Algebra & Number Theory

Volume 19
2025
No. 3

msp

Algebra & Number Theory

msp.org/ant

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2025 is US $565/year for the electronic version, and $820/year (+$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

ALGEBRA AND NUMBER THEORY 19:3 (2025)
https://doi.org/10.2140/ant.2025.19.415

The Lyndon–Demushkin method and crystalline lifts of G_2-valued Galois representations

Zhongyipan Lin

We develop obstruction theory for lifting characteristic-p local Galois representations valued in reductive groups of type B_l, C_l, D_l or G_2. An application of the Emerton–Gee stack then reduces the existence of crystalline lifts to a purely combinatorial problem when p is not too small.

As a toy example, we show for all local fields $K/\mathbb{Q}_p$, with $p > 3$, all representations $\bar{\rho} : G_K \to G_2(\bar{\mathbb{F}}_p)$ admit a crystalline lift $\rho : G_K \to G_2(\bar{\mathbb{Z}}_p)$, where G_2 is the exceptional Chevalley group of type G_2.

1. Introduction

Let $K/\mathbb{Q}_p$ be a p-adic field. Let G be a connected reductive group over $\bar{\mathbb{Z}}_p$. Let $\bar{\rho} : G_K \to G(\bar{\mathbb{F}}_p)$ be a Galois representation.

We will study whether there exist crystalline lifts of $\bar{\rho}$ to $G(\bar{\mathbb{Z}}_p)$. This question has been raised in various contexts, such as irreducible geometric Galois representations [Fakhruddin et al. 2018], the Serre weight conjecture [Gee et al. 2018] and ramification theory [Caruso and Liu 2011].

The pursuit of constructing characteristic-0 lifts of Galois representations (at least in higher dimensions) is, however, resistant to elementary techniques. Böckle [2003] was able to lift mod ϖ representations to a mod ϖ^2 representation for $G = \mathrm{GL}_N$. Muller [2013] constructed crystalline lifts of mod ϖ representations valued in $G = \mathrm{GL}_3$, and Emerton and Gee [2023] worked the GL_N-case for all N. Our earlier work [Lin 2022] answers this question for semisimple representations valued in general reductive groups G.

The method of [Emerton and Gee 2023] is purely local, and is based on an analysis of Galois cohomology. The image group $\bar{\rho}(G_K)$ is either an irreducible subgroup of $G(\bar{\mathbb{F}}_p)$ or factors through a proper maximal parabolic P of G. In the former case, our previous work [Lin 2022] shows $\bar{\rho}$ always admits a crystalline lift. In this paper, we focus on the latter case. Let $P = L \rtimes U_P$ be the Levi decomposition. Let $\bar{r} : G_K \xrightarrow{\bar{\rho}} P(\bar{\mathbb{F}}_p) \to L(\bar{\mathbb{F}}_p)$ be the Levi factor of $\bar{\rho}$. Then $\bar{\rho}$ defines a 1-cocycle $[\bar{c}] \in H^1(G_K, U_P(\bar{\mathbb{F}}_p))$. What we will actually do is to construct a lift $r : G_K \to L(\bar{\mathbb{Z}}_p)$ of $\bar{r}$ and a lift $[c] \in H^1(G_K, U_P(\bar{\mathbb{Z}}_p))$ of $[\bar{c}]$.

In the GL_N-case, all maximal proper parabolics have abelian unipotent radical, so it suffices to consider abelian cohomology. When G is not GL_N, parabolic subgroups with abelian unipotent radical are rare. For example, when G is the exceptional group G_2, all parabolics have nonabelian unipotent radical.

MSC2020: 11F80.
Keywords: Galois representations, exceptional group.

Fortunately, for groups of type A, B, C, D or G_2, the relevant nonabelian Galois cohomology can be replaced by abelian Galois cohomology equipped with a cup product structure and the strategy considered in [Emerton and Gee 2023] can be adapted to work. In this paper, we focus on the G_2-case, and prove the following theorem:

Theorem A (Theorem 7.1.3). *Assume $p > 3$. Every mod ϖ Galois representation valued in the exceptional group G_2,*

$$\bar{\rho} : G_K \to G_2(\overline{\mathbb{F}}_p),$$

admits a crystalline lift $\rho^\circ : G_K \to G_2(\overline{\mathbb{Z}}_p)$.

