_K, s) L((\chi)_\infty, s),$$

we get, by taking the derivative at $s = 0$,

$$L'((\chi_{/K})_\infty, 0) = L((\chi)_\infty \varepsilon_K, s) L'((\chi)_\infty, 0),$$

which is equivalent, by the above formulas, to

$$-3 f p^r w_{f p^r} B_{1,(\chi)_\infty \varepsilon_K} \sum_{a \in A} (\chi)_\infty(a) \log C^+(a)_\infty = \sum_{a \in A} (\chi)_\infty(a) \log F^+(a)_\infty.$$

Now $C^+(a)_\infty$ and $F^+(a)_\infty$ are p-units in the field $M_\infty = \mathbb{Q}\left(\cos \frac{2\pi i}{f p^r}\right)$. Let $E(M_\infty)$ denote the group of all p-units viewed as a finitely generated subgroup of $\mathbb{R}^\times$. Then we claim that the identity

$$-3 f p^r w_{f p^r} B_{1,(\chi)_\infty \varepsilon_K} \sum_{a \in A} (\chi)_\infty(a) \otimes C^+(a)_\infty = \sum_{a \in A} (\chi)_\infty(a) \otimes F^+(a)_\infty$$

holds in $\mathbb{C} \otimes_{\mathbb{Z}} E(M_\infty)$. The representation of $A = \mathrm{Gal}(M_\infty/\mathbb{Q})$ on this complex vector space is isomorphic to the regular representation, and the elements

$$\sum_{a \in A} (\chi)_\infty(a) C^+(a)_\infty, \quad \sum_{a \in A} (\chi)_\infty(a) F^+(a)_\infty$$

are both in the $(\chi)_\infty^{-1}$-eigenspace. Because this eigenspace is one-dimensional, the elements above differ by a complex scalar. Applying the $\mathbb{C}$-linear map

$$\mathbb{C} \otimes_{\mathbb{Z}} E(M_\infty) \xrightarrow{1 \otimes \log} \mathbb{R} \otimes \mathbb{C} \xrightarrow{\text{mult}} \mathbb{C}$$

and considering the identity above concerning special values of complex *L*-functions, we identify this scalar as $-3 f p^r w_{fp^r} B_{1,(\chi)_\infty \varepsilon_K}$. Thus our identity in $\mathbb{C} \otimes_{\mathbb{Z}} E(M_\infty)$ holds. Now applying our identification $i : \mathbb{C} \xrightarrow{\sim} \mathbb{C}_p$, we obtain the identity

$$-3 f p^r w_{fp^r} B_{1,\chi \varepsilon_K} \sum_{a \in A} \chi(a) \otimes C^+(a)_\infty = \sum_{a \in A} \chi(a) \otimes F^+(a)_\infty$$

in $\mathbb{C}_p \otimes E(M_p)$, where $M_p = i(M_\infty)$. Finally, applying the homomorphism

$$\mathbb{C}_p \otimes \mathbb{C}_p \xrightarrow{1 \otimes \log_p} \mathbb{C}_p \otimes \mathbb{C}_p \xrightarrow{\text{mult}} \mathbb{C}_p,$$

we obtain our identity of special values of *p*-adic *L*-functions. Now, to extend to general χ (including when χ is ramified at places dividing D_K), we use the functional equation of Theorem 27 and Lemma 30:

$$\frac{\langle f \rangle^s}{\prod_{\ell \mid f} \chi_\ell^{-1}(-\sqrt{D_K}) \mathfrak{g}_\ell(\chi)} L_p(\chi_{/K}, s)$$

$$= \frac{1}{G((\chi_{/K} \langle \mathbb{N}_K \rangle^s)_\infty^{-1}, -\sqrt{D_K})} L_p(\chi_{/K}, s)$$

$$= \frac{W((\chi_{/K} \langle \mathbb{N}_K \rangle^s)_\infty, \sqrt{D_K})}{G((\chi_{/K} \langle \mathbb{N}_K \rangle^s)_\infty^{-1}, -\sqrt{D_K})} L_p(\chi_{/K}^{-1} \omega_K^{-1}, 1-s)$$

$$= \frac{1}{G((\check{\chi}_{/K} \langle \mathbb{N}_K \rangle^{-s})_\infty^{-1}, \sqrt{D_K})} L_p((\chi \omega \varepsilon_K)_{/K}^{-1}, 1-s)$$

$$= \frac{\langle f \rangle^{1-s}}{\prod_{\ell \mid f} (\chi \omega \varepsilon_K)_\ell(-\sqrt{D_K}) \mathfrak{g}_\ell((\chi \omega \varepsilon_K)^{-1})} L_p((\chi \omega \varepsilon_K)_{/K}^{-1}, 1-s).$$

Here $\check{\chi}_{/K}$ denotes the dual of $\chi_{/K}$ and we have used the fact that, for $\ell \mid f$, the characters ω and ε_K are unramified at ℓ, as well as the equalities $\varepsilon_{K,\ell}(\ell) = 1$, since ℓ is split in K, and $(\varepsilon_K)_{/K} = 1$. $\qquad\square$

3.6. Eisenstein descent. We now define the notion of cuspforms which have *Eisenstein descent*. In this setting, we prove a congruence between the BDP *p*-adic *L*-function and the Katz *p*-adic *L*-function on the anticyclotomic line.

Definition 31. Fix a global or local field M containing E_f and fix an integral ideal $\mathfrak{m}$ of $\mathcal{O}_M$. Suppose (N_+, N_-, N_0) is a triple of pairwise coprime positive integers, where $N = N_+ N_- N_0$, $N_+ N_-$ is squarefree, N_0 is squarefull, and ψ_1 and ψ_2 are Dirichlet characters over $\mathbb{Q}$. We say that a normalized newform $f = \sum_{n=1}^{\infty} a_n q^n \in$

$S_k(\Gamma_0(N), \varepsilon_f)$, where k is a positive integer, has *partial Eisenstein descent of type* $(\psi_1, \psi_2, N_+, N_-, N_0)$ *(over M)* mod $\mathfrak{m}$ if $\psi_1\psi_2 = \varepsilon_f$ and if we have

(1) $a_\ell \equiv \psi_1(\ell) + \psi_2(\ell)\ell^{k-1} \pmod{\mathfrak{m}}$ for $\ell \nmid N$,

(2) $a_\ell \equiv \psi_1(\ell) \pmod{\mathfrak{m}}$ for $\ell \mid N_+$,

(3) $a_\ell \equiv \psi_2(\ell)\ell^{k-1} \pmod{\mathfrak{m}}$ for $\ell \mid N_-$,

(4) $a_\ell \equiv 0 \pmod{\mathfrak{m}}$ for $\ell \mid N_0$.

If, further, f satisfies

$$(5) \quad \delta_{\psi_1=1}\frac{B_{1,\psi_2} B_{k,\psi_1}}{k} \prod_{\ell \mid N_+}(1 - \psi_1(\ell)\ell^{k-1}) \prod_{\ell \mid N_-}(1 - \psi_2(\ell))$$
$$\times \prod_{\ell \mid N_0}(1 - \psi_1(\ell)\ell^{k-1})(1 - \psi_2(\ell)) \equiv 0 \pmod{\mathfrak{m}},$$

where

$$\delta_{\psi=1} := \begin{cases} 1 & \text{if } \psi = 1, \\ 0 & \text{otherwise,} \end{cases}$$

then we say f has *(full) Eisenstein descent of type* $(\psi_1, \psi_2, N_+, N_-, N_0)$ mod $\mathfrak{m}$.

Remark 32. Recall, for $k \geq 2$, that the Eisenstein series $E_k^{\psi_1,\psi_2,(N)}$ is an element of $N_k(\Gamma_0(N), \psi_1\psi_2)$. (When either $k > 2$ or $\psi_1 \neq 1$ or $\psi_2 \neq 1$, then in fact $E_k^{\psi_1,\psi_2,(N)}$ is an element of $M_k(\Gamma_0(N), \psi_1\psi_2)$.) It has q-expansion

$$E_k^{\psi_1,\psi_2,(N)}(q)$$

$$:= -\delta_{\psi_1=1} L^{(N_-N_0)}(\psi_2, 0) L^{(N_+N_0)}(\psi_1, 1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}^{\psi_1,\psi_2,(N)}(n)q^n$$

$$= -\delta_{\psi_1=1}\frac{B_{k,\psi_1}}{2k} \prod_{\ell \mid N_+}(1 - \psi_1(\ell)\ell^{k-1}) \prod_{\ell \mid N_-}(1 - \psi_2(\ell)) \prod_{\ell \mid N_0}(1 - \psi_1(\ell)\ell^{k-1})(1 - \psi_2(\ell))$$

$$+ \sum_{n=1}^{\infty} \sigma_{k-1}^{\psi_1,\psi_2,(N)}(n)q^n,$$

where $L^{(N)}(\psi, s)$ denotes the L-function of a Dirichlet character ψ with Euler factors at primes $\ell \mid N$ removed, and where

$$\sigma_{k-1}^{\psi_1,\psi_2,(N)}(n) := \sum_{\substack{0 < d \mid n \\ (d,N_+)=1 \\ (n/d,N_-)=1 \\ (n,N_0)=1}} \psi_1(n/d)\psi_2(d)d^{k-1}.$$

Here, in keeping with our conventions, $\psi(m) = 0$ if $(m, \mathfrak{f}(\psi)) \neq 1$. Then for $f \in S_k(\Gamma_0(N), \varepsilon_f)$ to have partial Eisenstein descent of type $(\psi_1, \psi_2, N_+, N_-, N_0)$

at $\lambda \mid p$ is equivalent to having

$$\theta^j f(q) \equiv \theta^j E_k^{\psi_1,\psi_2,(N)}(q) \pmod{\mathfrak{m}}$$

for all $j \geq 1$. When f has full Eisenstein descent, this congruence holds for $j \geq 0$.

Remark 33. Suppose we are given $f \in S_k(\Gamma_0(N), \varepsilon_f)$ with partial Eisenstein descent of type $(\psi_1, \psi_2, N_+, N_-, N_0)$ over M mod $\mathfrak{m}$, in the sense of Definition 31. In many situations, (5) is forced to hold *a priori* so that f automatically has full Eisenstein descent. Suppose $\mathfrak{m} \neq \mathcal{O}_M$ (for otherwise, the conditions of Definition 31 are vacuous).

If ψ_1 is nontrivial, then $\delta_{\psi=1} = 0$ and (5) holds. Now suppose that $\psi_1 = 1$. If k is odd, then $B_{k,\psi_1} = B_k = 0$, again forcing (5) to hold. Suppose k is even. Let $\lambda \mid \mathfrak{m}$ be a prime ideal of residual characteristic not equal to 2. By parts (3) and (1) of Theorem 34, we have $\psi_1 \psi_2 = \varepsilon_f$; in particular, we have $\psi_2(-1) = \varepsilon_f(-1) = (-1)^k = 1$. Hence ψ_2 is even, and so $B_{1,\psi_2} = 0$ unless $\psi_2 = 1$. Now further suppose that $\psi_2 = 1$. Then (5) is still forced to hold unless $N_- N_0 = 1$. Now suppose $N_- N_0 = 1$. Let $\lambda \mid \mathfrak{m}$ be a prime ideal of residual characteristic p. Then conditions (1)–(4) still imply

$$\theta f(q) \equiv \theta E_k^{\psi_1,\psi_2,(N)}(q) \pmod{\lambda}.$$

Suppose $p > k + 1$, so that, by [Serre 1973, Corollary 3, p. 326], θ is injective on mod-λ modular forms. Then the above congruence implies

$$f(q) \equiv E_k^{\psi_1,\psi_2,(N)}(q) \pmod{\lambda}.$$

Hence, if $\mathfrak{m}$ has order 0 or 1 at every prime of $\mathcal{O}_M$ and if the residual characteristic p of every prime $\lambda \mid \mathfrak{m}$ satisfies $p > k + 1$, then (5) is forced to hold. (See [Billerey and Menares 2013, Theorem 4.1] where a similar argument is given.) In particular,

$$\frac{B_k}{2k} \prod_{\ell \mid N_+} (1 - \ell^{k-1}) \equiv 0 \pmod{\mathfrak{m}}.$$

When $k = 2$, we have

$$\frac{1}{24} \prod_{\ell \mid N_+} (1 - \ell) \equiv 0 \pmod{\mathfrak{m}},$$

and therefore there exists at least one $\ell \mid N_+ = N$ such that $\ell \equiv 1 \pmod{\mathfrak{m}}$, i.e., $\ell \equiv 1 \pmod{\mathfrak{m} \cap \mathbb{Z}}$.

Suppose we have a normalized eigenform $f(q) = \sum_{n=0}^{\infty} a_n q^n \in M_k(\Gamma_0(N), \varepsilon_f)$. Again let M be a number field containing E_f. Let k_λ denote the residue field of $\mathcal{O}_M$ at a prime $\lambda \mid p$. By a construction of Deligne [1971] we can attach a unique

semisimple p-adic Galois representation $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(M_\lambda)$ unramified outside pN and such that $\rho_f(\mathrm{Frob}_\ell)$ has characteristic polynomial

$$T^2 - a_\ell T + \varepsilon_f(\ell)\ell^{k-1}$$

for all $\ell \nmid pN$. Taking a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable lattice and the reduction mod λ, we get a representation $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(k_\lambda)$ (whose semisimplification is independent of the choice of lattice). By Theorem 3 of [Atkin and Lehner 1970], we have $a_\ell = \pm\ell^{k/2-1}$ for $\ell \parallel N$, and $a_\ell = 0$ for $\ell^2 \mid N$.

We have the following characterization of partial Eisenstein descent mod λ. See [Billerey and Menares 2013, Theorem 4.1] for a similar result to part (2) below. The elliptic curves case of part (1) was essentially done in [Serre 1972].

Theorem 34. *Suppose $f \in S_k(\Gamma_0(N), \varepsilon_f)$ is a normalized newform, and define $\bar{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(k_\lambda)$ to be* (*the semisimplification of*) *the mod-λ reduction of the associated semisimple Galois representation ρ_f. Then the following hold*:

(1) *Suppose $\bar{\rho}_f$ is reducible. Then $\bar{\rho}_f \cong k_\lambda(\tilde{\psi}_1) \oplus k_\lambda(\tilde{\psi}_2\omega^{k-1})$, where we have $\tilde{\psi}_i = \psi_i \pmod{\lambda}$, $i = 1, 2$, for some Dirichlet characters ψ_1 and ψ_2 over $\mathbb{Q}$ with $\psi_1\psi_2 = \varepsilon_f$.*

(2) *Suppose $\bar{\rho}_f$ is reducible. Then, for all $\ell \parallel N$, either $a_\ell \equiv \psi_1(\ell) \pmod{\lambda}$ and $a_\ell \equiv \psi_1^{-1}(\ell)\ell^{k-2} \pmod{\lambda}$ and $\ell^{k-2} \equiv \psi_1^2(\ell) \pmod{\lambda}$, or $a_\ell \equiv \psi_2(\ell)\ell^{k-1} \pmod{\lambda}$ and $a_\ell \equiv \psi_2^{-1}(\ell)\ell^{-1} \pmod{\lambda}$ and $\ell^k \equiv \psi_2^{-2}(\ell) \pmod{\lambda}$.*

(3) *Let N_+ denote any product of all primes $\ell \parallel N$ satisfying $a_\ell \equiv \psi_1(\ell) \pmod{\lambda}$ and N_- any product of $\ell \parallel N$ satisfying $a_\ell \equiv \psi_2(\ell)\ell^{k-1} \pmod{\lambda}$, such that N_+N_- is the squarefree part of N (so that, in particular, $(N_+, N_-) = 1$). Let N_0 be the squarefull part of N. Then $\bar{\rho}_f$ is reducible if and only if f has partial Eisenstein descent of type $(\psi_1, \psi_2, N_+, N_-, N_0)$ over M_λ mod λ.*

Proof. (1) Since $\bar{\rho}_f$ is reducible and semisimple, we can write $\bar{\rho}_f = k_\lambda(\chi_1) \oplus k_\lambda(\chi_2)$, where $\chi_1, \chi_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to k_\lambda^\times$. Hence $\chi_1\chi_2 = \det(\bar{\rho}_f) = \varepsilon_f\omega^{k-1}$, and so for our statement it suffices to show that one of χ_1, χ_2 is unramified outside the squarefull part of N (since $\mathfrak{f}(\varepsilon_f)$ divides the squarefull part of N). Since $\bar{\rho}_f$ is unramified outside pN, clearly both χ_1, χ_2 are unramified outside pN. For $\ell \parallel N$, the local representation $\bar{\rho}_{f,\ell}$ (i.e., the restriction of $\bar{\rho}_{f,\ell}$ to the decomposition group $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$) has conductor ℓ. Thus the corresponding automorphic representation π_ℓ of ρ_ℓ has conductor ℓ, and so, by the classification of admissible representations of GL_2 over local fields (see [Gelbart 1975, p. 73]), at most one of χ_1 and χ_2 is ramified at ℓ. Thus χ_1, χ_2 are unramified inside the squarefree part of N. Finally, since $\bar{\rho}_{f,p}$ is reducible, by a theorem of Deligne (see [Gross 1990, Introduction]), a_p is not

congruent to 0 mod λ and $\bar{\rho}_{f,p}$ is of the form

$$\begin{pmatrix} \omega^{k-1}\mu_p(\varepsilon_f(p)/a_p) & * \\ 0 & \mu_p(a_p) \end{pmatrix},$$

where $\mu_p(\alpha)$ is the unramified character of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ taking Frob_p to α. Hence exactly one of χ_1, χ_2 is ramified at p.

Putting this all together, we see that $\{\chi_1, \chi_2\} = \{\psi_1 \bmod \lambda, \psi_2\omega^{k-1} \bmod \lambda\}$ for some Dirichlet characters ψ_1 and ψ_2 with $\psi_1\psi_2 = \varepsilon_f$, and so we are done.

(2) It is a theorem of Langlands (see [Loeffler and Weinstein 2012, Proposition 2.8]) that, for $\ell \parallel N$, $\bar{\rho}_{f,\ell}$ is of the form

$$\begin{pmatrix} \omega_\ell^{k/2}\mu_\ell(\varepsilon_f(\ell)\ell^{k/2-1}/a_\ell) & * \\ 0 & \omega_\ell^{k/2-1}\mu_\ell(a_\ell/\ell^{k/2-1}) \end{pmatrix},$$

where ω_ℓ is the localization of ω to ℓ. Thus by (1), we have

$$\{\psi_{1,\ell} \bmod \lambda, \psi_{2,\ell}\omega^{k-1} \bmod \lambda\} = \{\omega_\ell^{k/2}\mu_\ell(\varepsilon_f(\ell)\ell^{k/2-1}/a_\ell), \omega_\ell^{k/2}\mu_\ell(a_\ell/\ell^{k/2-1})\}.$$

Note that $\mu_\ell(\ell^{k/2-1}/a_\ell)$ is a quadratic character.

Suppose first that $\psi_{1,\ell} \equiv \omega_\ell^{k/2}\mu_\ell(\varepsilon_f(\ell)\ell^{k/2-1}/a_\ell)$ (mod λ), and that $\psi_{2,\ell}\omega_\ell^{k-1} \equiv \omega_\ell^{k/2-1}\mu_\ell(\ell^{k/2-1}/a_\ell)$ (mod λ). Plugging in Frob_ℓ to both congruences, the first congruence implies $a_\ell \equiv \psi_{2,\ell}(\ell)\ell^{k-1} = \psi_2(\ell)\ell^{k-1}$ (mod λ), and the second congruence implies $a_\ell \equiv \psi_{2,\ell}^{-1}(\ell)\ell^{-1} = \psi_2^{-1}(\ell)\ell^{-1}$ (mod λ).

Suppose next that $\psi_{1,\ell} \equiv \omega_\ell^{k/2-1}\mu_\ell(a_\ell/\ell^{k/2-1})$ (mod λ), and that $\psi_{2,\ell}\omega_\ell^{k-1} \equiv \omega_\ell^{k/2}\mu_\ell(\varepsilon_f(\ell)\ell^{k/2-1}/a_\ell)$ (mod λ). Plugging in Frob_ℓ to both congruences, the first congruence implies both $a_\ell \equiv \psi_{1,\ell}(\ell) = \psi_1(\ell)$ (mod λ) and $a_\ell \equiv \psi_{1,\ell}^{-1}(\ell)\ell^{k-2} = \psi_1^{-1}(\ell)\ell^{k-2}$ (mod λ) (we get both since we have $\mu_\ell(a_\ell/\ell^{k/2-1}) = \mu_\ell^{-1}(a_\ell/\ell^{k/2-1})$), and the second congruence gives no new congruences.

(3) For $\ell \nmid pN$ we have $a_\ell = \mathrm{trace}(\bar{\rho}_f)(\mathrm{Frob}_\ell) \equiv \psi_1(\ell) + \psi_2(\ell)\ell^{k-1}$ (mod λ). For $\ell \mid N_+$ we have $a_\ell \equiv \psi_1(\ell)$ (mod λ), for $\ell \mid N_-$ we have $a_\ell \equiv \psi_2(\ell)\ell^{k-1}$ (mod λ), and for $\ell \mid N_0$ we have $a_\ell \equiv 0$ (mod λ). Finally, by the Cebotarev density theorem and continuity of $\mathrm{trace}(\bar{\rho}_f)$, we have $a_p = \mathrm{trace}(\bar{\rho}_f(\mathrm{Frob}_p)) \equiv \psi_1(p) + \psi_2(p)p^{k-1} \equiv \psi_1(p)$ (mod λ). Hence f has partial Eisenstein descent of type $(\psi_1, \psi_2, N_+, N_-, N_0)$ at $\lambda \mid p$.

If f has partial Eisenstein descent of type $(\psi_1, \psi_2, N_+, N_-, N_0)$ at $\lambda \mid p$, then for $\ell \nmid N$ we have $\mathrm{trace}(\bar{\rho}_f)(\mathrm{Frob}_\ell) \equiv \psi_1(\ell) + \psi_2(\ell)\ell^{k-1}$ (mod λ). Hence if $\bar{\rho} := k_\lambda(\psi_1) \oplus k_\lambda(\psi_2\omega^{k-1})$, then $\mathrm{trace}(\bar{\rho}_f)(\mathrm{Frob}_\ell) \equiv \mathrm{trace}(\bar{\rho})(\mathrm{Frob}_\ell)$ for all $\ell \nmid N$. Thus by the Cebotarev density theorem and continuity of trace, $\mathrm{trace}(\bar{\rho}_f)(g) \equiv \mathrm{trace}(\bar{\rho})(g)$ for all $g \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Hence, by the Brauer–Nesbitt theorem, $\bar{\rho}_f \cong \bar{\rho}$. □

For $k = 2$ and $M = E_f = \mathbb{Q}$, we note the following corollary.

Theorem 35. *Suppose $E/\mathbb{Q}$ is an elliptic curve and p is a prime such that $E[p]$ is a reducible mod-p Galois representation. Then the associated normalized newform $f_E \in S_2(\Gamma_0(N))$ has partial Eisenstein descent over $\mathbb{Q}_p$ mod $p\mathbb{Z}_p$.*

4. Proof of the main theorem

First, we examine complex L-values arising from twisted traces of Eisenstein series evaluated at CM points, analogous to such traces for normalized newforms interpolated by Bertolini, Darmon, and Prasanna's p-adic L-function (see Theorem 24). Parts of the calculation in Section 4.1 are implicit in [Hida and Tilouine 1993], but for our purposes which require explicit identities, and for the sake of completeness, we include the full calculation here.

4.1. *Twisted traces of Eisenstein series over CM points.* Let $k \geq 2$ be an integer, and let ψ_1, ψ_2 be two Dirichlet characters over $\mathbb{Q}$ with conductors u and t, respectively. (Here and throughout this section, for simplicity, we identify these ideals in $\mathbb{Z}$ with their unique positive rational integer generators.) We also assume that $ut = N'$ (where u and t are not necessarily coprime), and that $(\psi_1\psi_2)(-1) = (-1)^k$. Recall our Eisenstein series (see Remark 32)

$$E_k^{\psi_1,\psi_2}(\tau) := \delta_{\psi_1=1}\tfrac{1}{2}L(\psi_1, 1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}^{\psi_1,\psi_2}(n)q^n,$$

where $q = e^{2\pi i\tau}$ and

$$\sigma_{k-1}^{\psi_1,\psi_2}(n) = \sum_{0<d\,|\,n} \psi_1(n/d)\psi_2(d)d^{k-1}.$$

Note that the nebentypus of $E_k^{\psi_1,\psi_2}$ is $\varepsilon_{E_k^{\psi_1,\psi_2}} = \psi_1\psi_2$.

Recalling the Maass–Shimura derivative ∂ defined in Section 3.1, one checks by direct computation that

$$\partial^j E_k^{\psi_1,\psi_2}(\tau) = \frac{t^k\Gamma(k+j)}{2(2\pi i)^{k+j}\mathfrak{g}(\psi_2^{-1})} \sum_{c=0}^{u-1}\sum_{d=0}^{t-1}\sum_{e=0}^{u-1} \sum_{\substack{(m,n)\equiv \\ (ct,d+et)(N')}} \frac{\psi_1(c)\psi_2^{-1}(d)}{(m\tau+n)^{k+2j}}\left(\frac{|m\tau+n|^2}{\tau-\bar\tau}\right)^j,$$

with the last sum over $(m, n) \in \mathbb{Z}^2 \setminus \{0\}$ satisfying $(m, n) \equiv (ct, d + et) \pmod{N'}$.

Recall that under our Assumptions 1, D_K is taken to be odd. (The calculations for the even case are entirely analogous to those of the odd case, but we do not explicitly write them out here.) Given an integral primitive (i.e., having no rational integral divisors other than ± 1) ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we can write

$$\mathfrak{a} = \mathbb{Z}\frac{b+\sqrt{D_K}}{2} + \mathbb{Z}a,$$

where $a = |\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{a})|$ and $b^2 - 4ac = D_K$; the triple $(a, -b, c)$ determines the primitive positive definite binary quadratic form associated with the ideal class of $\mathfrak{a}$. We set

$$\tau_{\mathfrak{a}} := \frac{b + \sqrt{D_K}}{2a}$$

so that $\tau_{\mathfrak{a}} \in \mathcal{H}^+$ is the root of the dehomogenized quadratic form $a\tau^2 - b\tau + c = 0$ with positive imaginary part. We call $\tau_{\mathfrak{a}}$ a *CM point*. Note that $\langle \tau_{\mathfrak{a}}, 1 \rangle$ generates $\bar{\mathfrak{a}}^{-1}$. (Here, for $\tau \in \mathcal{H}^+$, we have $\langle \tau, 1 \rangle = \mathbb{Z}\tau + \mathbb{Z}$.)

Suppose that K satisfies the Heegner hypothesis with respect to N'. Fix an ideal $\mathfrak{N}'$ such that $\mathcal{O}_K/\mathfrak{N}' = \mathbb{Z}/N'$, and write

$$\mathfrak{N}' = \mathbb{Z}\frac{b_{N'} + \sqrt{D_K}}{2} + \mathbb{Z}N', \quad \mathfrak{a}\mathfrak{N}' = \mathbb{Z}\frac{b_{aN'} + \sqrt{D_K}}{2} + \mathbb{Z}aN',$$

where $b_{aN'}^2 - 4aN'c = D_K$ for some $c \in \mathbb{Z}$. Write $\mathfrak{N}' = \mathfrak{u}\mathfrak{t}$, where $\mathcal{O}_K/\mathfrak{u} = \mathbb{Z}/u$ and $\mathcal{O}_K/\mathfrak{t} = \mathbb{Z}/t$.

Suppose we have a Dirichlet character $\phi : (\mathbb{Z}/N')^{\times} \to \mathbb{C}^{\times}$. By the identification $\mathcal{O}_K/\mathfrak{N}' = \mathbb{Z}/N'$, we can view ϕ as a character $\phi : \mathbb{A}_K^{\times, \mathfrak{N}'} \twoheadrightarrow \prod_{v \mid \mathfrak{N}'}(\mathcal{O}_{K,v}/\mathfrak{N}'\mathcal{O}_{K,v})^{\times} \cong (\mathcal{O}_K/\mathfrak{N}')^{\times} \to \mathbb{C}^{\times}$, where $\mathbb{A}_K^{\times, \mathfrak{N}'}$ denotes the idèles prime to $\mathfrak{N}'$; when we view ϕ in this way, we will write $\phi(x \bmod \mathfrak{N}')$ for its value at $x \in \mathbb{A}_K^{\times, \mathfrak{N}'}$. Given a Hecke character χ over K of finite type $(\mathfrak{N}', \phi)$ and infinity type (j_1, j_2), recall that the associated Grossencharacter on ideals $\mathfrak{a}$ prime to $\mathfrak{N}'$ is given by

$$\chi(\mathfrak{a}) = \chi(x)\phi(x \bmod \mathfrak{N}')x_{\infty}^{j_1}\bar{x}_{\infty}^{j_2},$$

where $x \in \mathbb{A}_K^{\times, \mathfrak{N}'}$ is such that $\mathrm{ord}_v(x) = \mathrm{ord}_v(\mathfrak{a})$ for all finite places v. We consider the twisted trace

$$\sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\overline{\mathfrak{a}\mathfrak{N}'})\partial^j E_k^{\psi_1, \psi_2}(\tau_{\mathfrak{a}\mathfrak{N}'}),$$

where $\mathfrak{a}$ ranges over a set of primitive integral ideal representatives of $\mathrm{Cl}(\mathcal{O}_K)$ chosen to be prime to N', and where χ is of infinity type $(k + j, -j)$ and of finite type $(\mathfrak{N}', \psi_1\psi_2)$ (so that the above summands depend only on the ideal classes of the $\overline{\mathfrak{a}\mathfrak{N}'}$).

Suppose $\alpha = m(b_{aN'} + \sqrt{D_K})/(2aut) + n \in (\overline{\mathfrak{a}\mathfrak{u}})^{-1}$ with $(m, n) \equiv (ct, d + et)$ (mod N'). Then $au\alpha = m(b_{aN'} + \sqrt{D_K})/(2t) + aun \in \mathfrak{a}\mathfrak{u} \subset \mathcal{O}_K$ is mapped to $b_{aN'}c \in \mathbb{Z}/u$ under the identification $\mathcal{O}_K/\bar{\mathfrak{u}} = \mathbb{Z}/u$. We see this by writing $m = ct + qN'$ for some $q \in \mathbb{Z}$ and

$$au\alpha = \frac{mb_{aN'}}{t} - m\frac{b_{aN'} - \sqrt{D_K}}{2} + aun$$

$$= b_{aN'}c - m\frac{b_{aN'} - \sqrt{D_K}}{2} + qu \equiv b_{aN'}c \pmod{\bar{\mathfrak{u}}}.$$

We thus have $\psi_1((au\alpha) \mod \bar{\mathfrak{u}}) = \psi_1(b_{aN'}c)$. Since $b_{aN'} + \sqrt{D_K} \in \mathfrak{a}\mathfrak{N}'$, in particular we have $b_{aN'} \equiv -\sqrt{D_K} \pmod{\mathfrak{u}}$, meaning $\psi_1(b_{aN'}) = \psi_1(-\sqrt{D_K} \mod \mathfrak{u})$; henceforth we will write $\psi_1(-\sqrt{D_K}) = \psi_1(-\sqrt{D_K} \mod \mathfrak{u})$ for simplicity. On the other hand, note that α is mapped to $d \in \mathbb{Z}/\mathfrak{t}$ under the isomorphism $(\overline{\mathfrak{a}\mathfrak{u}})^{-1}/(\overline{\mathfrak{a}\mathfrak{u}})^{-1}\mathfrak{t} \cong \mathcal{O}_K/\mathfrak{t} = \mathbb{Z}/\mathfrak{t}$. Thus, $\psi_2(\overline{\mathfrak{a}\mathfrak{u}}(\alpha) \mod \mathfrak{t}) = \psi_2(d)$ (since $\overline{\mathfrak{a}\mathfrak{u}}$ is prime to $\mathfrak{t}$). In all,

$$\frac{\psi_1(c)\overline{\psi_2}(d)}{(m\tau_{\mathfrak{a}\mathfrak{N}'} + n)^{k+2j}}\left(\frac{|m\tau_{\mathfrak{a}\mathfrak{N}'} + n|^2}{\tau_{\mathfrak{a}\mathfrak{N}'} - \overline{\tau_{\mathfrak{a}\mathfrak{N}'}}}\right)^j$$
$$= \frac{\psi_1^{-1}(-\sqrt{D_K})\psi_1((au\alpha) \mod \bar{\mathfrak{u}})\psi_2^{-1}(\overline{\mathfrak{a}\mathfrak{u}}(\alpha) \mod \mathfrak{t})}{\alpha^{k+2j}}\left(\frac{\mathrm{Nm}_{K/\mathbb{Q}}(\overline{\mathfrak{a}\mathfrak{N}'}(\alpha))}{\sqrt{D_K}}\right)^j.$$

Suppose $k > 2$. Then we can rewrite each summand in the twisted trace as

$$(\chi_j)^{-1}(\overline{\mathfrak{a}\mathfrak{N}'})\partial^j E_k^{\psi_1,\psi_2}(\tau_{\mathfrak{a}\mathfrak{N}'})$$

$$= \frac{t^k \Gamma(k+j)\psi_1^{-1}(-\sqrt{D_K})}{2(2\pi i)^{k+j}\mathfrak{g}(\psi_2^{-1})}(\chi_j)^{-1}(\overline{\mathfrak{a}\mathfrak{N}'})$$
$$\times \sum_{\substack{\alpha \in (\overline{\mathfrak{a}\mathfrak{N}'})^{-1} \\ (\overline{\mathfrak{a}\mathfrak{N}'}(\alpha), \bar{\mathfrak{u}}\mathfrak{N}')=1}} \frac{\psi_1((au\alpha) \mod \bar{\mathfrak{u}})\psi_2^{-1}(\overline{\mathfrak{a}\mathfrak{u}}(\alpha) \mod \mathfrak{t})}{\alpha^{k+2j}}\left(\frac{|\mathrm{Nm}_{K/\mathbb{Q}}(\overline{\mathfrak{a}\mathfrak{N}'}(\alpha))|}{\sqrt{D_K}}\right)^j$$

$$= \frac{t^k \Gamma(k+j)\psi_1^{-1}(-\sqrt{D_K})}{2(2\pi i)^{k+j}\mathfrak{g}(\psi_2^{-1})\sqrt{D_K}^j}\frac{\chi^{-1}(\bar{\mathfrak{t}})(\chi_{-k/2})^{-1}(\overline{\mathfrak{a}\mathfrak{u}})}{|\mathrm{Nm}_{K/\mathbb{Q}}(\overline{\mathfrak{a}\mathfrak{u}})|^{k/2}}$$
$$\times \sum_{\substack{\alpha \in (\overline{\mathfrak{a}\mathfrak{u}})^{-1} \\ (\overline{\mathfrak{a}\mathfrak{u}}(\alpha), \bar{\mathfrak{u}}\mathfrak{N}')=1}} \left(\frac{\bar{\alpha}}{\alpha}\right)^{k/2+j}\frac{\psi_1((au\alpha) \mod \bar{\mathfrak{u}})\psi_2^{-1}(\overline{\mathfrak{a}\mathfrak{u}}(\alpha) \mod \mathfrak{t})}{|\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)|^{k/2}}$$

$$= \frac{t^k \Gamma(k+j)\psi_1^{-1}(-\sqrt{D_K})\chi^{-1}(\bar{\mathfrak{t}})}{2(2\pi i)^{k+j}\mathfrak{g}(\psi_2^{-1})\sqrt{D_K}^j}$$
$$\times \sum_{\substack{\alpha \in (\overline{\mathfrak{a}\mathfrak{u}})^{-1} \\ (\overline{\mathfrak{a}\mathfrak{u}}(\alpha), \bar{\mathfrak{u}}\mathfrak{N}')=1}} (\chi_{-k/2})^{-1}(\overline{\mathfrak{a}\mathfrak{u}}(\alpha))\psi_1(\overline{\mathfrak{a}\mathfrak{u}}(\alpha) \mod \mathfrak{u})\psi_2(\overline{\mathfrak{a}\mathfrak{u}}(\alpha) \mod \mathfrak{t})$$
$$\times \frac{\psi_1((au\alpha) \mod \bar{\mathfrak{u}})\psi_2^{-1}(\overline{\mathfrak{a}\mathfrak{u}}(\alpha) \mod \mathfrak{t})}{|\mathrm{Nm}_{K/\mathbb{Q}}(\overline{\mathfrak{a}\mathfrak{u}}(\alpha))|^{k/2}}$$

$$= \frac{t^k \Gamma(k+j)\psi_1^{-1}(-\sqrt{D_K})\chi^{-1}(\bar{\mathfrak{t}})}{(2\pi i)^{k+j}\mathfrak{g}(\psi_2^{-1})\sqrt{D_K}^j}$$
$$\times \sum_{\substack{\alpha \in (\overline{\mathfrak{a}\mathfrak{u}})^{-1} \\ (\overline{\mathfrak{a}\mathfrak{u}}(\alpha), \bar{\mathfrak{u}}\mathfrak{N}')=1}} (\chi_{-k/2})^{-1}(\overline{\mathfrak{a}\mathfrak{u}}(\alpha))\frac{\psi_1((au\,\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)) \mod \mathfrak{u})}{|\mathrm{Nm}_{K/\mathbb{Q}}(\overline{\mathfrak{a}\mathfrak{u}}(\alpha))|^{k/2}}$$

$$= \frac{|\mathcal{O}_K^\times|}{2}\frac{t^k \Gamma(k+j)\psi_1^{-1}(-\sqrt{D_K})\chi^{-1}(\bar{\mathfrak{t}})}{(2\pi i)^{k+j}\mathfrak{g}(\psi_2^{-1})\sqrt{D_K}^j}\sum_{\substack{\mathfrak{b} \subset \mathcal{O}_K \\ [\mathfrak{b}]=[\overline{\mathfrak{a}\mathfrak{u}}]\in\mathrm{Cl}(\mathcal{O}_K) \\ (\mathfrak{b}, \bar{\mathfrak{u}}\mathfrak{N}')=1}}\frac{(\psi_{1/K}(\chi_{-k/2})^{-1})(\mathfrak{b})}{|\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{b})|^k/2}.$$

The penultimate equality is justified since $\psi_1((a u \alpha) \bmod \bar{\mathfrak{u}}) = \psi_1(\overline{a \mathfrak{u}}(\alpha) \bmod \mathfrak{u}) = \psi_1(a \mathfrak{u}(\bar{\alpha}) \bmod \mathfrak{u})$ (the first equality here follows since $a \mathfrak{u}$ is prime to $\bar{\mathfrak{u}}$). The factor of $|\mathcal{O}_K^\times|$ appears because any integral ideal $\mathfrak{b} \subset \mathcal{O}_K$ can be written as $\overline{a \mathfrak{u}}(\alpha)$ for some ideal class representative $\mathfrak{a}$ and some element $\alpha \in (\overline{a \mathfrak{u}})^{-1}$ determined uniquely up to an element of $\mathcal{O}_K^\times = \{\pm 1\}$. Since $(\psi_1 \psi_2)(-1) = (-1)^k = (-1)^{k+2j}$, we see that each summand of the second line has the same value for α or $-\alpha$. Now since $|\mathcal{O}_K^\times| = 2$, we finally have, after summing both sides of the above equality over all our ideal class representatives $\mathfrak{a}$,

$$\sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\overline{a \mathfrak{N}'}) \partial^j E_k^{\psi_1, \psi_2}(\tau_{a \mathfrak{N}'})$$
$$= \frac{t^k \Gamma(k+j) \psi_1^{-1}(-\sqrt{D_K}) \chi^{-1}(\mathfrak{t})}{(2\pi i)^{k+j} \mathfrak{g}(\psi_2^{-1}) \sqrt{D_K}^j} L\left(\psi_{1/K}(\chi_{-k/2})^{-1}, \frac{k}{2}\right).$$

For $k = 2$ note that, by the same calculation as above, we have, for all $s \in \mathbb{C}$ with $\Re(s) > 0$,

$$\sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\overline{a \mathfrak{N}'})$$
$$\sum_{\substack{\alpha \in (\overline{a \mathfrak{u}})^{-1} \\ (\overline{a \mathfrak{u}}(\alpha), \bar{\mathfrak{u}} \mathfrak{N}')=1}} \frac{\psi_1^{-1}(-\sqrt{D_K}) \psi_1(\bar{\mathfrak{a}}(a u \alpha) \bmod \bar{\mathfrak{u}}) \psi_2^{-1}(\overline{a \mathfrak{u}}(\alpha) \bmod \mathfrak{t})}{\alpha^{2+2j}} \left(\frac{|\mathrm{Nm}_{K/\mathbb{Q}}(\overline{a \mathfrak{N}'}(\alpha))|}{\sqrt{D_K}}\right)^{j-s}$$
$$= \frac{\psi_1^{-1}(-\sqrt{D_K}) \chi^{-1}(\mathfrak{t})}{\sqrt{D_K}^{j-s} t^s} L(\psi_{1/K}(\chi_{-1})^{-1}, 1+s).$$

Note that each summand of the inner sum can be written as the special value of a real analytic Eisenstein series at a certain CM point:

$$\sum_{c=0}^{u-1} \sum_{d=0}^{t-1} \sum_{e=0}^{u-1} \sum_{\substack{(m,n) \in \mathbb{Z}^2 \setminus \{0\} \\ (m,n) \equiv \\ (ct, d+et)(N')}} \frac{\psi_1(c) \psi_2^{-1}(d)}{(m \tau_{a \mathfrak{N}'} + n)^{2+2j}} \left(\frac{|m \tau_{a \mathfrak{N}'} + n|^2}{\tau_{a \mathfrak{N}'} - \overline{\tau_{a \mathfrak{N}'}}}\right)^{j-s}.$$

Using standard analytic arguments, one can show that the above expression tends to $\partial^j E_2^{\psi_1, \psi_2}(\tau_{a \mathfrak{N}'})$ as $s \to 0$. Hence, combining the above, we have

$$\sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\overline{a \mathfrak{N}'}) \partial^j E_2^{\psi_1, \psi_2}(\tau_{a \mathfrak{N}'})$$
$$= \lim_{s \to 0} \frac{t^2 \Gamma(2+j) \psi_1^{-1}(-\sqrt{D_K}) \chi^{-1}(\mathfrak{t})}{(2\pi i)^{2+j} \mathfrak{g}(\psi_2^{-1}) \sqrt{D_K}^{j-s} t^s} L(\psi_{1/K}(\chi_{-1})^{-1}, 1+s)$$
$$= \frac{t^2 \Gamma(2+j) \psi_1^{-1}(-\sqrt{D_K}) \chi^{-1}(\mathfrak{t})}{(2\pi i)^{2+j} \mathfrak{g}(\psi_2^{-1}) \sqrt{D_K}^j} L(\psi_{1/K}(\chi_{-1})^{-1}, 1).$$

Proposition 36. *Let $k \geq 2$ be an integer. Suppose χ is of infinity type $(k+j, -j)$ and $\chi_{-k/2}$ has trivial central character and is of finite type $(\mathfrak{N}', \psi_1\psi_2)$. Suppose also that ψ_1 and ψ_2 are Dirichlet characters over $\mathbb{Q}$ with conductors u and t, respectively, such that $ut = N$ and $(\psi_1\psi_2)(-1) = (-1)^k$. Then*

$$\sum_{[\mathfrak{a}]\in\mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a})\partial^j E_k^{\psi_1,\psi_2}(\tau_\mathfrak{a}) = \frac{t^k \Gamma(k+j)\psi_1^{-1}(-\sqrt{D_K})\chi^{-1}(\bar{\mathfrak{t}})}{(2\pi i)^{k+j}\mathfrak{g}(\psi_2^{-1})\sqrt{D_K}^j} L(\psi_{1/K}\chi^{-1}, 0).$$

4.2. *Stabilization operators.* We have the following "stabilization operators" acting on normalized $\Gamma_0(N')$-eigenforms F with character ε_F. Given a rational prime $\ell \nmid N'$, let a_ℓ denote the eigenvalue of F under the Hecke operator T_ℓ, let $(\alpha_\ell, \beta_\ell)$ denote (some henceforth fixed ordering of) the algebraic numbers such that $\alpha_\ell + \beta_\ell = a_\ell$, $\alpha_\ell\beta_\ell = \ell^{k-1}\varepsilon_F(\ell)$, and $\mathrm{ord}_\ell(\alpha_\ell) \leq \mathrm{ord}_\ell(\beta_\ell)$. Now define

$$F(q) \mapsto F^{(\ell^+)}(q) := F(q) - \beta_\ell F(q^\ell) \in M_k(\Gamma_0(N'\ell), \varepsilon_F),$$

$$F(q) \mapsto F^{(\ell^-)}(q) := F(q) - \alpha_\ell F(q^\ell) \in M_k(\Gamma_0(N'\ell), \varepsilon_F),$$

$$F(q) \mapsto F^{(\ell^0)}(q) := F(q) - a_\ell F(q^\ell) + \varepsilon_F(\ell)\ell^{k-1}F(q^{\ell^2}) \in M_k(\Gamma_0(N'\ell^2), \varepsilon_F).$$

Note that, for $\ell_1 \neq \ell_2$, the stabilization operators $F \mapsto F^{(\ell_1^{\epsilon_1})}$ and $F \mapsto F^{(\ell_2^{\epsilon_2})}$ commute for any $\epsilon_1, \epsilon_2 \in \{+, -, 0\}$. Then we define, for integers $S = \prod_i \ell_i^{e_i}$, $\epsilon, \epsilon_1, \epsilon_2 \in \{+, -, 0\}$,

$$F^{(S^\epsilon)} := F^{\prod_i(\ell_i^\epsilon)}, \quad F^{(S_1^{\epsilon_1}S_2^{\epsilon_2})} := F^{(S_1^{\epsilon_1}),(S_2^{\epsilon_2})}.$$

These operators clearly extend to p-adic modular forms. On the p-adic modular forms $\theta^j E_k^{\psi_1,\psi_2}$ from Section 4.1, we explicitly have

$$\theta^j E_k^{\psi_1,\psi_2,(\ell^+)}(q) := \delta_{\psi_1=1, j=0}L(\psi_1, 1-k)(1-\psi_2(\ell)\ell^{k-1}) + 2\sum_{n=1}^{\infty} n^j \sigma_{k-1}^{\psi_1,\psi_2,(\ell^+)}(n)q^n$$

$$= \theta^j E_k^{\psi_1,\psi_2}(q) - \psi_2(\ell)\ell^{k-1+j}\theta^j E_k^{\psi_1,\psi_2}(q^\ell),$$

$$\theta^j E_k^{\psi_1,\psi_2,(\ell^-)}(q) := \delta_{\psi_1=1, j=0}L(\psi_1, 1-k)(1-\psi_2(\ell)) + 2\sum_{n=1}^{\infty} n^j \sigma_{k-1}^{\psi_1,\psi_2,(\ell^-)}(n)q^n$$

$$= \theta^j E_k^{\psi_1,\psi_2}(q) - \psi_1(\ell)\ell^j\theta^j E_k^{\psi_1,\psi_2}(q^\ell),$$

$$\theta^j E_k^{\psi_1,\psi_2,(\ell^0)}(q) := \delta_{\psi_1=1, j=0}L(\psi_1, 1-k)(1-\psi_1(\ell) - \psi_2(\ell)\ell^{k-1} + \psi_2(\ell^2)\ell^{k-1})$$

$$+ 2\sum_{n=1}^{\infty} n^j \sigma_{k-1}^{\psi_1,\psi_2,(\ell^0)}(n)q^n$$

$$= \theta^j E_k^{\psi_1,\psi_2}(q) - \ell^j(\psi_1(\ell) + \psi_2(\ell)\ell^{k-1})\theta^j E_k^{\psi_1,\psi_2}(q^\ell)$$

$$+ (\psi_1\psi_2)(\ell)\ell^{k-1+2j}\theta^j E(q^{\ell^2}),$$

where $\delta_{\psi=1, j=0}$ equals 1 if ψ is trivial and $j = 0$, and 0 otherwise, and

$$\sigma_{k-1}^{\psi_1, \psi_2, (\ell^+)}(n) := \sum_{\substack{0 < d \mid n \\ (d, \ell) = 1}} \psi_1(n/d) \psi_2(d) d^{k-1},$$

$$\sigma_{k-1}^{\psi_1, \psi_2, (\ell^-)}(n) := \sum_{\substack{0 < d \mid n \\ (n/d, \ell) = 1}} \psi_1(n/d) \psi_2(d) d^{k-1},$$

$$\sigma_{k-1}^{\psi_1, \psi_2, (\ell^0)}(n) := \sum_{\substack{0 < d \mid n \\ (n, \ell) = 1}} \psi_1(n/d) \psi_2(d) d^{k-1}.$$

Let N' be as in Section 4.1, let $N'' = N''_+ N''_- N''_0$ be prime to N', and suppose additionally that K satisfies the Heegner hypothesis with respect to N'' so that every prime dividing $N := N'' N'$ is split in K. Let $\mathfrak{N} = \mathfrak{N}'' \mathfrak{N}'$, where $\mathfrak{N}'$ is as in Section 4.1 and $\mathfrak{N}''$ is some choice of integral ideal such that $\mathcal{O}_K / \mathfrak{N}'' = \mathbb{Z}/N''$. Write $\mathfrak{N}$ as a product of (distinct) primes $\prod_{\ell \mid N} v$, where $v \mid \ell$; in other words, for each $\ell \mid N$, we can write

$$v = \mathbb{Z} \frac{b_\ell + \sqrt{D_K}}{2} + \mathbb{Z}\ell$$

for some $b_\ell \in \mathbb{Z}$ such that $b_\ell^2 \equiv D_K \pmod{4\ell}$.