Moreover, if $\bar{\rho}$ factors through a maximal parabolic $P = L \ltimes U$ and the Levi factor $\bar{r}_{\bar{\rho}} : G_K \to L(\overline{\mathbb{F}}_p)$ of $\bar{\rho}$ admits a Hodge–Tate regular and crystalline lift $r_1 : G_K \to L(\overline{\mathbb{Z}}_p)$ such that the adjoint representation $G_K \xrightarrow{r_1} L(\overline{\mathbb{Z}}_p) \to \mathrm{GL}(\mathrm{Lie}(U(\overline{\mathbb{Z}}_p)))$ has Hodge–Tate weights slightly less than $\underline{0}$ (Definition 3.0.4), then ρ° can be chosen such that it factors through the maximal parabolic P and its Levi factor r_{ρ° lies on the same irreducible component of the spectrum of the crystalline lifting ring that r_1 does.

1.1. *Overview of the method and comparison with* [Lin 2023a].

To establish the existence of crystalline lifts, we proceed in four steps:

Step 1. Construct explicit cochain complexes *equipped with a natural cup product structure* that compute abelian Galois cohomology.

Step 2. Show that the cup product considered in Step 1 is nontrivial in certain special cases.

Step 3. Compute the dimension of certain substacks of the reduced Emerton–Gee stack.

Step 4. Invoke the machinery of [Emerton and Gee 2023] to produce crystalline lifts.

After the first draft of this paper was written, we have a more conceptual understanding of some constructions made in this paper; see the introduction section of [Lin 2023a]. For example, Sections 2 and 4 of this paper are conceptualized under the notion of *Heisenberg equations*. In [loc. cit.], we also establish the existence of de Rham lifts for many classical groups and in particular the existence of crystalline lifts for unramified unitary groups.

However, from the technical perspective, [loc. cit.] parallels this paper, instead of upgrades this paper. In [loc. cit.], we use *Herr complexes* as the explicit cochain complex computing Galois cohomology. Herr complexes are infinite-dimensional cochain complexes and are often not amenable to computation by hand. We can truncate Herr complexes to a finite-dimensional cochain complex but the truncation can't be made explicit in general. The upside of Herr complexes is better functoriality and in the case of classical groups, we can usually reduce the problems to the GL_n-case, which is well-understood.

In this paper, we use Lyndon's cochain complexes instead. Everything in this paper is totally explicit and is computable by hand or by a computer algebra system. The downside of this approach is that the complexity of computation grows exponentially, and quickly becomes out of hand for large-ranked classical groups.

We don't know how to deal with Herr complexes for exceptional groups because of their implicit nature, and the approach in this paper is still the only one we are aware of. In this paper, we establish the existence of crystalline lifts for the exceptional group G_2, which illustrates the usefulness of Lyndon's cochain complexes. Because of its explicit nature, our approach can potentially be extended to deal with more general exceptional groups, after upgrading the cup product structure to more complicated higher Massey product structures.

1.2. ***Obstruction theory for crystalline lifting.*** In this paper, we consider the case where U_P admits a quotient U such that

- the adjoint group $U^{\mathrm{ad}} := U/Z(U)$ is abelian;
- the center $Z(U)$ is isomorphic to $\mathbb{G}_a$; and
- there is a bijection of obstructions $H^2(G_K, U_P(\overline{\mathbb{F}}_p)) \cong H^2(G_K, U(\overline{\mathbb{F}}_p))$.

We call U a Heisenberg quotient of U_P. When G is of type B_l, C_l, D_l or G_2, it is always possible to choose a parabolic P whose unipotent radical admits a Heisenberg quotient (see Section 1.1).

Let Spec R be an irreducible component of a crystalline lifting ring Spec $R_{\bar{r}}^{\mathrm{crys},\underline{\lambda}}$ (Section 5.0.2) of $\bar{r}$. Let $r^{\mathrm{univ}} : G_K \to L(R)$ be the universal family. The Levi factor group acts on U via conjugation $\phi : L \to \mathrm{Aut}(U)$. Write $\phi^{\mathrm{ad}} : L \to \mathrm{GL}(U^{\mathrm{ad}})$ and $\phi^{z} : L \to \mathrm{GL}(Z(U))$ for the graded pieces of ϕ.