For any integral primitive ideal $\mathfrak{a}$ of $\mathcal{O}_K$ coprime to $\mathfrak{N}$, recall the associated point

$$\tau_{\mathfrak{a}\mathfrak{N}} = \frac{b_{aN} + \sqrt{D_K}}{2aN} \in \mathcal{H}^+$$

such that $(\overline{\mathfrak{a}\mathfrak{N}})^{-1} = \mathbb{Z}\tau_{\mathfrak{a}\mathfrak{N}} + \mathbb{Z}$. Note that, for $v \mid \mathfrak{N}''$, where $v \mid \ell$, we have

$$\bar{v}(\overline{\mathfrak{a}\mathfrak{N}})^{-1} = \left(\overline{\mathfrak{a} \prod_{v' \neq v} v'}\right)^{-1} = \mathbb{Z}\ell \frac{b_{aN} + \sqrt{D_K}}{2aN} + \mathbb{Z},$$

and hence

$$\bar{v}^{-1} \star (\overline{\mathfrak{a}\mathfrak{N}} \star \mathbb{C}/\mathcal{O}_K) = \mathbb{C}/(\bar{v}(\overline{\mathfrak{a}\mathfrak{N}})^{-1}) = \mathbb{C}/(\mathbb{Z}\ell\tau_{\mathfrak{a}\mathfrak{N}} + \mathbb{Z}).$$

In terms of the action of $\mathbb{I}^{\mathfrak{N}}$ on CM triples (A', t', ω'), for any $F \in M_k(\Gamma_0(N), \varepsilon_F)$, we have

$$F(\ell\tau_{\mathfrak{a}\mathfrak{N}}) = F(\bar{v}^{-1} \star (\mathbb{C}/(\mathbb{Z}\tau_{\mathfrak{a}\mathfrak{N}} + \mathbb{Z}), t, 2\pi i dz)) = F(\bar{v}^{-1}\overline{\mathfrak{a}\mathfrak{N}} \star (\mathbb{C}/\mathcal{O}_K, t, 2\pi i dz)),$$

$$F(\ell^2\tau_{\mathfrak{a}\mathfrak{N}}) = F(\bar{v}^{-2} \star (\mathbb{C}/(\mathbb{Z}\tau_{\mathfrak{a}\mathfrak{N}} + \mathbb{Z}), t, 2\pi i dz)) = F(\bar{v}^{-2}\overline{\mathfrak{a}\mathfrak{N}} \star (\mathbb{C}/\mathcal{O}_K, t, 2\pi i dz)).$$

Thus, for any normalized eigenform F, viewed as a p-adic modular form, recalling our notation $A_0 = \mathbb{C}/\mathcal{O}_K$, $t_0 \in A_0[\mathfrak{N}]$ from Section 3.4, and with ω_{can} as our

"canonical" differential on $\hat{\mathcal{A}}_0$ under our fixed isomorphism $i : \hat{\mathcal{A}}_0 \xrightarrow{\sim} \hat{\mathbb{G}}_m$ (see Section 3.4), we have for $\ell \nmid N'$

$$\theta^j F^{(\ell^+)}(\overline{\mathfrak{a}\mathfrak{N}} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$= \theta^j F(\overline{\mathfrak{a}\mathfrak{N}} \star (A_0, t_0, \omega_{\mathrm{can}})) - \beta_\ell \ell^j \theta^j F(\bar{v}^{-1} \overline{\mathfrak{a}\mathfrak{N}} \star (A_0, t_0, \omega_{\mathrm{can}})),$$

$$\theta^j F^{(\ell^-)}(\overline{\mathfrak{a}\mathfrak{N}} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$= \theta^j F(\overline{\mathfrak{a}\mathfrak{N}} \star (A_0, t_0, \omega_{\mathrm{can}})) - \alpha_\ell \ell^j \theta^j F(\bar{v}^{-1} \overline{\mathfrak{a}\mathfrak{N}} \star (A_0, t_0, \omega_{\mathrm{can}})),$$

$$\theta^j F^{(\ell^0)}(\overline{\mathfrak{a}\mathfrak{N}} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$= \theta^j F(\overline{\mathfrak{a}\mathfrak{N}} \star (A_0, t_0, \omega_{\mathrm{can}})) - \ell^j a_\ell \theta^j F(\bar{v}^{-1} \overline{\mathfrak{a}\mathfrak{N}} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$+ \varepsilon_F(\ell) \ell^{k-1+2j} \theta^j F(\bar{v}^{-2} \overline{\mathfrak{a}\mathfrak{N}} \star (A_0, t_0, \omega_{\mathrm{can}})).$$

Choosing some set of representatives $\mathfrak{a}$ prime to $\mathfrak{N}$, we thus have

$$\sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F^{(\ell^+)}(\mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$= \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F(\mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$- \beta_\ell \ell^j \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F(\bar{v}^{-1} \mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$= (1 - \beta_\ell (\chi_j)^{-1}(\bar{v}) \ell^j) \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F(\mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}})),$$

$$\sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F^{(\ell^-)}(\mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$= \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F(\mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$- \alpha_\ell \ell^j \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F(\bar{v}^{-1} \mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$= (1 - \alpha_\ell (\chi_j)^{-1}(\bar{v}) \ell^j) \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F(\mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}})),$$

$$\sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F^{(\ell^+)}(\mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$= \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F(\mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$- \ell^j a_\ell \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F(\bar{v}^{-1} \mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$+ \varepsilon_F(\ell) \ell^{k-1+2j} \sum_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a}) \theta^j F(\bar{v}^{-2} \mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$

$$= (1 - a_\ell(\chi_j)^{-1}(\bar{v})\ell^j$$
$$+ \varepsilon_F(\ell)(\chi_j)^{-2}(\bar{v})\ell^{k-1+2j}) \sum_{[\mathfrak{a}]\in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a})\theta^j F(\mathfrak{a}\star(A_0, t_0, \omega_{\mathrm{can}})).$$

Thus, rewriting the definitions of $E_k^{\psi_1, \psi_2, ((N''_+)^+ (N''_-)^- (N''_0)^0)}$ in terms of triples, and using the above general identities for p-adic modular forms and induction, we have

$$\sum_{[\mathfrak{a}]\in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a})\theta^j E_k^{\psi_1, \psi_2, ((N''_+)^+ (N''_-)^- (N''_0)^0)}(\mathfrak{a}\star(A_0, t_0, \omega_{\mathrm{can}}))$$
$$= \Xi_\chi(\psi_1, \psi_2, N_+, N_-, N_0) \sum_{[\mathfrak{a}]\in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a})\theta^j E_k^{\psi_1, \psi_2}(\mathfrak{a}\star(A_0, t_0, \omega_{\mathrm{can}})),$$

where $N_+ = N''_+ \cdot t/(u, t)$, $N_- = N''_- \cdot u/(u, t)$, $N_0 = N''_0 \cdot (u, t)^2$, and

$$\Xi_\chi(\psi_1, \psi_2, N_+, N_-, N_0)$$
$$= \prod_{\ell \mid N_+} (1 - (\psi_{2/K}\chi^{-1})(\bar{v})\ell^{k-1}) \prod_{\ell \mid N_-} (1 - (\psi_{1/K}\chi^{-1})(\bar{v}))$$
$$\times \prod_{\ell \mid N_0} (1 - (\psi_{2/K}\chi^{-1})(\bar{v})\ell^{k-1})(1 - (\psi_{1/K}\chi^{-1})(\bar{v})).$$

Henceforth, let $E_k^{(\psi_1, \psi_2, N_+, N_-, N_0)} := E_k^{\psi_1, \psi_2, ((N''_+)^+ (N''_-)^- (N''_0)^0)}$. Now, using the above calculation, Proposition 36, the fact that

$$\omega_{\mathrm{can}} = \frac{\Omega_\infty}{\Omega_p} \cdot 2\pi i\, dz$$

(where Ω_∞ and Ω_p are the complex and p-adic periods defined in Section 3.4) and part (3) of Theorem 21, we have:

Proposition 37. *Let $k \geq 2$ be an integer. Suppose χ is of infinity type $(k + j, -j)$ and $\chi_{-k/2}$ has trivial central character and is of finite type $(\mathfrak{N}, \psi_1\psi_2)$. Suppose also that ψ_1 and ψ_2 are Dirichlet characters over $\mathbb{Q}$ with conductors u and t, respectively, such that $ut = N$ and $(\psi_1\psi_2)(-1) = (-1)^k$. Then*

$$\sum_{[\mathfrak{a}]\in \mathrm{Cl}(\mathcal{O}_K)} (\chi_j)^{-1}(\mathfrak{a})\theta^j E_k^{(\psi_1, \psi_2, N_+, N_-, N_0)}(\mathfrak{a}\star(A_0, t_0, \omega_{\mathrm{can}}))$$
$$= \left(\frac{\Omega_p}{\Omega_\infty}\right)^{k+2j} \frac{t^k \Gamma(k + j)\psi_1^{-1}(-\sqrt{D_K})\chi^{-1}(\mathfrak{t})}{(2\pi i)^{k+j}\mathfrak{g}(\psi_2^{-1})\sqrt{D_K}^j}$$
$$\times \Xi_\chi(\psi_1, \psi_2, N_+, N_-, N_0)L(\psi_{1/K}\chi^{-1}, 0),$$

where

$$\Xi_\chi(\psi_1, \psi_2, N_+, N_-, N_0)$$
$$= \prod_{\ell \mid N_+}(1 - (\psi_{2/K}\chi^{-1})(\bar{v})\ell^{k-1}) \prod_{\ell \mid N_-}(1 - (\psi_{1/K}\chi^{-1})(\bar{v}))$$
$$\prod_{\ell \mid N_0}(1 - (\psi_{2/K}\chi^{-1})(\bar{v})\ell^{k-1})(1 - (\psi_{1/K}\chi^{-1})(\bar{v})).$$

Finally, since $p \nmid N$, note that the "p-depletion" operator $\flat$ of Section 3.2 coincides with the $((p^2)^0)$-stabilization operator on our family of Eisenstein series, i.e.,

$$(\theta^j E_k^{(\psi_1, \psi_2, N_+, N_-, N_0)})^\flat = \theta^j E_k^{(\psi_1, \psi_2, N_+, N_-, p^2N_0)}.$$

(Note that all the above stabilization operators on p-adic modular forms commute with θ, so the above notation is unambiguous.)

4.3. *Proof of main theorem.*

Proof of Theorem 3. Suppose, as in our assumptions, that $f \in S_k(\Gamma_0(N), \varepsilon_f)$ has partial Eisenstein descent of type $(\psi_1, \psi_2, N_+, N_-, N_0)$ over M mod $\mathfrak{m}$, where M is a p-adic field containing E_f. Recall the field F' defined in Section 3.4, with $\mathfrak{p}'$ being the prime ideal of $\mathcal{O}_{F'}$ above p determined by our embedding $i_p : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$. Thus,

$$\theta^j f(q) \equiv \theta^j E_k^{(\psi_1, \psi_2, N_+, N_-, N_0)}(q) \pmod{\mathfrak{m}\mathcal{O}_{F'_{\mathfrak{p}'}M}},$$

viewed as p-adic modular forms for all $j \geq 1$. Moreover,

$$\theta^j f^\flat(q) \equiv \theta^j E_k^{(\psi_1, \psi_2, N_+, N_-, p^2N_0)}(q) \pmod{\mathfrak{m}\mathcal{O}_{F'_{\mathfrak{p}'}M}}.$$

Henceforth, let $E_{k,\psi_1,\psi_2}^{(N)} = E_k^{(\psi_1, \psi_2, N_+, N_-, N_0)}$ and $E_{k,\psi_1,\psi_2}^{(pN)} = E_k^{(\psi_1, \psi_2, N_+, N_-, p^2N_0)}$, and recall our notation $A_0 = \mathbb{C}/\mathcal{O}_K$, $t_0 \in A_0[\mathfrak{N}]$ (see Section 3.4). Since p being split in K implies that the curves $i_p(\mathfrak{a} \star A_0)$ are ordinary (viewed as curves over $\mathbb{C}_p$), by the congruence above and the q-expansion principle [Gouvêa 1988, Sections I.3.2 and I.3.5] we have

$$\sum_{\mathfrak{a}\in\mathrm{Cl}(\mathcal{O}_K)}(\chi_j)^{-1}(\mathfrak{a})(\theta^j f)^\flat(\mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}}))$$
$$\equiv \sum_{\mathfrak{a}\in\mathrm{Cl}(\mathcal{O}_K)}(\chi_j)^{-1}(\mathfrak{a})(\theta^j E_{k,\psi_1,\psi_2}^{(pN)})(\mathfrak{a} \star (A_0, t_0, \omega_{\mathrm{can}})) \pmod{\mathfrak{m}\mathcal{O}_{F'_{\mathfrak{p}'}M}}.$$

By assumption, ε_f equals $\psi_1\psi_2$ and χ is of finite type $(\mathfrak{N}, \varepsilon_f) = (\mathfrak{N}, \psi_1\psi_2)$. Now by Proposition 37, we have

$$\sum_{\mathfrak{a}\in\mathrm{Cl}(\mathcal{O}_K)}(\chi_j)^{-1}(\mathfrak{a})(\theta^j E^{(pN)}_{k,\psi_1,\psi_2})(\mathfrak{a}\star(A_0, t_0, \omega_{\mathrm{can}}))$$

$$= \left(\frac{\Omega_p}{\Omega_\infty}\right)^{k+2j}\frac{t^k\Gamma(k+j)\psi_1^{-1}(-\sqrt{D_K})\chi^{-1}(\bar{\mathfrak{t}})}{(2\pi i)^{k+j}\mathfrak{g}(\psi_2^{-1})\sqrt{D_K}^j}$$

$$\times \Xi_\chi(\psi_1, \psi_2, N_+, N_-, p^2 N_0)L(\psi_{1/K}\chi^{-1}, 0),$$

where $\Xi_\chi(\psi_1, \psi_2, N_+, N_-, p^2 N_0)$ is defined as in Proposition 37.

Since χ is of finite type $(\mathfrak{N}, \varepsilon_f)$, it is unramified at $\mathfrak{p}$. Moreover, since $\mathfrak{p}\nmid u\mathcal{O}_K$, $\psi_{1/K}$ is unramified at $\mathfrak{p}$. Hence, by [Katz 1978, 5.2.27 Lemma, 5.2.28], we have $\mathrm{Local}_{\mathfrak{p}}(\psi_{1/K}\chi^{-1}) = 1$ and $\mathrm{Local}_{\mathfrak{p}}(\psi_{1/K}\chi^{-1}\mathbb{N}_K^{1-k}) = 1$.

Now using Theorems 24 and 27 with $\mathfrak{C} = \mathfrak{f}(\psi_{1/K}\chi^{-1}) = \mathrm{lcm}(u\mathcal{O}_K, \mathfrak{t})$, where $\mathfrak{F} = \mathrm{lcm}(\mathfrak{u}, \mathfrak{t})$, $\mathfrak{F}_c = \bar{\mathfrak{u}}$ and $\mathfrak{I} = 1$, we can write

$$\mathcal{L}_p(f, \chi)$$

$$= \left(\sum_{\mathfrak{a}\in\mathrm{Cl}(\mathcal{O}_K)}(\chi_j)^{-1}(\mathfrak{a})(\theta^j f)^\flat(\mathfrak{a}\star(A_0, t_0, \omega_{\mathrm{can}}))\right)^2$$

$$\equiv \left(\sum_{\mathfrak{a}\in\mathrm{Cl}(\mathcal{O}_K)}(\chi_j)^{-1}(\mathfrak{a})(\theta^j E^{(pN)}_{k,\psi_1,\psi_2})(\mathfrak{a}\star(A_0, t_0, \omega_{\mathrm{can}}))\right)^2$$

$$= \left(\left(\frac{\Omega_p}{\Omega_\infty}\right)^{k+2j}\frac{t^k\Gamma(k+j)\psi_1^{-1}(-\sqrt{D_K})\chi^{-1}(\bar{\mathfrak{t}})}{(2\pi i)^{k+j}\mathfrak{g}(\psi_2^{-1})\sqrt{D_K}^j}\right.$$

$$\left.\times \Xi_\chi(\psi_1, \psi_2, N_+, N_-, p^2 N_0)L(\psi_{1/K}\chi^{-1}, 0)\right)^2$$

$$= \psi_1^{-1}(D_K)\left(\frac{t^k\chi^{-1}(\bar{\mathfrak{t}})}{4\mathfrak{g}(\psi_2^{-1})(2\pi i)^{k+2j}}\Xi_\chi(\psi_1, \psi_2, N_+, N_-, N_0)L_p(\psi_{1/K}\chi^{-1}, 0)\right)^2$$

$$(\mathrm{mod}\ \mathfrak{m}\mathcal{O}_{F'_{\mathfrak{p}'},M}).$$

The above congruence now extends by *p*-adic continuity from $\Sigma^{(2)}_{\mathrm{cc}}(\mathfrak{N})$ to $\hat{\Sigma}_{\mathrm{cc}}(\mathfrak{N})$ (with respect to the topology described in Section 3.4). Thus the congruence holds on $\hat{\Sigma}_{\mathrm{cc}}(\mathfrak{N})$, and the theorem follows after setting $\Xi := \Xi_\chi(\psi_1, \psi_2, N_+, N_-, N_0)$. $\square$

Proof of Theorem 7. In this more specialized situation, we have $\psi_1 = \psi_2^{-1} = \psi$ and $u = t = |\mathfrak{f}(\psi)|$. Thus $\psi_1\psi_2$ equals 1 and χ is of finite type $(\mathfrak{N}, 1)$. Recall from Bertolini, Darmon, and Prasanna's *p*-adic Waldspurger formula (Theorem 25) that

$$\mathcal{L}_p(f, \mathbb{N}_K^{-k/2}) = \left(\frac{p^{k/2} - a_p(f) + p^{k/2-1}}{p^{k/2}\Gamma\left(\frac{k}{2}\right)}\right)^2\left(\mathrm{AJ}_{F'_{\mathfrak{p}'}}(\Delta_f(K))(\omega_f\wedge\omega_A^{k/2-1}\eta_A^{k/2-1})\right)^2.$$

The proof proceeds essentially by plugging $\chi = \mathbb{N}_K^{-k/2}$ into Theorem 3. We have, by Gross's factorization formula (Theorem 28) *applied to* $(\psi\omega^{-k/2})_0$ (see Definition 6),

$$\frac{|\mathfrak{f}(\psi)|^{k/2}}{\psi(-\sqrt{D_K})\mathfrak{g}(\psi)} L_p(\psi_{/K}\mathbb{N}_K^{k/2}, 0)$$

$$= \frac{\langle|\mathfrak{f}(\psi)|\rangle^{k/2}}{\prod_{\ell\,|\,\mathfrak{f}(\psi)}(\psi^{-1}\omega^{k/2})_{0,\ell}(-\sqrt{D_K})\omega_\ell^{-k/2}(\ell^{\mathrm{ord}_\ell(\mathfrak{f}(\psi))})\mathfrak{g}_\ell(\psi)} L_p\left((\psi\omega^{-k/2})_{0/K}, \frac{k}{2}\right)$$

$$= \frac{\langle|\mathfrak{f}(\psi)|\rangle^{k/2}}{\prod_{\ell\,|\,\mathfrak{f}(\psi)}(\psi^{-1}\omega^{k/2})_{0,\ell}(-\sqrt{D_K})\mathfrak{g}_\ell((\psi\omega^{-k/2})_0)} L_p\left((\psi\omega^{-k/2})_{0/K}, \frac{k}{2}\right)$$

$$= L_p\left(\psi_0(\varepsilon_K\omega)^{1-k/2}, \frac{k}{2}\right) L_p\left(\psi_0^{-1}(\varepsilon_K\omega)^{k/2}, 1-\frac{k}{2}\right).$$

Using the interpolation property of the Kubota–Leopoldt p-adic L-function, we have

$$L_p\left(\psi_0^{-1}(\varepsilon_K\omega)^{k/2}, 1-\frac{k}{2}\right) = -(1 - (\psi_0^{-1}\varepsilon_K^{k/2})(p)p^{k/2-1})\frac{2}{k} B_{\frac{k}{2},\psi_0^{-1}\varepsilon_K^{k/2}}$$

$$= -(1 - \psi_0^{-1}(p)p^{k/2-1})\frac{2}{k} B_{\frac{k}{2},\psi_0^{-1}\varepsilon_K^{k/2}},$$

where the last equality follows since p is split in K and so $\varepsilon_K(p) = 1$.

Suppose $\psi_0(\varepsilon_K\omega)^{1-k/2} \neq 1$. In this case, since $p^2 \nmid \mathfrak{f}(\psi_0(\varepsilon_K\omega)^{1-k/2}) \mid pf$, we have by Corollary 5.13 of [Washington 1997] that

$$L_p\left(\psi_0(\varepsilon_K\omega)^{1-k/2}, \frac{k}{2}\right) \equiv L_p(\psi_0(\varepsilon_K\omega)^{1-k/2}, 0)$$

$$= -(1 - (\psi_0\varepsilon_K(\varepsilon_K\omega)^{-k/2})(p))B_{1,\psi_0\varepsilon_K(\varepsilon_K\omega)^{-k/2}}$$

$$= -B_{1,\psi_0\varepsilon_K(\varepsilon_K\omega)^{-k/2}} \pmod{p},$$

where the last equality holds since $p \mid \mathfrak{f}(\psi_0\varepsilon_K(\varepsilon_K\omega)^{1-k/2})$. Note that this congruence also holds mod λ for any prime $\lambda \mid p$.

Now suppose $\psi_0(\varepsilon_K\omega)^{1-k/2} = 1$ and $k = 2$, i.e., $\psi_0 = 1$. From [Gross 1980, p. 90], the Katz p-adic L-function at $\psi_{0/K} = 1_{/K}$ has the special value

$$L_p(1_{/K}, 0) = \frac{4}{|\mathcal{O}_K^\times|}\frac{p-1}{p} \log_p \bar{\alpha} = 2\frac{p-1}{p} \log_p \bar{\alpha},$$

where $\bar{\alpha} \in \mathcal{O}_K$ such that $(\bar{\alpha}) = \bar{\mathfrak{p}}^{h_K}$. (Recall that $|\mathcal{O}_K^\times| = 2$ since we assume that $D_K < -4$.) The statement now follows directly from Theorem 3. $\qquad\square$

5. Concrete applications of the main theorem

In this section, we apply Theorem 7 to computations with algebraic cycles, in certain instances verifying a weak form of the Beilinson–Bloch conjecture (as described

in Section 2.2). In Section 5.5, we apply our results to the case of elliptic curves with reducible mod-p Galois representation, in particular deriving criteria to show that Heegner points on certain quadratic twists are nontorsion. In Section 5.6, we use this criterion to show that for semistable curves with reducible mod-3 Galois representation, a positive proportion of real quadratic twists have rank 1 and a positive proportion of imaginary quadratic twists have rank 0.

5.1. *Construction of newforms with Eisenstein descent of type* $(1, 1, 1, 1, 1)$.
We now give a procedure for constructing newforms $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ which have Eisenstein descent of type $(1, 1, 1, 1, 1)$.

Construction 38 (Eisenstein descent of type $(1, 1, 1, 1, 1)$). Fix an even integer $k \geq 4$ and a prime $p \mid B_k$. Recall the classical holomorphic Eisenstein series of weight k:

$$E_k(q) = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n.$$

(See Remark 32.) The Eisenstein series E_4 and E_6 generate $M_k(\mathrm{SL}_2(\mathbb{Z}))/S_k(\mathrm{SL}_2(\mathbb{Z}))$ as an algebra, and therefore if we normalize E_4 and E_6 to $G_4 = 240E_4$ and $G_6 = -504E_6$ to have constant term 1, then we have a cuspform

$$f_k := E_k + \frac{B_k}{2k}G_4^a G_6^b \in S_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q})$$

for some $a, b \in \mathbb{Z}_{\geq 0}$ with $k = 4a + 6b$.

Under our assumption $p \mid B_k$, we see immediately that $f_k \equiv E_k \pmod{p}$. However, there is no guarantee that f_k is a *newform*, a problem we can remedy as follows. Consider the Hecke algebra $\mathbb{T} \subset \mathrm{End}_{\mathbb{Z}_p}(S_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z}_p))$ generated by the classical Hecke operators T_ℓ at primes ℓ. Since $\mathbb{T}$ is a finite torsion-free $\mathbb{Z}_p$-algebra, it is flat. Minimal primes $\mathfrak{p}$ of $\mathbb{T}$ correspond to $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-conjugacy classes of weight-k eigenforms in $S_k(\mathrm{SL}_2(\mathbb{Z}))$, which also correspond to $\mathbb{Z}_p$-algebra homomorphisms $\phi : \mathbb{T} \to \bar{\mathbb{Q}}_p$ (with $\ker(\phi) = \mathfrak{p}$), which in turn correspond to eigenforms f_ϕ such that $T_\ell f_\phi = \phi(T_\ell)f_\phi$.

Now write $f_k(q) = \sum_{n=1}^{\infty} a_n q^n$ so that $a_n \equiv \sigma_{k-1}(n) \pmod{p}$, and define a homomorphism $\varphi : \mathbb{T} \to \mathbb{F}_p$ given by $\varphi(T_\ell) = a_\ell \equiv 1 + \ell^{k-1} \pmod{p}$. Since $\mathbb{F}_p$ is a field, $\mathfrak{m} := \ker(\varphi)$ is maximal, and there exists a minimal prime $\mathfrak{p} \subset \mathfrak{m}$ above p since $\mathbb{T}$ is flat over $\mathbb{Z}_p$. Then the minimal prime $\mathfrak{p}$ corresponds to a map $\phi : \mathbb{T} \to \bar{\mathbb{Q}}_p$ with $\ker(\phi) = \mathfrak{p}$ that satisfies $\phi \equiv \varphi \pmod{p}$. Let $F = \mathrm{Frac}(\phi(\mathbb{T}))$ denote the field of fractions of $\phi(\mathbb{T})$, and note that $\phi(\mathbb{T}) \subset \mathcal{O}_F$; since $\mathbb{T}$ is finite over $\mathbb{Z}_p$, F is finite over $\mathbb{Q}_p$. Now let λ denote the maximal ideal of $\mathcal{O}_F$. Since $T_\ell \equiv 1 + \ell^{k-1} \pmod{\mathfrak{m}}$ (because $\varphi : \mathbb{T}/\mathfrak{m} \xrightarrow{\sim} \mathbb{F}_p$), we have $\phi(T_\ell) \equiv 1 + \ell^{k-1} \pmod{\phi(\mathfrak{m})}$. Hence since

$\lambda \mid \phi(\mathfrak{m})$, the modular form f_ϕ corresponding to ϕ satisfies

$$f_\phi(q) \equiv \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \pmod{\lambda}$$

and is our desired newform.

Remark 39. The last paragraph of Construction 38 is commonly known as the "Deligne–Serre lifting lemma" (see [Deligne and Serre 1974, Lemme 6.11]).

5.2. *Construction of newforms with Eisenstein descent of type* $(1, 1, N_+, N_-, N_0)$.

Construction 40 (Eisenstein descent of type $(1, 1, N_+, N_-, N_0)$). We can easily use the normalized newform with Eisenstein descent of type $(1, 1, 1, 1, 1)$ obtained from Construction 38 to produce a newform of descent of type $(1, 1, N_+, N_-, N_0)$. We apply certain stabilization operators, as in Section 4.2. Suppose we are given a normalized newform $f \in S_k(\Gamma_1(N'))$ with Eisenstein descent of type $(1, 1, N'_+, N'_-, N'_0)$ mod λ. Applying the $(N_+^+ N_-^- N_0^0)$-stabilization operator, the resulting newform $f^{(N_+^+ N_-^- N_0^0)} \in S_k(\Gamma_1(N') \cap \Gamma_0(N))$ is a normalized newform which has Eisenstein descent of type $(1, 1, N'_+ N_+, N'_- N_-, N'_0 N_0)$ mod λ.

Applying the above $(N_+^+ N_-^- N_0^0)$-stabilization operator to $f_\phi \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ from Construction 38, we have

$$f_\phi^{(N_+^+ N_-^- N_0^0)}(q) \equiv \sum_{n=1}^{\infty} \sigma_{k-1}^{(N)}(n) q^n \pmod{\lambda},$$

where $\sigma_{k-1}^{(N)}$ is defined as in Remark 32. In other words, $f_\phi^{(N_+^+ N_-^- N_0^0)}$ has Eisenstein descent of type $(1, 1, N_+, N_-, N_0)$ mod λ.

Remark 41. We could similarly produce examples of newforms with Eisenstein descent of type $(\psi_1, \psi_2, N_+, N_-, N_0)$ by starting out with the Eisenstein series $E_k^{\psi_1, \psi_2}$ in Construction 38 and applying appropriate stabilization operators as in Construction 40.

5.3. *Application to algebraic cycles.* We now calculate an explicit example to demonstrate the main theorem. We first use Construction 38 to construct an appropriate newform with Eisenstein descent of type $(1, 1, 1, 1, 1)$. We thus look for a positive integer k, a rational prime p, a real quadratic extension $L/\mathbb{Q}$, and an imaginary quadratic extension $K/\mathbb{Q}$ such that p splits in K and such that $p \mid B_k$, $p \nmid B_{\frac{k}{2}, \varepsilon_L \varepsilon_K}$ and $p \nmid B_{1, \varepsilon_L \omega^{-k/2}}$. To this end, consider $k = 18$, $p = 43867$, $L = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{-5})$. Then 43867 splits in K, and $p \mid \frac{43867}{798} = B_{18} = B_k$. Furthermore,

$$B_{9, \varepsilon_K} = -5444415378 \equiv 5726 \pmod{43867},$$

and so $p \nmid B_{\frac{k}{2}, \varepsilon_{L \cdot K}} = B_{\frac{k}{2}, \varepsilon_K}$.

Remark 42. For certain values of k, we can simplify the above formula even further. Let $[m]$ denote the smallest nonnegative representative of the residue class mod $(p-1)$ of an integer m. In the case that $2 \le [-k/2] \le p-4$, by standard congruence theorems (see [Washington 1997, Chapter 5.3], for example), we have

$$B_{1,\omega^{[-k/2]}} \equiv \frac{B_{[-k/2]+1}}{[-k/2]+1} \pmod{p}$$

(and hence this congruence also holds mod $\lambda|p$).

Hence, by Remark 42, we have

$$B_{1,\omega^{-9}} \equiv \frac{B_{43858}}{43858} \equiv 11867 \pmod{43867},$$

and so $p \nmid B_{1,\varepsilon_L \omega^{-k/2}} = B_{1,\omega^{-9}}$. Hence, applying Construction 38, we get a newform $f_{18} \in S_{18}(\mathrm{SL}_2(\mathbb{Z}))$ such that

$$f_{18}(q) \equiv \sum_{n=1}^{\infty} \sigma_{17}(n)q^n \pmod{\lambda}$$

for some prime ideal $\lambda \mid p$ of a finite extension over $\mathbb{Q}_p$. Note that we can apply the $(N_+^+ N_-^- N_0^0)$-stabilization operator of Construction 40 to obtain a newform $f_{18}^{(N)}$ of weight 18 which has Eisenstein descent of type $(1, 1, N_+, N_-, N_0)$ mod λ. Choose $(N_+, N_-, N_0) = (7, 1, 1)$. Then 7 splits in $K = \mathbb{Q}(\sqrt{-5})$. Furthermore,

$$\Xi(1, 1, 7, 1, 1) = 1 - 7^8 \equiv 25644 \pmod{43867},$$

and thus $\Xi(1, 1, 7, 1, 1) \in \mathbb{Q}$ is not congruent to 0 (mod λ).

Let $F/H_{\mathfrak{N}}/K$ be in situation (S) as defined in Section 2.2. Applying Theorem 7, we determine the nontriviality of the associated generalized Heegner cycle

$$\epsilon_{(f_{18}, \mathbb{N}_K^{-8})/F} \Delta(\mathbb{N}_K^{-8}) \in \epsilon_{(f_{18}, \mathbb{N}_K^{-8})/F} \mathrm{CH}^{17}(X_{16})_{0, E_{f_{18}}}(F).$$

Thus we have constructed an algebraic cycle with nontrivial $(f_{18}, \mathbb{N}_K^{-8})$-isotypic component, whose existence is predicted by the Beilinson–Bloch conjecture since by the Heegner hypothesis we have $L(f_{18}, \mathbb{N}_K^8, 0) = 0$. (See Sections 2.2 and 3.4 for further details.)

5.4. *Application to the Ramanujan Δ function.*

Recall the Ramanujan Δ function, which is a weight-12 normalized newform of level 1 with q-expansion at ∞ given by

$$\Delta(q) = \sum_{n \ge 1} \tau(n)q^n.$$

It is well-known that τ satisfies the congruence $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$, and so, for any $j \geq 1$ and any quadratic Dirichlet character ψ, we have

$$(\theta^j \Delta \otimes \psi)(q) \equiv (\theta^j E_{12} \otimes \psi)(q) \pmod{691},$$

i.e., $\Delta \otimes \psi$ has partial Eisenstein descent over $\mathbb{Q}_p$ of type $(\psi, \psi, 1, 1, 1)$ at 691. Choosing an auxiliary imaginary quadratic field K satisfying Assumptions 1 with respect to $(681, \Delta \otimes \psi)$ and applying Theorem 7, we get:

Theorem 43.

$$\left(\frac{691^6 - \psi(691)\tau(691) + 691^5}{691^6 \cdot 5!} \right)^2 \left(\mathrm{AJ}_{F'_{\mathfrak{p}'}}(\Delta_{\Delta \otimes \psi}(\mathbb{N}_K^{-5}))(\omega_\Delta \wedge \omega_A^5 \eta_A^5) \right)^2$$

$$\equiv \frac{(B_{6,\psi_0} B_{1,\psi_0 \varepsilon_K \omega^{-6}})^2}{576} \pmod{691 \mathcal{O}_{F'}},$$

where ψ_0 is defined as in Definition 6.

Corollary 44. *Let $F/H_{\mathfrak{N}}/K$ be in situation (S) as defined in Section 2.2. Suppose ψ is a quadratic character and K is an imaginary quadratic field with odd discriminant $D_K < -4$ such that*

(1) $691 \nmid \mathfrak{f}(\psi)$,

(2) *each prime factor of $691 \cdot \mathfrak{f}(\psi)$ splits in K,*

(3) $691 \nmid B_{6,\psi_0} B_{1,\psi_0 \varepsilon_K \omega^{-6}}$.

Then

$$\epsilon_{(\Delta \otimes \psi, \mathbb{N}_K^{-5})/F} \Delta_{\Delta \otimes \psi}(\mathbb{N}_K^{-5}) \in \epsilon_{(\Delta \otimes \psi, \mathbb{N}_K^{-5})/F} \mathrm{CH}^{11}(X_{10})_{0,\mathbb{Q}}(F)$$

is nontrivial.

To elucidate this result, we include the following table exhibiting a few values of quadratic characters ψ over $\mathbb{Q}$ and imaginary quadratic fields K for which Theorem 43 implies the conclusion of Corollary 44:

K_ψ	$\mathfrak{f}(\psi)$	K	$B_{6,\psi_0} B_{1,\psi_0 \varepsilon_K \omega^{-6}} \pmod{691}$
$\mathbb{Q}(\sqrt{3})$	12	$\mathbb{Q}(\sqrt{-23})$	583
$\mathbb{Q}(\sqrt{3})$	12	$\mathbb{Q}(\sqrt{-95})$	126
$\mathbb{Q}(\sqrt{13})$	13	$\mathbb{Q}(\sqrt{-10})$	583
$\mathbb{Q}(\sqrt{-7})$	-7	$\mathbb{Q}(\sqrt{-10})$	176

5.5. Application to elliptic curves. We now focus on the case where $f_E \in S_2(\Gamma_0(N))$ is the weight-2 normalized newform associated with an elliptic curve $E/\mathbb{Q}$. If $E[p]$ is reducible, by Theorem 35, f_E has Eisenstein descent over $\mathbb{Q}_p$ mod p. We now prove our main application to elliptic curves, which is Theorem 13.

Proof of Theorem 13. Recall that f_E determines an invariant differential $\omega_{f_E} = 2\pi i f_E(z)dz \in \Omega^1_{X_1(N)/\mathbb{Q}}$. Let $\Phi_E : X_1(N) \twoheadrightarrow E$ be a modular parametrization (i.e., the Eichler–Shimura abelian variety quotient $\Phi_{f_E} : X_1(N) \twoheadrightarrow A_{f_E}$, postcomposed with an appropriate isogeny) and let $\omega_E \in \Omega^1_{E/\mathbb{Q}}$ be an invariant differential chosen so that $\Phi_E^* \omega_E = \omega_{f_E}$.

By Theorems 35 and 7 with $k = 2$,

$$\left(\frac{1 - a_p + p}{p}\right)^2 \log^2_{\omega_E} P_E(K) = \left(\frac{1 - a_p + p}{p}\right)^2 \log^2_{\omega_{f_E}} P(K)$$

is congruent to

$$\frac{\Xi^2}{4}\left(\frac{1}{2}(1 - \psi^{-1}(p)) B_{1, \psi_0^{-1}\varepsilon_K} B_{1, \psi_0 \omega^{-1}}\right)^2 \pmod{p\mathcal{O}_{K_{\mathfrak{p}}}}$$

if $\psi \neq 1$ and

$$\frac{\Xi^2}{4}\left(\frac{p - 1}{p}\log_p \bar{\alpha}\right)^2 \pmod{p\mathcal{O}_{K_{\mathfrak{p}}}}$$

if $\psi = 1$, where ψ_0 is defined as in Definition 6 and where

$$\Xi = \prod_{\ell \mid N_+}(1 - \psi^{-1}(\ell)) \prod_{\ell \mid N_-}\left(1 - \frac{\psi(\ell)}{\ell}\right) \prod_{\ell \mid N_0}(1 - \psi^{-1}(\ell))\left(1 - \frac{\psi(\ell)}{\ell}\right).$$

(Note that our congruence holds mod $p\mathcal{O}_{K_{\mathfrak{p}}}$ because both sides of the congruence are defined over $K_{\mathfrak{p}}$ in this situation.)

Our hypotheses on (E, p, K) and part (2) of Theorem 34 (with $k = 2$) ensure that none of the terms on the right-hand side of the above congruences vanish mod p, and hence $\log_{\omega_E} P_E(K) \neq 0$, i.e., $P_E(K)$ is nontorsion.   □

Remark 45. Suppose (E, p) is as in the statement of Theorem 13, and for simplicity suppose ψ is even and nontrivial. Thus, in particular $E[p](\mathbb{Q}) = 0$. We will show (Theorem 54) that there always exists an imaginary quadratic K satisfying the appropriate congruence conditions, so that the theorem gives $\text{rank}_{\mathbb{Z}} E(K) = 1$. In particular, this implies that we should be able to see that $\text{rank}_{\mathbb{Z}} E(\mathbb{Q}) \leq 1$ *a priori* from the congruence conditions on (E, p).

Indeed, one can show that $\text{rank}_{\mathbb{Z}/p} \text{Sel}_p(E/\mathbb{Q}) \leq 1$ (which implies $\text{rank}_{\mathbb{Z}} E(\mathbb{Q}) \leq 1$) through purely algebraic methods. Using standard techniques, one can show that the congruence conditions on (N_+, N_-, N_0) imply $\text{Sel}_p(E/\mathbb{Q}) \subset H^1(\mathbb{Q}, E[p]; \{p\})$. (Here, for $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module M and a finite set Σ of places of $\mathbb{Q}$, $H^1(\mathbb{Q}, M; \Sigma)$ denotes the subgroup of $H^1(\mathbb{Q}, M)$ consisting of classes unramified outside Σ.) See, for example, [Li 2014, Section 2.2] for the case $p = 3$ and E semistable; the case for general $p > 2$ and general E is completely analogous. The hypothesis $p \nmid B_{1, \psi\omega^{-1}}$ (which is equivalent to $p \nmid L_p(\psi, 1)$ since $\psi \neq 1$ and $p \nmid \mathfrak{f}(\psi)$) implies, via the main

theorem of Iwasawa theory over $\mathbb{Q}$ and standard Selmer group control theorems, that $H^1(\mathbb{Q}, \mathbb{F}_p(\psi); \{p\}) = 0$. Since $H^1(\mathbb{Q}, \mathbb{F}_p(\psi); \varnothing) \subset H^1(\mathbb{Q}, \mathbb{F}_p(\psi); \{p\})$, we have $H^1(\mathbb{Q}, \mathbb{F}_p(\psi); \varnothing) = 0$, which in turn implies that $H^1(\mathbb{Q}, \mathbb{F}_p(\psi^{-1}\omega); \{p\}) = \mathbb{Z}/p$ (see, for example, loc. cit. Proposition 2.13). Now if $\mathbb{F}_p(\psi) \subset E[p]$, from the standard long exact sequence of cohomology (see Section 2.3 of loc. cit., for example), one obtains a map $\phi : \mathrm{Sel}_p(E/\mathbb{Q}) \to H^1(\mathbb{Q}, \mathbb{F}_p(\psi^{-1}\omega))$ such that $\ker(\phi) \subset H^1(\mathbb{Q}, \mathbb{F}_p(\psi); \{p\}) = 0$ and $\mathrm{im}(\phi) \subset H^1(\mathbb{Q}, \mathbb{F}_p(\psi^{-1}\omega); \{p\}) = \mathbb{Z}/p$. Thus we get $\mathrm{Sel}_p(E/\mathbb{Q}) \subset \mathrm{im}(\phi) \subset H^1(\mathbb{Q}, \mathbb{F}_p(\psi^{-1}\omega); \{p\}) = \mathbb{Z}/p$. If, on the other hand, $\mathbb{F}_p(\psi^{-1}\omega) \subset E[p]$, one obtains $\phi : \mathrm{Sel}_p(E/\mathbb{Q}) \to H^1(\mathbb{Q}, \mathbb{F}_p(\psi))$ with $\ker(\phi) \subset H^1(\mathbb{Q}, \mathbb{F}_p(\psi^{-1}\omega); \{p\}) = \mathbb{Z}/p$ and $\mathrm{im}(\phi) \subset H^1(\mathbb{Q}, \mathbb{F}_p(\psi); \{p\}) = 0$. Thus we get $\mathrm{Sel}_p(E/\mathbb{Q}) \subset \ker(\phi) \subset H^1(\mathbb{Q}, \mathbb{F}_p(\psi^{-1}\omega); \{p\}) = \mathbb{Z}/p$.