The theorem we prove is:

Theorem B (Theorem 5.2.1). *Let $[\bar{c}] \in H^1(G_K, U(\mathbb{F}))$ be a characteristic-p cocycle, where U is a Heisenberg quotient of U_P.*

Assume

(1) $H^2(G_K, \phi^{\mathrm{ad}}(r^{\mathrm{univ}}))$ *is sufficiently generically regular* (*Definition 5.1.1*) *and set-theoretically supported on the special fiber of* Spec R;

(2) $p \neq 2$;

(3) *there exists a finite Galois extension K'/K of prime-to-p degree such that $\phi(\bar{r})|_{G_{K'}}$ is Lyndon–Demushkin* (*Definition 2.0.2*); *and*

(4) *there exists a $\overline{\mathbb{Z}}_p$-point of* Spec R *which is mildly regular* (*Definition 3.0.1*) *when restricted to $G_{K'}$.*

Then there exists a $\overline{\mathbb{Z}}_p$-point of Spec R *which gives rise to a Galois representation $r^\circ : G_K \to L(\overline{\mathbb{Z}}_p)$ such that if we endow $U(\overline{\mathbb{Z}}_p)$ with the G_K-action $G_K \xrightarrow{r^\circ} L(\overline{\mathbb{Z}}_p) \xrightarrow{\phi} \mathrm{Aut}(U(\overline{\mathbb{Z}}_p))$, the cocycle $[\bar{c}]$ has a characteristic-0 lift $[c] \in H^1(G_K, U(\overline{\mathbb{Z}}_p))$.*

Remark. Assumption (3) is automatically satisfied if p is sufficiently large, and (4) is automatically satisfied if p is sufficiently large and the labeled Hodge–Tate weights $\phi^{\mathrm{ad}}(\underline{\lambda})$ are slightly less than 0 (Definition 3.0.4).

Example 1.2.1 ($G = \mathrm{GL}_3$). Let $\bar{\rho} : G_K \to \mathrm{GL}_3(\overline{\mathbb{F}}_p)$ be a completely reducible Galois representation. There are two ways of encoding the data of $\bar{\rho}$ as a 1-cocycle in Galois cohomology.

(I) Use the fact $\bar{\rho}$ factors through a maximal parabolic

$$P=\begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{bmatrix}=\begin{bmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & * \end{bmatrix}\ltimes\begin{bmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}=L\ltimes A,$$

where $A\cong\mathbb{G}_a^{\oplus 2}$ is a rank-2 abelian group. Let $\bar{r}:G_K\xrightarrow{\bar{\rho}}P(\overline{\mathbb{F}}_p)\to L(\overline{\mathbb{F}}_p)$ be the Levi factor of $\bar{\rho}$. The information of $\bar{\rho}$ is encoded in a 1-cocycle $[\bar{c}]\in H^1(G_K,\phi(\bar{r}))=:H^1(G_K,A(\overline{\mathbb{F}}_p))$. We first construct a lift $r^\circ:G_K\to\mathrm{GL}_2(\overline{\mathbb{Z}}_p)$ of $\bar{r}$. Then we construct a lift $[c]\in H^1(G_K,A(\overline{\mathbb{Z}}_p))$ of $[\bar{c}]$.

(II) Use the fact $\bar{\rho}$ factors through a Borel (minimal parabolic)

$$B=\begin{bmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{bmatrix}=\begin{bmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{bmatrix}\ltimes\begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}=T\ltimes H,$$

where the Levi group T is a maximal torus, and the unipotent radical H is the Heisenberg group. Let $\bar{r}:G_K\to T(\overline{\mathbb{F}}_p)$ be the Levi factor of $\bar{\rho}$. To reconstruct $\bar{\rho}$ from $\bar{r}$, we only need the information of a 1-cocycle $[\bar{c}]\in H^1(G_K,H(\overline{\mathbb{F}}_p))$. We first construct a lift of $\bar{r}$, and then construct a lift of $\bar{c}$. Now $H^1(G_K,H(\overline{\mathbb{F}}_p))$ is nonabelian Galois cohomology.

We make use of the graded structure of $\operatorname{Lie}H$ when we construct a lift of $[\bar{c}]$. We have a short exact sequence

$$1\to\begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\to H\to\begin{bmatrix} 1 & * & \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}\to 1.$$

We will first construct a lift modulo $Z(H)$, and then extend the lift modulo $Z(H)$ to a cocycle on the whole unipotent radical H.

Theorem B applies in this situation, so we have a new proof for the group GL_3.

1.2.2. We have a short exact sequence of groups $0\to Z(U)\to U\to U^{\mathrm{ad}}\to 0$. Since $Z(U)$ is a central, normal subgroup, we have a long exact sequence of pointed sets

$$H^1(G_K,Z(U))\to H^1(G_K,U)\to H^1(G_K,U^{\mathrm{ad}})\xrightarrow{\delta}H^2(G_K,Z(U)).$$

Note that δ is a quadratic form, and there is an associated bilinear form

$$\cup:H^1(G_K,U^{\mathrm{ad}})\times H^1(G_K,U^{\mathrm{ad}})\to H^2(G_K,Z(U))$$

defined by $x\cup y=(\delta(x+y)-\delta(x)-\delta(y))/2$.

The technical heart of this paper is an analysis of $\cup$ on the cochain/cocycle level. So we need a finite cochain complex computing Galois cohomology which interacts nicely with the bilinear form $\cup$. Thanks to the theory of Demushkin groups, there is an explicitly defined cochain complex (the so-called Lyndon–Demushkin complex) which computes $H^\bullet(G_{K'},U^{\mathrm{ad}})$ and $H^\bullet(G_{K'},Z(U))$ after a finite Galois extension K'/K. When $[K':K]$ is prime to p, we can fully understand cup products on the cochain/cocycle level via Lyndon–Demushkin complexes endowed with $G_K/G_{K'}$-action.

We have the following nice obstruction theory:

Theorem C (Corollary 4.3.4). *Let $p \neq 2$ be a prime integer. Let L be a reductive group over $\mathcal{O}_E$ and fix an algebraic group homomorphism $L \to \operatorname{Aut}(U)$. Let $r : G_K \to L(\mathcal{O}_E)$ be a Galois representation.*

If there exists a finite Galois extension K'/K of prime-to-p degree such that $r|_{G_{K'}}$ is Lyndon–Demushkin and mildly regular, then there is a short exact sequence of pointed sets

$$H^1(G_K, U(\overline{\mathbb{Z}}_p)) \to H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{\delta} H^2(G_K, U^{\text{ad}}(\overline{\mathbb{Z}}_p)),$$

where δ has a factorization $H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{p} H^1(G_K, U^{\text{ad}}(\overline{\mathbb{F}}_p)) \to H^2(G_K, U^{\text{ad}}(\overline{\mathbb{Z}}_p))$.

1.3. *Organization.* In Section 2, we review the results of Lyndon and Demushkin and establish some notation. Sections 3 and 4 form the technical heart of this paper. Sections 5 and 6 are mild generalizations of results from [Emerton and Gee 2023]. The proofs are almost unchanged and we often just sketch the ideas of the proof and invite the readers to look at the proofs of [Emerton and Gee 2023].

We prove the main theorem in Section 7.

2. Lyndon–Demushkin theory

Assume $p \neq 2$. Let $K/\mathbb{Q}_p$ be a finite extension containing the p-th root of unity. The maximal pro-p quotient of the absolute Galois group G_K has a very nice description. The following well-known theorem can be found, for example, in [Serre 2002, Section II.5.6].

Theorem 2.0.1. *Let $G_K(p)$ be the maximal pro-p quotient of G_K. Then $G_K(p)$ is the pro-p completion of the one-relator group*

$$\langle x_0, \dots, x_{n+1} \mid x_0^q (x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1}) \rangle,$$

where $n = [K : \mathbb{Q}_p]$, and $q = p^s$ is the largest power of p such that K contains the q-th roots of unity. Here $(x, y) = xyx^{-1}y^{-1}$.

Definition 2.0.2. A continuous profinite G_K-module A is said to be *Lyndon–Demushkin* if the image of $G_K \to \operatorname{Aut}(A)$ is a pro-p group.