Remark 46. Since the congruence in the proof of Theorem 13 comes from p-adic interpolation of p-adically integral period sums, we should be able to see *a priori* that both sides of the congruence are p-adically integral. This is self-evident for the right-hand side, and also *a priori* true for the left-hand side as follows. Note that since $p \nmid N$, we have $p + 1 - a_p = |\tilde{E}(\mathbb{F}_p)|$ by the Eichler–Shimura relation. Let $\hat{E}$ denote the formal group of E, so that $\hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$ has index $|\tilde{E}(\mathbb{F}_p)|$ in $E(K_\mathfrak{p})$. (Recall that $\mathfrak{p}$ is the previously fixed prime above p determined by our embedding $K \hookrightarrow \overline{\mathbb{Q}}_p$.) Then $[1 - a_p + p]P_E(K) = [|\tilde{E}(\mathbb{F}_p)|]P_E(K) \in \hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$.

Suppose for the moment that $X_1(N) \twoheadrightarrow E$ is optimal (i.e., E is the strong Weil curve in its isogeny class). Well-known results due to Mazur [1978] on the Manin constant $c(E)$ imply that if $\ell \mid c(E)$, then $\ell^2 \mid 4N$. Thus for p odd of good reduction, we have $p \nmid c(E)$. Thus letting $\log_E$ denote the canonical formal logarithm on E (i.e., the formal logarithm arising from the unique normalized invariant differential on E), we have $\log_{\omega_E} T = c(E)^{-1} \log_E T$, meaning our normalization of the formal logarithm does not change the p-divisibility on the formal group. That is, $\log_{\omega_E} \hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}) \subset \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$. Thus by the previous paragraph, $((1 - a_p + p)/p) \log_{\omega_E} P_E(K)$ is p-adically integral.

For E nonoptimal, the choice of modular parametrization might change the normalization of the formal logarithm, since we are postcomposing the Eichler–Shimura projection with a $\mathbb{Q}$-isogeny which does not necessarily preserve normalizations of the formal logarithm. This can still be shown to not affect p-adic integrality of $\log_{\omega_E}$ on $\hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$.

Remark 47. Suppose that (E, p, K) is as in the hypotheses of Theorem 13. One can show that $\log_{\omega_E} P_E(K) \equiv 0 \pmod{p}$ as follows. Let $F = K(\mu_p)$, and choose a prime $\pi \mid p$ of F; note that $\mathfrak{p}$ is totally ramified in $K(\mu_p)$, so that $\mathcal{O}_{F_\pi}/\pi \cong \mathbb{F}_p$ and $\mathrm{ord}_\pi(p) = p - 1$. If $P_K(E)$ is torsion, then $\log_{\omega_E} P_E(K) = 0$ by properties of the formal logarithm (see [Silverman 2009, Chapter 4]), so assume that $P_E(K)$ is nontorsion. Suppose $\psi \neq 1$. Then $|\tilde{E}(\mathbb{F}_p)| - (1 + p) = -a_p \equiv -\psi(p) \neq -1 \pmod{p}$

implies $|\tilde{E}(\mathbb{F}_p)| \not\equiv 0 \pmod p$. Therefore, $\hat{E}(\pi \mathcal{O}_{F_\pi})$ has index prime to p in $E(F_\pi)$, and so $\log_{\omega_E} E(F_\pi) \subset \pi \mathcal{O}_{F_\pi}$, and $\log_{\omega_E} P_E(K) \in \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$.

Now suppose $\psi = 1$, so that $|\tilde{E}(\mathbb{F}_p)| - (1 + p) = -a_p \equiv -\psi(p) = -1 \pmod p$, and so $|\tilde{E}(\mathbb{F}_p)| \equiv 0 \pmod p$. Moreover, p is ordinary good reduction and so $|\tilde{E}(\mathbb{F})[p]| = |\tilde{E}(\overline{\mathbb{F}}_p)| = p$ implies $p \,|\, |\tilde{E}(\mathbb{F}_p)|$. Then, by Theorem 35, we have $E[p] = E(F)[p]$, and so the exact sequence

$$0 \to \hat{E}(\pi \mathcal{O}_{F_\pi}) \to E(F_\pi) \to \tilde{E}(\mathbb{F}_p) \to 0$$

splits, i.e., $E(F_\pi) = \hat{E}(\pi \mathcal{O}_{F_\pi}) \oplus \tilde{E}(\mathbb{F}_p)$, and moreover $\tilde{E}(\mathbb{F}_p) \subset E(F_\pi)^{\text{tor}}$. (The torsion of $E(F_\pi)$ that is outside of p injects into $\tilde{E}(\mathbb{F}_p)$, and $\tilde{E}(\mathbb{F}_p)[p] \subset E(F_\pi)[p]$.) Thus since $\log_{\omega_E} \hat{E}(\pi \mathcal{O}_{F_\pi}) \subset \pi \mathcal{O}_{F_\pi}$ and $\log_{\omega_E} \tilde{E}(\mathbb{F}_p) = 0$, we have $\log_{\omega_E} P_E(K) \in \pi \mathcal{O}_{F_\pi}$. Now since $P_E(K) \in E(K) \subset E(K_\mathfrak{p})$, we have $\log_{\omega_E} P_E(K) \in K_\mathfrak{p} \cap \pi \mathcal{O}_{F_\pi} = \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$.

Remark 48. While the proof of Theorem 13 accounts for the case $\psi = 1$, it gives no new information since the left side of the relevant special value congruence is always 0 (mod p): Remark 47 shows that $\log_{\omega_E} P_E(K) \equiv 0 \pmod p$, and $a_p \equiv \psi(p) = 1 \pmod p$ implies that $(1 - a_p + p)/p$ is a unit in $\mathcal{O}_{\mathbb{C}_p}$. Note that this forces $\Xi(1, N_{\text{split}}, N_{\text{nonsplit}}, N_{\text{add}}) \equiv 0 \pmod p$.

In fact, if $\psi = 1$, one can show that, for any elliptic curve, $N_{\text{split}} N_{\text{add}} \neq 1$ in the following way: assume $N_{\text{add}} = 1$, so that N is squarefree. A theorem of Ribet then shows that $N_{\text{split}} \neq 1$ (see the Ph.D. thesis of Hwajong Yoo [2015, Theorem 2.2] and the ensuing remark therein). Thus if $\psi = 1$, we have $\Xi(1, N_{\text{split}}, N_{\text{nonsplit}}, N_{\text{add}}) = 0$.

When $\psi \neq 1$, we have $a_p \equiv \psi(p) \neq 1 \pmod p$, and so the factor of $(1 - a_p + p)/p$ is congruent to (unit)$/p \pmod p$, thus canceling out a p-divisibility of $\log_{\omega_E} P_E(K)$ in the special value congruence.

Remark 49. Suppose we are in the situation of Theorem 13, so in particular $p \nmid N$ is a good prime which is split in K. Let ϖ be a local uniformizer at $\mathfrak{p}$. (Recall that $\mathfrak{p}$ is the prime above p determining the embedding $K \hookrightarrow \overline{\mathbb{Q}}_p$.) Then as $1 - a_p + p = |\tilde{E}(\mathbb{F}_p)|$, we have that $P := [1 - a_p + p]P_E(K)$ belongs to the formal group $\hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$. One can show that $\log_E P \in \varpi \mathcal{O}_{K_\mathfrak{p}}^\times = p\mathcal{O}_{K_\mathfrak{p}}^\times$ if and only if the image of P in $E(K_\mathfrak{p})/pE(K_\mathfrak{p})$ is not in the image of $E(K_\mathfrak{p})[p]$ as follows. If P is not in the image of $E(K_\mathfrak{p})[p]$ in $E(K_\mathfrak{p})/pE(K_\mathfrak{p})$, then suppose $\log_E P \notin \varpi \mathcal{O}_{K_\mathfrak{p}}^\times$. Since $P \in \hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$, we know that P is either torsion (i.e., $\log_E P = 0$) or $P \in \mathfrak{p}^2 \mathcal{O}_{K_\mathfrak{p}}$ (i.e., $\log_E P \in \mathfrak{p}^2 \mathcal{O}_{K_\mathfrak{p}}$). However, in the first case this implies $P \in E(K_\mathfrak{p})[p]$ (since $\hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$ has no p-torsion) and in the second it implies $P \in \hat{E}(\mathfrak{p}^2 \mathcal{O}_{K_\mathfrak{p}})$; thus P is p-divisible. Therefore, $P \in \hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}) + pE(K_\mathfrak{p})$, a contradiction. Conversely, if $\log_E P \in \varpi \mathcal{O}_{K_\mathfrak{p}}^\times$, then we have $P \notin E(K_\mathfrak{p})[p] + pE(K_\mathfrak{p})$; otherwise, we have $P \in E(K_\mathfrak{p})[p] + p\hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$ (since *a priori* $P \in \hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})$); thus $\log_E P \in \mathfrak{p}^2 \mathcal{O}_{K_\mathfrak{p}}$, a contradiction.

Thus the nonvanishing results of $\log_E P$ mod p provided by Theorem 13 give information on local p-divisibility of P (and thus also of $P_E(K)$). Note that if $p \geq 3$, then $\hat{E}(\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})[p] = 0$, and so $E(K_\mathfrak{p})[p] \hookrightarrow \tilde{E}(\mathbb{F}_p)[p]$. In particular, if p is of supersingular reduction, then $\tilde{E}(\mathbb{F}_p)[p] = 0$, so $E(K_\mathfrak{p})[p] = 0$ and the nonvanishing of $\log_E P$ mod p is equivalent to P having nontrivial image in $E(K_\mathfrak{p})/pE(K_\mathfrak{p})$, i.e., the condition that P not be p-divisible in $E(K_\mathfrak{p})$.

For any elliptic curve E over $\mathbb{Q}$, let $w(E)$ denote the global root number, which factors as a product of local root numbers

$$w(E) = w_\infty(E) \prod_{\ell < \infty} w_\ell(E).$$

Proposition 50. *Suppose that (E, p) is as in Theorem 13 and that ψ is a quadratic character. If either*

(1) $p \geq 5$, *or*

(2) $E = E' \otimes \psi$ *for some semistable elliptic curve E' of conductor coprime to $\mathfrak{f}(\psi)$,*

then $w(E) = -\psi(-1)$. Thus, $\operatorname{rank}_\mathbb{Z} E(\mathbb{Q}) = \frac{1}{2}(1 + \psi(-1))$, and $\operatorname{rank}_\mathbb{Z} E_K(\mathbb{Q}) = \frac{1}{2}(1 - \psi(-1))$ for any imaginary quadratic K as in Theorem 13.

Proof. By our assumptions in the statement of Theorem 13, $|\mathfrak{f}(\psi)|^2 \mid N_{\mathrm{add}}$ and $N_{\mathrm{split}} = 1$. By standard properties of the root number (see [Dokchitser 2013, Section 3.4]), we have

(1) if $\ell \parallel N$ (i.e., $\ell \mid N_{\mathrm{nonsplit}}$), then $w_\ell(E) = 1$,

(2) $w_\infty(E) = -1$.

Hence,

$$w(E) = -\prod_{\ell \mid N_{\mathrm{add}}} w_\ell(E).$$

Suppose first that (1) in the statement of the proposition holds, i.e., $p \geq 5$. By Theorem 34, $\bar{\rho}_{f_E} \cong \mathbb{F}_p \oplus \mathbb{F}_p(\omega)$. Hence $\bar{\rho}_{f_E} \cong \mathbb{F}_p(\psi) \oplus \mathbb{F}_p(\psi^{-1}\omega)$ and thus E admits a degree p isogeny $\phi : E \to E'$. Since $p \geq 5$, by [Dokchitser 2013, Theorem 3.25], for $\ell \mid N_{\mathrm{add}}$ we have

$$w_\ell(E) = (-1, F/\mathbb{Q}_\ell),$$

where $F := \mathbb{Q}_\ell$ (coordinates of points in $\ker(\phi)$), and where $(\,\cdot\,, F/\mathbb{Q}_\ell)$ is the norm residue symbol. By our assumptions, we see that $F = \mathbb{Q}_\ell(\mu_{2p}, \sqrt{\psi(-1)|\mathfrak{f}(\psi)|})$, which is ramified only if $\ell \mid p\mathfrak{f}(\psi)$. Thus $\mathbb{Q}_\ell(\mu_{2p})/\mathbb{Q}_\ell$ is an unramified extension. Thus, by class field theory, $(-1, F/\mathbb{Q}_\ell) = (-1, \mathbb{Q}_\ell(\sqrt{\psi(-1)|\mathfrak{f}(\psi)|})/\mathbb{Q}_\ell) = \psi_\ell(-1)$, and so $w_\ell(E) = \psi_\ell(-1)$. Hence, in all, we have

$$w(E) = -\prod_{\ell \mid N_{\mathrm{add}}} w_\ell(E) = -\prod_{\ell \mid N_{\mathrm{add}}} \psi_\ell(-1) = -\psi(-1),$$

where the last equality follows since $\mathfrak{f}(\psi) \mid N_{\text{add}}$.

Now suppose that (2) in the statement of the proposition holds. Let N' denote the conductor of E'. By the computations of [Balsam 2014, Proposition 1] describing the changes of local root numbers under quadratic twists,

(1) if $\ell \nmid N' \mathfrak{f}(\psi)$ then $w_\ell(E) = 1$,

(2) if $\ell \mid N'$ (so that $\ell \nmid \mathfrak{f}(\psi)$) then $w_\ell(E) = w_\ell(E')\psi_\ell(\ell) = -a_\ell(E')\psi_\ell(\ell)$,

(3) if $\ell \mid \mathfrak{f}(\psi)$ (so that $\ell \nmid N'$) then $w_\ell(E) = w_\ell(E')\psi_\ell(-1) = \psi_\ell(-1)$.

Hence by our assumptions in the statement of Theorem 13 and Remark 15, we have $w(E) = -\psi(-1) \prod_{\ell \mid N'} (-a_\ell(E')\psi_\ell(\ell)) = -\psi(-1)$. Putting this together, we compute $w(E) = -\psi(-1)$.

Now, by Theorem 13 and parity considerations, we immediately get $\text{rank}_{\mathbb{Z}} E(\mathbb{Q}) = \frac{1}{2}(1 + \psi(-1))$ and $\text{rank}_{\mathbb{Z}} E_K(\mathbb{Q}) = \frac{1}{2}(1 - \psi(-1))$ for any K as in Theorem 13. $\square$

5.6. *Calculating ranks in positive density subfamilies of quadratic twists.* In the case $p = 3$, the Teichmüller character ω is quadratic and is in fact the character associated with the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$. Thus we have (using $B_{1,\psi\omega^{-1}} = -L(\psi\omega^{-1}, 0)$, the functional equation, and the class number formula),

$$B_{1,\psi\omega^{-1}} = 2\frac{h_{K_\psi \cdot \mathbb{Q}(\sqrt{-3})}}{\left|\mathcal{O}^\times_{K_\psi \cdot \mathbb{Q}(\sqrt{-3})}\right|}.$$

Hence our nondivisibility criterion involving Bernoulli numbers in Theorem 13 reduces to the non-3-divisibility of the class numbers of a pair of imaginary quadratic fields, and is thus amenable to class number 3-divisibility results in the tradition of [Davenport and Heilbronn 1971].

For the remainder of this section, suppose $p = 3$ and suppose we are given $E/\mathbb{Q}$ of conductor $N = N_{\text{split}} N_{\text{nonsplit}} N_{\text{add}}$ such that $E[3]$ is reducible of type $(1, 1, N_{\text{split}}, N_{\text{nonsplit}}, N_{\text{add}})$. Let $L = K_\psi$, and furthermore suppose that L satisfies the congruence conditions

(1) 3 is inert in L,

(2) $3 \nmid h_{L \cdot \mathbb{Q}(\sqrt{-3})}$,

(3) if $\ell \mid N_{\text{split}}$, then ℓ is inert or ramified in L,

(4) if $\ell \mid N_{\text{nonsplit}}$, then ℓ is either split or ramified in L,

(5) if $\ell \mid N_{\text{add}}$, then ℓ is either inert in L and $\ell \not\equiv 2 \pmod{3}$, or ℓ is ramified in L.

Then we can apply Theorem 13 and Proposition 50 to the curve $E \otimes \psi$ (using the fact that $a_\ell(E \otimes \psi) = \psi(\ell)a_\ell(E)$, so that, by conditions (2) and (3), $a_\ell(E \otimes \psi) = -1$ for $\ell \mid N_{\text{split}} N_{\text{nonsplit}}$), thus obtaining $\text{rank}_{\mathbb{Z}}(E \otimes \psi)(\mathbb{Q}) = \frac{1}{2}(1 + \psi(-1))$. Using results of [Nakagawa and Horie 1988] and [Taya 2000] regarding 3-divisibilities

of class numbers of quadratic fields, we can produce a positive proportion of real quadratic L as above, thus showing that a positive proportion of quadratic twists of E have rank $\frac{1}{2}(1 + \psi(-1))$ over $\mathbb{Q}$.

Using these same class number divisibility results, we can also produce a positive proportion of imaginary quadratic K such that

(1) 3 is split in K,

(2) $3 \nmid h_{L \cdot K}$,

(3) K satisfies the Heegner hypothesis with respect to E,

and thus, using Theorem 13 and Proposition 50, we can show that a positive proportion of imaginary quadratic twists E_K of E have $\text{rank}_{\mathbb{Z}} E_K(\mathbb{Q}) = \frac{1}{2}(1 - \psi(-1))$.

To this end, let us recall the result of Horie and Nakagawa. For any $x \geq 0$, let $K^+(x)$ denote the set of real quadratic fields k with fundamental discriminant $D_k < x$ and $K^-(x)$ the set of imaginary quadratic fields k with fundamental discriminant $|D_k| < x$. Set

$$K^+(x, m, M) := \{k \in K^+(x) : D_k \equiv m \pmod{M}\},$$

$$K^-(x, m, M) := \{k \in K^-(x) : D_k \equiv m \pmod{M}\}.$$

Moreover, for a quadratic field k, we denote by $h_k[3]$ the number of ideal classes of k whose cubes are principal (i.e., the order of 3-torsion of the ideal class group).

Theorem 51 [Nakagawa and Horie 1988]. *Suppose that m and M are positive integers such that if ℓ is an odd prime number dividing (m, M), then ℓ^2 divides M but not m. Further, if M is even, suppose that*

(1) $4 \mid M$ *and* $m \equiv 1 \pmod 4$, *or*

(2) $16 \mid M$ *and* $m \equiv 8$ *or* $12 \pmod{16}$.

Then

$$\sum_{k \in K^+(x, m, M)} h_k[3] \sim \tfrac{4}{3} |K^+(x, m, M)| \quad (x \to \infty),$$

$$\sum_{k \in K^-(x, m, M)} h_k[3] \sim 2 |K^-(x, m, M)| \quad (x \to \infty).$$

Furthermore,

$$|K^+(x, m, M)| \sim |K^-(x, m, M)| \sim \frac{3x}{\pi^2 \Phi(M)} \prod_{\ell \mid M} \frac{q}{\ell + 1} \quad (x \to \infty).$$

Here $f(x) \sim g(x) \, (x \to \infty)$ means that $\lim_{x \to \infty} f(x)/g(x) = 1$, ℓ ranges over primes dividing M, $q = 4$ if $\ell = 2$, and $q = \ell$ otherwise.

Now set

$$K_*^+(x, m, M) := \{k \in K^+(x, m, M) : h_k[3] = 1\},$$
$$K_*^-(x, m, M) := \{k \in K^-(x, m, M) : h_k[3] = 1\}.$$

Taya's argument [2000] for estimating $|K_*^\pm(x, m, M)|$ goes as follows. Since $h_k[3] \geq 3$ if $h_k[3] \neq 1$, we have the bound

$$|K_*^\pm(x, m, M)| + 3(|K^\pm(x, m, M)| - |K_*^\pm(x, m, M)|) \leq \sum_{k \in K^\pm(x, m, M)} h_k[3].$$

Hence,

$$|K_*^\pm(x, m, M)| \geq \frac{3}{2}|K^\pm(x, m, M)| - \frac{1}{2} \sum_{k \in K^\pm(x, m, M)} h_k[3].$$

Now, by Theorem 51, we have

$$\frac{3}{2}|K^+(x, m, M)| - \frac{1}{2} \sum_{k \in K^+(x, m, M)} h_k[3] \sim \frac{5}{6}|K^+(x, m, M)| \quad (x \to \infty),$$

$$\frac{3}{2}|K^-(x, m, M)| - \frac{1}{2} \sum_{k \in K^-(x, m, M)} h_k[3] \sim \frac{1}{2}|K^-(x, m, M)| \quad (x \to \infty),$$

and hence,

$$\lim_{x \to \infty} \frac{|K_*^+(x, m, M)|}{x} \geq \frac{5}{2\pi^2 \Phi(M)} \prod_{\ell \mid M} \frac{q}{\ell + 1},$$

$$\lim_{x \to \infty} \frac{|K_*^-(x, m, M)|}{x} \geq \frac{3}{2\pi^2 \Phi(M)} \prod_{\ell \mid M} \frac{q}{\ell + 1}.$$

Thus, we have:

Proposition 52. *Suppose m and M satisfy the conditions of Theorem 51. Then*

$$\lim_{x \to \infty} \frac{|K_*^+(x, m, M)|}{|K^+(x, 1, 1)|} \geq \frac{5}{6\Phi(M)} \prod_{\ell \mid M} \frac{q}{\ell + 1},$$

$$\lim_{x \to \infty} \frac{|K_*^-(x, m, M)|}{|K^-(x, 1, 1)|} \geq \frac{1}{2\Phi(M)} \prod_{\ell \mid M} \frac{q}{\ell + 1},$$

where $q = 4$ if $\ell = 2$ and $q = \ell$ otherwise. In particular, the set of real (resp. imaginary) quadratic fields k such that $D_k \equiv m \pmod{M}$ and $3 \nmid h_k$ has positive density in the set of all real (resp. imaginary) quadratic fields.

Proof. This follows from the above asymptotic estimates and the fact that we have $|K^\pm(x, 1, 1)| \sim 3x/\pi^2$ by Theorem 51. □

We are now ready to prove our positive density results. For a quadratic field L, let E_L denote the quadratic twist of E by L.

Theorem 53. *Suppose* $(N_{\text{split}}, N_{\text{nonsplit}}, N_{\text{add}})$ *is a triple of pairwise coprime integers such that* $N_{\text{split}}N_{\text{nonsplit}}$ *is squarefree,* N_{add} *is squarefull and* $N_{\text{split}}N_{\text{nonsplit}}N_{\text{add}}$ *equals* N. *If* $2 \nmid N$ *let* $M' = N$, *if* $2 \| N$ *let* $M' = \text{lcm}(N, 8)$, *and if* $4 \mid N$ *let* $M' = \text{lcm}(N, 16)$. *Then a proportion of at least*

$$\frac{1}{12\Phi(M')} \prod_{\substack{\ell \mid N_{\text{split}}N_{\text{nonsplit}} \\ \ell \text{ odd}}} \tfrac{1}{2}(\ell-1) \prod_{\substack{\ell \mid N_{\text{add}} \\ \ell \text{ odd} \\ \ell \equiv 1 \ (\text{mod } 3)}} \tfrac{1}{2}(\ell+2)(\ell-1) \prod_{\substack{\ell \mid N_{\text{add}} \\ \ell \text{ odd} \\ \ell \equiv 2 \ (\text{mod } 3)}} (\ell-1) \prod_{4 \mid N_{\text{add}}} 2 \prod_{\ell \mid 3M'} \frac{q}{\ell+1}$$

real quadratic extensions $L/\mathbb{Q}$ *satisfy*

(1) 3 *is inert in* L,

(2) $3 \nmid h_{L \cdot \mathbb{Q}(\sqrt{-3})}$,

(3) $\ell \mid N_{\text{split}}$ *implies* ℓ *is inert in* L,

(4) $\ell \mid N_{\text{nonsplit}}$ *implies* ℓ *is split in* L,

(5) $\ell \mid N_{\text{add}}$ *implies* ℓ *is inert in* L *and* $\ell \not\equiv 2$ (mod 3), *or* ℓ *is ramified in* L,

(6) $4 \mid N$ *implies* $D_L \equiv 8$ *or* 12 (mod 16).

Moreover, a proportion of at least

$$\frac{1}{4\Phi(M')} \prod_{\substack{\ell \mid N_{\text{split}}N_{\text{nonsplit}} \\ \ell \text{ odd}}} \tfrac{1}{2}(\ell-1) \prod_{\substack{\ell \mid N_{\text{add}} \\ \ell \text{ odd} \\ \ell \equiv 1 \ (\text{mod } 3)}} \tfrac{1}{2}(\ell+2)(\ell-1) \prod_{\substack{\ell \mid N_{\text{add}} \\ \ell \text{ odd} \\ \ell \equiv 2 \ (\text{mod } 3)}} (\ell-1) \prod_{4 \mid N_{\text{add}}} 2 \prod_{\ell \mid 3M'} \frac{q}{\ell+1}$$

imaginary quadratic extensions $L/\mathbb{Q}$ *satisfy*

(1) 3 *is inert in* L,

(2) $3 \nmid h_L$,

(3) $\ell \mid N_{\text{split}}$ *implies* ℓ *is inert in* L,

(4) $\ell \mid N_{\text{nonsplit}}$ *implies* ℓ *is split in* L,

(5) $\ell \mid N_{\text{add}}$ *implies* ℓ *is inert in* L *and* $\ell \not\equiv 2$ (mod 3), *or* ℓ *is ramified in* L,

(6) $4 \mid N$ *implies* $D_L \equiv 8$ *or* 12 (mod 16).

(Here, again, $q = 4$ *for* $\ell = 2$, *and* $q = \ell$ *for odd primes* ℓ.)

Proof. We seek to apply Proposition 52. Let $M = 9N$ if $2 \nmid N$, let $M = 9\,\text{lcm}(N, 8)$ if $2 \| N$, and let $M = 9\,\text{lcm}(N, 16)$ if $4 \mid N$. Using the Chinese remainder theorem, choose a positive integer m such that

(1) $m \equiv 3$ (mod 9),

(2) ℓ odd prime, $\ell \mid N_{\text{split}} \Longrightarrow m \equiv -3$[quadratic nonresidue unit] (mod ℓ),

(3) $2 \mid N_{\text{split}} \Longrightarrow m \equiv 1$ (mod 8),

(4) ℓ odd prime, $\ell \mid N_{\text{nonsplit}} \Longrightarrow m \equiv -3[\text{quadratic residue unit}] \pmod{\ell}$,

(5) $2 \mid N_{\text{nonsplit}} \Longrightarrow m \equiv 5 \pmod 8$,

(6) ℓ odd prime, $\ell \mid N_{\text{add}}$, $\ell \equiv 1 \pmod 3 \Longrightarrow m \equiv -3[\text{quadratic nonresidue unit}]$ $\pmod{\ell}$ or $m \equiv 0 \pmod{\ell}$ and $m \not\equiv 0 \pmod{\ell^2}$,

(7) ℓ odd prime, $\ell \mid N_{\text{add}}$, $\ell \equiv 2 \pmod 3 \Longrightarrow m \equiv 0 \pmod{\ell}$ and $m \not\equiv 0 \pmod{\ell^2}$,

(8) $4 \mid N_{\text{add}} \Longrightarrow m \equiv 8$ or $12 \pmod{16}$.

Suppose L is any real quadratic field with fundamental discriminant D_L and $-3D_L \equiv m \pmod M$. Then the above congruence conditions on m along with our assumptions imply

(1) 3 is inert in L,

(2) ℓ prime, $\ell \mid N_{\text{split}} \Longrightarrow \ell$ is inert in L,

(3) ℓ prime, $\ell \mid N_{\text{nonsplit}} \Longrightarrow \ell$ is split in L,

(4) ℓ odd prime, $\ell \mid N_{\text{add}}$, $\ell \equiv 1 \pmod 3 \Longrightarrow \ell$ is inert or ramified in L,

(5) ℓ odd prime, $\ell \mid N_{\text{add}}$, $\ell \equiv 2 \pmod 3 \Longrightarrow \ell$ is ramified in L,

(6) $4 \mid N_{\text{add}} \Longrightarrow 2$ is ramified in L,

(7) if $2 \parallel N$, then $4 \mid M$ and $m \equiv 1 \pmod 4$,

(8) if $4 \mid N$, then $16 \mid M$ and $m \equiv 8$ or $12 \pmod{16}$.

Thus for real quadratic L such that $D_{L \cdot \mathbb{Q}(\sqrt{-3})} = -3D_L \equiv m \pmod M$, L satisfies all the desired congruence conditions except for possibly $3 \nmid h_{L \cdot \mathbb{Q}(\sqrt{-3})}$. Moreover, the congruence conditions above imply that m and M are valid positive integers for Theorem 51 (in particular implying that $4 \mid D_L$ if $4 \mid N$). (Note that in congruence conditions (2) and (3) above, we do not allow $m \equiv 0 \pmod{\ell}$, i.e., ℓ ramified in L, because the resulting pair m and M would violate the auxiliary hypothesis of Theorem 51.) Thus, by Proposition 52,

$$\lim_{x \to \infty} \frac{|K_*^-(x, m, M)|}{|K^-(x, 1, 1)|} \geq \frac{1}{2\Phi(M)} \prod_{\ell \mid M} \frac{q}{\ell + 1},$$

so a positive proportion of real quadratic L satisfy $D_{L \cdot \mathbb{Q}(\sqrt{-3})} = -3D_L \equiv m \pmod M$ and $3 \nmid h_{L \cdot \mathbb{Q}(\sqrt{-3})}$. Moreover, noticing that the congruence conditions (1)–(6) on m above are independent (again by the Chinese remainder theorem), we have

$$\prod_{\substack{\ell \mid N_{\text{split}} \\ \ell \text{ odd}}} \tfrac{1}{2}(\ell - 1) \prod_{\substack{\ell \mid N_{\text{nonsplit}} \\ \ell \text{ odd}}} \tfrac{1}{2}(\ell - 1) \prod_{\substack{\ell \mid N_{\text{add}} \\ \ell \text{ odd} \\ \ell \equiv 1 \pmod 3}} \tfrac{1}{2}(\ell + 2)(\ell - 1) \prod_{\substack{\ell \mid N_{\text{add}} \\ \ell \text{ odd} \\ \ell \equiv 2 \pmod 3}} (\ell - 1) \prod_{4 \mid N_{\text{add}}} 2$$

valid choices of residue classes for m mod M. Combining all the above and summing over each valid residue class m mod M, we immediately obtain our lower bound for the proportion of valid L (with $M = 9M'$).

For the second case (concerning imaginary quadratic fields), the asserted statement follows from taking M as above, then choosing a positive integer m such that

(1) $m \equiv -1 \pmod 3$,

(2) ℓ odd prime, $\ell \mid N_{\mathrm{split}} \Longrightarrow m \equiv$ [quadratic nonresidue unit] $\pmod \ell$,

(3) $2 \mid N_{\mathrm{split}} \Longrightarrow m \equiv 5 \pmod 8$,

(4) ℓ odd prime, $\ell \mid N_{\mathrm{nonsplit}} \Longrightarrow m \equiv$ [quadratic residue unit] $\pmod \ell$,

(5) $2 \mid N_{\mathrm{nonsplit}} \Longrightarrow m \equiv 1 \pmod 8$,

(6) ℓ odd prime, $\ell \mid N_{\mathrm{add}}$, $\ell \equiv 1 \pmod 3 \Longrightarrow m \equiv$ [quadratic nonresidue unit] $\pmod \ell$ or $m \equiv 0 \pmod \ell$ and $m \not\equiv 0 \pmod{\ell^2}$,

(7) ℓ odd prime, $\ell \mid N_{\mathrm{add}}$, $\ell \equiv 2 \pmod 3 \Longrightarrow m \equiv 0 \pmod \ell$ and $m \not\equiv 0 \pmod{\ell^2}$,

(8) $4 \mid N_{\mathrm{add}} \Longrightarrow m \equiv 8$ or $12 \pmod{16}$,

and proceeding by the same argument as above. $\qquad\square$

Theorem 54. *Suppose $E/\mathbb{Q}$ is any elliptic curve whose mod-3 Galois representation $E[3]$ is reducible of type $(1, 1, N_{\mathrm{split}}, N_{\mathrm{nonsplit}}, N_{\mathrm{add}})$, where 3 is a good prime of E. Let L be any quadratic field such that*

(1) *3 is inert in L,*

(2) *$3 \nmid h_{L \cdot \mathbb{Q}(\sqrt{-3})}$ if L is real, and $3 \nmid h_L$ if L is imaginary,*

(3) *$\ell \mid N_{\mathrm{split}}$ implies ℓ is inert in L,*

(4) *$\ell \mid N_{\mathrm{nonsplit}}$ implies ℓ is split in L,*

(5) *$\ell \mid N_{\mathrm{add}}$ implies ℓ is inert in L and $\ell \not\equiv 2 \pmod 3$, or ℓ is ramified in L,*

(6) *$4 \mid N$ implies $D_L \equiv 8$ or $12 \pmod{16}$.*

Let $M' = \mathrm{lcm}(N, D_L^2)$ if $\mathrm{lcm}(N, D_L^2)$ is odd, $M' = \mathrm{lcm}(N, D_L^2, 8)$ if $2 \parallel \mathrm{lcm}(N, D_L^2)$, and $M' = \mathrm{lcm}(N, D_L^2, 16)$ if $4 \mid \mathrm{lcm}(N, D_L^2)$. Then if L is real for a positive proportion of at least

$$\frac{1}{4\Phi(M')} \prod_{\substack{\ell \mid N_{\mathrm{split}} N_{\mathrm{nonsplit}} \\ \ell \nmid D_L \\ \ell\ \mathrm{odd}}} \tfrac{1}{2}(\ell - 1) \prod_{\substack{\ell \mid N_{\mathrm{add}} \\ \ell \nmid D_L \\ \ell\ \mathrm{odd}}} \tfrac{1}{2}\ell(\ell - 1) \prod_{\substack{\ell \mid D_L \\ \ell\ \mathrm{odd}}} \tfrac{1}{2}(\ell - 1) \prod_{\ell \mid 3M'} \frac{q}{\ell + 1}$$

imaginary quadratic fields K, and if L is imaginary for a positive proportion of at least

$$\frac{1}{12\Phi(M')} \prod_{\substack{\ell \,|\, N_{\mathrm{split}} N_{\mathrm{nonsplit}} \\ \ell \nmid D_L \\ \ell \ \mathrm{odd}}} \tfrac{1}{2}(\ell-1) \prod_{\substack{\ell \,|\, N_{\mathrm{add}} \\ \ell \nmid D_L \\ \ell \ \mathrm{odd}}} \tfrac{1}{2}\ell(\ell-1) \prod_{\substack{\ell \,|\, D_L \\ \ell \ \mathrm{odd}}} \tfrac{1}{2}(\ell-1) \prod_{\ell \,|\, 3M'} \frac{q}{\ell+1}$$

imaginary quadratic fields K, then K satisfies the Heegner hypothesis with respect to E_L, we have $(D_K, D_L) = 1$, and the Heegner point $P_{E_L}(K)$ is nontorsion. (Here, again, $q = 4$ for $\ell = 2$, and $q = \ell$ for odd primes ℓ.)

Proof. Again we seek to apply Proposition 52, as well as Theorem 13. First suppose that L is a real quadratic field. Let $M = 3 \operatorname{lcm}(N, D_L^2)$ if $\operatorname{lcm}(N, D_L^2)$ is odd, $M = 3 \operatorname{lcm}(N, D_L^2, 8)$ if $2 \,\|\, \operatorname{lcm}(N, D_L^2)$, and $M = 3 \operatorname{lcm}(N, D_L^2, 16)$ otherwise. Using the Chinese remainder theorem, choose a positive integer m such that

(1) $m \equiv 2 \pmod 3$,

(2) ℓ odd prime, $\ell \,|\, N_{\mathrm{split}} \Longrightarrow m \equiv$ [quadratic nonresidue unit] $\pmod \ell$,

(3) $2 \,|\, N_{\mathrm{split}} \Longrightarrow m \equiv 5 \pmod 8$,

(4) ℓ prime, $\ell \,|\, N_{\mathrm{nonsplit}} \Longrightarrow m \equiv$ [quadratic residue unit] $\pmod \ell$,

(5) $2 \,|\, N_{\mathrm{nonsplit}} \Longrightarrow m \equiv 1 \pmod 8$,

(6) ℓ odd prime, $\ell \,|\, N_{\mathrm{add}}$, $\ell \nmid D_L \Longrightarrow m \equiv$ [quadratic nonresidue unit] $\pmod \ell$,

(7) ℓ odd prime, $\ell \,|\, N_{\mathrm{add}}$, $\ell \,|\, D_L \Longrightarrow m \equiv 0 \pmod \ell$, where $m/D_L \equiv$ [quadratic residue unit] $\pmod \ell$,

(8) $4 \,|\, N \Longrightarrow m \equiv D_L \pmod{16}$.

Suppose K is any imaginary quadratic field with *odd* fundamental discriminant D_K such that $(D_L, D_K) = 1$ and $D_L D_K \equiv m \pmod M$. Since D_K is odd, we must have $D_K \equiv 1 \pmod 4$, and this is compatible with condition (6) which forces $D_K \equiv 1 \pmod 8$, which in turn forces 2 to split in K. Then the above congruence conditions on m, along with the congruence conditions of our assumptions, imply

(1) 3 is inert in L, split in K, and inert in $L \cdot K$,

(2) ℓ prime, $\ell \,|\, N_{\mathrm{split}}$, $\ell \nmid D_L \Longrightarrow \ell$ is inert in L, split in K, and inert in $L \cdot K$,

(3) ℓ prime, $\ell \,|\, N_{\mathrm{nonsplit}}$, $\ell \nmid D_L \Longrightarrow \ell$ is split in L, split in K, and split in $L \cdot K$,

(4) ℓ odd prime, $\ell \,|\, N_{\mathrm{add}}$, $\ell \nmid D_L \Longrightarrow \ell$ is inert in L, split in K, and inert in $L \cdot K$,

(5) ℓ odd prime, $\ell \,|\, D_L \Longrightarrow \ell$ is ramified in L, split in K, and ramified in $L \cdot K$,

(6) $4 \,|\, N_{\mathrm{add}} \Longrightarrow 2$ is ramified in L, split in K, and ramified in $L \cdot K$,

(7) if $2 \,\|\, N$, then $4 \,|\, M$ and $m \equiv 1 \pmod 4$,

(8) if $4 \,|\, N$, then $16 \,|\, M$ and $m \equiv 8$ or $12 \pmod{16}$.

Thus for imaginary quadratic K such that $D_{L \cdot K} = D_L D_K \equiv m \pmod{M}$, $(E, 3, L, K)$ satisfies all the congruence conditions of Theorem 13 except for possibly $3 \nmid h_{L \cdot K}$. Moreover, the congruence conditions above imply that m and M are valid positive integers for Theorem 51. Thus, by Proposition 52,

$$\lim_{x \to \infty} \frac{|K_*^-(x, m, M)|}{|K^-(x, 1, 1)|} \geq \frac{1}{2\Phi(M)} \prod_{\ell \mid M} \frac{q}{\ell + 1},$$

so a positive proportion of imaginary quadratic K satisfy $D_{L \cdot K} \equiv m \pmod{M}$ and $3 \nmid h_{L \cdot K}$. Thus, for these K, $(E, 3, L, K)$ satisfies all the congruence conditions of Theorem 13, and so $P_{E_L}(K)$ is nontorsion. Moreover, noticing that the congruence conditions (1)–(6) on m above are independent (again by the Chinese remainder theorem), we have

$$\prod_{\substack{\ell \mid N_{\text{split}} N_{\text{nonsplit}} \\ \ell \nmid D_L \\ \ell \text{ odd}}} \tfrac{1}{2}(\ell - 1) \prod_{\substack{\ell \mid N_{\text{add}} \\ \ell \nmid D_L \\ \ell \text{ odd}}} \tfrac{1}{2}\ell(\ell - 1) \prod_{\substack{\ell \mid D_L \\ \ell \text{ odd}}} \tfrac{1}{2}(\ell - 1)$$

choices for residue classes of m mod M. Combining all the above and summing over each valid residue class m mod M, we immediately obtain our lower bound for the proportion of valid K (with $M = 3M'$).

For the case when L is an imaginary quadratic field, let M be as above. Then choose a positive integer m such that

(1) $m \equiv 3 \pmod 9$,

(2) ℓ odd prime, $\ell \mid N_{\text{split}} \Longrightarrow m \equiv -3[\text{quadratic nonresidue unit}] \pmod \ell$,

(3) $2 \mid N_{\text{split}} \Longrightarrow m \equiv 1 \pmod 8$,

(4) ℓ odd prime, $\ell \mid N_{\text{nonsplit}} \Longrightarrow m \equiv -3[\text{quadratic residue unit}] \pmod \ell$,

(5) $2 \mid N_{\text{nonsplit}} \Longrightarrow m \equiv 5 \pmod 8$,

(6) ℓ odd prime, $\ell \mid N_{\text{add}}$, $\ell \nmid D_L \Longrightarrow m \equiv -3[\text{quadratic nonresidue unit}] \pmod \ell$,

(7) ℓ odd prime, $\ell \mid D_L \Longrightarrow m \equiv 0 \pmod \ell$, where $m/D_L \equiv -3[\text{quadratic residue unit}] \pmod \ell$,

(8) $4 \mid N \Longrightarrow m \equiv D_L \pmod{16}$.

The argument then proceeds in the same way as above to establish $3 \nmid h_{L \cdot K \cdot \mathbb{Q}(\sqrt{-3})}$ and thus $\text{rank}_{\mathbb{Z}} E_L(K) = 1$ by applying Theorem 13. $\qquad \square$

Proof of Corollary 18. Since $E[3]$ is a reducible mod-3 Galois representation, E has Eisenstein descent of type $(\psi, \psi^{-1}, N_{\text{split}}, N_{\text{nonsplit}}, N_{\text{add}})$ mod 3, where ψ is some quadratic Dirichlet character. We may assume without loss of generality that $\psi = 1$ (after possibly replacing E by $E \otimes \psi^{-1}$). From Theorem 53, a positive proportion of quadratic twists E_L satisfy the conditions of Theorem 54, and so

by that theorem a positive proportion of imaginary quadratic K have that $P_{E_L}(K)$ is nontorsion. If E is semistable, then E necessarily has Eisenstein descent of type $(1, 1, N_{\text{split}}, N_{\text{nonsplit}}, N_{\text{add}})$ by part (3) of Theorem 34 and by Theorem 35. Since $N_{\text{add}} = 1$, Theorems 53 and 54 produce twists E_L with $(N, D_L) = 1$ and $\text{rank}_{\mathbb{Z}} E(K) = 1$. Then by part (2) of Proposition 50, each E_L has $w(E_L) = -\varepsilon_L(-1)$ and so $\text{rank}_{\mathbb{Z}} E_L(\mathbb{Q}) = \frac{1}{2}(1 + \varepsilon_L(-1))$ and $\text{rank}_{\mathbb{Z}} E_{L \cdot K}(\mathbb{Q}) = \frac{1}{2}(1 - \varepsilon_L(-1))$. The more precise lower bounds on these positive proportions follow immediately from Theorems 53 and 54. □

Remark 55. There is no "double counting" resulting from using the lower bounds of Theorems 53 and 54 in tandem. The real quadratic twists E_L produced in Theorem 53, which have discriminant D_L prime to D_K, are distinct from the real twists $E_{L' \cdot K}$ produced in Theorem 54 (with L' imaginary), which have discriminant $D_{L'} D_K$. Similarly, the imaginary quadratic twists produced in Theorem 53 are distinct from those produced in Theorem 54.

Example 56. Let $E/\mathbb{Q}$ be the elliptic curve 19a1 in Cremona's labeling, which has minimal Weierstrass model

$$y^2 + y = x^3 + x^2 - 9x - 15.$$

Then $E(\mathbb{Q})^{\text{tor}} = \mathbb{Z}/3$, and so taking $p = 3$, one sees that $E[3]$ is a reducible mod-3 Galois representation. Furthermore, E has conductor $N = 19$, where 19 is of split multiplicative reduction. Taking the real quadratic field $L = \mathbb{Q}(\sqrt{41})$, one can check that 3 and 19 are inert in L. Taking the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-2})$, one sees that 3 splits in K and that K satisfies the Heegner hypothesis with respect to the quadratic twist E_L (and 3 and 19 split in K). Furthermore, 3 does not divide the class numbers $h_{L \cdot \mathbb{Q}(\sqrt{-3})} = h_{\mathbb{Q}(\sqrt{-123})} = 4$ and $h_{L \cdot K} = h_{\mathbb{Q}(\sqrt{-82})} = 2$. Our result now gives $\text{rank}_{\mathbb{Z}} E_L(K) = 1$. By Proposition 50, one sees that $\text{rank}_{\mathbb{Z}} E_L(\mathbb{Q}) = 1$ and $\text{rank}_{\mathbb{Z}} E_{L \cdot K}(\mathbb{Q}) = 0$. Taking the imaginary quadratic field $L' = \mathbb{Q}(\sqrt{-7})$, one can check that 3 and 19 are inert in L'. Furthermore, 3 does not divide the class numbers $h_{L'} = 1$ and $h_{L' \cdot K \cdot \mathbb{Q}(\sqrt{-3})} = h_{\mathbb{Q}(\sqrt{-42})} = 4$, so by Proposition 50 one sees that $\text{rank}_{\mathbb{Z}} E_{L'}(\mathbb{Q}) = 0$ and $\text{rank}_{\mathbb{Z}} E_{L' \cdot K}(\mathbb{Q}) = 1$. By Corollary 18 (and adding the explicit lower bounds given in Theorems 53 and 54 applied to E, E_L and $E_{L'}$), at least $\frac{19}{640} + \frac{19}{10240} = \frac{323}{10240}$ real quadratic twists of E have rank 1 and at least $\frac{57}{640} + \frac{19}{17920} = \frac{323}{3584}$ imaginary quadratic twists of E have rank 0.

Acknowledgements

References

[Atkin and Lehner 1970] A. O. L. Atkin and J. Lehner, "Hecke operators on $\Gamma_0(m)$", *Math. Ann.* **185** (1970), 134–160. MR 42 #3022 Zbl 0177.34901

[Balsam 2014] N. Balsam, "The parity of analytic ranks among quadratic twists of elliptic curves over number fields", preprint, 2014. arXiv http://arxiv.org/abs/1404.4964

[Bertolini and Darmon 2005] M. Bertolini and H. Darmon, "Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions", *Ann. of Math.* (2) **162**:1 (2005), 1–64. MR 2006g:11218 Zbl 1093.11037

[Bertolini et al. 2013] M. Bertolini, H. Darmon, and K. Prasanna, "Generalized Heegner cycles and p-adic Rankin L-series", *Duke Math. J.* **162**:6 (2013), 1033–1148. MR 3053566 Zbl 1302.11043

[Bertolini et al. 2015] M. Bertolini, H. Darmon, and K. Prasanna, "p-adic L-functions and the coniveau filtration on Chow groups", *J. Reine Angew. Math.* (online publication April 2015), 1–66.

[Billerey and Menares 2013] N. Billerey and R. Menares, "On the modularity of reducible mod l Galois representations", preprint, 2013. arXiv 1309.3717

[Davenport and Heilbronn 1971] H. Davenport and H. Heilbronn, "On the density of discriminants of cubic fields, II", *Proc. Roy. Soc. London Ser. A* **322**:1551 (1971), 405–420. MR 58 #10816 Zbl 0212.08101

[Deligne 1971] P. Deligne, "Formes modulaires et représentations l-adiques", exposé no. 355, 139–172 in *Séminaire Bourbaki* 1968/69, Lecture Notes in Math. **175**, Springer, Berlin, 1971. MR 3077124 Zbl 0206.49901

[Deligne and Serre 1974] P. Deligne and J.-P. Serre, "Formes modulaires de poids 1", *Ann. Sci. École Norm. Sup. (4)* **7** (1974), 507–530. MR 0379379 Zbl 0321.10026

[Deninger 1990] C. Deninger, "Higher regulators and Hecke L-series of imaginary quadratic fields, II", *Ann. of Math.* (2) **132**:1 (1990), 131–158. MR 91i:19003 Zbl 0721.14005

[Diamond 1979] J. Diamond, "On the values of p-adic L-functions at positive integers", *Acta Arith.* **35**:3 (1979), 223–237. MR 80j:12013 Zbl 0463.12007

[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

[Dokchitser 2013] T. Dokchitser, "Notes on the parity conjecture", pp. 201–249 in *Elliptic curves, Hilbert modular forms and Galois deformations*, edited by H. Darmon et al., Birkhäuser/Springer, Basel, 2013. MR 3184338 Zbl 1323.11047

[Geisser 1997] T. Geisser, "p-adic K-theory of Hecke characters of imaginary quadratic fields and an analogue of Beilinson's conjectures", *Duke Math. J.* **86**:2 (1997), 197–238. MR 97m:11086 Zbl 0899.11056

[Gelbart 1975] S. S. Gelbart, *Automorphic forms on adèle groups*, Annals of Mathematics Studies **83**, Princeton University Press, Princeton, N.J., University of Tokyo Press, Tokyo, 1975. MR 52 #280 Zbl 0329.10018

[Gouvêa 1988] F. Q. Gouvêa, *Arithmetic of p-adic modular forms*, Lecture Notes in Mathematics **1304**, Springer, Berlin, 1988. MR 91e:11056 Zbl 0641.10024

[Gross 1980] B. H. Gross, "On the factorization of *p*-adic *L*-series", *Invent. Math.* **57**:1 (1980), 83–95. MR 82a:12010 Zbl 0472.12011

[Gross 1990] B. H. Gross, "A tameness criterion for Galois representations associated to modular forms (mod *p*)", *Duke Math. J.* **61**:2 (1990), 445–517. MR 91i:11060 Zbl 0743.11030

[Harron and Snowden 2015] R. Harron and A. Snowden, "Counting elliptic curves with prescribed torsion", *J. Reine Angew. Math.* (online publication January 2015), 1–20.

[Hida and Tilouine 1993] H. Hida and J. Tilouine, "Anti-cyclotomic Katz *p*-adic *L*-functions and congruence modules", *Ann. Sci. École Norm. Sup.* (4) **26**:2 (1993), 189–259. MR 93m:11044 Zbl 0778.11061

[Katz 1976] N. M. Katz, "*p*-adic interpolation of real analytic Eisenstein series", *Ann. of Math.* (2) **104**:3 (1976), 459–571. MR 58 #22071 Zbl 0354.14007

[Katz 1978] N. M. Katz, "*p*-adic *L*-functions for CM fields", *Invent. Math.* **49**:3 (1978), 199–297. MR 80h:10039 Zbl 0417.12003

[Kolyvagin 1990] V. A. Kolyvagin, "Euler systems", pp. 435–483 in *The Grothendieck Festschrift*, vol. II, edited by P. Cartier et al., Progr. Math. **87**, Birkhäuser, Boston, 1990. MR 92g:11109 Zbl 0742.14017

[Li 2014] Z. K. Li, "Quadratic twists of elliptic curves with 3-Selmer rank 1", *Int. J. Number Theory* **10**:5 (2014), 1191–1217. MR 3231410 Zbl 1297.14037

[Liu et al. 2014] Y. Liu, S. Zhang, and W. Zhang, "On *p*-adic Waldspurger Formula", preprint, 2014, available at https://web.math.princeton.edu/ shouwu/publications/Coleman.pdf.

[Loeffler and Weinstein 2012] D. Loeffler and J. Weinstein, "On the computation of local components of a newform", *Math. Comp.* **81**:278 (2012), 1179–1200. MR 2012k:11064 Zbl 06028404

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162. MR 80h:14022 Zbl 0386.14009

[Mazur 1979] B. Mazur, "On the arithmetic of special values of *L* functions", *Invent. Math.* **55**:3 (1979), 207–240. MR 82e:14033 Zbl 0426.14009

[Nakagawa and Horie 1988] J. Nakagawa and K. Horie, "Elliptic curves with no rational points", *Proc. Amer. Math. Soc.* **104**:1 (1988), 20–24. MR 89k:11113 Zbl 0663.14023

[Robert 1973] G. Robert, *Unités elliptiques*, Société Mathématique de France, Paris, 1973. MR 57 #9669 Zbl 0314.12006

[Scholl 1990] A. J. Scholl, "Motives for modular forms", *Invent. Math.* **100**:2 (1990), 419–430. MR 91e:11054 Zbl 0760.14002

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[Serre 1973] J.-P. Serre, "Congruences et formes modulaires (d'après H. P. F. Swinnerton-Dyer)", exposé no. 416, 319–338 in *Séminaire Bourbaki,* 1971/1972, Lecture Notes in Math. **317**, Springer, Berlin, 1973. MR 57 #5904a Zbl 0276.14013

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009. MR 2010i:11005 Zbl 1194.11005

[Stark 1977] H. M. Stark, "Class fields and modular forms of weight one", pp. 277–287. Lecture Notes in Math., Vol. 601 in *Modular functions of one variable, V* (Proc. Second Internat. Conf., Univ. Bonn, 1976), edited by J.-P. Serre and D. B. Zagier, Springer, Berlin, 1977. MR 56 #8539 Zbl 0363.12010

[Taya 2000] H. Taya, "Iwasawa invariants and class numbers of quadratic fields for the prime 3", *Proc. Amer. Math. Soc.* **128**:5 (2000), 1285–1292. MR 2000j:11162 Zbl 0958.11069

[Vatsal 1999] V. Vatsal, "Canonical periods and congruence formulae", *Duke Math. J.* **98**:2 (1999), 397–419. MR 2000g:11032 Zbl 0979.11027

[Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, New York, 1997. MR 97h:11130 Zbl 0966.11047

[Yoo 2015] H. Yoo, "Nonoptimal levels of a reducible mod l modular representation", preprint, 2015. arXiv 1409.8342

dkriz@princeton.edu   *Department of Mathematics, Princeton University,*
                             Fine Hall, Washington Rd, Princeton, NJ 08544, United States

msp

Squarefree polynomials and Möbius values in short intervals and arithmetic progressions

Jonathan P. Keating and Zeev Rudnick

We calculate the mean and variance of sums of the Möbius function μ and the indicator function of the squarefrees μ^2, in both short intervals and arithmetic progressions, in the context of the ring $\mathbb{F}_q[t]$ of polynomials over a finite field $\mathbb{F}_q$ of q elements, in the limit $q \to \infty$. We do this by relating the sums in question to certain matrix integrals over the unitary group, using recent equidistribution results due to N. Katz, and then by evaluating these integrals. In many cases our results mirror what is either known or conjectured for the corresponding problems involving sums over the integers, which have a long history. In some cases there are subtle and surprising differences. The ranges over which our results hold is significantly greater than those established for the corresponding problems in the number field setting.

1. Introduction

The goal of this paper is to investigate the fluctuation of sums of two important arithmetic functions, the Möbius function μ and the indicator function of the squarefrees μ^2, in the context of the ring $\mathbb{F}_q[t]$ of polynomials over a finite field $\mathbb{F}_q$ of q elements, in the limit $q \to \infty$. The problems we address, which concern sums over short intervals and arithmetic progressions, mirror long-standing questions over the integers, where they are largely unknown. In our setting we succeed in giving definitive answers.

Our approach differs from those traditionally employed in the number field setting: we use recent equidistribution results due to N. Katz, valid in the large-q limit, to express the mean and variance of the fluctuations in terms of matrix integrals over the unitary group. Evaluating these integrals leads to explicit formulae and precise ranges of validity. For many of the problems we study, the formulae we obtain match the corresponding number-field results and conjectures exactly, providing further support in the latter case. However, the ranges of validity that we can establish are significantly greater than those known or previously conjectured for the integers, and we see our results as supporting extensions to much wider ranges of validity in the integer setting. Interestingly, in some other problems we uncover subtle and surprising differences between the function-field and number-field asymptotics, which we examine in detail.

We now set out our main results in a way that enables comparison with the corresponding problems for the integers.

The Möbius function. It is a standard heuristic to assume that the Möbius function behaves like a random ± 1 supported on the squarefree integers, which have density $1/\zeta(2)$ (see, e.g., [Chatterjee and Soundararajan 2012]). Proving anything in this direction is not easy. Even demonstrating cancellation in the sum $M(x) := \sum_{1 \le n \le x} \mu(n)$, that is that $M(x) = o(x)$, is equivalent to the prime number theorem. The Riemann hypothesis is equivalent to square root cancellation: $M(x) = O(x^{1/2+o(1)})$.

For sums of $\mu(n)$ in blocks of length H,

$$M(x; H) := \sum_{|n-x|<H/2} \mu(n) \tag{1-1}$$

it has been shown that there is cancellation for $H \gg x^{7/12+o(1)}$ [Motohashi 1976; Ramachandra 1976], and assuming the Riemann hypothesis one can take $H \gg x^{1/2+o(1)}$. If one wants cancellation only for "almost all" values of x, then more is known. In particular, very recently Matomäki and Radziwiłł [2015] have shown

(unconditionally) that

$$\frac{1}{X} \int_X^{2X} M(x; H)^2 dx = o(H^2)$$

whenever $H = H(X) \to \infty$ as $X \to \infty$, and in particular $M(x; H) = o(H)$ for almost all $x \in [X, 2X]$.

We expect the normalized sums $M(x; H)/\sqrt{H}$ to have mean zero (this follows from the Riemann hypothesis) and variance $6/\pi^2 = 1/\zeta(2)$:

$$\frac{1}{X} \int_X^{2X} |M(x; H)|^2 \sim \frac{H}{\zeta(2)}. \tag{1-2}$$

Moreover, $M(x; H)/\sqrt{H/\zeta(2)}$ is believed to have a normal distribution asymptotically. These conjectures were formulated and investigated numerically by Good and Churchhouse [1968], and further studied by Ng [2008], who carried out an analysis using the generalized Riemann hypothesis and a strong version of Chowla's conjecture on correlations of Möbius, showing that (1-2) is valid for $H \ll X^{1/4-o(1)}$ and that a Gaussian distribution holds (assuming these conjectures) for $H \ll X^\epsilon$. It is important that the length H of the interval be significantly smaller than its location, that is $H < X^{1-\epsilon}$, since otherwise one expects non-Gaussian statistics, see [Ng 2004].

Concerning arithmetic progressions, Hooley [1975] studied the following averaged form of the total variance (averaged over moduli)

$$V(X, Q) := \sum_{Q' \leq Q} \sum_{A \bmod Q'} \left(\sum_{\substack{n \leq X \\ n = A \bmod Q'}} \mu(n) \right)^2 \tag{1-3}$$

and showed that for $Q \leq X$,

$$V(X, Q) = \frac{6QX}{\pi^2} + O(X^2 (\log X)^{-C}) \tag{1-4}$$

for all $C > 0$, which yields an asymptotic result for $X/(\log X)^C \ll Q < X$.

For polynomials over a finite field $\mathbb{F}_q$, the Möbius function is defined as for the integers, namely by $\mu(f) = (-1)^k$ if f is a scalar multiple of a product of k distinct monic irreducibles, and $\mu(f) = 0$ if f is not squarefree. The analogue of the full sum $M(x)$ is the sum over all monic polynomials $\mathcal{M}_n$ of given degree n, for which we have

$$\sum_{f \in \mathcal{M}_n} \mu(f) = \begin{cases} 1, & n = 0, \\ -q, & n = 1, \\ 0, & n \geq 2, \end{cases} \tag{1-5}$$

so that in particular the issue of size is trivial[1]. However that is no longer the case when considering sums over "short intervals", that is over sets of the form

$$I(A; h) = \{f : \|f - A\| \le q^h\} \tag{1-6}$$

where $A \in \mathcal{M}_n$ has degree n, $0 \le h \le n - 2$ and[2] the norm is

$$\|f\| := \#\mathbb{F}_q[t]/(f) = q^{\deg f}. \tag{1-7}$$

To facilitate comparison between statements for number field results and for function fields, we use a rough dictionary:

$$
\begin{aligned}
X &\leftrightarrow q^n, & \log X &\leftrightarrow n, \\
H &\leftrightarrow q^{h+1}, & \log H &\leftrightarrow h + 1.
\end{aligned}
\tag{1-8}
$$

Set

$$\mathcal{N}_\mu(A; h) := \sum_{f \in I(A; h)} \mu(f). \tag{1-9}$$

The number of summands here is $q^{h+1} =: H$ and we want to display cancellation in this sum and study its statistics as we vary the "center" A of the interval.

We can demonstrate cancellation in the short interval sums $\mathcal{N}_\mu(A; h)$ in the large finite field limit $q \to \infty$, n fixed (we assume q is odd throughout the paper).

Theorem 1.1. *If $2 \le h \le n - 2$ then for all A of degree n,*

$$|\mathcal{N}_\mu(A; h)| \ll_n \frac{H}{\sqrt{q}}$$

the implied constant uniform in A, depending only on $n = \deg A$.

For $h = 0$, 1 this is no longer valid; that is, there are A's for which there is no cancellation. See Section 3.

We next investigate the statistics of $\mathcal{N}_\mu(A; h)$ as A varies over all monic polynomials of given degree n, and $q \to \infty$. It is easy to see that for $n \ge 2$, the mean value of $\mathcal{N}_\mu(A; h)$ is 0. Our main result concerns the variance.

Theorem 1.2. *If $0 \le h \le n - 5$ then as $q \to \infty$, q odd,*

$$\operatorname{Var} \mathcal{N}_\mu(\,\cdot\,; h) = \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} |\mathcal{N}_\mu(A; h)|^2 \sim H \int_{U(n-h-2)} |\operatorname{tr} \operatorname{Sym}^n U|^2 \, dU = H$$

---

[1]This ceases to be the case when dealing with function fields of higher genus, see, e.g., [Cha 2011; Humphries 2014].

[2]For $h = n - 1$, $I(A; n - 1) = \mathcal{M}_n$ is the set of all monic polynomials of degree n.

This is consistent with the Good–Churchhouse conjecture (1-2) if we write it as $H/\zeta_q(2)$, where

$$\zeta_q(s) = \sum_{f \text{ monic}} \frac{1}{\|f\|^s}, \quad \text{Re}(s) > 1,$$

which tends to 1 as $q \to \infty$, and $H = q^{h+1}$ is the number of monic polynomials in the short interval.

A version of Theorem 1.2 valid for $h < n/2$ ("very short" intervals) has recently been obtained by Bae, Cha and Jung [2015] using the method of our earlier paper [Keating and Rudnick 2014].

Analogous results can be obtained for sums over arithmetic progressions, see Section 8.

Squarefrees. It is well known that the density of squarefree integers is $1/\zeta(2) = 6/\pi^2$, and an elementary sieve shows

$$Q(x) := \#\{n \le x : n \text{ squarefree}\} = \frac{x}{\zeta(2)} + O(x^{1/2}). \tag{1-10}$$

No better exponent is known for the remainder term. Using zero-free regions for $\zeta(s)$, Walfisz gave a remainder term of the form $x^{1/2} \exp(-c(\log x)^{3/5+o(1)})$. Assuming the Riemann hypothesis, the exponent $1/2$ has been improved [Axer 1911; Montgomery and Vaughan 1981; Baker and Pintz 1985], currently to $17/54 = 0.31$ [Jia 1993]. It is expected that

$$Q(x) = \frac{x}{\zeta(2)} + O(x^{1/4+o(1)}). \tag{1-11}$$

Since the density is known, we wish to understand to what extent we can guarantee the existence of squarefrees in short intervals $(x, x + H]$; moreover, when do we still expect to have an asymptotic formula for the number

$$Q(x, H) := \sum_{|n-x| \le \frac{H}{2}} \mu^2(n) = Q(x + H) - Q(x) \tag{1-12}$$

of squarefrees in the interval $(x, x + H]$; that is, when do we still have

$$Q(x; H) \sim \frac{H}{\zeta(2)}. \tag{1-13}$$

In view of the bound of $O(x^{1/2})$ for the remainder term in (1-10), this holds for $H \gg x^{1/2+o(1)}$. However, one can do better without improving on the remainder term in (1-10). This was first done by Roth [1951] who by an elementary method showed that the asymptotic (1-13) persists for $H \gg x^{1/3+o(1)}$. Following improvements by Roth himself (exponent $3/13$) and Richert [1954] (exponent $2/9$), the current best bound is by Tolev [2006] (building on earlier work by Filaseta and Trifonov)

who gave $H \gg x^{1/5+o(1)}$. It is believed that (1-13) should hold for $H \gg x^{\epsilon}$ for any $\epsilon > 0$, though there are intervals of size $H \gg \log x / \log \log x$ which contain no squarefrees, see [Erdös 1951].

As for almost-everywhere results, one way to proceed goes through a study of the variance of $Q(x, H)$. In this direction, Hall [1982] showed that provided $H = O(x^{2/9-o(1)})$, the variance of $Q(x, H)$ admits an asymptotic formula:

$$\frac{1}{x} \sum_{n \le x} \left| Q(n, H) - \frac{H}{\zeta(2)} \right|^2 \sim A\sqrt{H}, \tag{1-14}$$

with

$$A = \frac{\zeta(3/2)}{\pi} \prod_p \frac{p^3 - 3p + 2}{p^3}. \tag{1-15}$$

Based on our results below, we expect this asymptotic formula to hold for H as large as $x^{1-\epsilon}$.

Concerning arithmetic progressions, denote by

$$S(x; Q, A) = \sum_{\substack{n \le x \\ n = A \bmod Q}} \mu(n)^2$$

the number of squarefree integers in the arithmetic progression $n = A \bmod Q$. Prachar [1958] showed that for $Q < x^{2/3-\epsilon}$, and A coprime to Q,

$$S(x; Q, A) \sim \frac{1}{\zeta(2)} \prod_{p|Q} \left(1 - \frac{1}{p^2}\right)^{-1} \frac{x}{Q} = \frac{1}{\zeta(2)} \prod_{p|Q} \left(1 + \frac{1}{p}\right)^{-1} \frac{x}{\phi(Q)} \tag{1-16}$$

In order to understand the size of the remainder term, one studies the variance

$$\mathrm{Var}(S) = \frac{1}{\phi(Q)} \sum_{\gcd(A,Q)=1} \left| S(x; Q, A) - \frac{1}{\zeta(2)} \prod_{p|Q} \left(1 - \frac{1}{p^2}\right)^{-1} \frac{x}{Q} \right|^2 \tag{1-17}$$

as well as a version where the sum is over all residue classes $A \bmod Q$, not necessarily coprime to Q, and the further averaged form over all moduli $Q' \le Q$ à la Barban, Davenport and Halberstam, see [Warlimont 1980].

Without averaging over moduli, Blomer [2008, Theorem 1.3] gave an upper bound for the variance, which was very recently improved by Nunes [2015], who gave an asymptotic expression for the variance in the range $X^{\frac{31}{41}+\epsilon} < Q < X^{1-\epsilon}$:

$$\mathrm{Var}(S) \sim A \prod_{p|Q} \left(1 - \frac{1}{p}\right)^{-1} \left(1 + \frac{2}{p}\right)^{-1} \frac{X^{1/2}}{Q^{1/2}}, \tag{1-18}$$

where A is given by (1-15). It is apparently not known in what range of Q to expect (1-18) to hold. Based on our results below, we conjecture that (1-18) holds down to $X^\epsilon < Q$.

Our goal here is to study analogous problems for $\mathbb{F}_q[t]$. The total number of squarefree monic polynomials of degree $n > 1$ is (exactly)

$$\sum_{f \in \mathcal{M}_n} \mu(f)^2 = \frac{q^n}{\zeta_q(2)}. \tag{1-19}$$

The number of squarefree polynomials in the short interval $I(A; h)$ is

$$\mathcal{N}_{\mu^2}(A; h) = \sum_{f \in I(A; h)} \mu(f)^2. \tag{1-20}$$

Asymptotics. We show that for any short interval or arithmetic progression, we still have an asymptotic count of the number of squarefrees.

Theorem 1.3. (i) *If* $\deg Q < n$ *and* $\gcd(A, Q) = 1$ *then*

$$\#\{f \in \mathcal{M}_n : f = A \bmod Q \ f \text{ squarefree}\} = \frac{q^n}{|Q|} \left(1 + O_n(1/q)\right).$$

(ii) *If* $0 < h \le n - 2$ *then for all* $A \in \mathcal{M}_n$,

$$\#\{f \in I(A; h) : f \text{ squarefree}\} = \frac{H}{\zeta_q(2)} + O(H/q) = H + O_n(H/q).$$

In both cases the implied constants depend only on n.

Note that for $h = 0$, Theorem 1.3(ii) need not hold: If $q = p^k$ with p a fixed odd prime, $n = p$ then the short interval $I(t^n; 0) = \{t^n + b : b \in \mathbb{F}_q\}$ has no squarefrees, since $t^p + b = (t + b^{q/p})^p$ has multiple zeros for any $b \in \mathbb{F}_q$.

Variance. We are able to compute the variance, the size of which turns out to depend on the parity of the interval-length parameter h in a surprising way.

Theorem 1.4. *Let* $0 \le h \le n - 6$. *Assume* $q \to \infty$ *with all* q's *coprime to* 6.

(i) *If* h *is even then*

$$\operatorname{Var} \mathcal{N}_{\mu^2}(\bullet\,; h) \sim q^{\frac{h}{2}} \int_{U(n-h-2)} |\mathrm{tr}\, \mathrm{Sym}^{\frac{h}{2}+1} U|^2 \, dU = \frac{\sqrt{H}}{\sqrt{q}}$$

(*the matrix integral works out to be* 1).

(ii) *If h is odd then*

$$\operatorname{Var}\mathcal{N}_{\mu^2}(\,\bullet\,;h) \sim q^{\frac{h-1}{2}} \int\limits_{U(n-h-2)} |\mathrm{tr}\, U|^2 \, dU \int\limits_{U(n-h-2)} \left|\mathrm{tr}\, \mathrm{Sym}^{\frac{h+3}{2}} U'\right|^2 dU' = \frac{\sqrt{H}}{q}$$

(*both matrix integrals equal* 1).

To compare with Hall's result (1-14), where the variance is of order $\sqrt{H}$, one wants to set $H = \#I(A;h) = q^{h+1}$ and then in the limit $q \to \infty$ we get smaller variance — either $\sqrt{H}/q^{1/2}$ (h even) or $\sqrt{H}/q$ (h odd). We found this sufficiently puzzling to check the analogue of Hall's result for the polynomial ring $\mathbb{F}_q[t]$ for the large degree limit of *fixed q* and $n \to \infty$. The result, presented in the Appendix, is consistent with Theorem 1.4 in that for $H < (q^n)^{\frac{2}{9}-o(1)}$, the variance is

$$\operatorname{Var}(\mathcal{N}_{\mu^2}(\,\bullet\,;h)) \sim \sqrt{H} \frac{\beta_q}{1-1/q^3} \times \begin{cases} \frac{1+1/q^2}{\sqrt{q}}, & h \text{ even}, \\ \frac{1+1/q}{q}, & h \text{ odd}, \end{cases}$$

so that it is of order $\sqrt{H}$ for fixed q.

We also obtain a similar result for arithmetic progressions. Let $Q \in \mathbb{F}_q[t]$ be a squarefree polynomial of degree ≥ 2, and let A be coprime to Q. We set

$$\mathcal{S}(A) = \sum_{\substack{f = A \bmod Q \\ f \in \mathcal{M}_n}} \mu^2(f). \tag{1-21}$$

The expected value over such A is

$$\langle \mathcal{S} \rangle_Q = \frac{1}{\Phi(Q)} \sum_{\substack{f \in \mathcal{M}_n \\ (f,Q)=1}} \mu^2(f) \sim \frac{q^n/\zeta_q(2)}{\Phi(Q)} \sim \frac{q^n}{|Q|}. \tag{1-22}$$

We will show that the variance satisfies:

Theorem 1.5. *Fix $n > N \geq 1$. For any sequence of finite fields $\mathbb{F}_q$, with q odd, and squarefree polynomials $Q \in \mathbb{F}_q[t]$ with $\deg Q = N + 1$, as $q \to \infty$,*

$$\operatorname{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{|Q|^{1/2}} \times \begin{cases} 1/\sqrt{q}, & n \neq \deg Q \bmod 2, \\ 1/q, & n = \deg Q \bmod 2. \end{cases}$$

General approach. It may be helpful to give an informal sketch of the general approach we take in proving most of the theorems stated above. Short intervals are transformed into sums over special arithmetic progressions, a feature special to function fields that was used in our earlier work [Keating and Rudnick 2014]. Sums involving μ and μ^2 that run over all monic polynomials of a given degree may be evaluated in terms of a zeta function that is the function-field analogue of the Riemann zeta function. Restricting to short intervals or arithmetic progressions

leads to sums over Dirichlet characters involving the associated L-functions. The L-functions in question may be written in terms of unitary matrices. It has recently been established by N. Katz that, in the limit when $q \to \infty$, these matrices become equidistributed in the unitary group, in the sense that the character sums we need are, in the large-q limit, equal to integrals over the unitary group. Evaluating these integrals leads to the formulae appearing in our theorems.

2. Asymptotics for squarefrees: Proof of Theorem 1.3

We want to show that almost all polynomials in an arithmetic progression, or in a short interval are squarefree. We recall the statement:

(i) If $\deg Q < n$ and $\gcd(A, Q) = 1$ then

$$\#\{f \in \mathcal{M}_n : f = A \bmod Q, \ f \text{ squarefree}\} \sim \frac{q^n}{|Q|} \sim \frac{q^n}{\Phi(Q)}. \qquad (2\text{-}1)$$

(ii) If $0 < h \le n - 2$ then

$$\#\{f \in I(A; h) : f \text{ squarefree}\} = \frac{H}{\zeta_q(2)} + O(H/q) = H + O(H/q). \qquad (2\text{-}2)$$

These follow from a general result [Rudnick 2014]:

Theorem 2.1. *Given a separable polynomial $F(x, t) \in \mathbb{F}_q[x, t]$ with squarefree content, the number of monic polynomials $a \in \mathcal{M}_m$, $m > 0$, for which $F(a(t), t)$ is squarefree (in $\mathbb{F}_q[t]$) is asymptotically*

$$q^m + O\big(q^{m-1}\big(m \deg F + \text{Ht}(F)\big) \deg F\big).$$

Here if $F(x, t) = \sum_{j=0}^{\deg F} \gamma_j(t) x^j$ with $\gamma_j(t) \in \mathbb{F}_q[t]$ polynomials, the content of F is $\gcd(\gamma_0, \gamma_1, \dots,)$ and the height is $\text{Ht}(f) = \max_j \deg \gamma_j$.

For an arithmetic progression $f = A \bmod Q$, $f \in \mathcal{M}_n$ monic of degree n, with $\gcd(A, Q) = 1$, $\deg A < \deg Q$, we take the corresponding polynomial to be

$$F(x, t) = A(t) + \frac{1}{\text{sign } Q} Q(t) x,$$

where $\text{sign } Q \in \mathbb{F}_q^\times$ is such that $Q(t)/\text{sign } Q$ is monic. Then $F(x, t)$ has degree one (in x), hence is certainly separable, and has content equal to $\gcd(A, Q) = 1$, so is in fact primitive. The height of F is $\max(\deg Q, \deg A) = \deg Q < n$ which is independent of q.

Since $\deg A < \deg Q$, it follows that $f = A + aQ/\text{sign}(Q)$ is monic of degree n if and only if a is monic of degree $n - \deg Q > 0$, and by Theorem 2.1 the number

of such a for which $F(a(t), t)$ is squarefree is

$$q^{n-\deg Q} + O(q^{n-\deg Q-1}) = \frac{q^n}{|Q|}(1 + O(1/q)).$$

This proves (2-1).

To deal with the short interval case, let $0 < h \le n - 2$, and $A \in \mathcal{M}_n$ be monic of degree n. We want to show that the number of polynomials f in the short interval $I(A; h)$ which are squarefree is $H + O(H/q)$ (recall $H = \#I(A; h) = q^{h+1}$).

We write

$$I(A; h) = (A + \mathcal{P}_{\le h-1}) \cup \coprod_{c \in \mathbb{F}_q^\times} (A + c\mathcal{M}_h).$$

The number of squarefrees in $A + \mathcal{P}_{\le h-1}$ is at most $\#\mathcal{P}_{\le h-1} = q^h$. The squarefrees in $A + c\mathcal{M}_h$ are the squarefree values at monic polynomials of degree h of the polynomial $F(x, t) = A(t) + cx$, which has degree 1, content $\gcd(A(t), c) = 1$ and height $\mathrm{Ht}(F) = \deg A = n$. By Theorem 2.1 the number of substitutions $a \in \mathcal{M}_h$ for which $F(a)$ is squarefree is

$$q^h + O(nq^{h-1}).$$

Hence number of squarefrees in $I(A; h)$ is

$$\sum_{c \in \mathbb{F}_q^\times} (q^h + O(nq^{h-1})) + O(q^h) = H + O(H/q),$$

proving (2-2).

3. Asymptotics for Möbius sums

In this section we deal with cancellation in the individual sums

$$\mathcal{N}_\mu(A; h) = \sum_{f \in I(A;h)} \mu(f).$$

Note that the interval $I(A; h)$ consists of all polynomials of the form $A + g$, where $g \in \mathcal{P}_{\le h}$ is the set of all polynomials of degree at most h.

Small h. We first point out that for $h = 0, 1$ there need not be any cancellation. We recall Pellet's formula for the discriminant (in odd characteristic)

$$\mu(f) = (-1)^{\deg f} \chi_2(\mathrm{disc}\, f) \tag{3-1}$$

where $\chi_2 : \mathbb{F}_q^\times \to \{\pm 1\}$ is the quadratic character of $\mathbb{F}_q$ and $\mathrm{disc}\, f$ is the discriminant of f. From Pellet's formula we find (as in [Carmon and Rudnick 2014])

$$\mathcal{N}_\mu(A; h) = (-1)^{\deg A} \sum_{g \in \mathcal{P}_{\le h}} \chi_2(\mathrm{disc}(A + g)). \tag{3-2}$$

Let $A(t) = t^n$. The discriminant of the trinomial $t^n + at + b$ is (see, e.g., [Swan 1962])

$$\text{disc}(t^n + at + b) = (-1)^{n(n-1)/2}\left(n^n b^{n-1} + (1-n)^{n-1}a^n\right). \qquad (3\text{-}3)$$

Hence for the interval $I(t^n; 1) = \{t^n + at + b : a, b \in \mathbb{F}_q\}$ we obtain

$$\mathcal{N}_\mu(t^n; 1) = (-1)^n \chi_2(-1)^{n(n-1)/2} \sum_{a,b\in\mathbb{F}_q} \chi_2\left(n^n b^{n-1} + (1-n)^{n-1}a^n\right). \qquad (3\text{-}4)$$

Therefore if $q = p^k$ with p an odd prime and $2p \mid n$ then

$$\mathcal{N}_\mu(t^n; 1) = \chi_2(-1)^{n/2}q \sum_{a\in\mathbb{F}_q} \chi_2(a)^n = \pm q(q-1), \qquad (3\text{-}5)$$

so that $|\mathcal{N}_\mu(t^n; 1)| \gg q^2 = H$. A similar construction also works for $h = 0$.

Large h. We also note that for $h = n - 2$, and $p \nmid n$ (p is the characteristic of $\mathbb{F}_q$) the Möbius sums all coincide. This is because $\mu(f(t)) = \mu(f(t+c))$ if $\deg f \geq 1$. Therefore

$$\mathcal{N}_\mu(A(t); h) = \mathcal{N}_\mu(A(t+c); h).$$

Now if $A(t) = t^n + a_{n-1}t^{n-1} + \cdots$ is the center of the interval, then choosing $c = -a_{n-1}/n$ gives

$$A(t+c) = t^n + \tilde{a}_{n-2}t^{n-2} + \cdots$$

which contains no term of the form t^{n-1}. Therefore if $h = n - 2$ then

$$\mathcal{N}_\mu(t^n + a_{n-1}t^{n-1}; n - 2) = \mathcal{N}_\mu(t^n; n - 2)$$

has just one possible value.

Thus we may assume that $h \leq n - 3$.

We note that the same is true for the squarefree case.

Proof of Theorem 1.1. We show that for $h \geq 2$, for any (monic) $A(t)$ of degree n,

$$\sum_{a\in\mathcal{P}_{\leq h}} \mu(A+a) \ll \frac{H}{\sqrt{q}}. \qquad (3\text{-}6)$$

Writing $a(t) = a_h t^h + \cdots + a_1 t + b$, it suffices to show that there is a constant $C = C(n, h)$ (independent of A and $\vec{a} = (a_1, \ldots, a_h)$) such that for "most" choices of $\vec{a}$, (i.e., for all but $O(q^{h-1})$) we have

$$\left|\sum_{b\in\mathbb{F}_q} \mu(A(t) + a_h t^h + \cdots + a_1 t + b)\right| \leq C\sqrt{q}. \qquad (3\text{-}7)$$

Using Pellet's formula, we need to show that for most $\vec{a}$,

$$\left|\sum_{b \in \mathbb{F}_q} \chi_2\big(\mathrm{disc}(A(t) + a_h t^h + \cdots + a_1 t + b)\big)\right| \leq C\sqrt{q} \qquad (3\text{-}8)$$

Now $D_a(b) := \mathrm{disc}(A(t) + a_h t^h + \cdots + a_1 t + b)$ is a polynomial in b, of degree $\leq n - 1$, and if we show that for most $\vec{a}$ it is nonconstant and squarefree then by Weil's theorem we will get that (3-8) holds for such $\vec{a}$'s, with $C = n - 2$. The argument in [Carmon and Rudnick 2014, Section 4] works verbatim here to prove that. □

An alternative argument is to use the work of Bank, Bary-Soroker and Rosenzweig [2015] who prove equidistribution of cycle types of polynomials in any short interval $I(A; h)$ for $2 \leq h \leq n - 2$ and q odd (this also uses [Carmon and Rudnick 2014]). Now for $f \in \mathcal{M}_n$ squarefree, $\mu(f) = (-1)^n \mathrm{sign}(\sigma_f)$ where $\sigma_f \subset S_n$ is the conjugacy class of permutations induced by the Frobenius acting on the roots of f, and sign is the sign character. For any $f \in \mathcal{M}_n$, not necessarily squarefree, we denote by $\lambda(f) = (\lambda_1, \ldots, \lambda_n)$ the cycle structure of f, which for squarefree f coincides with the cycle structure of the permutation σ_f. Then $\mathrm{sign}(\sigma_f) = \mathrm{sign}(\lambda(f)) := \prod_{j=1}^{n} (-1)^{(j-1)\lambda_j}$. Thus

$$\sum_{f \in I(A;h)} \mu(f) = (-1)^n \sum_{\substack{f \in I(A;h) \\ \text{squarefree}}} \mathrm{sign}(\sigma_f). \qquad (3\text{-}9)$$

By Theorem 1.3, all but $O_n(H/q)$ of the polynomials in the short interval $I(A; h)$ are squarefree, hence

$$\sum_{\substack{f \in I(A;h) \\ \text{squarefree}}} \mathrm{sign}(\sigma_f) = \sum_{f \in I(A;h)} \mathrm{sign}(\sigma_f) + O\left(\frac{H}{q}\right)$$

$$= H\left(\frac{1}{n!} \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) + O\left(\frac{1}{\sqrt{q}}\right)\right) = O\left(\frac{H}{\sqrt{q}}\right), \qquad (3\text{-}10)$$

by equidistribution of cycle types in short intervals [Bank et al. 2015], and recalling that $\sum_{\sigma \in S_n} \mathrm{sign}(\sigma) = 0$ for $n > 1$.

4. Variance in arithmetic progressions: General theory

Let $\alpha : \mathbb{F}_q[t] \to \mathbb{C}$ be a function on polynomials, which is "even" in the sense that

$$\alpha(cf) = \alpha(f)$$

for the units $c \in \mathbb{F}_q^\times$. We assume that

$$\max_{\deg f \leq n} |\alpha(f)| \leq A_n \qquad (4\text{-}1)$$

with A_n independent of q. We will require some further constraints on α later on.

We denote by $\langle\alpha\rangle_n$ the mean value of α over all monic polynomials of degree n:

$$\langle\alpha\rangle_n := \frac{1}{q^n}\sum_{f\in\mathcal{M}_n}\alpha(f). \tag{4-2}$$

Let $Q \in \mathbb{F}_q[t]$ be squarefree, of positive degree. For an arithmetic function $\alpha : \mathbb{F}_q[t] \to \mathbb{C}$, we define its mean value over coprime residue classes by

$$\langle\alpha\rangle_Q := \frac{1}{\Phi(Q)}\sum_{\substack{A \bmod Q \\ \gcd(A,Q)=1}}\alpha(A). \tag{4-3}$$

The sum of α over all monic polynomials of degree n lying in the arithmetic progressions $f = A \bmod Q$ is

$$\mathcal{S}_{\alpha,n,Q}(A) := \sum_{\substack{f\in\mathcal{M}_n \\ f=A \bmod Q}}\alpha(f). \tag{4-4}$$

We wish to study the fluctuations in $\mathcal{S}(A)$ as we vary A over residue classes coprime to Q. The mean value of $\mathcal{S}$ is

$$\langle\mathcal{S}_\alpha\rangle_Q = \frac{1}{\Phi(Q)}\sum_{\substack{f\in\mathcal{M}_n \\ (f,Q)=1}}\alpha(f), \tag{4-5}$$

where $\Phi(Q)$ is the number of invertible residues modulo Q.

Our goal is to compute the variance

$$\mathrm{Var}_Q(\mathcal{S}_\alpha) = \frac{1}{\Phi(Q)}\sum_{\substack{A \bmod Q \\ (A,Q)=1}}|\mathcal{S}_\alpha(A) - \langle\mathcal{S}_\alpha\rangle|^2. \tag{4-6}$$

A formula for the variance. Expanding in Dirichlet characters modulo Q gives

$$\mathcal{S}(A) = \frac{1}{\Phi(Q)}\sum_{\chi \bmod Q}\bar{\chi}(A)\mathcal{M}(n;\alpha\chi), \tag{4-7}$$

where

$$\mathcal{M}(n;\alpha\chi) := \sum_{f\in\mathcal{M}_n}\chi(f)\alpha(f). \tag{4-8}$$

The mean value is the contribution of the trivial character χ_0:

$$\langle\mathcal{S}\rangle_Q = \frac{1}{\Phi(Q)}\sum_{\substack{f\in\mathcal{M}_n \\ \gcd(f,Q)=1}}\alpha(f), \tag{4-9}$$

so that

$$\mathcal{S}(A) - \langle S \rangle_Q = \frac{1}{\Phi(Q)} \sum_{\chi \neq \chi_0 \bmod Q} \bar{\chi}(A) \mathcal{M}(n; \alpha\chi). \tag{4-10}$$

Inserting (4-7) and using the orthogonality relations for Dirichlet characters as in [Keating and Rudnick 2014], we see that the variance is

$$\mathrm{Var}_Q(\mathcal{S}) = \langle |S - \langle S \rangle_Q|^2 \rangle_Q = \frac{1}{\Phi(Q)^2} \sum_{\chi \neq \chi_0} |\mathcal{M}(n; \alpha\chi)|^2. \tag{4-11}$$

Small n. If $n < \deg Q$, then there is at most *one* f with $\deg f = n$ and $f = A \bmod Q$, and in this case

$$\mathrm{Var}_Q(\mathcal{S}) \sim \frac{q^n}{\Phi(Q)} \langle \alpha^2 \rangle_n, \quad n < \deg Q. \tag{4-12}$$

Indeed, if $n < \deg Q$, then

$$|\langle S \rangle_Q| = \left| \frac{1}{\Phi(Q)} \sum_{\substack{f \in \mathcal{M}_n \\ \gcd(f,Q)=1}} \alpha(f) \right| \leq \frac{1}{\Phi(Q)} \sum_{f \in \mathcal{M}_n} |\alpha(f)| \leq \frac{A_n q^n}{\Phi(Q)} \ll_n \frac{1}{q}. \tag{4-13}$$

Hence

$$\mathrm{Var}_Q(\mathcal{S}) = \frac{1}{\Phi(Q)} \sum_{\substack{A \bmod Q \\ \gcd(A,Q)=1}} |\mathcal{S}(A)|^2 (1 + O(q^{-1}))$$

$$= \frac{1}{\Phi(Q)} \sum_{\substack{f \in \mathcal{M}_n \\ \gcd(f,Q)=1}} |\alpha(f)|^2 (1 + O(q^{-1}))$$

$$= \frac{q^n}{\Phi(Q)} \langle |\alpha|^2 \rangle_n (1 + O(q^{-1}))$$

as claimed.

5. Variance in short intervals: General theory

Given an arithmetic function $\alpha : \mathbb{F}_q[t] \to \mathbb{C}$, define its sum on short intervals as

$$\mathcal{N}_\alpha(A; h) = \sum_{f \in I(A;h)} \alpha(f). \tag{5-1}$$

The mean value of $\mathcal{N}_\alpha$ is (see Lemma 5.2)

$$\langle \mathcal{N}_\alpha(\bullet, h) \rangle = q^{h+1} \langle \alpha \rangle_n = H \langle \alpha \rangle_n. \tag{5-2}$$

Our goal will be to compute the variance of $\mathcal{N}_\alpha$,

$$\mathrm{Var}\, \mathcal{N}_\alpha = \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} |\mathcal{N}_\alpha(A) - \langle \mathcal{N}_\alpha \rangle|^2, \tag{5-3}$$

and more generally, given two such functions α, β, to compute the covariance

$$\mathrm{cov}(\mathcal{N}_\alpha, \mathcal{N}_\beta) = \langle(\mathcal{N}_\alpha - \langle\mathcal{N}_\alpha\rangle)(\mathcal{N}_\beta - \langle\mathcal{N}_\beta\rangle)\rangle. \tag{5-4}$$

Background on short intervals (see [Keating and Rudnick 2014]). Let

$$\mathcal{P}_n = \{f \in \mathbb{F}_q[t] : \deg f = n\} \tag{5-5}$$

be the set of polynomials of degree n,

$$\mathcal{P}_{\leq n} = \{0\} \cup \bigcup_{0 \leq m \leq n} \mathcal{P}_m \tag{5-6}$$

the space of polynomials of degree at most n (including 0), and $\mathcal{M}_n \subset \mathcal{P}_n$ the subset of monic polynomials.

By definition of short intervals,

$$I(A; h) = A + \mathcal{P}_{\leq h}, \tag{5-7}$$

and hence

$$\#I(A; h) = q^{h+1} =: H. \tag{5-8}$$

For $h = n - 1$, $I(A; n-1) = \mathcal{M}_n$ is the set of all monic polynomials of degree n. For $h \leq n - 2$, if $\|f - A\| \leq q^h$ then $\deg f = \deg A$ and A is monic if and only if f is monic. Hence for A monic, $I(A; h)$ consists of only monic polynomials and all monic f's of degree n are contained in one of the intervals $I(A; h)$ with A monic of degree n. Moreover,

$$I(A_1; h) \cap I(A_2; h) \neq \varnothing \leftrightarrow \deg(A_1 - A_2) \leq h \leftrightarrow I(A_1; h) = I(A_2; h), \tag{5-9}$$

and we get a partition of $\mathcal{P}_n$ into disjoint "intervals" parameterized by $B \in \mathcal{P}_{n-(h+1)}$:

$$\mathcal{P}_n = \coprod_{B \in \mathcal{P}_{n-(h+1)}} I(t^{h+1}B; h), \tag{5-10}$$

and likewise for monics (recall $h \leq n - 2$):

$$\mathcal{M}_n = \coprod_{B \in \mathcal{M}_{n-(h+1)}} I(t^{h+1}B; h). \tag{5-11}$$

An involution. Let $n \geq 0$. We define a map $\theta_n : \mathcal{P}_{\leq n} \to \mathcal{P}_{\leq n}$ by

$$\theta_n(f)(t) = t^n f(t^{-1}),$$

which takes $f(t) = f_0 + f_1 t + \cdots + f_n t^n$, $n = \deg f$ to the "reversed" polynomial

$$\theta_n(f)(t) = f_0 t^n + f_1 t^{n-1} + \cdots + f_n. \tag{5-12}$$

For $0 \neq f \in \mathbb{F}_q[t]$ we define

$$f^*(t) := t^{\deg f} f(t^{-1}) \tag{5-13}$$

so that $\theta_n(f) = f^*$ if $f(0) \neq 0$. Note that if $f(0) = 0$ then this is false, for example $(t^k)^* = 1$ but $\theta_n(t^k) = t^{n-k}$ if $k \leq n$.