2.1. *Comparing cohomology of Demushkin groups and Galois cohomology.* Let Γ^{disc} be the discrete group with one relator

$$\langle x_0, \dots, x_n, x_{n+1} \mid x_0^q (x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1}) \rangle.$$

Let $K/\mathbb{Q}_p$ be a p-adic field containing the group of p-th root of unity. Let A be a Lyndon–Demushkin G_K-module. Write $H^\bullet(\Gamma^{\text{disc}}, A)$ for the usual group cohomology, and write $H^\bullet(G_K, A)$ for the continuous profinite cohomology.

Note that there is a functorial map

$$H^\bullet(G_K, A) \to H^\bullet(\Gamma^{\text{disc}}, A) \tag{2-1}$$

induced from the forgetful functor $\operatorname{Mod}_{\text{cont}}(G_K(p)) \to \operatorname{Mod}(\Gamma^{\text{disc}})$.

Lemma 2.1.1. *Let $\mathbb{F}_p$ be the G_K-module with trivial G_K-action. Then* (2-1) *induces isomorphisms*:

(1) $H^1(G_K, \mathbb{F}_p) = H^1(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)$.

(2) $H^2(G_K, \mathbb{F}_p) = H^2(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)$.

Proof. (1) We have

$$\begin{aligned} H^1(G_K, \mathbb{F}_p) &= \mathrm{Hom}_{\mathrm{cont}}(G_K, \mathbb{F}_p) = \mathrm{Hom}_{\mathrm{cont}}(G_K(p), \mathbb{F}_p), \\ H^1(\Gamma^{\mathrm{disc}}, \mathbb{F}_p) &= \mathrm{Hom}(\Gamma^{\mathrm{disc}}, \mathbb{F}_p). \end{aligned}$$

Note that $\mathrm{Hom}_{\mathrm{cont}}(G_K(p), \mathbb{F}_p) = \mathrm{Hom}(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)$ because $G_K(p)$ is the pro-p completion of Γ^{disc}.

(2) We have a commutative diagram

$$\begin{tikzcd} H^1(G_K, \mathbb{F}_p) \times H^1(G_K, \mathbb{F}_p) \arrow[r, "\cup"] \arrow[d] & H^2(G_K, \mathbb{F}_p) \arrow[d] \\ H^1(\Gamma^{\mathrm{disc}}, \mathbb{F}_p) \times H^1(\Gamma^{\mathrm{disc}}, \mathbb{F}_p) \arrow[r, "\cup"] & H^2(\Gamma^{\mathrm{disc}}, \mathbb{F}_p) \end{tikzcd}$$

Note that the first row is a nondegenerate pairing, and $H^2(G_K, \mathbb{F}_p) \cong \mathbb{F}_p$ by local Tate duality. By Lyndon's theorem or Corollary 2.2.2, we have $H^2(\Gamma^{\mathrm{disc}}, \mathbb{F}_p) \cong \mathbb{F}_p$. So it remains to show the cup product of the second row is nontrivial. Let $[c_1]$, $[c_2] \in H^1(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)$. $[c_1] \cup [c_2] = 0$ if and only if there exists a group homomorphism

$$\Gamma^{\mathrm{disc}} \to \begin{bmatrix} 1 & c_1 & * \\ & 1 & c_2 \\ & & 1 \end{bmatrix}$$

for some $*$. Indeed, if $c_1 \cup c_2 = dz$ for some $z \in C^1(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)$, then

$$\Gamma^{\mathrm{disc}} \to \begin{bmatrix} 1 & c_1 & z \\ & 1 & c_2 \\ & & 1 \end{bmatrix}$$

is a group homomorphism by unravelling the definition of cup products; here $C^1(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)$ is the usual cochain group defining group cohomology. Define $c_i : \Gamma^{\mathrm{disc}} \to \mathbb{F}_p$ by sending x_i to 1 and other generators to 0, $i = 0, 1$. Then it is clear $[c_1] \cup [c_2] \neq 0$. □

Corollary 2.1.2. *Let A be a finite $\mathbb{F}_p$-vector space endowed with Lyndon–Demushkin G_K-action. Then there is a canonical isomorphism $H^\bullet(G_K, A) = H^\bullet(\Gamma^{\mathrm{disc}}, A)$.*