We have $\deg \theta_n(f) \leq n$ with equality if and only if $f(0) \neq 0$. Moreover for $f \neq 0$, $f^*(0) \neq 0$ and $f(0) \neq 0$ if and only if $\deg f^* = \deg f$. When restricted to polynomials which do not vanish at 0 (equivalently, which are coprime to t), the operator $*$ is an involution:

$$f^{**} = f, \quad f(0) \neq 0. \tag{5-14}$$

We also have multiplicativity:

$$(fg)^* = f^* g^*. \tag{5-15}$$

The map θ_m gives a bijection

$$\theta_m : \mathcal{M}_m \to \{C \in \mathcal{P}_{\leq m} : C(0) = 1\}$$
$$B \mapsto \theta_m(B) \tag{5-16}$$

with polynomials of degree $\leq m$ with constant term 1. Thus as B ranges over $\mathcal{M}_m$, $\theta_m(B)$ ranges over all invertible residue classes $C \mod t^{m+1}$ such that $C(0) = 1$.

Short intervals as arithmetic progressions modulo t^{n-h}. Suppose $h \leq n - 2$. Define the arithmetic progression

$$\mathcal{P}_{\leq n}(t^{n-h}; C) = \{g \in \mathcal{P}_{\leq n} : g \equiv C \mod t^{n-h}\} = C + t^{n-h}\mathcal{P}_{\leq h}. \tag{5-17}$$

Note that the progression contains q^{h+1} elements.

Lemma 5.1. *Let $h \leq n - 2$ and $B \in \mathcal{M}_{n-h-1}$. Then the map θ_n takes the "interval" $I(t^{h+1}B; h)$ bijectively onto the arithmetic progression $\mathcal{P}_{\leq n}(t^{n-h}; \theta_{n-h-1}(B))$, with $f \in I(t^{h+1}B; h)$ such that $f(0) \neq 0$ mapping onto those $g \in \mathcal{P}_{\leq n}(t^{n-h}; \theta_{n-h-1}(B))$ of degree exactly n.*

Proof. We first check that θ_n maps the interval $I(t^{h+1}B; h)$ to the arithmetic progression $\mathcal{P}_{\leq n}(t^{n-h}; \theta_{n-h-1}(B))$. Indeed if $B = b_0 + \cdots + b_{n-h-1}t^{n-h-1}$, with $b_{n-h-1} = 1$, and $f = f_0 + \cdots + f_n t^n \in I(t^{h+1}B; h)$ then

$$f = f_0 + \cdots + f_h t^h + t^{h+1}(b_0 + \cdots + b_{n-h-1}t^{n-h-1}) \tag{5-18}$$

so that

$$\theta_n(f) = f_0 t^n + \cdots + f_h t^{n-h} + b_0 t^{n-h-1} + \cdots + b_{n-h-1}$$
$$= \theta_{n-h-1}(B) \mod t^{n-h}. \tag{5-19}$$

Hence $\theta_n(f) \in \mathcal{P}_{\leq n}(t^{n-h}; \theta_{n-h-1}(B))$.

Now the map $\theta_n : \mathcal{P}_{\leq n} \to \mathcal{P}_{\leq n}$ is a bijection, and both $\mathcal{P}_{\leq n}(t^{n-h}; \theta_{n-h-1}(B))$ and $I(t^{h+1}B; h)$ have size q^{h+1}. Therefore $\theta_n : I(t^{h+1}B; h) \to \mathcal{P}_{\leq n}(t^{n-h}; B^*)$ is a bijection. □

The mean value.

Lemma 5.2. *The mean value of* $\mathcal{N}_\alpha(\bullet \, ; h)$ *over* $\mathcal{M}_n$ *is*

$$\langle \mathcal{N}_\alpha(\bullet \, ; h) \rangle = q^{h+1} \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \alpha(f) = H \langle \alpha \rangle_n. \tag{5-20}$$

Proof. From the definition, we have

$$\langle \mathcal{N}_\alpha(\bullet \, ; h) \rangle = \frac{1}{\#\mathcal{M}_{n-h-1}} \sum_{B \in \mathcal{M}_{n-h-1}} \mathcal{N}_\alpha(t^{h+1}B; h)$$

$$= \frac{1}{q^{n-h-1}} \sum_{B \in \mathcal{M}_{n-h-1}} \sum_{f \in I(t^{h+1}B; h)} \alpha(f)$$

$$= q^{h+1} \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \alpha(f) = q^{h+1} \langle \alpha \rangle_n. \tag{5-21}$$

□

A class of arithmetic functions. Let $\alpha : \mathbb{F}_q[t] \to \mathbb{C}$ be a function on polynomials, which is:

- *Even* in the sense that

$$\alpha(cf) = \alpha(f), \quad c \in \mathbb{F}_q^\times.$$

- *Multiplicative*, that is, $\alpha(fg) = \alpha(f)\alpha(g)$ if f and g are coprime. In fact we will only need a weaker condition , "weak multiplicativity": If $f(0) \neq 0$, i.e., $\gcd(f, t) = 1$ then

$$\alpha(t^k f) = \alpha(t^k)\alpha(f), \quad f(0) \neq 0.$$

- *Bounded*, that is, it satisfies the growth condition

$$\max_{f \in \mathcal{M}_n} |\alpha(f)| \leq A_n$$

independent of q.

- *Symmetric* under the map $f^*(t) := t^{\deg f} f(t^{-1})$,

$$\alpha(f^*) = \alpha(f), \quad f(0) \neq 0.$$

Examples are the Möbius function μ, its square μ^2 which is the indicator function of squarefree-integers, and the divisor functions (see [Keating et al. 2015]).

Note that multiplicativity (and the "weak multiplicativity" condition) excludes the case of the von Mangoldt function, treated in [Keating and Rudnick 2014] where we are counting prime polynomials in short intervals or arithmetic progressions. A related case of almost primes was treated by Rodgers [2015].

A formula for $\mathcal{N}_\alpha(A; h)$. We present a useful formula for the short interval sums $\mathcal{N}_\alpha(\bullet, h)$ in terms of sums over even Dirichlet characters modulo t^{n-h}. Recall that a Dirichlet character χ is "even" if $\chi(cf) = \chi(f)$ for all scalars $c \in \mathbb{F}_q^\times$, and we say that χ is "odd" otherwise. The number of even characters modulo t^m is $\Phi_{\mathrm{ev}}(t^m) = q^{m-1}$. We denote by χ_0 the trivial character.

Lemma 5.3. *If* $\alpha : \mathbb{F}_q[t] \to \mathbb{C}$ *is even, symmetric and weakly multiplicative, and* $0 \le h \le n - 2$, *then for all* $B \in \mathcal{M}_{n-h-1}$,

$$\mathcal{N}_\alpha(t^{h+1}B; h) = \langle \mathcal{N}_\alpha(\bullet; h) \rangle$$

$$+ \frac{1}{\Phi_{\mathrm{ev}}(t^{n-h})} \sum_{m=0}^{n} \alpha(t^{n-m}) \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \ne \chi_0 \text{ even}}} \bar{\chi}(\theta_{n-h-1}(B)) \mathcal{M}(m; \alpha\chi), \quad (5\text{-}22)$$

where

$$\mathcal{M}(n; \alpha\chi) = \sum_{f \in \mathcal{M}_n} \alpha(f)\chi(f). \tag{5-23}$$

Proof. Writing each $f \in \mathcal{M}_n$ uniquely as $f = t^{n-m}f_1$ with $f_1 \in \mathcal{M}_m$ and $f_1(0) \ne 0$, for which $\theta_n(f) = \theta_m(f_1) = f_1^*$, we obtain, using (weak) multiplicativity,

$$\mathcal{N}_\alpha(t^{h+1}B; h) = \sum_{m=0}^{n} \sum_{\substack{f_1 \in \mathcal{M}_m \\ f_1(0) \ne 0 \\ t^{n-m}f_1 \in I(t^{h+1}B; h)}} \alpha(t^{n-m}f_1)$$

$$= \sum_{m=0}^{n} \alpha(t^{n-m}) \sum_{\substack{f_1 \in \mathcal{M}_m \\ f_1(0) \ne 0 \\ t^{n-m}f_1 \in I(t^{h+1}B; h)}} \alpha(f_1). \tag{5-24}$$

Since $f_1(0) \ne 0$, we have that $f_1^* = \theta_m(f_1)$ runs over all polynomials g of degree m (not necessarily monic) so that $g \equiv \theta_{n-h-1}(B) \bmod t^{n-h}$ by Lemma 5.1, and moreover $\alpha(f_1) = \alpha(f_1^*) = \alpha(\theta_m(f_1))$. Hence

$$\mathcal{N}_\alpha(t^{h+1}B; h) = \sum_{m=0}^{n} \alpha(t^{n-m}) \sum_{\substack{\deg g = m \\ g \equiv \theta_{n-h-1}(B) \bmod t^{n-h}}} \alpha(g). \tag{5-25}$$

Using characters to pick out the conditions $g \equiv \theta_{n-h-1}(B)$ mod t^{n-h} (note that since B is monic, $\theta_{n-h-1}(B)$ is coprime to t^{n-h}) gives

$$\sum_{\substack{\deg g = m \\ g \equiv \theta_{n-h-1}(B) \bmod t^{n-h}}} \alpha(g) = \frac{1}{\Phi(t^{n-h})} \sum_{\chi \bmod t^{n-h}} \bar{\chi}(\theta_{n-h-1}(B)) \widetilde{\mathcal{M}}(m; \alpha\chi), \quad (5\text{-}26)$$

where

$$\widetilde{\mathcal{M}}(m; \alpha\chi) = \sum_{\deg g = m} \chi(g)\alpha(g), \quad (5\text{-}27)$$

the sum running over all g of degree m.

Since α is even, we find that

$$\begin{aligned}
\widetilde{\mathcal{M}}(m; \alpha\chi) &= \sum_{f \in \mathcal{M}_m} \sum_{c \in \mathbb{F}_q^{\times}} \chi(cf)\alpha(cf) \\
&= \sum_{f \in \mathcal{M}_m} \alpha(f)\chi(f) \sum_{c \in \mathbb{F}_q^{\times}} \chi(c) \\
&= \begin{cases} (q-1) \sum_{f \in \mathcal{M}_m} \alpha(f)\chi(f), & \chi \text{ even,} \\ 0, & \chi \text{ odd,} \end{cases}
\end{aligned}$$

where now the sum is over monic polynomials of degree m.

Thus we get, on noting that $\Phi(t^{n-h})/(q-1) = \Phi_{\mathrm{ev}}(t^{n-h})$, that

$$\sum_{\substack{\deg g = m \\ g \equiv \theta_{n-h-1}(B) \bmod t^{n-h}}} \alpha(g) = \frac{1}{\Phi_{\mathrm{ev}}(t^{n-h})} \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \text{ even}}} \bar{\chi}(\theta_{n-h-1}(B)) \mathcal{M}(m; \alpha\chi). \quad (5\text{-}28)$$

Therefore

$$\mathcal{N}_\alpha(t^{h+1}B; h) = \sum_{m=0}^{n} \alpha(t^{n-m}) \frac{1}{\Phi_{\mathrm{ev}}(t^{n-h})} \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \text{ even}}} \bar{\chi}(\theta_{n-h-1}(B)) \mathcal{M}(m; \alpha\chi).$$

$$(5\text{-}29)$$

The trivial character χ_0 contributes a term

$$\frac{1}{\Phi_{\mathrm{ev}}(t^{n-h})} \sum_{m=0}^{n} \sum_{\substack{g \in \mathcal{M}_m \\ g(0) \neq 0}} \alpha(t^{n-m})\alpha(g) = \frac{q^{h+1}}{q^n} \sum_{f \in \mathcal{M}_n} \alpha(f) \quad (5\text{-}30)$$

on using weak multiplicativity. Inserting this into (5-29) and using Lemma 5.2 we obtain the formula claimed. $\square$

Formulae for variance and covariance. Given an arithmetic function α, the variance of $\mathcal{N}_\alpha$ is

$$
\begin{aligned}
\mathrm{Var}(\mathcal{N}_\alpha) &= \left\langle |\mathcal{N}_\alpha - \langle \mathcal{N}_\alpha \rangle|^2 \right\rangle \\
&= \frac{1}{q^{n-h-1}} \sum_{B \in \mathcal{M}_{n-h-1}} \left| \mathcal{N}_\alpha(t^{h+1}B; h) - \langle \mathcal{N}_\alpha \rangle \right|^2
\end{aligned}
\tag{5-31}
$$

and likewise given two such functions α, β, the covariance of $\mathcal{N}_\alpha$ and $\mathcal{N}_\beta$ is

$$
\mathrm{cov}(\mathcal{N}_\alpha, \mathcal{N}_\beta) = \left\langle (\mathcal{N}_\alpha - \langle \mathcal{N}_\alpha \rangle)(\mathcal{N}_\beta - \langle \mathcal{N}_\beta \rangle) \right\rangle.
\tag{5-32}
$$

We use the following lemma, an extension of the argument of [Keating and Rudnick 2014].

Lemma 5.4. *If* α, β *are even, symmetric and weakly multiplicative, and* $0 \le h \le n - 2$, *then*

$$
\mathrm{cov}(\mathcal{N}_\alpha, \mathcal{N}_\beta) =
$$

$$
\frac{1}{\Phi_{\mathrm{ev}}(t^{n-h})^2} \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \ne \chi_0 \text{ even}}} \sum_{m_1, m_2 = 0}^{n} \alpha(t^{n-m_1}) \overline{\beta(t^{n-m_2})} \mathcal{M}(m_1; \alpha\chi) \overline{\mathcal{M}(m_2; \beta\chi)}.
\tag{5-33}
$$

Proof. By Lemma 5.3, $\mathrm{cov}(\mathcal{N}_\alpha, \mathcal{N}_\beta)$ equals

$$
\frac{1}{\Phi_{\mathrm{ev}}(t^{n-h})^2} \sum_{\substack{\chi_1, \chi_2 \bmod t^{n-h} \\ \chi_1, \chi_2 \ne \chi_0 \text{ even}}} \sum_{m_1, m_2 = 0}^{n} \alpha(t^{n-m_1}) \overline{\beta(t^{n-m_2})} \mathcal{M}(m_1; \alpha\chi_1) \overline{\mathcal{M}(m_2; \beta\chi_2)}
$$

$$
\times \frac{1}{q^{n-h-1}} \sum_{B \in \mathcal{M}_{n-h-1}} \bar{\chi}_1(\theta_{n-h-1}(B)) \chi_2(\theta_{n-h-1}(B)).
$$

As B runs over the monic polynomials $\mathcal{M}_{n-h-1}$, the image $\theta_{n-h-1}(B)$ runs over all polynomials $C \bmod t^{n-h}$ with $C(0) = 1$ (see (5-16)). Thus

$$
\sum_{B \in \mathcal{M}_{n-h-1}} \bar{\chi}_1(\theta_{n-h-1}(B)) \chi_2(\theta_{n-h-1}(B)) = \sum_{\substack{C \bmod t^{n-h} \\ C(0)=1}} \bar{\chi}_1(C) \chi_2(C).
\tag{5-34}
$$

Since χ_1, χ_2 are both even, we may ignore the condition $C(0) = 1$ and use the orthogonality relation (recall $\Phi_{\mathrm{ev}}(t^{n-h}) = q^{n-h-1}$) to get

$$
\frac{1}{q^{n-h-1}} \sum_{\substack{C \bmod t^{n-h} \\ C(0)=1}} \bar{\chi}_1(C) \chi_2(C) = \delta(\chi_1, \chi_2)
\tag{5-35}
$$

(see [Keating and Rudnick 2014, Lemma 3.2]), so that

$$\mathrm{cov}(\mathcal{N}_\alpha, \mathcal{N}_\beta) =$$

$$\frac{1}{\Phi_{\mathrm{ev}}(t^{n-h})^2} \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \neq \chi_0 \text{ even}}} \sum_{m_1, m_2 = 0}^{n} \alpha(t^{n-m_1}) \overline{\beta(t^{n-m_2})} \mathcal{M}(m_1; \alpha \chi) \overline{\mathcal{M}(m_2; \beta \chi)} \quad (5\text{-}36)$$

as claimed.   □

6. Characters, L-functions and equidistribution

Before applying the variance formulae presented above, we survey some background on Dirichlet characters, their L-functions and recent equidistribution theorems due to N. Katz.

Background on Dirichlet characters and L-functions. Recall that a Dirichlet character χ is "even" if $\chi(cf) = \chi(f)$ for all scalars $c \in \mathbb{F}_q^\times$, and we say that χ is "odd" otherwise. The number of even characters modulo t^m is $\Phi_{\mathrm{ev}}(t^m) = q^{m-1}$. We denote by χ_0 the trivial character.

A character χ is *primitive* if there is no proper divisor $Q' \mid Q$ such that $\chi(F) = 1$ whenever F is coprime to Q and $F = 1 \bmod Q'$. We denote by $\Phi_{\mathrm{prim}}(Q)$ the number of primitive characters modulo Q. As $q \to \infty$, almost all characters are primitive in the sense that

$$\frac{\Phi_{\mathrm{prim}}(Q)}{\Phi(Q)} = 1 + O(1/q), \quad (6\text{-}1)$$

the implied constant depending only on deg Q.

Moreover, as $q \to \infty$ with deg Q fixed, almost all characters are primitive and odd:

$$\frac{\Phi_{\mathrm{prim}}^{\mathrm{odd}}(Q)}{\Phi(Q)} = 1 + O(1/q), \quad (6\text{-}2)$$

the implied constant depending only on deg Q.

One also has available similar information about the number $\Phi_{\mathrm{prim}}^{\mathrm{ev}}(Q)$ of even primitive characters. What we will need to note is that for $Q(t) = t^m$, $m \geq 2$,

$$\Phi_{\mathrm{prim}}^{\mathrm{ev}}(t^m) = q^{m-2}(q - 1). \quad (6\text{-}3)$$

The L-function $L(u, \chi)$ attached to χ is defined as

$$L(u, \chi) = \prod_{P \nmid Q} (1 - \chi(P) u^{\deg P})^{-1}, \quad (6\text{-}4)$$

where the product is over all monic irreducible polynomials in $\mathbb{F}_q[t]$. The product is absolutely convergent for $|u| < 1/q$. If $\chi = \chi_0$, i.e., χ is the trivial character

modulo Q, then

$$L(u, \chi_0) = Z(u) \prod_{P|Q} (1 - u^{\deg P}), \qquad (6\text{-}5)$$

where

$$Z(u) = \prod_{P \text{ prime}} (1 - u^{\deg P})^{-1} = \frac{1}{1 - qu}$$

is the zeta function of $\mathbb{F}_q[t]$. Also set $\zeta_q(s) := Z(q^{-s})$.

If $Q \in \mathbb{F}_q[t]$ is a polynomial of degree $\deg Q \geq 2$, and $\chi \neq \chi_0$ (χ is a nontrivial character mod Q), then the L-function $L(u, \chi)$ is a polynomial in u of degree $\deg Q - 1$. Moreover, if χ is an "even" character, then there is a "trivial" zero at $u = 1$.

We may factor $L(u, \chi)$ in terms of the inverse roots

$$L(u, \chi) = \prod_{j=1}^{\deg Q - 1} (1 - \alpha_j(\chi)u). \qquad (6\text{-}6)$$

The Riemann hypothesis, proved by Andre Weil (1948), is that for each (nonzero) inverse root, either $\alpha_j(\chi) = 1$ or

$$|\alpha_j(\chi)| = q^{1/2}. \qquad (6\text{-}7)$$

If χ is a *primitive* and *odd* character modulo Q, then all inverse roots α_j have absolute value $\sqrt{q}$, and for χ primitive and *even* the same holds except for the trivial zero at 1. We then write the nontrivial inverse roots as $\alpha_j = q^{1/2}e^{i\theta_j}$ and define a unitary matrix

$$\Theta_\chi = \text{diag}(e^{i\theta_1}, \ldots, e^{i\theta_N}). \qquad (6\text{-}8)$$

which determines a unique conjugacy class in the unitary group $U(N)$, where $N = \deg Q - 1$ for χ odd, and $N = \deg Q - 2$ for χ even. The unitary matrix Θ_χ (or rather, the conjugacy class of unitary matrices) is called the unitarized Frobenius matrix of χ.

Katz's equidistribution theorems. Crucial ingredients in our results on the variance are equidistribution and independence results for the Frobenii Θ_χ due to N. Katz.

Theorem 6.1. (i) [Katz 2013b] *Fix[3] $m \geq 4$. The unitarized Frobenii Θ_χ for the family of even primitive characters mod T^{m+1} become equidistributed in the projective unitary group $PU(m-1)$ of size $m-1$, as $q \to \infty$.*

[3]If the characteristic of $\mathbb{F}_q$ is different than 2 or 5 then the result also holds for $m = 3$.

(ii) [Katz 2015b] *If $m \geq 5$ and in addition the q's are coprime to 6, then the set of pairs of conjugacy classes $(\Theta_\chi, \Theta_{\chi^2})$ become equidistributed in the space of conjugacy classes of the product $PU(m-1) \times PU(m-1)$.*

For odd characters, the corresponding equidistribution and independence results are

Theorem 6.2. (i) [Katz 2013a] *Fix $m \geq 2$. Suppose we are given a sequence of finite fields $\mathbb{F}_q$ and squarefree polynomials $Q(T) \in \mathbb{F}_q[T]$ of degree m. As $q \to \infty$, the conjugacy classes Θ_χ with χ running over all primitive odd characters modulo Q, are uniformly distributed in the unitary group $U(m-1)$.*

(ii) [Katz 2015a] *If in addition we restrict to q odd, then the set of pairs of conjugacy classes $(\Theta_\chi, \Theta_{\chi^2})$ become equidistributed in the space of conjugacy classes of the product $U(m-1) \times U(m-1)$.*

7. Variance of the Möbius function in short intervals

For $n \geq 2$, the mean value of $\mathcal{N}_\mu(A; h)$ over all $A \in \mathcal{M}_n$ is

$$\langle \mathcal{N}_\mu(\bullet; h) \rangle = 0. \tag{7-1}$$

Indeed, by Lemma 5.2

$$\langle \mathcal{N}_\mu(\bullet; h) \rangle = \frac{H}{q^n} \sum_{f \in \mathcal{M}_n} \mu(f). \tag{7-2}$$

Now as is well known and easy to see, for $n \geq 2$,

$$\sum_{f \in \mathcal{M}_n} \mu(f) = 0, \tag{7-3}$$

hence we obtain (7-1).

We will demonstrate the following asymptotic property of the variance.

Theorem 7.1. *If $0 \leq h \leq n-5$ then*

$$\operatorname{Var} \mathcal{N}_\mu(\bullet; h) \sim H, \quad q \to \infty. \tag{7-4}$$

We use the general formula of Lemma 5.4 which gives

$$\operatorname{Var}(\mathcal{N}_\mu(\bullet; h)) = \frac{1}{q^{2(n-h-1)}} \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \neq \chi_0 \text{ even}}} |\mathcal{M}(n; \mu\chi) - \mathcal{M}(n-1; \mu\chi)|^2, \tag{7-5}$$

where

$$\mathcal{M}(n; \mu\chi) = \sum_{f \in \mathcal{M}_n} \mu(f)\chi(f). \tag{7-6}$$

Lemma 7.2. *Suppose that χ is a primitive even character modulo t^{n-h}. Then*

$$\mathcal{M}(n; \mu\chi) = \sum_{k=0}^{n} q^{k/2} \operatorname{tr} \operatorname{Sym}^k \Theta_\chi, \tag{7-7}$$

where Sym^n is the symmetric n-th power representation ($n = 0$ corresponds to the trivial representation). In particular,

$$\mathcal{M}(n; \mu\chi) - \mathcal{M}(n-1; \mu\chi) = q^{n/2} \operatorname{tr} \operatorname{Sym}^n \Theta_\chi. \tag{7-8}$$

If $\chi \neq \chi_0$ and χ is not primitive, then

$$|\mathcal{M}(n; \mu\chi)| \ll_n q^{n/2}. \tag{7-9}$$

Proof. We compute the generating function

$$\sum_{n=0}^{\infty} \mathcal{M}(n; \mu\chi) u^n = \sum_{f \text{ monic}} \chi(f)\mu(f) u^{\deg f} = \frac{1}{L(u, \chi)}, \tag{7-10}$$

where $L(u, \chi) = \sum_{f \text{ monic}} \chi(f) u^{\deg f}$ is the associated Dirichlet L-function. Now if χ is *primitive* and *even*, then

$$L(u, \chi) = (1 - u) \det(I - uq^{1/2}\Theta_\chi), \tag{7-11}$$

where $\Theta_\chi \in U(n - h - 2)$ is the unitarized Frobenius class. Therefore we find

$$(1 - u) \sum_{n=0}^{\infty} \mathcal{M}(n; \mu\chi) u^n = \frac{1}{\det(I - uq^{1/2}\Theta_\chi)} = \sum_{k=0}^{\infty} q^{k/2} \operatorname{tr} \operatorname{Sym}^k \Theta_\chi u^k, \tag{7-12}$$

where we have used the identity

$$\frac{1}{\det(I - uA)} = \sum_{k=0}^{\infty} u^k \operatorname{tr} \operatorname{Sym}^k A. \tag{7-13}$$

Comparing coefficients gives (7-7).

For nonprimitive but nontrivial characters $\chi \neq \chi_0$, the L-function still has the form $L(u, \chi) = \prod_{j=1}^{n-h-1}(1 - \alpha_j u)$ with all inverse roots $|\alpha_j| \leq \sqrt{q}$, and hence we obtain (7-9). □

We can now compute the variance using (7-5). We start by bounding the contribution of nonprimitive characters, whose number is $O(\frac{1}{q}\Phi_{\text{ev}}(t^{n-h})) = O(q^{n-h-2})$, and by (7-9) each contributes $O(q^n)$ to the sum in (7-5), hence the total contribution of nonprimitive characters is bounded by $O_n(q^h)$. Consequently we find

$$\operatorname{Var} \mathcal{N}_\mu(\bullet; h) = \frac{q^{h+1}}{\Phi_{\text{ev}}(t^{n-h})} \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \text{ even and primitive}}} |\operatorname{tr} \operatorname{Sym}^n \Theta_\chi|^2 + O(q^h). \tag{7-14}$$

Using Theorem 6.1(i) we get, once we replace the projective group by the unitary group,

$$\lim_{q\to\infty} \frac{\text{Var}(\mathcal{N}_\mu(\,\bullet\,;h))}{q^{h+1}} = \int_{U(n-h-2)} |\text{tr Sym}^n U|^2 \, dU. \tag{7-15}$$

Note that by Schur–Weyl duality (and Weyl's unitary trick), Sym^n is an *irreducible* representation. Hence

$$\int_{U(n-h-2)} |\text{tr Sym}^n U|^2 \, dU = 1, \tag{7-16}$$

and we conclude that $\text{Var}(\mathcal{N}_\mu(\,\bullet\,;h)) \sim q^{h+1} = H$, as claimed.

8. Variance of the Möbius function in arithmetic progressions

We define

$$\mathcal{S}_{\mu,n,Q}(A) = \mathcal{S}_\mu(A) = \sum_{\substack{f\in\mathcal{M}_n \\ f=A \bmod Q}} \mu(f).$$

Theorem 8.1. *If $n \geq \deg Q \geq 2$ then the mean value of $\mathcal{S}_\mu(A)$ tends to 0 as $q \to \infty$, and*

$$\text{Var}_Q(\mathcal{S}_\mu) \sim \frac{q^n}{\Phi(Q)} \int_{U(Q-1)} \left|\text{tr Sym}^n U\right|^2 dU = \frac{q^n}{\Phi(Q)}. \tag{8-1}$$

The mean value over all residues coprime to Q is

$$\langle \mathcal{S}_\mu \rangle = \frac{1}{\Phi(Q)} \sum_{\substack{f\in\mathcal{M}_n \\ \gcd(f,Q)=1}} \mu(f) = \frac{1}{\Phi(Q)} \mathcal{M}(n,\mu\chi_0). \tag{8-2}$$

To evaluate this quantity, we consider the generating function

$$\sum_{n=0}^\infty \mathcal{M}(n,\mu\chi_0)u^n = \sum_{\gcd(f,Q)=1} \mu(f)u^{\deg f}$$

$$= \prod_{P\nmid Q}(1-u^{\deg P}) = \frac{1-qu}{\prod_{P\mid Q}(1-u^{\deg P})}$$

$$= \frac{1-qu}{\prod_k(1-u^k)^{\lambda_k}}, \tag{8-3}$$

where λ_k is the number of prime divisors of Q of degree k. Using the expansion

$$\frac{1}{(1-z)^\lambda} = \sum_{n=0}^\infty \binom{n+\lambda-1}{\lambda-1} z^n$$

gives

$$\frac{1}{\prod_k (1 - u^k)^{\lambda_k}} = \sum_{n=0}^{\infty} C(n) u^n$$

with

$$C(n) = \sum_{\sum_k k n_k = n} \prod_k \binom{n_k + \lambda_k - 1}{\lambda_k - 1},$$

and hence for $n \geq 1$,

$$\mathcal{M}(n, \mu \chi_0) = C(n) - q C(n - 1).$$

Thus we find that for $n \geq 1$,

$$\langle \mathcal{S}_\mu \rangle = \frac{C(n) - q C(n - 1)}{\Phi(Q)} \tag{8-4}$$

and in particular for $\deg Q > 1$,

$$|\langle \mathcal{S}_\mu \rangle| \ll \frac{q}{|Q|} \to 0, \quad q \to \infty. \tag{8-5}$$

For the variance we use (4-11) which gives

$$\mathrm{Var}_Q(\mathcal{S}_\mu) = \frac{1}{\Phi(Q)^2} \sum_{\chi \neq \chi_0} |\mathcal{M}(n; \mu \chi)|^2. \tag{8-6}$$

As in (7-10), the generating function of $\mathcal{M}(n; \mu \chi)$ is $1/L(u, \chi)$. Now for χ odd and primitive, $L(u, \chi) = \det(I - u q^{1/2} \Theta_\chi)$ with $\Theta_\chi \in U(\deg Q - 1)$ unitary. Hence for χ odd and primitive,

$$\mathcal{M}(n; \mu \chi) = q^{n/2} \, \mathrm{tr} \, \mathrm{Sym}^n \, \Theta_\chi. \tag{8-7}$$

For nontrivial χ that is not odd and primitive, we can still write

$$L(u, \chi) = \prod_{j=1}^{\deg Q - 1} (1 - \alpha_j u)$$

with all inverse roots $|\alpha_j| \leq \sqrt{q}$, and hence for $\chi \neq \chi_0$ we have a bound

$$|\mathcal{M}(n; \mu \chi)| \ll_n q^{n/2}. \tag{8-8}$$

The number of even characters is $\Phi_{\mathrm{ev}}(Q) = \Phi(Q)/(q - 1)$ and the number of nonprimitive characters is $O(\Phi(Q)/q)$, hence the number of characters which are

not odd and primitive is $O(\Phi(Q)/q)$. Inserting the bound (8-8) into (8-6) shows that the contribution of such characters is $O(q^{n-1}/\Phi(Q))$. Hence

$$\operatorname{Var}_Q \mathcal{S}_\mu = \frac{q^n}{\Phi(Q)} \frac{1}{\Phi(Q)} \sum_{\chi \text{ odd primitive}} |\operatorname{tr} \operatorname{Sym}^n \Theta_\chi|^2 + O\left(\frac{q^{n-1}}{\Phi(Q)}\right). \tag{8-9}$$

Using Theorem 6.2(i) gives that, as $q \to \infty$,

$$\operatorname{Var}_Q \mathcal{S}_\mu \sim \frac{q^n}{\Phi(Q)} \int_{U(Q-1)} |\operatorname{tr} \operatorname{Sym}^n U|^2 \, dU = \frac{q^n}{\Phi(Q)}. \tag{8-10}$$

9. The variance of squarefrees in short intervals

In this section we study the variance of the number of squarefree polynomials in short intervals. The total number of squarefree monic polynomials of degree $n > 1$ is (exactly)

$$\sum_{f \in \mathcal{M}_n} \mu(f)^2 = \frac{q^n}{\zeta_q(2)} = q^n \left(1 - \frac{1}{q}\right). \tag{9-1}$$

The number of squarefree polynomials in the short interval $I(A; h)$ is

$$\mathcal{N}_{\mu^2}(A; h) = \sum_{f \in I(A;h)} \mu(f)^2. \tag{9-2}$$

Theorem 9.1. *Let* $0 \le h \le n - 6$. *Assume* $q \to \infty$ *with all* q's *coprime to* 6.

(i) *If* h *is even then*

$$\operatorname{Var} \mathcal{N}_{\mu^2}(\,\bullet\,; h) \sim q^{\frac{h}{2}} \int_{U(n-h-2)} \left|\operatorname{tr} \operatorname{Sym}^{\frac{h}{2}+1} U\right|^2 dU = \frac{\sqrt{H}}{\sqrt{q}}. \tag{9-3}$$

(ii) *If* h *is odd then*

$$\operatorname{Var} \mathcal{N}_{\mu^2}(\,\bullet\,; h) \sim q^{\frac{h-1}{2}} \int_{U(n-h-2)} |\operatorname{tr} U|^2 \, dU \int_{U(n-h-2)} \left|\operatorname{tr} \operatorname{Sym}^{\frac{h+3}{2}} U'\right|^2 dU'$$

$$= \frac{\sqrt{H}}{q}. \tag{9-4}$$

Proof. To compute the variance, we use Lemma 5.4. Since $\mu^2(t^m) = 1$ for $m = 0, 1$ and equals 0 for $m > 1$, we obtain

$$\operatorname{Var}(\mathcal{N}_{\mu^2}(\,\bullet\,; h)) = \frac{1}{\Phi_{\mathrm{ev}}(t^{n-h})^2} \sum_{\substack{\chi \ne \chi_0 \bmod t^{n-h} \\ \chi \text{ even}}} \left|\mathcal{M}(n; \mu^2\chi) + \mathcal{M}(n-1; \mu^2\chi)\right|^2, \tag{9-5}$$

where

$$\mathcal{M}(n; \mu^2\chi) = \sum_{f \in \mathcal{M}_n} \mu(f)^2 \chi(f). \tag{9-6}$$

To obtain an expression for $\mathcal{M}(n; \mu^2\chi)$, we consider the generating function

$$\sum_{n=0}^{\infty} \mathcal{M}(n; \mu^2\chi)u^n = \sum_f \mu(f)^2 \chi(f) u^{\deg f} = \frac{L(u, \chi)}{L(u^2, \chi^2)}. \tag{9-7}$$

Assume that χ is primitive, and that χ^2 is also[4] primitive (modulo t^{n-h}). Then

$$L(u, \chi) = (1 - u) \det(I - uq^{1/2}\Theta_\chi),$$
$$L(u^2, \chi^2) = (1 - u^2) \det(I - u^2 q^{1/2}\Theta_{\chi^2}).$$

Writing for $U \in U(N)$

$$\det(I - xU) = \sum_{j=0}^{N} \lambda_j(U)x^j,$$
$$\frac{1}{\det(I - xU)} = \sum_{k=0}^{\infty} \operatorname{tr} \operatorname{Sym}^k U x^k, \tag{9-8}$$

gives, on abbreviating

$$\lambda_j(\chi) := \lambda_j(\Theta_\chi), \quad \operatorname{Sym}^k(\chi^2) = \operatorname{tr} \operatorname{Sym}^k \Theta_{\chi^2},$$

that

$$\frac{L(u, \chi)}{L(u^2, \chi^2)} = \frac{\det(I - uq^{1/2}\Theta_\chi)}{(1 + u) \det(I - u^2 q^{1/2}\Theta_{\chi^2})}$$
$$= \sum_{m=0}^{\infty} \sum_{0 \le j \le N} \sum_{k=0}^{\infty} (-1)^m \lambda_j(\chi) \operatorname{Sym}^k(\chi^2) q^{(j+k)/2} u^{m+j+2k},$$

and hence

$$\mathcal{M}(n; \mu^2\chi) = (-1)^n \sum_{\substack{j+2k \le n \\ 0 \le j \le N \\ k \ge 0}} (-1)^j \lambda_j(\chi) \operatorname{Sym}^k(\chi^2) q^{(j+k)/2}. \tag{9-9}$$

---

[4]If q is odd then primitivity of χ and of χ^2 are equivalent.

Therefore

$$\mathcal{M}(n; \mu^2\chi) + \mathcal{M}(n-1; \mu^2\chi) = (-1)^n \sum_{\substack{j+2k\le n \\ 0\le j\le N \\ k\ge 0}} (-1)^j \lambda_j(\chi) \operatorname{Sym}^k(\chi^2) q^{\frac{j+k}{2}}$$

$$+ (-1)^{n-1} \sum_{\substack{j+2k\le n-1 \\ 0\le j\le N \\ k\ge 0}} (-1)^j \lambda_j(\chi) \operatorname{Sym}^k(\chi^2) q^{\frac{j+k}{2}}$$

$$= (-1)^n \sum_{\substack{j+2k=n \\ 0\le j\le N \\ k\ge 0}} (-1)^j \lambda_j(\chi) \operatorname{Sym}^k(\chi^2) q^{\frac{j+k}{2}}$$

$$= q^{n/4} \sum_{\substack{0\le j\le N \\ j=n \bmod 2}} \lambda_j(\chi) \operatorname{Sym}^{\frac{n-j}{2}}(\chi^2) q^{j/4}.$$

Therefore, recalling that $N = n - h - 2$,

$$\mathcal{M}(n; \mu^2\chi) + \mathcal{M}(n-1; \mu^2\chi)$$

$$= (-1)^n (1 + O(q^{-1/2})) \times \begin{cases} q^{\frac{n}{2} - \frac{h+1}{4} - \frac{1}{4}} \lambda_N(\chi) \operatorname{Sym}^{\frac{h+2}{2}}(\chi^2), & n = N \bmod 2, \\ q^{\frac{n}{2} - \frac{h+1}{4} - \frac{1}{2}} \lambda_{N-1}(\chi) \operatorname{Sym}^{\frac{h+3}{2}}(\chi^2), & n \ne N \bmod 2. \end{cases}$$

Noting that $n = N \bmod 2$ is equivalent to h even, we finally obtain

$$|\mathcal{M}(n; \mu^2\chi) + \mathcal{M}(n-1; \mu^2\chi)|^2$$

$$= (1 + O(q^{-1/2})) \times \begin{cases} q^{n - \frac{h+1}{2} - \frac{1}{2}} |\lambda_N(\chi) \operatorname{Sym}^{\frac{h+2}{2}}(\chi^2)|^2, & h \text{ even}, \\ q^{n - \frac{h+1}{2} - 1} |\lambda_{N-1}(\chi) \operatorname{Sym}^{\frac{h+3}{2}}(\chi^2)|^2, & h \text{ odd}. \end{cases} \quad (9\text{-}10)$$

Inserting (9-10) into (9-5) gives an expression for the variance, up to terms which are smaller by $q^{-1/2}$. The contribution of nonprimitive characters is bounded as in previous sections and we skip this verification. We separate cases according to h even or odd.

h even. We have $|\lambda_N(\chi)| = |\det \Theta_\chi| = 1$, so that

$$\operatorname{Var} \mathcal{N}_{\mu^2}(\,\bullet\,; h) \sim q^{\frac{h}{2}} \frac{1}{\Phi_{\mathrm{ev}}(t^{n-h})} \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \text{ primitive even}}} |\operatorname{Sym}^{\frac{h+2}{2}}(\chi^2)|^2. \quad (9\text{-}11)$$

Here the change of variable $\chi \mapsto \chi^2$ is an automorphism of the group of even characters if q is odd, since then the order of the group is $\Phi_{\mathrm{ev}}(t^{n-h}) = q^{n-h-1}$, which is odd. Using Theorem 6.1(i) for even primitive characters modulo t^{n-h}

allows us to replace the average over characters by a matrix integral, leading to

$$\operatorname{Var} \mathcal{N}_{\mu^2}(\, \bullet \,; h) \sim q^{\frac{h}{2}} \int\limits_{U(n-h-2)} |\operatorname{tr} \operatorname{Sym}^{\frac{h}{2}+1} U|^2 \, dU. \tag{9-12}$$

Since the symmetric powers Sym^k are irreducible representations, the matrix integral works out to be 1. Hence (with $H = q^{h+1}$)

$$\operatorname{Var} \mathcal{N}_{\mu^2}(\, \bullet \,; h) \sim q^{h/2} = \frac{\sqrt{H}}{\sqrt{q}} \, . \tag{9-13}$$

h odd. In this case

$$\operatorname{Var} \mathcal{N}_{\mu^2}(\, \bullet \,; h) \sim q^{\frac{h-1}{2}} \frac{1}{\Phi_{\mathrm{ev}}(t^{n-h})} \sum_{\substack{\chi \bmod t^{n-h} \\ \chi \text{ primitive even}}} |\lambda_{N-1}(\chi) \operatorname{Sym}^{\frac{h+3}{2}} (\chi^2)|^2. \tag{9-14}$$

Note that $|\lambda_{N-1}(U)| = |\operatorname{tr} U|$, because $\lambda_{N-1}(U) = (-1)^{N-1} \det U \operatorname{tr} U^{-1}$ and for unitary matrices, $|\det U| = 1$ and $\operatorname{tr} U^{-1} = \overline{\operatorname{tr} U}$.

We now use Theorem 6.1(ii), which asserts that, for $0 \le h \le n - 6$ and $q \to \infty$ with q coprime to 6, both Θ_χ and Θ_{χ^2} are uniformly distributed in $PU(n - h - 2)$ and that $\Theta_\chi, \Theta_{\chi^2}$ are *independent*. We obtain

$$\operatorname{Var} \mathcal{N}_{\mu^2}(\, \bullet \,; h) \sim q^{\frac{h-1}{2}} \int\limits_{U(n-h-2)} |\operatorname{tr} U|^2 \, dU \int\limits_{U(n-h-2)} |\operatorname{tr} \operatorname{Sym}^{\frac{h+3}{2}} U'|^2 \, dU'$$

$$= \frac{\sqrt{H}}{q}, \tag{9-15}$$

by irreducibility of the symmetric power representations. $\qquad\square$

10. Squarefrees in arithmetic progressions

As in previous sections, we set

$$S(A) = \sum_{\substack{f = A \bmod Q \\ f \in \mathcal{M}_n}} \mu^2(f). \tag{10-1}$$

We have the expected value

$$\langle S \rangle_Q = \frac{1}{\Phi(Q)} \sum_{\substack{f \in \mathcal{M}_n \\ (f, Q) = 1}} \mu^2(f) \sim \frac{q^n / \zeta_q(2)}{\Phi(Q)} \sim \frac{q^n}{|Q|} \tag{10-2}$$

and the variance

$$\text{Var}_Q(\mathcal{S}) = \frac{1}{\Phi(Q)^2} \sum_{\chi \neq \chi_0} |\mathcal{M}(n; \mu^2 \chi)|^2. \tag{10-3}$$

Theorem 10.1. *Fix $n > N \geq 1$. For any sequence of finite fields $\mathbb{F}_q$, with q odd, and squarefree polynomials $Q \in \mathbb{F}_q[t]$ with $\deg Q = N + 1$, as $q \to \infty$,*

$$\text{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{|Q|^{1/2}} \times \begin{cases} 1/\sqrt{q}, & n \neq \deg Q \bmod 2, \\ 1/q, & n = \deg Q \bmod 2. \end{cases}$$

Proof. The generating function of $\mathcal{M}(n; \mu^2 \chi)$ is

$$\sum_{n=0}^{\infty} \mathcal{M}(n; \mu^2 \chi) u^n = \sum_f \mu(f)^2 \chi(f) u^{\deg f} = \frac{L(u, \chi)}{L(u^2, \chi^2)}. \tag{10-4}$$

If both χ, χ^2 are primitive, odd, characters (which happens for almost all χ), then

$$L(u, \chi) = \det(I - u q^{1/2} \Theta_\chi), \quad L(u^2, \chi^2) = \det(I - u^2 q^{1/2} \Theta_{\chi^2}), \tag{10-5}$$

and writing (with $N = \deg Q - 1$)

$$\det(I - u q^{1/2} \Theta_\chi) = \sum_{j=0}^{N} \lambda_j(\chi) q^{j/2} u^j, \tag{10-6}$$

$$\frac{1}{\det(I - q^{1/2} u^2 \Theta_{\chi^2})} = \sum_{k=0}^{\infty} \text{Sym}^k(\chi^2) q^{k/2} u^{2k}, \tag{10-7}$$

we get, since $n \geq N$,

$$\mathcal{M}(n; \mu^2 \chi) = \sum_{\substack{j+2k=n \\ 0 \leq j \leq N \\ k \geq 0}} \lambda_j(\chi) \text{Sym}^k(\chi^2) q^{\frac{j+k}{2}}$$

$$= q^{\frac{n}{4}} \sum_{\substack{j=0 \\ j=n \bmod 2}}^{N} \lambda_j(\chi) \text{Sym}^{\frac{n-j}{2}}(\chi^2) q^{\frac{j}{4}}, \tag{10-8}$$

and hence

$$\mathcal{M}(n; \mu^2 \chi) =$$

$$(1 + O(q^{-\frac{1}{2}})) q^{\frac{n+N}{4}} \times \begin{cases} \lambda_N(\chi) \text{Sym}^{\frac{n-N}{2}}(\chi^2), & n = N \bmod 2, \\ q^{-\frac{1}{4}} \lambda_{N-1}(\chi) \text{Sym}^{\frac{n-N+1}{2}}(\chi^2), & n \neq N \bmod 2. \end{cases} \tag{10-9}$$

Since $\lambda_N(\chi) = \det \Theta_\chi$, which has absolute value one, we find

$$|\mathcal{M}(n; \mu^2\chi)|^2 =$$
$$(1 + O(q^{-\frac{1}{2}}))q^{\frac{n+N}{2}} \times \begin{cases} |\operatorname{Sym}^{\frac{n-N}{2}}(\chi^2)|^2, & n = N \bmod 2 \\ q^{-\frac{1}{2}}|\lambda_{N-1}(\chi)\operatorname{Sym}^{\frac{n-N+1}{2}}(\chi^2)|^2, & n \neq N \bmod 2. \end{cases} \quad (10\text{-}10)$$

If $\chi \neq \chi_0$ and χ is not odd, or not primitive, we may use the same computation to show that

$$|\mathcal{M}(n; \mu^2\chi)| \ll_n q^{(n+N)/4}, \quad \chi \neq \chi_0 \text{ and is even or imprimitive.} \quad (10\text{-}11)$$

We thus have a formula for $\operatorname{Var}(\mathcal{S})$. We may neglect the contribution of characters χ for which χ or χ^2 are nonprimitive or even, as these form a proportion $\leq 1/q$ of all characters, and thus their contribution is

$$\ll \frac{1}{\Phi(Q)} \frac{1}{q} q^{(n+N)/2} \ll \frac{1}{q} \frac{q^{n/2}}{|Q|^{1/2}\sqrt{q}},$$

which is negligible relative to the claimed main term in the Theorem.