Proof. Let $G_K(p)$ be the maximal pro-p quotient of G_K. Then A is a $G_K(p)$-module. Since $G_K(p)$ is a pro-p group, A must contain the trivial representation $\mathbb{F}_p$. In particular, there is a short exact sequence

$$0 \to \mathbb{F}_p \to A \to A' \to 0$$

which induces the long exact sequence

$$\begin{tikzcd}
H^0(G_K, A') \arrow[r] \arrow[d] & H^1(G_K, \mathbb{F}_p) \arrow[r] \arrow[d] & H^1(G_K, A) \arrow[r] \arrow[d] & H^1(G_K, A') \arrow[r] \arrow[d] & H^2(G_K, \mathbb{F}_p) \arrow[d] \\
H^0(\Gamma^{\mathrm{disc}}, A') \arrow[r] & H^1(\Gamma^{\mathrm{disc}}, \mathbb{F}_p) \arrow[r] & H^1(\Gamma^{\mathrm{disc}}, A) \arrow[r] & H^1(\Gamma^{\mathrm{disc}}, A') \arrow[r] & H^2(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)
\end{tikzcd}$$

We apply induction on the length of A. By the five lemma, we have $H^1(G_K, A) = H^1(\Gamma^{\mathrm{disc}}, A)$.

We also have the long exact sequence

$$\begin{tikzcd}
H^1(G_K, A') \arrow[r] \arrow[d] & H^2(G_K, \mathbb{F}_p) \arrow[r] \arrow[d] & H^2(G_K, A) \arrow[r] \arrow[d] & H^2(G_K, A') \arrow[r] \arrow[d] & H^3(G_K, \mathbb{F}_p) \arrow[d] \\
H^1(\Gamma^{\mathrm{disc}}, A') \arrow[r] & H^2(\Gamma^{\mathrm{disc}}, \mathbb{F}_p) \arrow[r] & H^2(\Gamma^{\mathrm{disc}}, A) \arrow[r] & H^2(\Gamma^{\mathrm{disc}}, A') \arrow[r] & H^3(\Gamma^{\mathrm{disc}}, \mathbb{F}_p)
\end{tikzcd}$$

By Lyndon's theorem, $H^3(\Gamma^{\mathrm{disc}}, \mathbb{F}_p) = 0$. By local Tate duality, $H^3(G_K, \mathbb{F}_p) = 0$. Again by the five lemma, we have $H^2(G_K, A) = H^2(\Gamma^{\mathrm{disc}}, A)$. Finally, both cohomology groups are supported on degrees [0, 2]. □

By induction on the order of A, (2-1) is an isomorphism for any finite p-power torsion group A.

Corollary 2.1.3. *Let A be a finite $\mathbb{Z}_p$-module endowed with the Lyndon–Demushkin G_K-action. Then there is a canonical isomorphism $H^\bullet(G_K, A) = H^\bullet(\Gamma^{\mathrm{disc}}, A)$.*

Proof. We have a short exact sequence for each $k > 0$,

$$0 \to \varprojlim_i{}^1 H^{k-1}(G_K, A/p^i A) \to H^k(G_K, A) \to \varprojlim_i H^k(G_K, A/p^i A) \to 0,$$

see, for example [Stacks, Tag 0BKN]; here $\varprojlim_i^1$ is the derived inverse limit. The first term is 0 due to the finiteness of the cohomology of torsion G_K-modules. So $H^k(G_K, A) = \varprojlim_i H^k(G_K, A/p^i A)$, and the corollary is reduced to the p-power torsion case.

We can do the same thing for the discrete cohomology. Since any finite $\mathbb{Z}_p$-module is p-adically complete, the Lyndon–Demushkin complex (see Section 2.3.7) computing $H^\bullet(\Gamma^{\mathrm{disc}}, A)$ is the inverse limit of the Lyndon–Demushkin complex mod p^i. So $H^k(\Gamma^{\mathrm{disc}}, A) = \varprojlim_i H^k(\Gamma^{\mathrm{disc}}, A/p^i)$. □

The lemma above tells us that, for our purposes, the cohomology groups of $G_K(p)$ can be computed via the discrete model. So we can make use of the fine machineries of combinatorial group theory.

2.2. *Discrete group cohomology of Demushkin groups.*

The main reference of this subsection is [Lyndon 1950].

Derivations. A derivation of a group G is a left G-module M, together with a map $D : G \to M$ such that $D(uv) = Du + uDv$.

Say F is a free group with generators $x_1, \ldots x_m$. Denote by dFJ the module of universal derivations. Then dFJ is the free $\mathbb{Z}[F]$-module with basis $\{dx_i \mid i = 1, \ldots, m\}$.

Let $u \in F$. We can write $du \in dFJ$ as a linear combination of the basis elements:

$$du = \sum \frac{\partial u}{\partial x_i}\, dx_i,$$

where $\frac{\partial u}{\partial x_i} \in \mathbb{Z}[F]$. The computation rules for $\frac{\partial u}{\partial x_i}$ can be found in the first line of page 654 of [Lyndon 1950].

Theorem 2.2.1 [Lyndon 1950, Theorem 11.1]. *Let $G = \langle x_1, \ldots, x_m | R\rangle$ be a one-relator group where $R = Q^q$ for no $q > 1$. Let K be any left G-module. Then*

$$H^2(G, K) \cong K \Big/ \left(\frac{\partial R}{\partial x_1}, \ldots \frac{\partial R}{\partial x_m}\right) K$$

and $H^n(G, K) = 0$ for all $n > 2$.

Corollary 2.2.2. *We have $H^2(\Gamma^{\mathrm{disc}}, \mathbb{F}_p) = \mathbb{F}_p$.*

Proof. We have

$$\begin{aligned}
\frac{\partial R}{\partial x_0} &= 1 + x_0 + \cdots + x_0^{q-2} + x_0^{q-1} x_1^{-1}, \\
\frac{\partial R}{\partial x_1} &= x_0^{q-1} x_1^{-1}(x_0 - 1), \\
\frac{\partial R}{\partial x_2} &= x_0^q (x_0, x_1) x_2^{-1}(x_3 - 1), \\
\frac{\partial R}{\partial x_3} &= x_0^q (x_0, x_1) x_2^{-1} x_3^{-1}(x_2 - 1), \\
&\vdots \\
\frac{\partial R}{\partial x_{2k}} &= x_0^q (x_0, x_1) \cdots (x_{2k-2}, x_{2k-1}) x_{2k}^{-1}(x_{2k+1} - 1), \\
\frac{\partial R}{\partial x_{2k+1}} &= x_0^q (x_0, x_1) \cdots (x_{2k-2}, x_{2k-1}) x_{2k}^{-1} x_{2k+1}^{-1}(x_{2k} - 1), \\
&\vdots
\end{aligned}$$

Since

$$H^2(\Gamma^{\mathrm{disc}}, \mathbb{F}_p) = \frac{\mathbb{F}_p}{(\partial R/\partial x_0, \ldots, \partial R/x_{n+1})},$$

it suffices to show

$$\frac{\partial R}{\partial x_0}\mathbb{F}_p = \cdots = \frac{\partial R}{\partial x_{n+1}}\mathbb{F}_p = 0.$$

Since $\mathbb{F}_p$ is a trivial G_K-module, it is clear that

$$\frac{\partial R}{\partial x_1}\mathbb{F}_p = \cdots = \frac{\partial R}{\partial x_{n+1}}\mathbb{F}_p = 0.$$

We also have $\frac{\partial R}{\partial x_0} = 1 + 1 + \cdots + 1 = q = 0 \bmod p$. □

Proposition 2.2.3. *Let A be a G_K-module whose underlying abelian group is a finitely generated $\mathbb{Z}_p$-module such that the image of G_K in* $\mathrm{Aut}(A)$ *is a pro-p group. Then*

$$H^2(G_K, A) \cong A \Big/ \left(\frac{\partial R}{\partial x_0}, \dots, \frac{\partial R}{\partial x_{n+1}} \right) A,$$

where $R = x_0^q (x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1})$.

Proof. Combine Corollary 2.1.3 and Lyndon's theorem. □

2.3. *Lyndon–Demushkin complex.*

2.3.1. *Abelian coefficient case.* Let A be a G_K-module whose underlying abelian group is a finitely generated $\mathbb{Z}_p$-module such that the image of G_K in $\mathrm{Aut}(A)$ is a pro-p group.

Then there is an explicit co-chain complex computing the Galois cohomology $H^\bullet(G_K, A)$.