To handle the contribution of primitive odd characters we invoke Theorem 6.2(ii) which asserts that both Θ_χ and Θ_{χ^2} are uniformly distributed in $U(\deg Q - 1)$ and are independent (for q odd). To specify the implications, we separate into cases:

If $n = N \bmod 2$ (i.e., $n \neq \deg Q \bmod 2$) then

$$\operatorname{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{|Q|^{1/2}q^{1/2}} \frac{1}{\Phi(Q)} \sum_{\chi, \chi^2 \text{ primitive}} |\operatorname{Sym}^{\frac{n-N}{2}}(\chi^2)|^2. \quad (10\text{-}12)$$

By equidistribution

$$\frac{1}{\Phi(Q)} \sum_{\chi, \chi^2 \text{primitive}} |\operatorname{Sym}^{\frac{n-N}{2}}(\chi^2)|^2 \sim \int_{U(N)} |\operatorname{tr} \operatorname{Sym}^{\frac{n-N}{2}} U|^2 \, dU. \quad (10\text{-}13)$$

Note that $\int_{U(N)} |\operatorname{tr} \operatorname{Sym}^{\frac{n-N}{2}} U|^2 \, dU = 1$ by irreducibility of Sym^k. Thus we obtain

$$\operatorname{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{|Q|^{1/2}q^{1/2}}, \quad n \neq \deg Q \bmod 2. \quad (10\text{-}14)$$

If $n \neq N \bmod 2$ (i.e., $n = \deg Q \bmod 2$), then we get

$$\operatorname{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{q|Q|^{1/2}} \frac{1}{\Phi(Q)} \sum_{\chi, \chi^2 \text{ primitive}} |\lambda_{N-1}(\chi)\operatorname{Sym}^{\frac{n-N+1}{2}}(\chi^2)|^2. \quad (10\text{-}15)$$

Note that as in Section 9, $|\lambda_{N-1}(\chi)| = |\mathrm{tr}\,\Theta_\chi|$. By Theorem 6.2(ii),

$$\frac{1}{\Phi(Q)} \sum_{\chi,\chi^2 \text{ primitive}} \left|\lambda_{N-1}(\chi)\,\mathrm{Sym}^{\frac{n-N+1}{2}}(\chi^2)\right|^2 \sim$$

$$\iint\limits_{U(N)\times U(N)} |\mathrm{tr}\,U|^2 \cdot \left|\mathrm{tr}\,\mathrm{Sym}^{\frac{n-N+1}{2}}U'\right|^2 dU\,dU' = 1, \quad (10\text{-}16)$$

and hence

$$\mathrm{Var}_Q(\mathcal{S}) \sim \frac{q^{n/2}}{q|Q|^{1/2}}. \quad (10\text{-}17)$$

Thus we find

$$\mathrm{Var}_Q(\mathcal{S}) \sim \begin{cases} \dfrac{q^{n/2}}{|Q|^{1/2}q^{1/2}}, & n \neq \deg Q \bmod 2, \\[2mm] \dfrac{q^{n/2}}{|Q|^{1/2}q}, & n = \deg Q \bmod 2, \end{cases} \quad (10\text{-}18)$$

as claimed. $\qquad\square$

Appendix: Hall's theorem for $\mathbb{F}_q[t]$: The large degree limit

Let $Q(n, H)$ be the number of squarefree integers in an interval of length H about n:

$$Q(n, H) := \sum_{j=1}^{H} \mu^2(n + j). \quad (A\text{-}1)$$

Hall [1982] studied the variance of $Q(n, H)$ as n varies up to X. He showed that provided $H = O(X^{2/9-o(1)})$, the variance grows like $\sqrt{H}$ and in fact admits an asymptotic formula:

$$\frac{1}{X} \sum_{n \leq X} \left|Q(n, H) - \frac{H}{\zeta(2)}\right|^2 \sim A\sqrt{H}, \quad (A\text{-}2)$$

with

$$A = \frac{\zeta(3/2)}{\pi} \prod_p \left(1 - \frac{3}{p^2} + \frac{2}{p^3}\right). \quad (A\text{-}3)$$

We give a version of Hall's theorem for the polynomial ring $\mathbb{F}_q[t]$ with q fixed. Let

$$\mathcal{N}(A) = \sum_{|f-A|\leq q^h} \mu^2(f)$$

be the number of squarefree polynomials in a short interval $I(A; h)$ around $A \in \mathcal{M}_n$, with $h \leq n - 2$. Note that

$$\#I(A; h) = q^{h+1} =: H.$$

We wish to compute the variance of $\mathcal{N}$ as we average over all short intervals with q fixed and $n \to \infty$.

Let

$$\beta_q = \prod_P \left(1 - \frac{3}{|P|^2} + \frac{2}{|P|^3} \right). \tag{A-4}$$

Theorem A.1. *As $h \to \infty$,*

$$\operatorname{Var} \mathcal{N} = \sqrt{H} \frac{\beta_q}{1 - q^{-3}} \times \begin{cases} \dfrac{1 + q^{-2}}{\sqrt{q}}, & h \text{ even} \\[2mm] \dfrac{1 + q^{-1}}{q}, & h \text{ odd} \end{cases} + O\left(\frac{H^2 n}{q^{n/3}} \right) + O_q(H^{1/4 + o(1)}).$$

In particular we get an asymptotic result provided $h < \left(\frac{2}{9} - o(1) \right) n$, or equivalently $H < (q^n)^{\frac{2}{9} - o(1)}$. It is likely that one can improve the factor $2/9$ a bit.

The probability that f and $f + J$ are both squarefree. As in the number field case, we start with an expression for the probability that both f and $f + J$ are squarefree. For a nonzero polynomial $J \in \mathbb{F}_q[t]$, define the "singular series"

$$\mathfrak{S}(J) = \prod_P \left(1 - \frac{2}{|P|^2} \right) \prod_{P^2 | J} \frac{|P|^2 - 1}{|P|^2 - 2}, \tag{A-5}$$

the product over all prime polynomials. We will first show this:

Theorem A.2. *For $0 \neq J \in \mathbb{F}_q[t]$, $\deg J < n$,*

$$S(J; n) := \sum_{f \in \mathcal{M}_n} \mu^2(f) \mu^2(f + J) = \mathfrak{S}(J) q^n + O(n q^{\frac{2n}{3}}), \tag{A-6}$$

the implied constant absolute, with $\mathfrak{S}(J)$ given by (A-5).

Note that Theorem A.2 is uniform in J as long as $\deg J < n$.

Theorem A.2 is the exact counterpart for the analogous quantity over the integers, which has been known in various forms since the 1930's. The proof below is roughly the same as the one given in [Hall 1982, Theorem 1]. The exponent $2/3$ has been improved, by Heath-Brown [1984] to $7/11$ and by Reuss [2014] to about 0.578.

A decomposition of μ^2. We start with the identity

$$\mu^2(f) = \sum_{d^2|f} \mu(d) \tag{A-7}$$

(the sum over monic d). Pick an integer parameter $0 < z \le n/2$, write $Z = q^z$, and decompose the sum into two parts, one over "small" divisors, that is with $\deg d < z$, and one over "large" divisors:

$$\mu^2 = \mu_z^2 + e_z, \tag{A-8}$$

$$\mu_z^2(f) = \sum_{\substack{d^2|f \\ \deg d < z}} \mu(d), \quad e_z(f) = \sum_{\substack{d^2|f \\ \deg d \ge z}} \mu(d). \tag{A-9}$$

Let

$$S_z(J; n) := \sum_{f \in \mathcal{M}_n} \mu_z^2(f) \mu_z^2(f + J). \tag{A-10}$$

We want to replace S by S_z.

Bounding $S(J; n) - S_z(n; J)$.

Proposition A.3. *If $z \le n/2$ then*

$$|S(J; n) - S_z(J; n)| \ll \frac{q^n}{Z},$$

where $Z = q^z$.

Proof. Note that

$$\mu^2(f)\mu^2(f+J) =$$
$$\mu_z^2(f)\mu_z^2(f+J) + e_z(f)\mu^2(f+J) - \mu^2(f)e_z(f+J) - e_z(f)e_z(f+J) \tag{A-11}$$

so that (recall $\mu^2(f) \le 1$)

$$\left|\mu^2(f)\mu^2(f+J) - \mu_z^2(f)\mu_z^2(f+J)\right| \le |e_z(f)| + |e_z(f+J)| + |e_z(f)e_z(f+J)|$$
$$\le |e_z(f)| + |e_z(f+J)| + \tfrac{1}{2}|e_z(f)|^2 + \tfrac{1}{2}|e_z(f+J)|^2 \tag{A-12}$$

and therefore, summing (A-12) over $f \in \mathcal{M}_n$ and noting that since $\deg J < n$, sums of $f + J$ are the same as sums of f,

$$|S(J; n) - S_z(J; n)| \le 2 \sum_{f \in \mathcal{M}_n} |e_z(f)| + \sum_{f \in \mathcal{M}_n} |e_z(f)|^2. \tag{A-13}$$

We have

$$|e_z(f)| = \left| \sum_{\substack{d^2|f \\ \deg d \ge z}} \mu(d) \right| \le \sum_{\substack{d^2|f \\ \deg d \ge z}} 1,$$

so that

$$\sum_{f \in \mathcal{M}_n} |e_z(f)| \le \sum_{f \in \mathcal{M}_n} \sum_{\substack{d^2 | f \\ \deg d \ge z}} 1$$

$$= \sum_{z \le \deg d \le n/2} \#\{f \in \mathcal{M}_n : d^2 \mid f\}$$

$$= \sum_{z \le \deg d \le n/2} \frac{q^n}{|d|^2} \le \frac{2q^n}{Z}. \tag{A-14}$$

Moreover,

$$\sum_{f \in \mathcal{M}_n} |e_z(f)|^2 \le \sum_{f \in \mathcal{M}_n} \sum_{\substack{d_1^2 | f \\ \deg d_1 \ge z}} \sum_{\substack{d_2^2 | f \\ \deg d_2 \ge z}} 1$$

$$\le \sum_{z \le \deg d_1, \deg d_2 \le n/2} \#\{f \in \mathcal{M}_n : d_1^2 \mid f \text{ and } d_2^2 \mid f\}.$$

Now the conditions $d_1^2 \mid f$ and $d_2^2 \mid f$ are equivalent to $[d_1, d_2]^2 \mid f$, where $[d_1, d_2]$ is the least common multiple of d_1 and d_2, and this can only happen if $\deg[d_1, d_2] \le \deg f/2 = n/2$, in which case the number of such f is $q^n/|[d_1, d_2]|^2$ and is zero otherwise. Thus

$$\sum_{f \in \mathcal{M}_n} |e_z(f)|^2 \le \sum_{\substack{z \le \deg d_1, \deg d_2 \le n/2 \\ \deg[d_1, d_2] \le n/2}} \frac{q^n}{|[d_1, d_2]|^2}$$

$$\le q^n \sum_{\deg d_1, \deg d_2 \ge z} \frac{1}{|[d_1, d_2]|^2}. \tag{A-15}$$

We claim the following analogue of [Hall 1982, Lemma 2]:

Lemma A.4. $$\sum_{\deg d_1, \deg d_2 \ge z} \frac{1}{|[d_1, d_2]|^2} \ll \frac{1}{Z}.$$

Inserting Lemma A.4 in (A-15) we will get

$$\sum_{f \in \mathcal{M}_n} |e_z(f)|^2 \ll \frac{q^n}{Z}. \tag{A-16}$$

Inserting (A-14) and (A-16) in (A-13) we conclude Proposition A.3.

To prove Lemma A.4, use $[d_1, d_2] = d_1 d_2 / \gcd(d_1, d_2)$ to rewrite the sum as

$$\sum_{\deg d_1, \deg d_2 \geq z} \frac{1}{|[d_1, d_2]|^2} = \sum_{\deg d_1, \deg d_2 \geq z} \frac{|\gcd(d_1, d_2)|^2}{|d_1|^2 |d_2|^2}$$

$$= \sum_{k \text{ monic}} |k|^2 \sum_{\substack{\deg d_1, \deg d_2 \geq z \\ \gcd(d_1, d_2) = k}} \frac{1}{|d_1|^2 |d_2|^2} \, .$$

In the sum above, we write $d_j = k \delta_j$ with $\gcd(\delta_1, \delta_2) = 1$. The condition $\deg d_j \geq z$ gives no restriction on δ_j if $\deg k \geq z$, and otherwise translates into $\deg \delta_j \geq z - \deg k$. Thus

$$\sum_{\deg d_1, \deg d_2 \geq z} \frac{1}{|[d_1, d_2]|^2} \ll \sum_{k \text{ monic}} \frac{1}{|k|^2} \sum_{\substack{\deg \delta_1, \deg \delta_2 \geq z - \deg k \\ \gcd(\delta_1, \delta_2) = 1}} \frac{1}{|\delta_1|^2 |\delta_2|^2}$$

$$\leq \sum_{k \text{ monic}} \frac{1}{|k|^2} \left(\sum_{\deg \delta \geq z - \deg k} \frac{1}{|\delta|^2} \right)^2,$$

after ignoring the coprimality condition. Therefore

$$\sum_{k \text{ monic}} \frac{1}{|k|^2} \left(\sum_{\deg \delta \geq z - \deg k} \frac{1}{|\delta|^2} \right)^2 \leq \sum_{\deg k \leq z} \frac{1}{|k|^2} \left(\sum_{\deg \delta \geq z - \deg k} \frac{1}{|\delta|^2} \right)^2$$

$$+ \sum_{\deg k > z} \frac{1}{|k|^2} \left(\sum_{\delta} \frac{1}{|\delta|^2} \right)^2$$

$$\ll \sum_{\deg k \leq z} \frac{1}{|k|^2} \left(\frac{|k|}{q^z} \right)^2 + \frac{1}{q^{z+1}}$$

$$\ll \frac{1}{Z},$$

which proves Lemma A.4.   □

Evaluating $S_z(J; n)$.

Proposition A.5. *If $z \leq n/2$ then*

$$S_z(J; n) = q^n \mathfrak{S}(J) + O\left(\frac{q^n z}{Z} \right) + O(Z^2),$$

with $Z = q^z$.

Proof. Using the definition of μ_z^2, we obtain

$$
\begin{aligned}
S_z(J; n) &:= \sum_{f \in \mathcal{M}_n} \mu_z^2(f) \mu_z^2(f + J) \\
&= \sum_{\deg d_1 \leq z} \sum_{\deg d_2 \leq z} \mu(d_1) \mu(d_2) \#\{f \in \mathcal{M}_n : d_1^2 \mid f, \, d_2^2 \mid f + J\}.
\end{aligned}
$$

Decomposing into residue classes modulo $[d_1, d_2]^2$ gives

$$
\#\{f \in \mathcal{M}_n : d_1^2 \mid f, \, d_2^2 \mid f + J\} = \sum_{\substack{c \bmod [d_1, d_2]^2 \\ c = 0 \bmod d_1^2 \\ c = -J \bmod d_2^2}} \#\{f \in \mathcal{M}_n : f = c \bmod [d_1, d_2]^2\}.
$$

If $\deg[d_1, d_2]^2 \leq n$ then

$$
\#\{f \in \mathcal{M}_n : f = c \bmod [d_1, d_2]^2\} = \frac{q^n}{|[d_1, d_2]|^2}.
$$

Otherwise there is at most *one* $f \in \mathcal{M}_n$ with $f = c \bmod [d_1, d_2]^2$. So we write

$$
\#\{f \in \mathcal{M}_n : f = c \bmod [d_1, d_2]^2\} = \frac{q^n}{|[d_1, d_2]|^2} + O(1).
$$

Let $\kappa(d_1, d_2; J)$ be the number of solutions $c \bmod [d_1, d_2]^2$ of the system of congruences $c = 0 \bmod d_1^2$, $c = -J \bmod d_2^2$; it is either 1 or 0 depending on whether $\gcd(d_1, d_2)^2 \mid J$ or not. Then we have found that

$$
\begin{aligned}
S_z(J; n) &= \sum_{\deg d_1 \leq z} \sum_{\deg d_2 \leq z} \mu(d_1) \mu(d_2) \kappa(d_1, d_2; J) \left(\frac{q^n}{|[d_1, d_2]|^2} + O(1) \right) \\
&= q^n \sum_{\deg d_1 \leq z} \sum_{\deg d_2 \leq z} \mu(d_1) \mu(d_2) \frac{\kappa(d_1, d_2; J)}{|[d_1, d_2]|^2} + O(Z^2).
\end{aligned}
$$

The double sum can be extended to include all d_1, d_2:

$$
\sum_{\deg d_1 \leq z} \sum_{\deg d_2 \leq z} \mu(d_1) \mu(d_2) \frac{\kappa(d_1, d_2; J)}{|[d_1, d_2]|^2} = \sum_{d_1, d_2} \mu(d_1) \mu(d_2) \frac{\kappa(d_1, d_2; J)}{|[d_1, d_2]|^2}
$$

$$
+ O\left(\sum_{\deg d_1 > z} \sum_{d_2} \frac{1}{|[d_1, d_2]|^2} \right),
$$

so that

$$S_z(J; n) = q^n \sum_{d_1, d_2} \mu(d_1)\mu(d_2)\frac{\kappa(d_1, d_2; J)}{|[d_1, d_2]|^2}$$

$$+ O\left(\sum_{\deg d_1 > z} \sum_{d_2} \frac{1}{|[d_1, d_2]|^2}\right) + O(Z^2). \quad \text{(A-17)}$$

The sum in the remainder term of (A-17) is bounded in the following analogue of [Hall 1982, Lemma 3].

Lemma A.6.
$$\sum_{\deg d_1 > z} \sum_{d_2} \frac{1}{|[d_1, d_2]|^2} \ll \frac{z}{q^z} = \frac{z}{Z}.$$

Proof. We argue as in the proof of Lemma A.4: We write the least common multiple as $[d_1, d_2] = d_1 d_2 / \gcd(d_1, d_2)$ and sum over all pairs of d_1, d_2 with given gcd:

$$\sum_{\deg d_1 > z} \sum_{d_2} \frac{1}{|[d_1, d_2]|^2} = \sum_k |k|^2 \sum_{\deg d_1 > z} \sum_{\substack{d_2 \\ \gcd(d_1, d_2) = k}} \frac{1}{|d_1|^2 |d_2|^2}$$

$$= \sum_k |k|^2 \sum_{\deg \delta_1 > z - \deg k} \frac{1}{|k|^2 |\delta_1|^2} \sum_{\substack{\delta_2 \\ \gcd(\delta_1, \delta_2) = 1}} \frac{1}{|k|^2 |\delta_2|^2}.$$

after writing $d_j = k\delta_j$ with δ_1, δ_2 coprime.

Ignoring the coprimality condition gives

$$\sum_{\deg d_1 > z} \sum_{d_2} \frac{1}{|[d_1, d_2]|^2} \ll \sum_k \frac{1}{|k|^2} \sum_{\deg \delta_1 > z - \deg k} \frac{1}{|\delta_1|^2} \sum_{\delta_2} \frac{1}{|\delta_2|^2}$$

$$\ll \sum_{\deg k \leq z} \frac{1}{|k|^2} \sum_{\deg \delta_1 > z - \deg k} \frac{1}{|\delta_1|^2} + \sum_{\deg k > z} \frac{1}{|k|^2} \sum_{\delta_1} \frac{1}{|\delta_1|^2}$$

$$\ll \sum_{\deg k \leq z} \frac{1}{|k|^2} \frac{|k|}{q^z} + \sum_{\deg k > z} \frac{1}{|k|^2}$$

$$\ll \frac{z}{q^z} = \frac{z}{Z},$$

which proves Lemma A.6. $\qquad \square$

Putting together (A-17) and Lemma A.6, we have shown that

$$S_z(J; n) = q^n \sum_{d_1} \sum_{d_2} \mu(d_1)\mu(d_2)\frac{\kappa(d_1, d_2; J)}{|[d_1, d_2]|^2} + O\left(\frac{q^n z}{Z}\right) + O(Z^2). \quad \text{(A-18)}$$

It remains to show that the infinite sum in (A-18) coincides with the singular series $\mathfrak{S}(J)$.

Lemma A.7.
$$\sum_{d_1}\sum_{d_2} \mu(d_1)\mu(d_2)\frac{\kappa(d_1, d_2; J)}{|[d_1, d_2]|^2} = \mathfrak{S}(J).$$

Proof. This is done exactly as in [Hall 1982, Appendix]. We write
$$\sum_{d_1}\sum_{d_2} \mu(d_1)\mu(d_2)\frac{\kappa(d_1, d_2; J)}{|[d_1, d_2]|^2} = \sum_m \frac{s(m; J)}{|m|^2},$$

where
$$s(m; J) = \sum_{\substack{[d_1, d_2]=m \\ \gcd(d_1, d_2)^2 | J}} \mu(d_1)\mu(d_2).$$

One checks that $s(m; J)$ is multiplicative in m, and that for P prime
$$s(P^\alpha; P^j) = \sum_{\substack{\max(u, v)=\alpha \\ 2\min(u, v)\le j}} \mu(P^u)\mu(P^v),$$

so that $s(P^\alpha; P^j) = 0$ for $\alpha \ge 2$, while for $\alpha = 1$
$$s(P; P^j) = \sum_{\substack{\max(u, v)=1 \\ \min(u, v)\le j/2}} \mu(P^u)\mu(P^v).$$

If $j < 2$ (that is if $P^2 \nmid P^j$), then the sum is over $\max(u, v) = 1$ and $\min(u, v) = 0$, i.e., $(u, v) = (0, 1), (1, 0)$, which works out to $s(P, P^j) = -2$ for $j = 0, 1$, while for $j \ge 2$ the only restriction is $\max(u, v) = 1$, i.e., $(u, v) = (1, 0), (0, 1), (1, 1)$, which gives $s(P, P^j) = -1$ for $j \ge 2$. Thus
$$\sum_m \frac{s(m; J)}{|m|^2} = \prod_P \left(1 + \frac{s(P, J)}{|P|^2}\right)$$
$$= \prod_{P^2|J} \left(1 - \frac{1}{|P|^2}\right) \prod_{P^2\nmid J} \left(1 - \frac{2}{|P|^2}\right),$$

which is exactly $\mathfrak{S}(J)$. $\qquad\square$

We now conclude the proof of Proposition A.5: By Propositions A.3, A.5 we have shown that for $z \le n/2$,
$$S(J; n) = q^n \mathfrak{S}(J) + O\left(\frac{q^n z}{Z}\right) + O(Z^2)$$

Taking $z \approx n/3$ gives that for all $J \neq 0$ with $\deg J < n$,

$$S(J; n) = q^n \mathfrak{S}(J) + O(nq^{2n/3})$$

as claimed.   □

Computing the variance. As described on page 389 of Section 5, we have a partition of the set $\mathcal{M}_n$ of monic polynomials of degree n as

$$\mathcal{M}_n = \coprod_{A \in \mathcal{A}} I(A; h)$$

where

$$\mathcal{A} = \{A = t^n + a_{n-1}t^{n_1} + \cdots + a_{h+1}t^{h+1} : a_j \in \mathbb{F}_q\}.$$

The mean value of $\mathcal{N}$ is, for $n \geq 2$,

$$\langle \mathcal{N} \rangle = \frac{1}{\#\mathcal{A}} \sum_{A \in \mathcal{A}} \mathcal{N}(A) = \frac{q^{h+1}}{\zeta(2)}, \quad n \geq 2.$$

The variance is

$$\operatorname{Var} \mathcal{N} = \langle \mathcal{N}^2 \rangle - \langle \mathcal{N} \rangle^2. \tag{A-19}$$

We have

$$\begin{aligned}
\langle \mathcal{N}^2 \rangle &= \frac{1}{\#\mathcal{A}} \sum_{A \in \mathcal{A}} \sum_{|f-A| \leq q^h} \sum_{|g-A| \leq q^h} \mu^2(f)\mu^2(g) \\
&= \frac{1}{\#\mathcal{A}} \sum_{f \in \mathcal{M}_n} \mu^2(f) + \frac{1}{\#\mathcal{A}} \sum_{\substack{f \neq g \\ |f-g| \leq q^h}} \mu^2(f)\mu^2(g) \\
&= \langle \mathcal{N} \rangle + q^{h+1} \sum_{0 \neq J \in \mathcal{P}_{\leq h}} \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \mu^2(f)\mu^2(f+J).
\end{aligned}$$

We use Theorem A.2:

$$\sum_{f \in \mathcal{M}_n} \mu^2(f)\mu^2(f+J) = q^n \mathfrak{S}(J) + O(nq^{2n/3}), \tag{A-20}$$

where

$$\mathfrak{S}(J) = \prod_P \left(1 - \frac{2}{|P|^2}\right) \prod_{P^2 | J} \frac{|P|^2 - 1}{|P|^2 - 2} = \alpha \mathfrak{s}(J) \tag{A-21}$$

with

$$\alpha = \prod_P \left(1 - \frac{2}{|P|^2}\right) \tag{A-22}$$

and

$$\mathfrak{s}(J) = \prod_{P^2 | J} \frac{|P|^2 - 1}{|P|^2 - 2}.$$

This gives that

$$\text{Var} = \langle \mathcal{N} \rangle - \langle \mathcal{N} \rangle^2 + \alpha q^{h+1} \sum_{0 \neq J \in \mathcal{P}_{\leq h}} \mathfrak{s}(J) + O(H^2 n q^{-n/3})$$

$$= \frac{q^{h+1}}{\zeta(2)} - \left(\frac{q^{h+1}}{\zeta(2)} \right)^2 + \alpha q^{h+1}(q-1) \sum_{j=0}^{h} \sum_{J \in \mathcal{M}_j} \mathfrak{s}(J) + O(H^2 n q^{-n/3}),$$

(A-23)

the last step using homogeneity: $\mathfrak{S}(cJ) = \mathfrak{S}(J)$, $c \in \mathbb{F}_q^\times$.

Computing $\sum_J \mathfrak{s}(J)$. To evaluate the sum of $\mathfrak{s}(J)$ in (A-23), we form the generating series

$$F(u) = \sum_{J \text{ monic}} \mathfrak{s}(J) u^{\deg J}.$$

Since $\mathfrak{s}(J)$ is multiplicative, and $\mathfrak{s}(P^k) = 1$ if $k = 0, 1$, and $\mathfrak{s}(P^k) = \mathfrak{s}(P^2) = \frac{|P|^2 - 1}{|P|^2 - 2}$ if $k \geq 2$, we find

$$F(u) = \prod_P \left(1 + u^{\deg P} + \mathfrak{s}(P^2) \sum_{k \geq 2} u^{k \deg P} \right)$$

$$= \prod_P \left(1 + u^{\deg P} + \frac{|P|^2 - 1}{|P|^2 - 2} \frac{u^{2 \deg P}}{1 - u^{\deg P}} \right)$$

$$= Z(u) \prod_P \left(1 + \frac{1}{|P|^2 - 2} u^{2 \deg P} \right),$$

with

$$Z(u) = \prod_P (1 - u^{\deg P})^{-1} = \frac{1}{1 - qu}.$$

We further factor

$$\prod_P \left(1 + \frac{1}{|P|^2 - 2} u^{2 \deg P} \right) = Z(u^2/q^2) \prod_P \left(1 + \frac{2u^{2 \deg P} - u^{4 \deg P}}{|P|^2 (|P|^2 - 2)} \right),$$

with the product absolutely convergent for $|u| < q^{3/4}$.

We have

$$\sum_{j=0}^{h}\sum_{J\in\mathcal{M}_j} \mathfrak{s}(J) = \frac{1}{2\pi i}\oint F(u)\frac{1-u^{-(h+1)}}{u-1}\,du$$

$$= \frac{1}{2\pi i}\oint F(u)\frac{1}{u-1}\,du + \frac{1}{2\pi i}\oint F(u)\frac{u^{-(h+1)}}{1-u}\,du, \qquad \text{(A-24)}$$

where the contour of integration is a small circle around the origin not including any pole of $F(u)$, say $|u| = 1/q^2$, traversed counterclockwise.

The first integral is zero, because the integrand is analytic near $u = 0$. As for the second integral, we shift the contour of integration to $|u| = q^{3/4-\delta}$, and obtain

$$\frac{1}{2\pi i}\oint F(u)\frac{u^{-(h+1)}}{1-u}\,du = -\operatorname*{Res}_{u=1/q} - \operatorname*{Res}_{u=1} - \operatorname*{Res}_{u=\pm\sqrt{q}} + \frac{1}{2\pi i}\oint_{|u|=q^{3/4-\delta}} F(u)\frac{u^{-(h+1)}}{1-u}\,du.$$

As $h \to \infty$, we may bound the integral around $|u| = q^{3/4-\delta}$ by

$$\frac{1}{2\pi i}\oint_{|u|=q^{3/4-\delta}} F(u)\frac{u^{-(h+1)}}{1-u}\,du \ll_q q^{-(3/4-\delta)(h+1)},$$

the implied constant depending on q.

The residue at $u = 1/q$ gives

$$-\operatorname*{Res}_{u=1/q} = \frac{1}{\alpha\zeta(2)^2}\frac{q^{h+1}}{(q-1)}$$

and hence its contribution to $\operatorname{Var}\mathcal{N}$ is

$$\left(\frac{q^{h+1}}{\zeta(2)}\right)^2, \qquad \text{(A-25)}$$

which exactly cancels out the term $-\langle\mathcal{N}\rangle^2$ in (A-23).

The residue at $u = 1$ gives

$$-\operatorname*{Res}_{u=1}\frac{F(u)u^{-(h+1)}}{1-u} = F(1) = \frac{1}{1-q}\prod_{P}\left(1 + \frac{1}{|P|^2 - 2}\right)$$

$$= -\frac{1}{(q-1)\alpha\zeta_q(2)} \qquad \text{(A-26)}$$

and its contribution to $\operatorname{Var}\mathcal{N}$ is

$$-\frac{q^{h+1}}{\zeta_q(2)}, \qquad \text{(A-27)}$$

which exactly cancels out the term $\langle\mathcal{N}\rangle$ in (A-23).

The residue at $u = +\sqrt{q}$ gives

$$- \operatorname*{Res}_{u=+\sqrt{q}} = \frac{\beta_q}{2\alpha} \frac{q^{-\frac{h}{2}-2}}{(1-q^{-3/2})(1-q^{-1/2})} , \tag{A-28}$$

and the residue at $u = -\sqrt{q}$ gives

$$- \operatorname*{Res}_{u=-\sqrt{q}} = \frac{\beta_q}{2\alpha}(-1)^h \frac{q^{-\frac{h}{2}-2}}{(1+q^{-3/2})(1+q^{-1/2})} ,$$

with $\beta_q = \prod_P \left(1 - \frac{3}{|P|^2} + \frac{2}{|P|^3}\right)$. Hence

$$- \operatorname*{Res}_{u=+\sqrt{q}} - \operatorname*{Res}_{u=-\sqrt{q}} = +\frac{\beta_q}{\alpha} q^{-\frac{h}{2}-1} \frac{(1+q^{-2})\frac{1+(-1)^h}{2} + q^{-1/2}(1+q^{-1})\frac{1-(-1)^h}{2}}{(1-q^{-3})(q-1)} .$$

Therefore we find

$$\operatorname{Var} \mathcal{N} = \frac{\beta_q}{1-q^{-3}} q^{(h+1)/2} \times \begin{cases} \dfrac{1+q^{-2}}{\sqrt{q}}, & h \text{ even} \\[2mm] \dfrac{1+q^{-1}}{q}, & h \text{ odd} \end{cases} + O\left(\frac{H^2 n}{q^{n/3}}\right) + O_q(H^{1/4+\delta}).$$

This concludes the proof of Theorem A.1.

Acknowledgements

References

[Axer 1911] A. Axer, "Über einige Grenzwertsätze", *S.-B. Math.-Natur. Kl. Akad. Wiss. Wien (2a)* **120** (1911), 1253–1298. JFM 42.0224.02

[Bae et al. 2015] S. Bae, B. Cha, and H. Jung, "Möbius function in short intervals for function fields", *Finite Fields Appl.* **34** (2015), 235–249. MR 3333147 Zbl 06444825

[Baker and Pintz 1985] R. C. Baker and J. Pintz, "The distribution of squarefree numbers", *Acta Arith.* **46**:1 (1985), 73–79. MR 87f:11064 Zbl 0535.10045

[Bank et al. 2015] E. Bank, L. Bary-Soroker, and L. Rosenzweig, "Prime polynomials in short intervals and in arithmetic progressions", *Duke Math. J.* **164**:2 (2015), 277–295. MR 3306556 Zbl 06416949

[Blomer 2008] V. Blomer, "The average value of divisor sums in arithmetic progressions", *Q. J. Math.* **59**:3 (2008), 275–286. MR 2009j:11158 Zbl 1228.11153

[Carmon and Rudnick 2014] D. Carmon and Z. Rudnick, "The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field", *Q. J. Math.* **65**:1 (2014), 53–61. MR 3179649 Zbl 1302.11073

[Cha 2011] B. Cha, "The summatory function of the Möbius function in function fields", preprint, 2011. arXiv 1008.4711

[Chatterjee and Soundararajan 2012] S. Chatterjee and K. Soundararajan, "Random multiplicative functions in short intervals", *Int. Math. Res. Not.* **2012**:3 (2012), 479–492. MR 2885978 Zbl 1248.11056

[Erdös 1951] P. Erdös, "Some problems and results in elementary number theory", *Publ. Math. Debrecen* **2** (1951), 103–109. MR 13,627a Zbl 0044.03604

[Good and Churchhouse 1968] I. J. Good and R. F. Churchhouse, "The Riemann hypothesis and pseudorandom features of the Möbius sequence", *Math. Comp.* **22** (1968), 857–861. MR 39 #1416 Zbl 0182.37503

[Hall 1982] R. R. Hall, "Squarefree numbers on short intervals", *Mathematika* **29**:1 (1982), 7–17. MR 83m:10077 Zbl 0502.10027

[Heath-Brown 1984] D. R. Heath-Brown, "The square sieve and consecutive square-free numbers", *Math. Ann.* **266**:3 (1984), 251–259. MR 85h:11050 Zbl 0514.10038

[Hooley 1975] C. Hooley, "On the Barban–Davenport–Halberstam theorem, III", *J. London Math. Soc.* (2) **10** (1975), 249–256. MR 52 #3090c Zbl 0304.10029

[Humphries 2014] P. Humphries, "On the Mertens conjecture for function fields", *Int. J. Number Theory* **10**:2 (2014), 341–361. MR 3189983 Zbl 1303.11109

[Jia 1993] C. H. Jia, "The distribution of square-free numbers", *Sci. China Ser. A* **36**:2 (1993), 154–169. MR 94f:11095 Zbl 0772.11033

[Katz 2013a] N. M. Katz, "On a question of Keating and Rudnick about primitive Dirichlet characters with squarefree conductor", *Int. Math. Res. Not.* **2013**:14 (2013), 3221–3249. MR 3085758 Zbl 06437663

[Katz 2013b] N. M. Katz, "Witt vectors and a question of Keating and Rudnick", *Int. Math. Res. Not.* **2013**:16 (2013), 3613–3638. MR 3090703 Zbl 06437675

[Katz 2015a] N. M. Katz, "On two questions of Entin, Keating, and Rudnick on primitive Dirichlet characters", *Int. Math. Res. Not.* **2015**:15 (2015), 6044–6069. MR 3384472 Zbl 06505082

[Katz 2015b] N. M. Katz, "Witt vectors and a question of Entin, Keating, and Rudnick", *Int. Math. Res. Not.* **2015**:14 (2015), 5959–5975. MR 3384464 Zbl 06513161

[Keating and Rudnick 2014] J. P. Keating and Z. Rudnick, "The variance of the number of prime polynomials in short intervals and in residue classes", *Int. Math. Res. Not.* **2014**:1 (2014), 259–288. MR 3158533 Zbl 1319.11084

[Keating et al. 2015] J. P. Keating, E. Roditty-Gershon, and Z. Rudnick, "Sums of divisor functions in $\mathbb{F}_q[t]$ and matrix integrals", preprint, 2015. arXiv 1504.07804

[Matomäki and Radziwiłł 2015] K. Matomäki and M. Radziwiłł, "Multiplicative functions in short intervals", *Ann. of Math.* (online publication October 2015).

[Montgomery and Vaughan 1981] H. L. Montgomery and R. C. Vaughan, "The distribution of squarefree numbers", pp. 247–256 in *Recent progress in analytic number theory* (Durham, 1979), vol. 1, edited by H. Halberstam and C. Hooley, Academic Press, London, 1981. MR 83d:10010 Zbl 0462.10029

[Motohashi 1976] Y. Motohashi, "On the sum of the Möbius function in a short segment", *Proc. Japan Acad.* **52**:9 (1976), 477–479. MR 54 #12685 Zbl 0372.10033

[Ng 2004] N. Ng, "The distribution of the summatory function of the Möbius function", *Proc. London Math. Soc.* (3) **89**:2 (2004), 361–389. MR 2005f:11215 Zbl 1138.11341

[Ng 2008] N. Ng, "The Möbius function in short intervals", pp. 247–257 in *Anatomy of integers* (Montréal, 2006), edited by J.-M. De Koninck et al., CRM Proceedings and Lecture Notes **46**, American Mathematical Society, Providence, RI, 2008. MR 2009i:11118 Zbl 1187.11025

[Nunes 2015] R. M. Nunes, "Squarefree numbers in arithmetic progressions", *J. Number Theory* **153** (2015), 1–36. MR 3327562 Zbl 06435729

[Prachar 1958] K. Prachar, "Über die kleinste quadratfreie Zahl einer arithmetischen Reihe", *Monatsh. Math.* **62** (1958), 173–176. MR 19,1160g Zbl 0083.03704

[Ramachandra 1976] K. Ramachandra, "Some problems of analytic number theory", *Acta Arith.* **31**:4 (1976), 313–324. MR 54 #12682 Zbl 0291.10034

[Reuss 2014] T. Reuss, "Pairs of k-free numbers, consecutive square-full numbers", preprint, 2014. arXiv 1212.3150

[Richert 1954] H.-E. Richert, "On the difference between consecutive squarefree numbers", *J. London Math. Soc.* **29** (1954), 16–20. MR 15,289c Zbl 0055.04001

[Rodgers 2015] B. Rodgers, "The covariance of almost-primes in $\mathbb{F}_q[T]$", *Int. Math. Res. Not.* **2015**:14 (2015), 5976–6004. MR 3384465 Zbl 06513162

[Roth 1951] K. F. Roth, "On the gaps between squarefree numbers", *J. London Math. Soc.* **26** (1951), 263–268. MR 13,208d Zbl 0043.04802

[Rudnick 2014] Z. Rudnick, "Square-free values of polynomials over the rational function field", *J. Number Theory* **135** (2014), 60–66. MR 3128452

[Swan 1962] R. G. Swan, "Factorization of polynomials over finite fields", *Pacific J. Math.* **12** (1962), 1099–1106. MR 26 #2432 Zbl 0113.01701

[Tolev 2006] D. I. Tolev, "On the distribution of r-tuples of squarefree numbers in short intervals", *Int. J. Number Theory* **2**:2 (2006), 225–234. MR 2008a:11111 Zbl 1196.11130

[Warlimont 1980] R. Warlimont, "Squarefree numbers in arithmetic progressions", *J. London Math. Soc.* (2) **22**:1 (1980), 21–24. MR 82b:10055 Zbl 0444.10036

j.p.keating@bristol.ac.uk   *School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*

rudnick@post.tau.ac.il   *Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel*

Equidistribution of values of linear forms on a cubic hypersurface

Sam Chow

Let C be a cubic form with integer coefficients in n variables, and let h be the h-invariant of C. Let $L_1, \ldots, L_r$ be linear forms with real coefficients such that, if $\boldsymbol{\alpha} \in \mathbb{R}^r \setminus \{\boldsymbol{0}\}$, then $\boldsymbol{\alpha} \cdot \boldsymbol{L}$ is not a rational form. Assume that $h > 16 + 8r$. Let $\boldsymbol{\tau} \in \mathbb{R}^r$, and let η be a positive real number. We prove an asymptotic formula for the weighted number of integer solutions $\boldsymbol{x} \in [-P, P]^n$ to the system $C(\boldsymbol{x}) = 0$, $|\boldsymbol{L}(\boldsymbol{x}) - \boldsymbol{\tau}| < \eta$. If the coefficients of the linear forms are algebraically independent over the rationals, then we may replace the h-invariant condition with the hypothesis $n > 16 + 9r$ and show that the system has an integer solution. Finally, we show that the values of $\boldsymbol{L}$ at integer zeros of C are equidistributed modulo 1 in $\mathbb{R}^r$, requiring only that $h > 16$.

1. Introduction

Recently Sargent [2014] used ergodic methods to establish the equidistribution of values of real linear forms on a rational quadric, subject to modest conditions. His ideas stemmed from quantitative refinements [Dani and Margulis 1993; Eskin et al. 1998] of Margulis' proof [1989] of the Oppenheim conjecture. Such techniques do not readily apply to higher-degree hypersurfaces. Our purpose here is to use analytic methods to obtain similar results on a cubic hypersurface.

Our first theorem is stated in terms of the *h-invariant* of a nontrivial rational cubic form C in n variables, which is defined to be the least positive integer h such that

$$C(\boldsymbol{x}) = A_1(\boldsymbol{x})B_1(\boldsymbol{x}) + \cdots + A_h(\boldsymbol{x})B_h(\boldsymbol{x}) \tag{1-1}$$

identically, for some rational linear forms $A_1, \ldots, A_h$ and some rational quadratic forms $B_1, \ldots, B_h$. The h-invariant describes the geometry of the hypersurface $\{C = 0\}$, and in fact $n - h$ is the greatest affine dimension of any rational linear space contained in this hypersurface (therefore $1 \leqslant h \leqslant n$).

Theorem 1.1. *Let C be a cubic form with integer coefficients in n variables, and let $h = h(C)$ be the h-invariant of C. Let $L_1, \ldots, L_r$ be linear forms with real coefficients in n variables such that, if $\boldsymbol{\alpha} \in \mathbb{R}^r \setminus \{\mathbf{0}\}$, then $\boldsymbol{\alpha} \cdot \boldsymbol{L}$ is not a rational form. Assume that*

$$h > 16 + 8r. \tag{1-2}$$

Let $\boldsymbol{\tau} \in \mathbb{R}^r$ and $\eta > 0$. Let

$$w(\boldsymbol{x}) = \begin{cases} \exp\left(-\sum_{j \leqslant n} 1/(1 - x_j^2)\right) & \text{if } |\boldsymbol{x}| < 1, \\ 0 & \text{if } |\boldsymbol{x}| \geqslant 1, \end{cases} \tag{1-3}$$

and define the weighted counting function

$$N_w(P) = \sum_{\substack{\boldsymbol{x} \in \mathbb{Z}^n : C(\boldsymbol{x})=0 \\ \text{and } |\boldsymbol{L}(\boldsymbol{x})-\boldsymbol{\tau}|<\eta}} w(\boldsymbol{x}/P).$$

Then

$$N_w(P) = (2\eta)^r \mathfrak{S} \chi_w P^{n-r-3} + o(P^{n-r-3}) \tag{1-4}$$

as $P \to \infty$, where

$$\mathfrak{S} = \sum_{q \in \mathbb{N}} q^{-n} \sum_{\substack{a \bmod q \\ (a,q)=1}} \sum_{\boldsymbol{x} \bmod q} e_q(aC(\boldsymbol{x})) \tag{1-5}$$

and

$$\chi_w = \int_{\mathbb{R}^{r+1}} \int_{\mathbb{R}^n} w(\boldsymbol{x}) e(\beta_0 C(\boldsymbol{x}) + \boldsymbol{\alpha} \cdot \boldsymbol{L}(\boldsymbol{x})) \, d\boldsymbol{x} \, d\beta_0 \, d\boldsymbol{\alpha}. \tag{1-6}$$

Further, we have $\mathfrak{S} \chi_w > 0$.

The condition that no form in the real pencil of the linear forms is rational cannot be avoided, for if $|\boldsymbol{L}(\boldsymbol{x}) - \boldsymbol{\tau}| < \eta$, then $|\boldsymbol{\alpha} \cdot \boldsymbol{L}(\boldsymbol{x}) - \boldsymbol{\alpha} \cdot \boldsymbol{\tau}| < \eta|\boldsymbol{\alpha}|$, and the values taken by a rational form at integer points are discrete. As a simple example, the inequality

$$\left| x_1 + \cdots + x_n - \tfrac{1}{2} \right| < \tfrac{1}{4}$$

admits no integer solutions $\boldsymbol{x}$.

We interpret $N_w(P)$ as a weighted count for the number of integer solutions $\boldsymbol{x} \in (-P, P)^n$ to the system

$$C(\boldsymbol{x}) = 0, \quad |\boldsymbol{L}(\boldsymbol{x}) - \boldsymbol{\tau}| < \eta. \tag{1-7}$$

The smooth weight function $w(\boldsymbol{x})$ defined in (1-3) is taken from [Heath-Brown 1996]. Importantly, it has bounded support and bounded partial derivatives of all orders. One advantage of the weighted approach is that it enables the use of Poisson summation.

The *singular series* $\mathfrak{S}$ may be interpreted as a product of p-adic densities of points on the hypersurface $\{C = 0\}$ [Birch 1962, §7]. Note that this captures the

arithmetic of C but that no such arithmetic is present for the linear forms $L_1, \ldots, L_r$ since they are "irrational" in a precise sense.

The weighted *singular integral* χ_w arises naturally in our proof as the right-hand side of (1-6). Using [Schmidt 1982b; 1985], we can interpret χ_w as the weighted real density of points on the variety $\{C = L_1 = \cdots = L_r = 0\}$. For $L > 0$ and $\xi \in \mathbb{R}$, let

$$\psi_L(\xi) = L \cdot \max(0, 1 - L|\xi|).$$

For $\boldsymbol{\xi} \in \mathbb{R}^{r+1}$, put

$$\Psi_L(\boldsymbol{\xi}) = \prod_{v \leqslant r+1} \psi_L(\xi_v).$$

With $\boldsymbol{f} = (C, \boldsymbol{L})$, set

$$I_L(\boldsymbol{f}) = \int_{\mathbb{R}^n} w(\boldsymbol{x}) \Psi_L(\boldsymbol{f}(\boldsymbol{x})) \, \mathrm{d}\boldsymbol{x},$$

and define

$$\chi_w = \lim_{L \to \infty} I_L(\boldsymbol{f}). \tag{1-8}$$

We shall see that the limit (1-8) exists and that this definition is equivalent to the analytic definition (1-6).

We may replace the condition on the h-invariant by a condition on the number of variables, at the expense of assuming that the coefficients of the linear forms are in "general position".

Theorem 1.2. *Let C be a cubic form with rational coefficients in n variables. Let $L_1, \ldots, L_r$ be linear forms in n variables with real coefficients that are algebraically independent over $\mathbb{Q}$. Assume that*

$$n > 16 + 9r.$$

Let $\boldsymbol{\tau} \in \mathbb{R}^r$ and $\eta > 0$. Then there exists $\boldsymbol{x} \in \mathbb{Z}^n$ satisfying (1-7).

This algebraic independence condition is stronger than the real pencil condition imposed on the linear forms in Theorem 1.1 — we show in Section 8 that the algebraic independence condition in fact implies the real pencil condition. The real pencil condition is probably sufficient, in truth; however, our proof relies on algebraic independence.

The point of this work is to show that the zeros of a rational cubic form are, in a strong sense, well distributed. Similar methods may be applied if C is replaced by a higher-degree form; the simplest results would concern nonsingular forms of odd degree. The unweighted analogue of the case $r = 0$ of Theorem 1.1 has been solved, assuming only that $h \geqslant 16$; see remark (B) in the introduction of [Schmidt 1985]. For the case $r = 0$ of Theorem 1.2, we can choose $\boldsymbol{x} = \boldsymbol{0}$ or note from [Heath-Brown 2007] that fourteen variables suffice to ensure a nontrivial solution. We shall assume throughout that $r \geqslant 1$.

The fact that we have linear inequalities rather than equations does genuinely increase the difficulty of the problem. For example, suppose we wished to nontrivially solve the system of equations $C = L_1 = \cdots = L_r = 0$, where here the L_i are linear forms with rational coefficients; assume for simplicity that the L_i are linearly independent. Using the linear equations, we could determine r of the variables in terms of the remaining $n - r$ variables, and substituting into $C(\boldsymbol{x}) = 0$ would yield a homogeneous cubic equation in $n - r$ variables. Thus, by [Heath-Brown 2007], we could solve the system given $n \geqslant 14 + r$ variables.

We use the work of Browning, Dietmann, and Heath-Brown [Browning et al. 2015] as a benchmark for comparison. Those authors investigate simultaneous rational solutions to one cubic equation $C = 0$ and one quadratic equation $Q = 0$. They establish the smooth Hasse principle under the assumption that

$$\min(h(C), \operatorname{rank}(Q)) \geqslant 37.$$

We expect to do somewhat better when considering one cubic equation and one linear inequality simultaneously, and we do. Substituting $r = 1$ into (1-2), we see that we only require $h(C) > 24$.

To prove Theorem 1.1, we use the Hardy–Littlewood method [Vaughan 1997] in unison with Freeman's variant [2002] of the Davenport–Heilbronn method [1946]. The central objects to study are the weighted exponential sums

$$S(\alpha_0, \boldsymbol{\alpha}) = \sum_{\boldsymbol{x} \in \mathbb{Z}^n} w(\boldsymbol{x}/P) e(\alpha_0 C(\boldsymbol{x}) + \boldsymbol{\alpha} \cdot \boldsymbol{L}(\boldsymbol{x})).$$

If $|S(\alpha_0, \boldsymbol{\alpha})|$ is substantially smaller than the trivial estimate $O(P^n)$, then we may adapt [Davenport and Lewis 1964, Lemma 4] to rationally approximate α_0 (see Section 2).

In Section 3, we use Poisson summation to approximately decompose our exponential sum into archimedean and nonarchimedean components. In Section 4, we use Heath-Brown's first-derivative bound [1996, Lemma 10] and a classical pruning argument [Davenport 2005, Lemma 15.1] to essentially obtain good simultaneous rational approximations to α_0 and $\boldsymbol{\alpha}$. In Section 5, we combine classical ideas with Heath-Brown's first-derivative bound to obtain a mean-value estimate of the correct order of magnitude. In Section 6, we define our Davenport–Heilbronn arcs and in particular use the methods of Bentkus, Götze, and Freeman [Bentkus and Götze 1999; Freeman 2002; Wooley 2003] to obtain nontrivial cancellation on the minor arcs, thereby establishing the asymptotic formula (1-4). We complete the proof of Theorem 1.1 in Section 7 by explaining why $\mathfrak{S}$ and χ_w are positive. It is then that we justify the interpretation of χ_w as a weighted real density.

We prove Theorem 1.2 in Section 8. By Theorem 1.1, it suffices to consider the case where the h-invariant is not too large. With $A_1, \ldots, A_h$ as in (1-1), we solve

the system (1-7) by solving the linear system

$$A(x) = 0, \quad |L(x) - \tau| < \eta.$$

Since the h-invariant is not too large, this system has more variables than constraints and can be solved using methods from linear algebra and diophantine approximation, provided that the coefficients of $L_1, \ldots, L_r$ are algebraically independent over $\mathbb{Q}$.

In Section 9, we shall prove the following equidistribution result.

Theorem 1.3. *Let C be a cubic form with rational coefficients in n variables, let $h = h(C)$ be the h-invariant of C, and assume that $h > 16$. Let $r \in \mathbb{N}$, and let $L_1, \ldots, L_r$ be linear forms with real coefficients in n variables such that, if $\boldsymbol{\alpha} \in \mathbb{R}^r \setminus \{\mathbf{0}\}$, then $\boldsymbol{\alpha} \cdot \boldsymbol{L}$ is not a rational form. Let*

$$Z = \{x \in \mathbb{Z}^n : C(x) = 0\},$$

and order this set by height $|x|$. Then the values of $\boldsymbol{L}(Z)$ are equidistributed modulo 1 in $\mathbb{R}^r$.

A little surprisingly, perhaps, we do not require h to grow with r. By a multi-dimensional Weyl criterion [Cassels 1957, p. 66], it will suffice to investigate $S_u(\alpha_0, \boldsymbol{k})$ for a fixed nonzero integer vector $\boldsymbol{k}$, where

$$S_u(\alpha_0, \boldsymbol{\alpha}) = \sum_{|x| < P} e(\alpha_0 C(x) + \boldsymbol{\alpha} \cdot \boldsymbol{L}(x))$$

is the unweighted analogue of $S(\alpha_0, \boldsymbol{\alpha})$. A simplification of the method employed to prove Theorem 1.1 will complete the argument.

Rather than using the h-invariant, one could instead consider the dimension of the *singular locus* of the affine variety $\{C = 0\}$, as in [Birch 1962]. Such an analysis would imply results for arbitrary nonsingular cubic forms in sufficiently many variables. These types of theorems are discussed in Section 10.

We adopt the convention that ε denotes an arbitrarily small positive number, so its value may differ between instances. For $x \in \mathbb{R}$ and $q \in \mathbb{N}$, we put $e(x) = e^{2\pi i x}$ and $e_q(x) = e^{2\pi i x/q}$. Boldface will be used for vectors; for instance we shall abbreviate $(x_1, \ldots, x_n)$ to $\boldsymbol{x}$ and define $|\boldsymbol{x}| = \max(|x_1|, \ldots, |x_n|)$. We will use the unnormalized sinc function, given by $\operatorname{sinc}(x) = \sin(x)/x$ for $x \in \mathbb{R} \setminus \{0\}$ and $\operatorname{sinc}(0) = 1$. For $x \in \mathbb{R}$, we write $\|x\|$ for the distance from x to the nearest integer.

We regard τ and η as constants. The word *large* shall mean in terms of C, $\boldsymbol{L}$, ε, and constants, together with any explicitly stated dependence. Similarly, the implicit constants in Vinogradov's and Landau's notation may depend on C, $\boldsymbol{L}$, ε, and constants, and any other dependence will be made explicit. The pronumeral P denotes a large positive real number. The word *small* will mean in terms of C, $\boldsymbol{L}$, and constants. We sometimes use such language informally, for the sake of motivation; we make this distinction using quotation marks.

2. One rational approximation

First we use Freeman's kernel functions [2002, §2.1] to relate $N_w(P)$ to our exponential sums $S(\alpha_0, \boldsymbol{\alpha})$. We shall define

$$T : [1, \infty) \to [1, \infty)$$

in due course. For now, it suffices to note that

$$T(P) \leqslant P \tag{2-1}$$

and that $T(P) \to \infty$ as $P \to \infty$. Put

$$L(P) = \max(1, \log T(P)), \qquad \rho = \eta L(P)^{-1}, \tag{2-2}$$

and

$$K_\pm(\alpha) = \frac{\sin(\pi\alpha\rho)\sin(\pi\alpha(2\eta \pm \rho))}{\pi^2\alpha^2\rho}. \tag{2-3}$$

From [Freeman 2002, Lemma 1] and its proof, we have

$$K_\pm(\alpha) \ll \min(1, L(P)|\alpha|^{-2}) \tag{2-4}$$

and

$$0 \leqslant \int_{\mathbb{R}} e(\alpha t) K_-(\alpha)\, d\alpha \leqslant U_\eta(t) \leqslant \int_{\mathbb{R}} e(\alpha t) K_+(\alpha)\, d\alpha \leqslant 1, \tag{2-5}$$

where

$$U_\eta(t) = \begin{cases} 1 & \text{if } |t| < \eta, \\ 0 & \text{if } |t| \geqslant \eta. \end{cases}$$

For $\boldsymbol{\alpha} \in \mathbb{R}^r$, write

$$\mathbb{K}_\pm(\boldsymbol{\alpha}) = \prod_{k \leqslant r} K_\pm(\alpha_k). \tag{2-6}$$

Let U be a unit interval, to be specified later. The inequalities (2-5) and the identity

$$\int_U e(\alpha m)\, d\alpha = \begin{cases} 1 & \text{if } m = 0, \\ 0 & \text{if } m \in \mathbb{Z} \setminus \{0\} \end{cases} \tag{2-7}$$

now give

$$R_-(P) \leqslant N_w(P) \leqslant R_+(P),$$

where

$$R_\pm(P) = \int_{\mathbb{R}^r} \int_U S(\alpha_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \mathbb{K}_\pm(\boldsymbol{\alpha})\, d\alpha_0\, d\boldsymbol{\alpha}.$$

In order to prove (1-4), it therefore remains to show that

$$R_\pm(P) = (2\eta)^r \mathfrak{S} \chi_w P^{n-r-3} + o(P^{n-r-3}). \tag{2-8}$$

We shall in fact need to investigate the more general exponential sum

$$g(\alpha_0, \boldsymbol{\lambda}) = \sum_{\boldsymbol{x} \in \mathbb{Z}^n} w(\boldsymbol{x}/P) e(\alpha_0 C(\boldsymbol{x}) + \boldsymbol{\lambda} \cdot \boldsymbol{x}).$$

We note at once that

$$S(\alpha_0, \boldsymbol{\alpha}) = g(\alpha_0, \Lambda \boldsymbol{\alpha}),$$

where

$$L_i(\boldsymbol{x}) = \lambda_{i,1} x_1 + \cdots + \lambda_{i,n} x_n \quad (1 \leqslant i \leqslant r) \tag{2-9}$$

and

$$\Lambda = \begin{pmatrix} \lambda_{1,1} & \cdots & \lambda_{r,1} \\ \vdots & & \vdots \\ \lambda_{1,n} & \cdots & \lambda_{r,n} \end{pmatrix}. \tag{2-10}$$

Fix a large positive constant C_1.

Lemma 2.1. *If $0 < \theta < 1$ and*

$$|g(\alpha_0, \boldsymbol{\lambda})| \geqslant P^{n-(h/4)\theta+\varepsilon},$$

then there exist relatively prime integers q and a satisfying

$$1 \leqslant q \leqslant C_1 P^{2\theta}, \qquad |q\alpha_0 - a| < P^{2\theta-3}. \tag{2-11}$$

The same is true if we replace $g(\alpha_0, \boldsymbol{\lambda})$ by

$$g_u(\alpha_0, \boldsymbol{\lambda}) := \sum_{|\boldsymbol{x}| < P} e(\alpha_0 C(\boldsymbol{x}) + \boldsymbol{\lambda} \cdot \boldsymbol{x}) \tag{2-12}$$

or by

$$\sum_{1 \leqslant x_1, \ldots, x_n \leqslant P} e(\alpha_0 C(\boldsymbol{x}) + \boldsymbol{\lambda} \cdot \boldsymbol{x}).$$

Proof. Our existence statement is a weighted analogue of [Davenport and Lewis 1964, Lemma 4]. One can follow [loc. cit., §3], mutatis mutandis. The only change required is in proving the analogue of [loc. cit., Lemma 1]. Weights are introduced into the linear exponential sums that arise from Weyl differencing, but these weights are easily handled using partial summation. Our final statement holds with the same proof: one imitates [loc. cit., §3]. □

For $\theta \in (0, 1)$, $q \in \mathbb{N}$, and $a \in \mathbb{Z}$, let $\mathfrak{N}_{q,a}(\theta)$ be the set of $(\alpha_0, \boldsymbol{\alpha}) \in U \times \mathbb{R}^r$ satisfying (2-11), and let $\mathfrak{N}(\theta)$ be the union of the sets $\mathfrak{N}_{q,a}(\theta)$ over relatively prime q and a. This union is disjoint if $\theta < \frac{3}{4}$. Indeed, suppose we have (2-11) for some relatively prime integers q and a and that we also have relatively prime integers q' and a' satisfying

$$1 \leqslant q' \ll P^{2\theta}, \qquad |q'\alpha_0 - a'| < P^{2\theta-3}.$$

The triangle inequality then yields

$$|a/q - a'/q'| < P^{2\theta-3}(1/q + 1/q') < 1/(qq')$$

as P is large. Hence, $a/q = a'/q'$, so $a' = a$ and $q' = q$.

We prune our arcs using the well known procedure in [Davenport 2005, Lemma 15.1]. Fix a small positive real number δ. The following corollary shows that we may restrict attention to $\mathfrak{N}(\frac{1}{2} - \delta)$.

Corollary 2.2. *We have*

$$\int_{U \times \mathbb{R}^r \setminus \mathfrak{N}(1/2-\delta)} |S(\alpha_0, \boldsymbol{\alpha})\mathbb{K}_{\pm}(\boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} = o(P^{n-r-3}).$$

Proof. Choose real numbers $\psi_1, \ldots, \psi_{t-1}$ such that

$$\tfrac{1}{2} - \delta = \psi_0 < \psi_1 < \cdots < \psi_{t-1} < \psi_t = 0.8.$$

Dirichlet's approximation theorem [Vaughan 1997, Lemma 2.1] implies $\mathfrak{N}(\psi_t) = U \times \mathbb{R}^r$. Let $\mathfrak{U}$ be an arbitrary unit hypercube in r dimensions, and put $\mathcal{U} = U \times \mathfrak{U}$. Since

$$\text{meas}(\mathfrak{N}(\theta) \cap \mathcal{U}) \ll P^{4\theta-3},$$

[Lemma 2.1] gives

$$\int_{(\mathfrak{N}(\psi_g) \setminus \mathfrak{N}(\psi_{g-1})) \cap \mathcal{U}} |S(\alpha_0, \boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} \ll P^{4\psi_g - 3 + n - h\psi_{g-1}/4 + \varepsilon} \quad (1 \leqslant g \leqslant t).$$

This is $O(P^{n-r-3-\varepsilon})$ if $\psi_{g-1}/\psi_g \simeq 1$ since $\psi_{g-1} \geqslant \frac{1}{2} - \delta$ and $h \geqslant 17 + 8r$. Thus, we can choose $\psi_1, \ldots, \psi_{t-1}$ with $t \ll 1$ satisfactorily to ensure that

$$\int_{\mathcal{U} \setminus \mathfrak{N}(1/2-\delta)} |S(\alpha_0, \boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} \ll P^{n-r-3-\varepsilon}.$$

The desired inequality now follows from (2-1), (2-2), (2-4), and (2-6). $\qquad \square$

Thus, to prove (2-8) and hence (1-4), it remains to show that

$$\int_{\mathfrak{N}(\frac{1}{2}-\delta)} S(\alpha_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \mathbb{K}_{\pm}(\boldsymbol{\alpha}) \, d\alpha_0 \, d\boldsymbol{\alpha} = (2\eta)^r \mathfrak{S} \chi_w P^{n-r-3} + o(P^{n-r-3}). \quad (2\text{-}13)$$

3. Poisson summation

Put

$$\alpha_0 = \frac{a}{q} + \beta_0, \qquad \boldsymbol{\lambda} = q^{-1}\boldsymbol{a} + \boldsymbol{\beta}, \qquad (3\text{-}1)$$

where $q \geqslant 1$ and a are relatively prime integers and where $\boldsymbol{a} \in \mathbb{Z}^n$. By periodicity,

$$g(\alpha_0, \boldsymbol{\lambda}) = \sum_{\boldsymbol{y} \bmod q} e_q(aC(\boldsymbol{y}) + \boldsymbol{a} \cdot \boldsymbol{y}) I_{\boldsymbol{y}}(q, \beta_0, \boldsymbol{\beta}),$$

where

$$I_y(q, \beta_0, \boldsymbol{\beta}) = \sum_{\boldsymbol{x} \equiv \boldsymbol{y} \bmod q} w(\boldsymbol{x}/P) e(\beta_0 C(\boldsymbol{x}) + \boldsymbol{\beta} \cdot \boldsymbol{x}).$$

Since

$$I_y(q, \beta_0, \boldsymbol{\beta}) = \sum_{\boldsymbol{z} \in \mathbb{Z}^n} w\left(\frac{\boldsymbol{y} + q\boldsymbol{z}}{P}\right) e(\beta_0 C(\boldsymbol{y} + q\boldsymbol{z}) + \boldsymbol{\beta} \cdot (\boldsymbol{y} + q\boldsymbol{z})),$$

Poisson summation yields

$$I_y(q, \beta_0, \boldsymbol{\beta}) = \sum_{\boldsymbol{c} \in \mathbb{Z}^n} \int_{\mathbb{R}^n} w\left(\frac{\boldsymbol{y} + q\boldsymbol{z}}{P}\right) e(\beta_0 C(\boldsymbol{y} + q\boldsymbol{z}) + \boldsymbol{\beta} \cdot (\boldsymbol{y} + q\boldsymbol{z}) - \boldsymbol{c} \cdot \boldsymbol{z}) \, d\boldsymbol{z}.$$

Changing variables now gives

$$I_y(q, \beta_0, \boldsymbol{\beta}) = (P/q)^n \sum_{\boldsymbol{c} \in \mathbb{Z}^n} e_q(\boldsymbol{c} \cdot \boldsymbol{y}) I(P^3 \beta_0, P(\boldsymbol{\beta} - \boldsymbol{c}/q)),$$

where

$$I(\gamma_0, \boldsymbol{\gamma}) = \int_{\mathbb{R}^n} w(\boldsymbol{x}) e(\gamma_0 C(\boldsymbol{x}) + \boldsymbol{\gamma} \cdot \boldsymbol{x}) \, d\boldsymbol{x}. \tag{3-2}$$

Write

$$S_{q,a,\boldsymbol{a}} = \sum_{\boldsymbol{y} \bmod q} e_q(aC(\boldsymbol{y}) + \boldsymbol{a} \cdot \boldsymbol{y}), \tag{3-3}$$

and let

$$g_0(\alpha_0, \boldsymbol{\lambda}) = (P/q)^n S_{q,a,\boldsymbol{a}} I(P^3 \beta_0, P\boldsymbol{\beta})$$

be the $\boldsymbol{c} = \boldsymbol{0}$ contribution to $g(\alpha_0, \boldsymbol{\lambda})$. Then

$$g(\alpha_0, \boldsymbol{\lambda}) - g_0(\alpha_0, \boldsymbol{\lambda}) = (P/q)^n \sum_{\boldsymbol{c} \neq \boldsymbol{0}} S_{q,a,\boldsymbol{a}+\boldsymbol{c}} I(P^3 \beta_0, P(\boldsymbol{\beta} - \boldsymbol{c}/q)). \tag{3-4}$$

We shall bound the right-hand side from above, in the case where we have (2-11) and $|\boldsymbol{\beta}| \leqslant 1/(2q)$. For future reference, we note that specializing $(q, a, \boldsymbol{a}) = (1, 0, \boldsymbol{0})$ in (3-4) gives

$$g(\alpha_0, \boldsymbol{\lambda}) - P^n I(P^3 \alpha_0, P\boldsymbol{\lambda}) = P^n \sum_{\boldsymbol{c} \neq \boldsymbol{0}} I(P^3 \alpha_0, P\boldsymbol{\lambda} - P\boldsymbol{c}). \tag{3-5}$$

We bound $S_{q,a,\boldsymbol{a}}$ by imitating [Davenport 2005, Lemma 15.3].

Lemma 3.1. *Let $q \geqslant 1$ and a be relatively prime integers, and let $\psi > 0$. Then*

$$S_{q,a,\boldsymbol{a}} \ll_\psi q^{n-h/8+\psi}. \tag{3-6}$$

Proof. Suppose for a contradiction that q is large in terms of ψ and

$$|S_{q,a,\boldsymbol{a}}| > q^{n-h/8+\psi}.$$

Recall that

$$S_{q,a,\boldsymbol{a}} = \sum_{1 \leqslant y_1, \ldots, y_n \leqslant q} e_q(aC(\boldsymbol{y}) + \boldsymbol{a} \cdot \boldsymbol{y}).$$

We may assume without loss that $\psi < 1$. By Lemma 2.1, with $P = q$ and $\theta = \frac{1}{2} - \psi/n$, there exist $s, b \in \mathbb{Z}$ such that

$$1 \leqslant s < q, \qquad |sa/q - b| < q^{-1}.$$

Now $b/s = a/q$, which is impossible because $(a, q) = 1$ and $1 \leqslant s < q$. □

Let $\boldsymbol{c} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$, and suppose we have (2-11) for some $\theta \in (0, \frac{1}{2} - \delta]$ and some relatively prime $q, a \in \mathbb{Z}$. Define a_j by rounding $q\lambda_j$ to the nearest integer, rounding down if $q\lambda_j$ is half of an odd integer ($1 \leqslant j \leqslant n$). Since $|\boldsymbol{c}|/q \geqslant 1/q \geqslant 2|\boldsymbol{\beta}|$,

$$|P(\boldsymbol{\beta} - \boldsymbol{c}/q)| \gg P|\boldsymbol{c}|/q \gg P/q \gg P^{3+2\delta}|\beta_0|.$$

Now [Heath-Brown 1996, Lemma 10] gives

$$I(P^3\beta_0, P(\boldsymbol{\beta} - \boldsymbol{c}/q)) \ll (P|\boldsymbol{c}|/q)^{-n-\varepsilon}. \tag{3-7}$$

By (3-4), (3-6), and (3-7),

$$g(\alpha_0, \boldsymbol{\lambda}) - g_0(\alpha_0, \boldsymbol{\lambda}) \ll P^{-\varepsilon} q^{n+2\varepsilon-h/8} \ll q^{n-h/8+\varepsilon}. \tag{3-8}$$

Let $\mathfrak{U}$ be an arbitrary unit hypercube in r dimensions, and put $\mathcal{U} = U \times \mathfrak{U}$. With $\theta = \frac{1}{2} - \delta$, we now have

$$\int_{\mathfrak{N}(\theta) \cap \mathcal{U}} |S(\alpha_0, \boldsymbol{\alpha}) - S_0(\alpha_0, \boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} \ll \sum_{q \leqslant C_1 P^{2\theta}} q^{n-h/8+\varepsilon} P^{2\theta-3},$$

where for $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{N}_{q,a}(\theta)$ with $(a, q) = 1$ we have written

$$S_0(\alpha_0, \boldsymbol{\alpha}) = g_0(\alpha_0, \Lambda\boldsymbol{\alpha}).$$

Hence,

$$\int_{\mathfrak{N}(\theta) \cap \mathcal{U}} |S(\alpha_0, \boldsymbol{\alpha}) - S_0(\alpha_0, \boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} \ll P^{4\theta-3}(P^{2\theta})^{n-h/8+\varepsilon} \ll P^{n-r-3-\varepsilon}$$

since $h \geqslant 17 + 8r$. The bounds (2-1), (2-2), (2-4), and (2-6) now yield

$$\int_{\mathfrak{N}(\theta)} |S(\alpha_0, \boldsymbol{\alpha}) - S_0(\alpha_0, \boldsymbol{\alpha})| \cdot |\mathbb{K}_{\pm}(\boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} = o(P^{n-r-3}).$$

Thus, to prove (2-13) and hence (1-4), it suffices to show that

$$\int_{\mathfrak{N}(\frac{1}{2}-\delta)} S_0(\alpha_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \mathbb{K}_{\pm}(\boldsymbol{\alpha}) \, d\alpha_0 \, d\boldsymbol{\alpha} = (2\eta)^r \mathfrak{S} \chi_w P^{n-r-3} + o(P^{n-r-3}). \tag{3-9}$$

4. More rational approximations

For $\theta \in (0, \frac{1}{2}]$ and integers $q, a, a_1, \ldots, a_n$, let $\mathfrak{R}_{q,a,\boldsymbol{a}}(\theta)$ denote the set of $(\alpha_0, \boldsymbol{\alpha}) \in U \times \mathbb{R}^r$ satisfying

$$|q\alpha_0 - a| < P^{2\theta - 3}, \qquad |q\Lambda\boldsymbol{\alpha} - \boldsymbol{a}| < P^{(2+\delta)\theta - 1}, \qquad (4\text{-}1)$$

and let $\mathfrak{R}(\theta)$ be the union of the sets $\mathfrak{R}_{q,a,\boldsymbol{a}}(\theta)$ over integers $q, a, a_1, \ldots, a_n$ satisfying

$$1 \leqslant q \leqslant C_1 P^{2\theta}, \qquad (a, q) = 1. \qquad (4\text{-}2)$$

Note that this union is disjoint if $\theta < (2+\delta)^{-1}$. Let $\mathfrak{U}$ be an arbitrary unit hypercube in r dimensions, and put $\mathcal{U} = U \times \mathfrak{U}$. Then

$$\text{meas}(\mathfrak{R}(\theta) \cap \mathcal{U}) \ll P^{4\theta - 3 - r + (2+\delta)\theta r}$$

since our hypothesis on $\boldsymbol{L}$ implies that Λ has r linearly independent rows.

Fix a small positive real number θ_0. The following lemma shows that we may restrict attention to $\mathfrak{R}(\theta_0)$.

Lemma 4.1. *We have*

$$\int_{\mathfrak{N}(1/2 - \delta) \setminus \mathfrak{R}(\theta_0)} |S_0(\alpha_0, \boldsymbol{\alpha}) \mathbb{K}_{\pm}(\boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} = o(P^{n-r-3}).$$

Proof. Note that $\mathfrak{N}(\frac{1}{2} - \delta) \subseteq \mathfrak{N}(\frac{1}{2}) = \mathfrak{R}(\frac{1}{2})$. Let

$$(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{N}(\tfrac{1}{2} - \delta) \cap \mathfrak{R}(\theta_g) \setminus \mathfrak{R}(\theta_{g-1})$$

for some $g \in \{1, 2, \ldots, t\}$, where

$$0 < \theta_0 < \theta_1 < \cdots < \theta_t = \tfrac{1}{2}.$$

First suppose that $|S(\alpha_0, \boldsymbol{\alpha})| \geqslant P^{n - h\theta_{g-1}/4 + \varepsilon}$. By [Lemma 2.1](#), there exist relatively prime integers q and a satisfying

$$1 \leqslant q \leqslant C_1 P^{2\theta_{g-1}}, \qquad |q\alpha_0 - a| < P^{2\theta_{g-1} - 3}.$$

Let $\beta_0, \boldsymbol{a}$, and $\boldsymbol{\beta}$ be as in [Section 3](#), with $\boldsymbol{\lambda} = \Lambda\boldsymbol{\alpha}$. Since $(\alpha_0, \boldsymbol{\alpha}) \notin \mathfrak{R}(\theta_{g-1})$, we must have $q|\boldsymbol{\beta}| \geqslant P^{(2+\delta)\theta_{g-1} - 1}$. Now

$$P|\boldsymbol{\beta}| \gg q^{-1} P^{(2+\delta)\theta_{g-1}} \gg P^{\delta\theta_{g-1}} P^3 |\beta_0|,$$

so [Heath-Brown 1996, Lemma 10] yields

$$I(P^3 \beta_0, P\boldsymbol{\beta}) \ll_N (q^{-1} P^{(2+\delta)\theta_{g-1}})^{-N} \ll P^{-N\delta\theta_{g-1}}$$

for any $N > 0$. Choosing N large now gives $S_0(\alpha_0, \boldsymbol{\alpha}) \ll 1$.

Now suppose instead that $|S(\alpha_0, \boldsymbol{\alpha})| < P^{n - h\theta_{g-1}/4 + \varepsilon}$. As $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{N}(\frac{1}{2} - \delta)$, there exist relatively prime integers q and a such that $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{N}_{q,a}(\frac{1}{2} - \delta)$. From (3-8),

$$S(\alpha_0, \boldsymbol{\alpha}) - S_0(\alpha_0, \boldsymbol{\alpha}) \ll q^{n - h/8 + \varepsilon} \ll P^{n - h/8},$$

and now the triangle inequality yields

$$S_0(\alpha_0, \boldsymbol{\alpha}) \ll \max(P^{n - h\theta_{g-1}/4 + \varepsilon}, P^{n - h/8}) = P^{n - h\theta_{g-1}/4 + \varepsilon}. \qquad (4\text{-}3)$$

The bound (4-3) is valid in both cases, so

$$\int |S_0(\alpha_0, \boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} \ll P^{4\theta_g - 3 - r + (2 + \delta)\theta_g r} \, P^{n - h\theta_{g-1}/4 + \varepsilon},$$

where the integral is over $\mathfrak{N}(\frac{1}{2} - \delta) \cap \mathcal{U} \cap \mathfrak{R}(\theta_g) \setminus \mathfrak{R}(\theta_{g-1})$. The right-hand side is $O(P^{n - r - 3 - \varepsilon})$ if $\theta_g / \theta_{g-1} \simeq 1$ since $h \geqslant 17 + 8r$. We can therefore choose $\theta_1, \ldots, \theta_{t-1}$ with $t \ll 1$ satisfactorily to ensure that

$$\int_{\mathcal{U} \cap \mathfrak{N}(1/2 - \delta) \setminus \mathfrak{R}(\theta_0)} |S_0(\alpha_0, \boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} \ll P^{n - r - 3 - \varepsilon}.$$

The desired inequality now follows from (2-1), (2-2), (2-4), and (2-6). $\qquad \square$

Thus, to prove (3-9) and hence (1-4), it suffices to show that

$$\int_{\mathfrak{R}} S_0(\alpha_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \mathbb{K}_{\pm}(\boldsymbol{\alpha}) \, d\alpha_0 \, d\boldsymbol{\alpha} = (2\eta)^r \mathfrak{S} \chi_w P^{n - r - 3} + o(P^{n - r - 3}), \quad (4\text{-}4)$$

where now and henceforth we write

$$\mathfrak{R} = \mathfrak{R}_P = \mathfrak{R}(\theta_0), \qquad \mathfrak{R}(q, a, \boldsymbol{a}) = \mathfrak{R}_{q,a,\boldsymbol{a}}(\theta_0).$$

We now choose our unit interval

$$U = (P^{2\theta_0 - 3}, 1 + P^{2\theta_0 - 3}]. \qquad (4\text{-}5)$$

This choice ensures that, if the conditions (4-1) and (4-2) hold with $\theta = \theta_0$ for some $(\alpha_0, \boldsymbol{\alpha}) \in \mathbb{R} \times \mathbb{R}^r$, then $\alpha_0 \in U$ if and only if $1 \leqslant a \leqslant q$. In particular, the set $\mathfrak{R}$ is the disjoint union of the sets $\mathfrak{R}(q, a, \boldsymbol{a})$ over integers $q, a, a_1, \ldots, a_n$ satisfying

$$1 \leqslant a \leqslant q \leqslant C_1 P^{2\theta_0}, \qquad (a, q) = 1. \qquad (4\text{-}6)$$

5. A mean-value estimate

We begin by bounding $I(\gamma_0, \boldsymbol{\gamma})$. In light of (3-5), the first step is to bound $g(\alpha_0, \boldsymbol{\lambda})$.

Lemma 5.1. *Let ξ be a small positive real number. Let $\alpha_0 \in \mathbb{R}$ and $\boldsymbol{\lambda} \in \mathbb{R}^n$ with $|\alpha_0| < P^{-3/2}$. Then*

$$g(\alpha_0, \boldsymbol{\lambda}) \ll P^{n + \xi} (P^3 |\alpha_0|)^{-h/8}$$

and

$$g_u(\alpha_0, \lambda) \ll P^{n+\xi}(P^3|\alpha_0|)^{-h/8},$$

where $g_u(\alpha_0, \lambda)$ is given by (2-12).

Proof. This follows from the argument of the corollary to [Birch 1962, Lemma 4.3], using Lemma 2.1. □

Lemma 5.2. *We have*

$$I(\gamma_0, \boldsymbol{\gamma}) \ll \frac{1}{1 + (|\gamma_0| + |\boldsymbol{\gamma}|)^{h/8-\varepsilon}}. \tag{5-1}$$

Proof. As $I(\gamma_0, \boldsymbol{\gamma}) \ll 1$, we may assume that $|\gamma_0| + |\boldsymbol{\gamma}|$ is large. From (3-5),

$$I(\gamma_0, \boldsymbol{\gamma}) = P^{-n}g(\gamma_0/P^3, \boldsymbol{\gamma}/P) - \sum_{\boldsymbol{c} \neq \boldsymbol{0}} I(\gamma_0, \boldsymbol{\gamma} - P\boldsymbol{c}).$$

Since $I(\gamma_0, \boldsymbol{\gamma})$ is independent of P, we are free to choose $P = (|\gamma_0| + |\boldsymbol{\gamma}|)^n$. By Lemma 5.1 and [Heath-Brown 1996, Lemma 10], we now have

$$I(\gamma_0, \boldsymbol{\gamma}) \ll P^{\varepsilon/n}|\gamma_0|^{-h/8} = \frac{(|\gamma_0| + |\boldsymbol{\gamma}|)^\varepsilon}{|\gamma_0|^{h/8}}. \tag{5-2}$$

Let C_2 be a large positive constant. If $|\boldsymbol{\gamma}| \geqslant C_2|\gamma_0|$, then [Heath-Brown 1996, Lemma 10] yields $I(\gamma_0, \boldsymbol{\gamma}) \ll_N |\boldsymbol{\gamma}|^{-N} \ll_N (|\gamma_0| + |\boldsymbol{\gamma}|)^{-N}$ for any $N > 0$ while, if $|\boldsymbol{\gamma}| < C_2|\gamma_0|$, then (5-2) gives

$$I(\gamma_0, \boldsymbol{\gamma}) \ll (|\gamma_0| + |\boldsymbol{\gamma}|)^{\varepsilon-h/8}.$$

The latter bound is valid in either case. As $|\gamma_0| + |\boldsymbol{\gamma}|$ is large, our proof is complete. □

We now have all of the necessary ingredients to obtain a mean-value estimate of the correct order of magnitude. Let $\mathfrak{U}$ be an arbitrary unit hypercube in r dimensions, and put $\mathcal{U} = U \times \mathfrak{U}$. Let $V \subseteq \{1, 2, \ldots, n\}$ index r linearly independent rows of Λ. When $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{R}(q, a, \boldsymbol{a})$ and $(a, q) = 1$, write

$$F(\alpha_0, \boldsymbol{\alpha}) = F(\alpha_0, \boldsymbol{\alpha}; P) = \prod_{v \leqslant n}(q + P|q\lambda_v - a_v|)^{-1},$$

where $\boldsymbol{\lambda} = \Lambda\boldsymbol{\alpha}$. As $h/8 > r + 2$, Lemmas 3.1 and 5.2 imply that

$$S_0(\alpha_0, \boldsymbol{\alpha})F(\alpha_0, \boldsymbol{\alpha})^{-\varepsilon}$$
$$\ll P^n q^{-r-2-\varepsilon}(1 + P^3|\alpha_0 - a/q|)^{-1-\varepsilon} \prod_{v \in V}(1 + P|\lambda_v - a_v/q|)^{-1-\varepsilon}.$$

For each q, we can choose from $O(q^{r+1})$ values of a and a_v ($v \in V$) for which $\mathfrak{R}(q, a, \boldsymbol{a}) \cap \mathcal{U}$ is nonempty. Thus, an invertible change of variables gives

$$\int_{\mathfrak{R} \cap \mathcal{U}} |S_0(\alpha_0, \boldsymbol{\alpha})| F(\alpha_0, \boldsymbol{\alpha})^{-\varepsilon} \, d\alpha_0 \, d\boldsymbol{\alpha}$$

$$\ll P^n \sum_{q \in \mathbb{N}} q^{-1-\varepsilon} \int_{\mathbb{R}} (1 + P^3 |\beta_0|)^{-1-\varepsilon} \, d\beta_0 \cdot \int_{\mathbb{R}^r} \prod_{j \leqslant r} (1 + P|\alpha'_j|)^{-1-\varepsilon} \, d\boldsymbol{\alpha}'$$

$$\ll P^{n-r-3}. \tag{5-3}$$

Positivity has permitted us to complete the summation and the integrals to infinity for an upper bound.

6. The Davenport–Heilbronn method

In this section, we specify our Davenport–Heilbronn dissection and complete the proof of (1-4). The bound (5-3) will suffice on the Davenport–Heilbronn major and trivial arcs, but on the minor arcs, we shall need to bound $F(\alpha_0, \boldsymbol{\alpha})$ nontrivially. Using the methods of Bentkus, Götze, and Freeman, as exposited in [Wooley 2003, Lemmas 2.2 and 2.3], we will show that $F(\alpha_0, \boldsymbol{\alpha}) = o(1)$ in the case that $|\boldsymbol{\alpha}|$ is of "intermediate" size. The success of our endeavor depends crucially on our irrationality hypothesis for $\boldsymbol{L}$.

In order for the argument to work, we need to essentially replace F with a function $\mathcal{F}$ defined on $\mathbb{R}^r$. For $\boldsymbol{\alpha} \in \mathbb{R}^r$, let $\mathcal{F}(\boldsymbol{\alpha}; P)$ be the supremum of the quantity

$$\prod_{v \leqslant n} (q + P|q\lambda_v - a_v|)^{-1}$$

over $q \in \mathbb{N}$ and $\boldsymbol{a} \in \mathbb{Z}^n$, where $\boldsymbol{\lambda} = \Lambda \boldsymbol{\alpha}$. Note that, if $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{R}_P$, then

$$F(\alpha_0, \boldsymbol{\alpha}; P) \leqslant \mathcal{F}(\boldsymbol{\alpha}; P). \tag{6-1}$$

Moreover, since Λ has full rank, we have

$$|\boldsymbol{\alpha}| \ll |\Lambda \boldsymbol{\alpha}| \ll |\boldsymbol{\alpha}|. \tag{6-2}$$

Lemma 6.1. *Let $0 < V \leqslant W$. Then*

$$\sup_{V \leqslant |\Lambda \boldsymbol{\alpha}| \leqslant W} \mathcal{F}(\boldsymbol{\alpha}; P) \to 0 \quad (P \to \infty). \tag{6-3}$$

Proof. Suppose for a contradiction that (6-3) is false. Then there exist $\psi > 0$ and

$$(\boldsymbol{\alpha}^{(m)}, P_m, q_m, \boldsymbol{a}^{(m)}) \in \mathbb{R}^r \times [1, \infty) \times \mathbb{N} \times \mathbb{Z}^n \quad (m \in \mathbb{N})$$

such that the sequence (P_m) increases monotonically to infinity and such that, if $m \in \mathbb{N}$, then

(i)
$$V \leqslant |\boldsymbol{\lambda}^{(m)}| \leqslant W,$$

(ii)
$$\prod_{v \leqslant n} (q_m + P_m |q_m \lambda_v^{(m)} - a_v^{(m)}|) < \psi^{-1}, \qquad (6\text{-}4)$$

where $\boldsymbol{\lambda}^{(m)} = \Lambda \boldsymbol{\alpha}^{(m)}$ $(m \in \mathbb{N})$. Now $q_m < \psi^{-1} \ll 1$, so $|\boldsymbol{a}^{(m)}| \ll 1$. In particular, there are only finitely many possible choices for $(q_m, \boldsymbol{a}^{(m)})$, so this pair must take a particular value infinitely often, say $(q, \boldsymbol{a})$.

From (6-4), we see that $q\boldsymbol{\lambda}^{(m)}$ converges to $\boldsymbol{a}$ on a subsequence. The sequence $(|\boldsymbol{\alpha}^{(m)}|)_m$ is bounded, so by compactness, we know that $\boldsymbol{\alpha}^{(m)}$ converges to some vector $\boldsymbol{\alpha}$ on a subsubsequence. Therefore, $q\Lambda\boldsymbol{\alpha} = \boldsymbol{a}$ and in particular $\Lambda\boldsymbol{\alpha}$ is a rational vector, so $\boldsymbol{\alpha} \cdot \boldsymbol{L}$ is a rational form. Note that $\boldsymbol{\alpha} \neq \boldsymbol{0}$ since $|\boldsymbol{\alpha}^{(m)}| \gg 1$. This contradicts our hypothesis on $\boldsymbol{L}$, thereby establishing (6-3). □

Corollary 6.2. *Let θ be a small positive real number. Then there exists a function $T : [1, \infty) \to [1, \infty)$, increasing monotonically to infinity, such that $T(P) \leqslant P^\theta$ and*

$$\sup_{P^{\theta-1} \leqslant |\Lambda\boldsymbol{\alpha}| \leqslant T(P)} \mathcal{F}(\boldsymbol{\alpha}; P) \leqslant T(P)^{-1}. \qquad (6\text{-}5)$$

Proof. Lemma 6.1 yields a sequence (P_m) of large positive real numbers such that

$$\sup_{1/m \leqslant |\Lambda\boldsymbol{\alpha}| \leqslant m} \mathcal{F}(\boldsymbol{\alpha}; P_m) \leqslant 1/m.$$

We may assume that this sequence is increasing and that $P_m^\theta \geqslant m$ $(m \in \mathbb{N})$. Define $T(P)$ by $T(P) = 1$ $(1 \leqslant P \leqslant P_1)$ and $T(P) = m$ $(P_m \leqslant P < P_{m+1})$. Note that $T(P) \leqslant P^\theta$ and that $T(P)$ increases monotonically to infinity. Now

$$\sup_{T(P)^{-1} \leqslant |\Lambda\boldsymbol{\alpha}| \leqslant T(P)} \mathcal{F}(\boldsymbol{\alpha}; P) \leqslant T(P)^{-1},$$

for if $P \geqslant P_m$, then $\mathcal{F}(\boldsymbol{\alpha}; P) \leqslant \mathcal{F}(\boldsymbol{\alpha}; P_m)$.

The inequality (6-5) plainly holds if $P \leqslant P_1$. Thus, it remains to show that, if P is large and

$$|\Lambda\boldsymbol{\alpha}| < T(P)^{-1} < \mathcal{F}(\boldsymbol{\alpha}; P), \qquad (6\text{-}6)$$

then $|\Lambda\boldsymbol{\alpha}| < P^{\theta-1}$. Suppose we have (6-6), with P large. Writing $\boldsymbol{\lambda} = \Lambda\boldsymbol{\alpha}$, we have

$$\prod_{v \leqslant n} (q + P|q\lambda_v - a_v|) < T(P)$$

for some $q \in \mathbb{N}$ and some $\boldsymbol{a} \in \mathbb{Z}^n$. Now $q < T(P)^{1/n}$ and

$$|q\boldsymbol{\lambda} - \boldsymbol{a}| < T(P)/P,$$

so the triangle inequality and (6-6) give

$$|\boldsymbol{a}| < T(P)/P + T(P)^{1/n-1} < 1.$$

Therefore, $a = 0$, and so

$$|\Lambda\boldsymbol{\alpha}| \leqslant |q\boldsymbol{\lambda}| < T(P)/P \leqslant P^{\theta-1},$$

completing the proof.   □

Let C_3 be a large positive constant. Let $T(P)$ be as in Corollary 6.2 with $\theta = \delta^2\theta_0$. We define our Davenport–Heilbronn major arc by

$$\mathfrak{M} = \{(\alpha_0, \boldsymbol{\alpha}) \in \mathbb{R} \times \mathbb{R}^r : |\boldsymbol{\alpha}| < C_3 P^{\delta^2\theta_0 - 1}\},$$

our minor arcs by

$$\mathfrak{m} = \{(\alpha_0, \boldsymbol{\alpha}) \in \mathbb{R} \times \mathbb{R}^r : C_3 P^{\delta^2\theta_0 - 1} \leqslant |\boldsymbol{\alpha}| \leqslant C_3^{-1} T(P)\},$$

and our trivial arcs by

$$\mathfrak{t} = \{(\alpha_0, \boldsymbol{\alpha}) \in \mathbb{R} \times \mathbb{R}^r : |\boldsymbol{\alpha}| > C_3^{-1} T(P)\}.$$

It follows from (6-1), (6-2), and (6-5) that

$$\sup_{\mathfrak{R}\cap\mathfrak{m}} F(\alpha_0, \boldsymbol{\alpha}) \leqslant T(P)^{-1}. \tag{6-7}$$

Let $\mathfrak{U}$ be an arbitrary unit hypercube in r dimensions, and put $\mathcal{U} = U \times \mathfrak{U}$. By (5-3) and (6-7),

$$\int_{\mathfrak{R}\cap\mathfrak{m}\cap\mathcal{U}} |S_0(\alpha_0, \boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} \ll T(P)^{-\varepsilon} P^{n-r-3}.$$

Now (2-2), (2-4), and (2-6) yield

$$\int_{\mathfrak{R}\cap\mathfrak{m}} |S_0(\alpha_0, \boldsymbol{\alpha})\mathbb{K}_{\pm}(\boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} = o(P^{n-r-3}). \tag{6-8}$$

Note that

$$0 < F(\alpha_0, \boldsymbol{\alpha}) \leqslant 1. \tag{6-9}$$

Together with (2-2), (2-4), (2-6), and (5-3), this gives

$$\int_{\mathfrak{R}\cap\mathfrak{t}} |S_0(\alpha_0, \boldsymbol{\alpha})\mathbb{K}_{\pm}(\boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} \ll P^{n-r-3} L(P)^r \sum_{n=0}^{\infty} (C_3^{-1} T(P) + n)^{-2}$$

$$\ll P^{n-r-3} L(P)^r T(P)^{-1} = o(P^{n-r-3}). \tag{6-10}$$

Coupling (6-8) with (6-10) yields

$$\int_{\mathfrak{R}\setminus\mathfrak{M}} |S_0(\alpha_0, \boldsymbol{\alpha})\mathbb{K}_{\pm}(\boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} = o(P^{n-r-3}).$$

Recall that to show (1-4) it remains to establish (4-4). Defining

$$S_1 = \int_{\mathfrak{R}\cap\mathfrak{M}} S_0(\alpha_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \mathbb{K}_{\pm}(\boldsymbol{\alpha}) \, d\alpha_0 \, d\boldsymbol{\alpha},$$

it now suffices to prove that

$$S_1 = (2\eta)^r \mathfrak{S}\chi_w P^{n-r-3} + o(P^{n-r-3}).$$

By (2-3),

$$K_{\pm}(\alpha) = (2\eta \pm \rho) \cdot \mathrm{sinc}(\pi\alpha\rho) \cdot \mathrm{sinc}(\pi\alpha(2\eta \pm \rho)).$$

Now (2-1), (2-2), and the Taylor expansion of $\mathrm{sinc}(\,\cdot\,)$ yield

$$K_{\pm}(\alpha) = 2\eta + O(L(P)^{-1}) \quad (|\alpha| < P^{-1/2}).$$

Substituting this into (2-6) shows that, if $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{M}$, then

$$\mathbb{K}_{\pm}(\boldsymbol{\alpha}) = (2\eta)^r + O(L(P)^{-1}). \tag{6-11}$$

Moreover, it follows from (5-3) and (6-9) that

$$\int_{\mathfrak{R}\cap\mathfrak{M}} |S_0(\alpha_0, \boldsymbol{\alpha})| \, d\alpha_0 \, d\boldsymbol{\alpha} \ll P^{n-r-3}. \tag{6-12}$$

From (6-11) and (6-12), we infer that

$$S_1 = (2\eta)^r \int_{\mathfrak{R}\cap\mathfrak{M}} S_0(\alpha_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \, d\alpha_0 \, d\boldsymbol{\alpha} + o(P^{n-r-3}).$$

Thus, to prove (1-4), it remains to show that

$$S_2 = \mathfrak{S}\chi_w P^{n-r-3} + o(P^{n-r-3}), \tag{6-13}$$

where

$$S_2 = \int_{\mathfrak{R}\cap\mathfrak{M}} S_0(\alpha_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \, d\alpha_0 \, d\boldsymbol{\alpha}.$$

For $q \in \mathbb{N}$ and $a \in \{1, 2, \ldots, q\}$, let $X(q, a)$ be the set of $(\alpha_0, \boldsymbol{\alpha}) \in \mathbb{R} \times \mathbb{R}^r$ satisfying

$$q \leqslant C_1 P^{2\theta_0}, \qquad |q\alpha_0 - a| < P^{2\theta_0 - 3}.$$

Lemma 6.3. *Assume* (4-6). *Then* $\mathfrak{R}(q, a, \mathbf{0}) \cap \mathfrak{M} = X(q, a) \cap \mathfrak{M}$.

Proof. As $\mathfrak{R}(q, a, \mathbf{0}) \subseteq X(q, a)$, we have $\mathfrak{R}(q, a, \mathbf{0}) \cap \mathfrak{M} \subseteq X(q, a) \cap \mathfrak{M}$. Next, suppose that $(\alpha_0, \boldsymbol{\alpha}) \in X(q, a) \cap \mathfrak{M}$. Then $|\boldsymbol{\alpha}| < C_3 P^{\delta^2\theta_0 - 1}$, so

$$|\Lambda\boldsymbol{\alpha}| \ll P^{\delta^2\theta_0 - 1}.$$

Now $|q\Lambda\boldsymbol{\alpha}| \ll P^{(2+\delta^2)\theta_0 - 1}$, and in particular, we have (4-1) with $\theta = \theta_0$ and $\boldsymbol{a} = \mathbf{0}$. Thus, we have $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{R}(q, a, \mathbf{0})$, and plainly $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{M}$. $\square$

Note also that, if $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{R} \cap \mathfrak{M}$, then $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{R}(q, a, \mathbf{0})$ for some $q, a \in \mathbb{Z}$ satisfying (4-6). Indeed, if $(\alpha_0, \boldsymbol{\alpha}) \in \mathfrak{R}(q, a, \boldsymbol{a}) \cap \mathfrak{M}$ for some q, a, and $\boldsymbol{a}$ satisfying (4-6), then the triangle inequality implies that $\boldsymbol{a} = \mathbf{0}$. By Lemma 6.3, we conclude

that $\mathfrak{R} \cap \mathfrak{M}$ is the disjoint union of the sets $X(q, a) \cap \mathfrak{M}$ over $q, a \in \mathbb{Z}$ satisfying (4-6). Put

$$V(q) = [-q^{-1} P^{2\theta_0 - 3}, q^{-1} P^{2\theta_0 - 3}] \quad (q \in \mathbb{N})$$

and

$$W = [-C_3 P^{\delta^2 \theta_0 - 1}, C_3 P^{\delta^2 \theta_0 - 1}]^r.$$

Now

$$S_2 = \sum_{q \leqslant C_1 P^{2\theta_0}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{V(q) \times W} f_{q,a}(\beta_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \, d\beta_0 \, d\boldsymbol{\alpha},$$

where

$$f_{q,a}(\beta_0, \boldsymbol{\alpha}) = (P/q)^n S_{q,a,\mathbf{0}} I(P^3 \beta_0, P \Lambda \boldsymbol{\alpha}). \tag{6-14}$$

To prove (6-13), we complete the integrals and the outer sum to infinity. In light of (1-2), it follows from Lemmas 3.1 and 5.2 that, if $(a, q) = 1$, then

$$f_{q,a}(\beta_0, \boldsymbol{\alpha}) \ll P^n q^{-3} (1 + P^3 |\beta_0|)^{-1-\varepsilon} \prod_{v \in V} (1 + P |\lambda_v|)^{-1-\varepsilon}, \tag{6-15}$$

where V is as in Section 5 and $\boldsymbol{\lambda} = \Lambda \boldsymbol{\alpha}$. Let

$$S_3 = \sum_{q \leqslant C_1 P^{2\theta_0}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathbb{R} \times W} f_{q,a}(\beta_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \, d\beta_0 \, d\boldsymbol{\alpha}.$$

By (6-15) and an invertible change of variables,

$$S_2 - S_3 \ll P^n \sum_{q \in \mathbb{N}} q^{-3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{q^{-1} P^{2\theta_0 - 3}}^{\infty} (P^3 \beta_0)^{-1-\varepsilon} \, d\beta_0 \int_{\mathbb{R}^r} \prod_{v \in V} (1 + P |\lambda_v|)^{-1-\varepsilon} \, d\boldsymbol{\lambda}_V$$

$$= o(P^{n-r-3}), \tag{6-16}$$

where $\boldsymbol{\lambda}_V = (\lambda_v)_{v \in V}$.

Let

$$S_4 = \sum_{q \leqslant C_1 P^{2\theta_0}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathbb{R}^{r+1}} f_{q,a}(\beta_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \, d\beta_0 \, d\boldsymbol{\alpha}.$$

By (6-15) and an invertible change of variables,

$$S_3 - S_4 \ll P^n \sum_{q \in \mathbb{N}} q^{-3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathbb{R}} (1 + P^3 |\beta_0|)^{-1-\varepsilon} \, d\beta_0 \int \prod_{j \leqslant r} (1 + P |\alpha'_j|)^{-1-\varepsilon} \, d\boldsymbol{\alpha}'.$$

Here the inner integral is over $\boldsymbol{\alpha}' \in \mathbb{R}^r$ such that $\Lambda_V^{-1} \boldsymbol{\alpha}' \notin W$, where Λ_V is the

submatrix of Λ determined by taking rows indexed by V. With c a small positive constant, we now have

$$S_3 - S_4 \ll P^{n-r-2} \int_{cP^{\delta^2 \theta_0 - 1}}^{\infty} (P\alpha)^{-1-\varepsilon} \, d\alpha = o(P^{n-r-3}). \qquad (6\text{-}17)$$

Let

$$S_5 = \sum_{q \in \mathbb{N}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathbb{R}^{r+1}} f_{q,a}(\beta_0, \boldsymbol{\alpha}) e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) \, d\beta_0 \, d\boldsymbol{\alpha}.$$

By (6-15) and an invertible change of variables,

$$S_4 - S_5 \ll P^n \sum_{q > C_1 P^{2\theta_0}} q^{-3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\mathbb{R}} (1+P^3|\beta_0|)^{-1-\varepsilon} \, d\beta_0 \int_{\mathbb{R}^r} \prod_{j \leqslant r} (1+P|\alpha_j'|)^{-1-\varepsilon} \, d\boldsymbol{\alpha}'$$

$$\ll P^{n-r-3} \sum_{q > C_1 P^{2\theta_0}} q^{-2} = o(P^{n-r-3}). \qquad (6\text{-}18)$$

In view of (1-5), (3-3), and (6-14),

$$S_5 = P^n \mathfrak{S} \int_{\mathbb{R}^{r+1}} e(-\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) I(P^3 \beta_0, P \Lambda \boldsymbol{\alpha}) \, d\beta_0 \, d\boldsymbol{\alpha}.$$

Changing variables yields

$$S_5 = P^{n-r-3} \mathfrak{S} \int_{\mathbb{R}^{r+1}} e(-P^{-1}\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) I(\beta_0, \Lambda \boldsymbol{\alpha}) \, d\beta_0 \, d\boldsymbol{\alpha}. \qquad (6\text{-}19)$$

By (1-6) and (3-2),

$$\chi_w = \int_{\mathbb{R}^{r+1}} I(\beta_0, \Lambda \boldsymbol{\alpha}) \, d\beta_0 \, d\boldsymbol{\alpha}.$$

As $h \geqslant 17 + 8r$, the bounds (5-1) and

$$e(-P^{-1}\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) - 1 \ll P^{-1}|\boldsymbol{\alpha}|$$

imply that

$$\int_{\mathbb{R}^{r+1}} e(-P^{-1}\boldsymbol{\alpha} \cdot \boldsymbol{\tau}) I(\beta_0, \Lambda \boldsymbol{\alpha}) \, d\beta_0 \, d\boldsymbol{\alpha} = \chi_w + O(P^{-1}).$$

Substituting this into (6-19) yields

$$S_5 = P^{n-r-3} \mathfrak{S} \chi_w + o(P^{n-r-3}).$$

Combining this with (6-16), (6-17), and (6-18) yields (6-13), completing the proof of (1-4).

7. Positivity of the singular series and singular integral

In this section, we confirm that $\mathfrak{S} > 0$ and $\chi_w > 0$, thereby completing the proof of Theorem 1.1. Since $\mathfrak{S}$ is the singular series associated to the cubic form C, its positivity is already well understood. Davenport [1959, §7] showed the sufficiency of a certain p-adic solubility property, invariant under equivalence (invertible change of basis). He also showed that any cubic form that is nondegenerate in at least ten variables has this property [Davenport 1959, Lemma 2.8]. If C is degenerate, then it is equivalent to a cubic form C^* in which $n_1 \leqslant n - 1$ variables appear explicitly so that $h(C^*) \leqslant n_1$ and we may repeat the argument. Since $h(C) \geqslant 25$, and since the h-invariant is invariant under equivalence, we conclude that $\mathfrak{S} > 0$.

For positivity of the singular integral, we begin by establishing the equivalence of the definitions (1-6) and (1-8). Lemma 5.2 provides the appropriate analogy to [Schmidt 1982b, Lemma 11]. Thus, following Chapter 11 therein shows that the two definitions are equivalent.

We now work with the definition (1-8). We claim that $I_L(\boldsymbol{f}) \gg 1$. Since $w(\boldsymbol{x}) \gg 1$ for $\boldsymbol{x} \in B := \left\{ \boldsymbol{x} \in \mathbb{R}^n : |\boldsymbol{x}| \leqslant \frac{1}{2} \right\}$, it suffices to show that

$$\int_B \Psi_L(\boldsymbol{f}(\boldsymbol{x})) \, \mathrm{d}\boldsymbol{x} \gg 1. \tag{7-1}$$

Define a real manifold

$$\mathcal{M} = \{ C = L_1 = \cdots = L_r = 0 \} \subseteq \mathbb{R}^n.$$

All of our forms have odd degree, so $\mathcal{M} \cap A \neq \{\boldsymbol{0}\}$ for every $(r + 2)$-dimensional subspace A of $\mathbb{R}^n$. Thus, by [Schmidt 1982a, Lemma 1], $\dim(\mathcal{M}) \geqslant n - r - 1$. The argument of [Schmidt 1982b, Lemma 2] now confirms (7-1), thereby establishing the positivity of χ_w. This completes the proof of Theorem 1.1.

8. A more general result

In this section, we prove Theorem 1.2. We begin by establishing that, if $\boldsymbol{\alpha} \in \mathbb{R}^r \setminus \{\boldsymbol{0}\}$, then $\boldsymbol{\alpha} \cdot \boldsymbol{L}$ is not a rational form. Suppose that $\boldsymbol{\alpha} \cdot \boldsymbol{L}$ is a rational form, for some $\boldsymbol{\alpha} \in \mathbb{R}^r$. Then $\Lambda \boldsymbol{\alpha} = \boldsymbol{q}$ for some $\boldsymbol{q} \in \mathbb{Q}^n$, where Λ is given by (2-10). Note that Λ has full rank since its entries are algebraically independent over $\mathbb{Q}$ and its $r \times r$ minors are nontrivial integer polynomials in these entries. It therefore follows from $\Lambda \boldsymbol{\alpha} = \boldsymbol{q}$ that $\alpha_1, \ldots, \alpha_r$ are rational functions in the entries of Λ_V over $\mathbb{Q}$, where V is as in Section 5 and Λ_V is the submatrix of Λ determined by taking rows indexed by V. Let $i \in \{1, 2, \ldots, n\} \setminus V$, and consider the equation

$$\alpha_1 \lambda_{1,i} + \alpha_r \lambda_{r,i} = q_i. \tag{8-1}$$

Since $\alpha_1, \ldots, \alpha_r$ are rational functions in the entries of Λ_V over $\mathbb{Q}$, (8-1) and the

algebraic independence of the entries of Λ necessitate that $\boldsymbol{\alpha} = \mathbf{0}$. We conclude that, if $\boldsymbol{\alpha} \in \mathbb{R}^r \setminus \{\mathbf{0}\}$, then $\boldsymbol{\alpha} \cdot \boldsymbol{L}$ is not a rational form.

By rescaling if necessary, we may assume that C has integer coefficients. By Theorem 1.1, we may now assume that $h \leqslant 16 + 8r$, and so $n - h > r$. Write

$$C = A_1 B_1 + \cdots + A_h B_h,$$

where $A_1, \ldots, A_h$ are rational linear forms and $B_1, \ldots, B_h$ are rational quadratic forms. The vector space defined by

$$A_1 = \cdots = A_h = 0$$

has a rational subspace of dimension $n - h$, by the rank-nullity theorem. Let $z_1, \ldots, z_{n-h}$ be linearly independent integer points in this subspace. Define

$$L_i'(\boldsymbol{y}) = L_i(y_1 z_1 + \cdots + y_{n-h} z_{n-h}) \quad (1 \leqslant i \leqslant r).$$

We seek to show that $\boldsymbol{L}'(\mathbb{Z}^{n-h})$ is dense in $\mathbb{R}^r$. Writing $z_j = (z_{j,1}, \ldots, z_{j,n})$ $(1 \leqslant j \leqslant n - h)$ and recalling (2-9),

$$L_i'(\boldsymbol{y}) = \sum_{j \leqslant n-h} \lambda_{i,j}' y_j,$$

where

$$\lambda_{i,j}' = \sum_{k \leqslant n} \lambda_{i,k} z_{j,k} \quad (1 \leqslant i \leqslant r, \ 1 \leqslant j \leqslant n - h).$$

Lemma 8.1. *The $\lambda_{i,j}'$ are algebraically independent over $\mathbb{Q}$.*

Proof. Extend $z_1, \ldots, z_{n-h}$ to a basis $z_1, \ldots, z_n$ for $\mathbb{Q}^n$, and define

$$\lambda_{i,j}' = \sum_{k \leqslant n} \lambda_{i,k} z_{j,k} \quad (1 \leqslant i \leqslant r, \ n - h < j \leqslant n).$$

We now have an invertible rational matrix

$$Z = \begin{pmatrix} z_{1,1} & \cdots & z_{1,n} \\ \vdots & & \vdots \\ z_{n,1} & \cdots & z_{n,n} \end{pmatrix},$$

where $z_j = (z_{j,1}, \ldots, z_{j,n})$ $(1 \leqslant j \leqslant n)$. Put

$$\Lambda' = \begin{pmatrix} \lambda_{1,1}' & \cdots & \lambda_{r,1}' \\ \vdots & & \vdots \\ \lambda_{1,n}' & \cdots & \lambda_{r,n}' \end{pmatrix},$$

and note that $\Lambda' = Z\Lambda$.

We shall prove, a fortiori, that the entries of Λ' are algebraically independent over $\mathbb{Q}$. Let P' be a rational polynomial in rn variables such that $P'(\Lambda') = 0$. Define a rational polynomial P in rn variables by

$$P(\Xi) = P'(Z\Xi), \quad \Xi \in \mathrm{Mat}_{n \times r}.$$

Now

$$P(\Lambda) = P'(Z\Lambda) = P'(\Lambda') = 0,$$

so the algebraic independence of the entries of Λ forces P to be the zero polynomial. Since

$$P'(\Xi) = P(Z^{-1}\Xi)$$

identically, the polynomial P' must also be trivial.   □

Thus, the entries of the matrix

$$A = \begin{pmatrix} \lambda'_{1,1} & \cdots & \lambda'_{1,n-h} \\ \vdots & & \vdots \\ \lambda'_{r,1} & \cdots & \lambda'_{r,n-h} \end{pmatrix}$$

are algebraically independent over $\mathbb{Q}$, and we seek to show that

$$\{A\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^{n-h}\}$$

is dense in $\mathbb{R}^r$. We put A in the form $(I \mid \Lambda'')$, where I is the $r \times r$ identity matrix and Λ'' is an $r \times (n - h - r)$ matrix, by the following operations.

(i) Divide the top row by A_{11} so that now $A_{11} = 1$.

(ii) Subtract multiples of the top row from other rows so that

$$A_{21} = \cdots = A_{r1} = 0.$$

(iii) Proceed similarly for columns $2, 3, \ldots, r$.

It suffices to show that the image of $\mathbb{Z}^{n-h}$ under left multiplication by $(I \mid \Lambda'')$ is dense in $\mathbb{R}^r$.

Lemma 8.2. *The entries of Λ'' are algebraically independent over $\mathbb{Q}$.*

Proof. After step (i), the entries of A other than the top-left entry are algebraically independent. Indeed, suppose

$$P\left(\frac{A_{12}}{A_{11}}, \ldots, \frac{A_{1,n-h}}{A_{11}}, (A_{ij})_{\substack{2 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant n-h}} \right) = 0$$

for some polynomial P with rational coefficients, where the A_{ij} are the entries of A prior to step (i). For some $t \in \mathbb{N}$, we can multiply the left-hand side by A_{11}^t to obtain a polynomial P^* in $(A_{ij})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant n-h}}$ with rational coefficients. The algebraic

independence of the A_{ij} implies that P^* is the zero polynomial, and so P must also be the zero polynomial.

After step (ii), the entries of A excluding the first column are algebraically independent. Indeed, suppose

$$P\left(A_{12}, \ldots, A_{1,n-h}, (A_{ij} - A_{i1}A_{1j})_{\substack{2 \leqslant i \leqslant r \\ 2 \leqslant j \leqslant n-h}}\right) = 0$$

for some polynomial P with rational coefficients, where the A_{ij} are the entries of A prior to step (ii). The left-hand side may be regarded as a polynomial P^* in the A_{ij} ($(i, j) \neq (1, 1)$). The algebraic independence of the A_{ij} ($(i, j) \neq (1, 1)$) implies that P^* is the zero polynomial, and so P must also be the zero polynomial.

We may now ignore column 1 and deal with columns $2, 3, \ldots, r$ similarly. $\qquad \square$

Next, consider the forms $L''_1, \ldots, L''_r$ given by

$$L''_i(x) = \mu_{i,1}x_1 + \cdots + \mu_{i,n-h-r}x_{n-h-r} \quad (1 \leqslant i \leqslant r),$$

where $\mu_{i,j} = \Lambda''_{ij}$ ($1 \leqslant i \leqslant r, 1 \leqslant j \leqslant n-h-r$). It remains to show that $L''(\mathbb{Z}^{n-h-r})$ is dense modulo 1 in $\mathbb{R}^r$. We shall in fact establish equidistribution modulo 1 of the values of $L''(\mathbb{N}^{n-h-r})$.

For this, we use a multidimensional Weyl criterion [Cassels 1957, p. 66]. With $m = n - h - r$, we need to show that, if $h \in \mathbb{Z}^r \setminus \{0\}$, then

$$P^{-m} \sum_{x_1, \ldots, x_m \leqslant P} e(h \cdot L''(x)) \to 0$$

as $P \to \infty$. The summation equals

$$\prod_{j \leqslant m} \sum_{x_j \leqslant P} e\left(x_j \sum_{i \leqslant r} h_i \mu_{i,j}\right),$$

so it suffices to show that

$$\sum_{i \leqslant r} h_i \mu_{i,1} \notin \mathbb{Q}.$$

This follows from the algebraic independence of the $\mu_{i,j}$, so we have completed the proof of Theorem 1.2.

9. Equidistribution

In this section, we prove Theorem 1.3. Let k be a fixed nonzero integer vector in r variables. By a multidimensional Weyl criterion [Cassels 1957, p. 66], we need to show that

$$N_u(P)^{-1} \sum_{\substack{|x| < P \\ C(x) = 0}} e(k \cdot L(x)) \to 0$$

as $P \to \infty$, where

$$N_u(P) = \#\{\boldsymbol{x} \in \mathbb{Z}^n : |\boldsymbol{x}| < P, \ C(\boldsymbol{x}) = 0\}.$$

It is known that $P^{n-3} \ll N_u(P) \ll P^{n-3}$; see remark (B) in the introduction of [Schmidt 1985]. Thus, it remains to show that

$$\sum_{\substack{|\boldsymbol{x}|<P \\ C(\boldsymbol{x})=0}} e(\boldsymbol{k} \cdot \boldsymbol{L}(\boldsymbol{x})) = o(P^{n-3}). \tag{9-1}$$

Let θ_0 be a small positive real number, and let U be as in (4-5). By rescaling if necessary, we may assume that C has integer coefficients. By (2-7), the left-hand side of (9-1) is equal to

$$\int_U S_u(\alpha_0, \boldsymbol{k}) \, d\alpha_0,$$

where $S_u(\,\cdot\,,\,\cdot\,)$ is as defined in the introduction. Recall (2-9) and (2-10). Note that

$$S_u(\alpha_0, \boldsymbol{k}) = g_u(\alpha_0, \boldsymbol{\lambda}^*),$$

where $g_u(\,\cdot\,,\,\cdot\,)$ is as defined in (2-12) and $\boldsymbol{\lambda}^* = \Lambda \boldsymbol{k} \in \mathbb{R}^n$ is fixed.

For $q \in \mathbb{N}$ and $a \in \mathbb{Z}$, let $\mathfrak{N}'(q, a)$ be the set of $\alpha_0 \in U$ such that

$$|q\alpha_0 - a| < P^{2\theta_0 - 3}.$$

Recall that C_1 is a large positive real number. For positive integers $q \leqslant C_1 P^{2\theta_0}$, let $\mathfrak{N}'(q)$ be the disjoint union of the sets $\mathfrak{N}'(q, a)$ over integers a that are relatively prime to q. Let $\mathfrak{N}'$ be the disjoint union of the sets $\mathfrak{N}'(q)$. By Lemma 2.1 and the classical pruning argument in [Davenport 2005, Lemma 15.1], it now suffices to prove that

$$\int_{\mathfrak{N}'} S_u(\alpha_0, \boldsymbol{k}) \, d\alpha_0 = o(P^{n-3}).$$

Let $\alpha_0 \in \mathfrak{N}'(q, a)$, with $q \leqslant C_1 P^{2\theta_0}$ and $(a, q) = 1$. Then

$$S_u(\alpha_0, \boldsymbol{k}) = \sum_{\boldsymbol{y} \bmod q} e_q(aC(\boldsymbol{y})) S_{\boldsymbol{y}}(q, \beta_0, \boldsymbol{\lambda}^*),$$

where $\beta_0 = \alpha_0 - a/q$ and where in general we define

$$S_{\boldsymbol{y}}(q, \beta_0, \boldsymbol{\lambda}) = \sum_{z:|\boldsymbol{y}+q\boldsymbol{z}|<P} e(\beta_0 C(\boldsymbol{y}+q\boldsymbol{z}) + \boldsymbol{\lambda} \cdot (\boldsymbol{y}+q\boldsymbol{z})).$$

Note that $|q\beta_0| < P^{2\theta_0 - 3}$. Let $\mathfrak{Q}$ denote the set of positive integers $q \leqslant C_1 P^{2\theta_0}$ such that

$$\|q\lambda_v^*\| < P^{7\theta_0 - 1} \quad (1 \leqslant v \leqslant n),$$

and put

$$\mathfrak{Q}' = \{q \in \mathbb{N} : q \leqslant C_1 P^{2\theta_0}\} \setminus \mathfrak{Q}.$$

Suppose $q \in \mathfrak{Q}'$, and let j be such that $\|q\lambda_j^*\| \geqslant P^{7\theta_0-1}$. To bound $S_{\boldsymbol{y}}(q, \beta_0, \boldsymbol{\lambda}^*)$, we reorder the summation, if necessary, so that the sum over z_j is on the inside. We bound this inner sum using the Kusmin–Landau inequality [Graham and Kolesnik 1991, Theorem 2.1] and then bound the remaining sums trivially. Note that, as a function of z_j, the phase

$$\beta_0 C(\boldsymbol{y} + q\boldsymbol{z}) + \boldsymbol{\lambda}^* \cdot (\boldsymbol{y} + q\boldsymbol{z})$$

has derivative

$$\beta_0 \frac{\partial}{\partial z_j} C(\boldsymbol{y} + q\boldsymbol{z}) + q\lambda_j^*,$$

which is monotonic in at most two stretches. As $\|q\lambda_j^*\| \geqslant P^{7\theta_0-1}$ and

$$\beta_0 \frac{\partial}{\partial z_j} C(\boldsymbol{y} + q\boldsymbol{z}) \ll P^{2\theta_0-1}$$

over the range of summation, the Kusmin–Landau inequality tells us that the sum over z_j is $O(P^{1-7\theta_0})$. The remaining sums are over ranges of length $O(P/q)$, so

$$S_{\boldsymbol{y}}(q, \beta_0, \boldsymbol{\lambda}^*) \ll (P/q)^{n-1} P^{1-7\theta_0}.$$

Therefore,

$$S_u(\alpha_0, \boldsymbol{k}) \ll q P^{n-7\theta_0}.$$

Since $\operatorname{meas}(\mathfrak{N}'(q)) \ll P^{2\theta_0-3}$, we now have

$$\sum_{q \in \mathfrak{Q}'} \int_{\mathfrak{N}'(q)} S_u(\alpha_0, \boldsymbol{k}) \, d\alpha_0 \ll \sum_{q \leqslant C_1 P^{2\theta_0}} P^{2\theta_0-3} q P^{n-7\theta_0} = o(P^{n-3}).$$

It therefore remains to show that

$$\sum_{q \in \mathfrak{Q}} \int_{\mathfrak{N}'(q)} S_u(\alpha_0, \boldsymbol{k}) \, d\alpha_0 = o(P^{n-3}).$$

We shall need to study the more general exponential sums $g_u(\alpha_0, \boldsymbol{\lambda})$. Let $q \in \mathbb{N}$ with $q \leqslant P$, and let $a, a_1, \ldots, a_n \in \mathbb{Z}$. Set α_0 and $\boldsymbol{\lambda}$ as in (3-1), and write

$$g_u^*(\alpha_0, \boldsymbol{\lambda}) = (P/q)^n S_{q,a,\boldsymbol{a}} I_u(P^3 \beta_0, P\boldsymbol{\beta}),$$

where $S_{q,a,\boldsymbol{a}}$ is given by (3-3) and where

$$I_u(\gamma_0, \boldsymbol{\gamma}) = \int_{[-1,1]^n} e(\gamma_0 C(\boldsymbol{x}) + \boldsymbol{\gamma} \cdot \boldsymbol{x}) \, d\boldsymbol{x}.$$

Lemma 9.1. *We have*

$$g_u(\alpha_0, \boldsymbol{\lambda}) - g_u^*(\alpha_0, \boldsymbol{\lambda}) \ll q P^{n-1}(1 + P^3|\beta_0| + P|\boldsymbol{\beta}|). \tag{9-2}$$

Proof. First observe that

$$g_u(\alpha_0, \boldsymbol{\lambda}) = \sum_{\boldsymbol{y} \bmod q} e_q(aC(\boldsymbol{y}) + \boldsymbol{a} \cdot \boldsymbol{y}) S_{\boldsymbol{y}}(q, \beta_0, \boldsymbol{\beta}) \tag{9-3}$$

and that

$$S_{\boldsymbol{y}}(q, \beta_0, \boldsymbol{\beta}) = \sum_{\substack{|\boldsymbol{x}| < P \\ \boldsymbol{x} \equiv \boldsymbol{y} \bmod q}} e(\beta_0 C(\boldsymbol{x}) + \boldsymbol{\beta} \cdot \boldsymbol{x}).$$

By [Browning 2009, Lemma 8.1], we now have

$$S_{\boldsymbol{y}}(q, \beta_0, \boldsymbol{\beta}) = q^{-n} \int_{[-P,P]^n} e(\beta_0 C(\boldsymbol{x}) + \boldsymbol{\beta} \cdot \boldsymbol{x}) \, d\boldsymbol{x} + O\left(\frac{P^{n-1}(1 + P^3|\beta_0| + P|\boldsymbol{\beta}|)}{q^{n-1}}\right)$$

$$= (P/q)^n I_u(P^3 \beta_0, P\boldsymbol{\beta}) + O\left(\frac{P^{n-1}(1 + P^3|\beta_0| + P|\boldsymbol{\beta}|)}{q^{n-1}}\right).$$

Substituting this into (9-3) yields (9-2). □

Suppose $\alpha_0 \in \mathfrak{N}'(q, a)$ with $q \in \mathfrak{Q}$. With $\boldsymbol{\lambda} = \boldsymbol{\lambda}^*$ and a_v the nearest integer to $q\lambda_v$ ($1 \leqslant v \leqslant n$), put (3-1) and $S_u^*(\alpha_0, \boldsymbol{k}) = g_u^*(\alpha_0, \boldsymbol{\lambda}^*)$. In light of the inequalities

$$1 \leqslant q \leqslant C_1 P^{2\theta_0}, \qquad |q\beta_0| < P^{2\theta_0 - 3}, \qquad |q\boldsymbol{\beta}| < P^{7\theta_0 - 1},$$

the error bound (9-2) implies that

$$S_u(\alpha_0, \boldsymbol{k}) - S_u^*(\alpha_0, \boldsymbol{k}) \ll P^{n-1+7\theta_0}.$$

Since

$$\text{meas}\left(\bigcup_{q \in \mathfrak{Q}} \mathfrak{N}'(q)\right) \ll P^{4\theta_0 - 3},$$

it now suffices to prove that

$$\sum_{q \in \mathfrak{Q}} \int_{\mathfrak{N}'(q)} S_u^*(\alpha_0, \boldsymbol{k}) \, d\alpha_0 = o(P^{n-3}). \tag{9-4}$$

The final ingredient that we need for a satisfactory mean-value estimate is an unweighted analogue of (5-1).

Lemma 9.2. *We have*

$$I_u(\gamma_0, \boldsymbol{\gamma}) \ll \frac{1}{1 + |\gamma_0|^{h/8-\varepsilon} + |\boldsymbol{\gamma}|^{1/3}}. \tag{9-5}$$

Proof. Since $I_u(\gamma_0, \boldsymbol{\gamma}) \ll 1$, we may assume that $|\gamma_0| + |\boldsymbol{\gamma}|$ is large. Specializing $(q, a, \boldsymbol{a}) = (1, 0, \boldsymbol{0})$ in (9-2), it follows that

$$I_u(\gamma_0, \boldsymbol{\gamma}) = P^{-n} g_u(\gamma_0/P^3, \boldsymbol{\gamma}/P) + O(P^{-1}(|\gamma_0| + |\boldsymbol{\gamma}|)).$$

Since $I_u(\gamma_0, \boldsymbol{\gamma})$ is independent of P, we are free to choose $P = (|\gamma_0| + |\boldsymbol{\gamma}|)^n$. By Lemma 5.1, with $\xi = \varepsilon/n^2$, we now have

$$I_u(\gamma_0, \boldsymbol{\gamma}) \ll P^{\varepsilon/n^2} |\gamma_0|^{-h/8} + \frac{|\gamma_0| + |\boldsymbol{\gamma}|}{P} \ll P^{\varepsilon/n^2} |\gamma_0|^{-h/8},$$

so

$$I_u(\gamma_0, \boldsymbol{\gamma}) \ll \frac{(|\gamma_0| + |\boldsymbol{\gamma}|)^{\varepsilon/n}}{|\gamma_0|^{h/8}}. \tag{9-6}$$

Let C_4 be a large positive constant. As $|\gamma_0| + |\boldsymbol{\gamma}|$ is large and $h \geqslant 17$, the desired inequality follows from (9-6) if $|\boldsymbol{\gamma}| < C_4|\gamma_0|$. Thus, we may assume that $|\boldsymbol{\gamma}| \geqslant C_4|\gamma_0|$. Choose $j \in \{1, 2, \ldots, n\}$ such that $|\boldsymbol{\gamma}| = |\gamma_j|$. Observe that

$$I_u(\gamma_0, \boldsymbol{\gamma}) \ll \sup_{-1 \leqslant x_i \leqslant 1 \ (i \neq j)} \left| \int_{-1}^{1} e(\gamma_0 C(\boldsymbol{x}) + \gamma_j x_j) \, dx_j \right|.$$

As $|\gamma_j| \geqslant C_4|\gamma_0|$, the bound in [Vaughan 1997, Theorem 7.3] now implies that

$$I_u(\gamma_0, \boldsymbol{\gamma}) \ll |\gamma_j|^{-1/3} = |\boldsymbol{\gamma}|^{-1/3}.$$

Combining this with (9-6) gives

$$I_u(\gamma_0, \boldsymbol{\gamma}) \ll \frac{(|\gamma_0| + |\boldsymbol{\gamma}|)^{\varepsilon/n}}{|\gamma_0|^{h/8} + |\boldsymbol{\gamma}|^{1/3}(|\gamma_0| + |\boldsymbol{\gamma}|)^{\varepsilon/n}} \ll \frac{|\boldsymbol{\gamma}|^{\varepsilon/n}}{|\gamma_0|^{h/8} + |\boldsymbol{\gamma}|^{1/3+\varepsilon/n}}.$$

Considering cases and recalling that $h \leqslant n$, we now have

$$I_u(\gamma_0, \boldsymbol{\gamma}) \ll \frac{1}{|\gamma_0|^{h/8-\varepsilon} + |\boldsymbol{\gamma}|^{1/3}}.$$

This delivers the sought estimate (9-5) since $|\gamma_0| + |\boldsymbol{\gamma}| \gg 1$. $\qquad \square$

Let $\alpha_0 \in \mathfrak{N}'(q, a)$, with $q \in \mathfrak{Q}$ and $(a, q) = 1$. The inequalities (3-6), (9-5), and $h \geqslant 17$ give

$$S_u^*(\alpha_0, \boldsymbol{k}) \ll P^n q^{-2-\varepsilon} (1 + P^3|\alpha_0 - a/q|)^{-1-\varepsilon} F(\boldsymbol{k}; q, P)^\varepsilon,$$

where

$$F(\boldsymbol{k}; q, P) = \prod_{v \leqslant n} (q + P\|q\lambda_v^*\|)^{-1}.$$

Therefore,

$$\sum_{q \in \mathfrak{Q}} \int_{\mathfrak{N}'(q)} |S_u^*(\alpha_0, \boldsymbol{k})| F(\boldsymbol{k}; q, P)^{-\varepsilon} \, d\alpha_0 \ll P^n \sum_{q \in \mathbb{N}} q^{-1-\varepsilon} \int_{\mathbb{R}} (1 + P^3|\beta_0|)^{-1-\varepsilon} \, d\beta_0$$

$$\ll P^{n-3}. \tag{9-7}$$

As $\boldsymbol{k}$ is a fixed nonzero vector, we have $1 \ll |\boldsymbol{k}| \ll 1$. In particular, by (6-2), we have $1 \ll |\Lambda \boldsymbol{k}| \ll 1$. Thus, Corollary 6.2 gives

$$F(\boldsymbol{k}; q, P) \leqslant \mathcal{F}(\boldsymbol{k}; P) = o(1)$$

as $P \to \infty$. Coupling this with (9-7) yields (9-4), completing the proof of Theorem 1.3.

10. The singular locus

The *singular locus* of C is the complex variety cut out by vanishing of ∇C. Let $\mathcal{S}$ be the singular locus of C, and let σ be the affine dimension of $\mathcal{S}$. Let h be the h-invariant of C, and let $A_1, \ldots, A_h, B_1, \ldots, B_h$ be as in (1-1). Then $\mathcal{S}$ contains the variety $\{A_1 = \cdots = A_h = B_1 = \cdots = B_h = 0\}$, and so $\sigma \geqslant n - 2h$. In particular, the conclusions of Theorem 1.1 are valid if the hypothesis (1-2) is replaced by the condition

$$n - \sigma > 32 + 16r.$$

Thus, these conclusions hold for any nonsingular cubic form in more than $32 + 16r$ variables.

However, one could improve upon this using a direct approach. Note that h could be replaced by $n - \sigma$ in Lemma 2.1; the resulting lemma would be almost identical to [Birch 1962, Lemma 4.3], and again the weights and lower-order terms are of no significance. The remainder of the analysis would be identical and lead us to conclude that Theorem 1.1 is valid with h replaced by $n - \sigma$. We could even use the same argument for positivity of the singular series, for if $r \geqslant 1$, then

$$h \geqslant \frac{n - \sigma}{2} > \frac{16 + 8r}{2} \geqslant 12 > 9.$$

In particular, the conclusions of Theorem 1.1 would hold for any nonsingular cubic form in more than $16 + 8r$ variables. Similarly, Theorem 1.3 is valid with h replaced by $n - \sigma$, and so its conclusion would hold for any nonsingular cubic form in more than sixteen variables.

Finally, we challenge the reader to improve upon these statements using more sophisticated technology, for instance to reduce the number of variables needed to solve the system (1-7). It is likely that van der Corput differencing could be profitably incorporated, similarly to [Heath-Brown 2007]. One might also hope to do better by assuming that C is nonsingular, as in [Heath-Brown 1983].

Acknowledgments

References

[Bentkus and Götze 1999] V. Bentkus and F. Götze, "Lattice point problems and distribution of values of quadratic forms", *Ann. of Math.* (2) **150**:3 (1999), 977–1027. MR 2001b:11087 Zbl 0979.11048

[Birch 1962] B. J. Birch, "Forms in many variables", *Proc. Roy. Soc.* (*A*) **265** (1962), 245–263. MR 27 #132 Zbl 0103.03102

[Browning 2009] T. D. Browning, *Quantitative arithmetic of projective varieties*, Progress in Mathematics **277**, Birkhäuser, Basel, 2009. MR 2010i:11004 Zbl 1188.14001

[Browning et al. 2015] T. D. Browning, R. Dietmann, and D. R. Heath-Brown, "Rational points on intersections of cubic and quadric hypersurfaces", *J. Inst. Math. Jussieu* **14**:4 (2015), 703–749. MR 3394125 Zbl 1327.11043

[Cassels 1957] J. W. S. Cassels, *An introduction to Diophantine approximation*, Cambridge Tracts in Mathematics and Mathematical Physics **45**, Cambridge University, New York, 1957. MR 19,396h Zbl 0077.04801

[Dani and Margulis 1993] S. G. Dani and G. A. Margulis, "Limit distributions of orbits of unipotent flows and values of quadratic forms", pp. 91–137 in *I. M. Gelfand Seminar*, edited by S. Gelfand and S. Gindikin, Advances in Soviet Mathematics **16**, American Mathematical Society, Providence, RI, 1993. MR 95b:22024 Zbl 0814.22003

[Davenport 1959] H. Davenport, "Cubic forms in thirty-two variables", *Philos. Trans. Roy. Soc. London.* (*A*) **251**:993 (1959), 193–232. MR 21 #4136 Zbl 0084.27202

[Davenport 2005] H. Davenport, *Analytic methods for Diophantine equations and Diophantine inequalities*, 2nd ed., Cambridge University, 2005. MR 2006a:11129 Zbl 1125.11018

[Davenport and Heilbronn 1946] H. Davenport and H. Heilbronn, "On indefinite quadratic forms in five variables", *J. London Math. Soc.* **21**:3 (1946), 185–193. MR 8,565e Zbl 0060.11914

[Davenport and Lewis 1964] H. Davenport and D. J. Lewis, "Non-homogeneous cubic equations", *J. London Math. Soc.* **39** (1964), 657–671. MR 29 #4731 Zbl 0125.02402

[Eskin et al. 1998] A. Eskin, G. A. Margulis, and S. Mozes, "Upper bounds and asymptotics in a quantitative version of the Oppenheim conjecture", *Ann. of Math.* (2) **147**:1 (1998), 93–141. MR 99a:11043 Zbl 0906.11035

[Freeman 2002] D. E. Freeman, "Asymptotic lower bounds and formulas for Diophantine inequalities", pp. 57–74 in *Number theory for the millennium, II* (Urbana, IL, 2000), edited by M. A. Bennett et al., A K Peters, Natick, MA, 2002. MR 2003j:11035 Zbl 1042.11022

[Graham and Kolesnik 1991] S. W. Graham and G. Kolesnik, *Van der Corput's method of exponential sums*, London Mathematical Society Lecture Note Series **126**, Cambridge University, 1991. MR 92k:11082 Zbl 0713.11001

[Heath-Brown 1983] D. R. Heath-Brown, "Cubic forms in ten variables", *Proc. London Math. Soc.* (3) **47**:2 (1983), 225–257. MR 85b:11025 Zbl 0494.10012

[Heath-Brown 1996] D. R. Heath-Brown, "A new form of the circle method, and its application to quadratic forms", *J. Reine Angew. Math.* **481** (1996), 149–206. MR 97k:11139 Zbl 0857.11049

[Heath-Brown 2007] D. R. Heath-Brown, "Cubic forms in 14 variables", *Invent. Math.* **170**:1 (2007), 199–230. MR 2010a:11063 Zbl 1135.11031

[Margulis 1989] G. A. Margulis, "Discrete subgroups and ergodic theory", pp. 377–398 in *Number theory, trace formulas and discrete groups* (Oslo, 1987), edited by K. E. Aubert et al., Academic Press, Boston, 1989. MR 90k:22013a Zbl 0675.10010

[Sargent 2014] O. Sargent, "Equidistribution of values of linear forms on quadratic surfaces", *Algebra Number Theory* **8**:4 (2014), 895–932. MR 3248989 Zbl 1314.11018

[Schmidt 1982a] W. M. Schmidt, "On cubic polynomials, IV: Systems of rational equations", *Monatsh. Math.* **93**:4 (1982), 329–348. MR 83m:10063 Zbl 0481.10015

[Schmidt 1982b] W. M. Schmidt, "Simultaneous rational zeros of quadratic forms", pp. 281–307 in *Séminaire de Théorie des Nombres: Séminaire Delange–Pisot–Poitou* (Paris, 1980–1981), edited by M.-J. Bertin, Progress in Mathematics **22**, Birkhäuser, Boston, 1982. MR 84g:10041 Zbl 0492.10017

[Schmidt 1985] W. M. Schmidt, "The density of integer points on homogeneous varieties", *Acta Math.* **154**:3–4 (1985), 243–296. MR 86h:11027 Zbl 0561.10010

[Vaughan 1997] R. C. Vaughan, *The Hardy–Littlewood method*, 2nd ed., Cambridge Tracts in Mathematics **125**, Cambridge University, 1997. MR 98a:11133 Zbl 0868.11046

[Wooley 2003] T. D. Wooley, "On Diophantine inequalities: Freeman's asymptotic formulae", in *Proceedings of the Session in Analytic Number Theory and Diophantine Equations* (Bonn, 2002), edited by D. R. Heath-Brown and B. Z. Moroz, Bonner Mathematische Schriften **360**, Universität Bonn, 2003. MR 2005d:11048 Zbl 1196.11055

sam.chow@bristol.ac.uk   *School of Mathematics, University of Bristol,*
                                University Walk, Bristol, BS8 1TW, United Kingdom

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.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

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