Define $C^\bullet_{\mathrm{LD}}(A) = [C^0_{\mathrm{LD}}(A) \xrightarrow{d^1} C^1_{\mathrm{LD}}(A) \xrightarrow{d^2} C^2_{\mathrm{LD}}(A)]$ as the following cochain complex supported on degrees [0,2]:

$$A \xrightarrow{\begin{bmatrix} 1 - x_0 \\ \vdots \\ 1 - x_{n+1} \end{bmatrix}} A^{\oplus(n+2)} \xrightarrow{\begin{bmatrix} \partial R/\partial x_0 \\ \vdots \\ \partial R/\partial x_{n+1} \end{bmatrix}^T} A.$$

Then, by [Lyndon 1950, Theorem 11.1],

$$H^\bullet(C^\bullet_{LD}(A)) = H^\bullet(G_K, A).$$

The idea of a Lyndon–Demushkin complex is simple. A 1-cochain $c \in C^1_{\mathrm{LD}}(A)$ is simply a set-theoretical function

$$c : \{x_0, \dots, x_{n+1}\} \to A.$$

We can extend c to be a function on the free group

$$c : \langle x_0, \dots, x_{n+1} \rangle \to A$$

by setting $c(gh) := c(g) + g \cdot c(h)$ for any g, h in the free group with $n+2$ generators. Let

$$R = x_0^q (x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1})$$

be the single relation defining the Demushkin group. The differential operator $d^2 : C^1_{\mathrm{LD}}(A) \to C^2_{\mathrm{LD}}(A)$ is nothing but the evaluation of the extended map c at the relation R, that is, $d^2(c) = c(R)$. So a 1-cochain c is a 1-cocycle if and only if its evaluation at R is 0.

2.3.2. *Nilpotent coefficients.* Let $E/\mathbb{Q}_p$ be a finite extension with ring of integers $\mathcal{O}_E$, residue field $\mathbb{F}$, and uniformizer ϖ.

Let U be a unipotent (smooth connected) linear algebraic group over $\operatorname{Spec} \mathcal{O}_E$, admitting an upper central series

$$1 = U_0 \subset U_1 \cdots \subset U_k = U.$$

Assume there exists an embedding $\iota : U \hookrightarrow \mathrm{GL}_N \subset \mathrm{Mat}_{N\times N}$ such that $(\iota(x)-1)^{k+1} = 0$ for all $x \in U$. Write $\log = \log_{\leq k}$ for the truncated logarithmic function $1 + x \mapsto x - x^2/2 + \cdots + (-1)^{k+1}x^k/k$.

Assume $p > k$. There is an isomorphism of schemes $U \cong \operatorname{Lie} U$ sending $g \mapsto \log g$, defined through the commutative diagram

$$\begin{tikzcd} U \arrow[r] \arrow[d, "\log"] & \mathrm{GL}_N \arrow[d, "\log"] \\ \operatorname{Lie} U \arrow[r] & \mathrm{Mat}_{N\times N} \end{tikzcd}$$

We assume $k = 2$ from now on because it suffices for our applications.

Fix a Galois action $G_K \to \mathrm{Aut}(U)(\mathcal{O}_E)$ such that the image group is a pro-p subgroup of $\mathrm{Aut}(U)(\mathcal{O}_E)$.

Let A be an $\mathcal{O}_E$-algebra. Recall that a *nonabelian crossed homomorphism* valued in $U(A)$ is a map $c : G_K \to U(A)$ such that

$$c(gh) = c(g)(g \cdot c(h))$$

for all $g, h \in G_K$. Set $\mathfrak{c} := \log(c) : G_K \to \operatorname{Lie} U(A)$. By the Baker–Campbell–Hausdorff formula,

$$\mathfrak{c}(gh) = \mathfrak{c}(g) + g \cdot \mathfrak{c}(h) + \tfrac{1}{2}[\mathfrak{c}(g), g \cdot \mathfrak{c}(h)]. \tag{2-2}$$

Our definition of the Lyndon–Demushkin cochain complex is motivated by (2-2).

Definition 2.3.3. Let A be an $\mathcal{O}_E$-algebra. The Lyndon–Demushkin complex with unipotent coefficients is defined to be the following cochain complex $C^\bullet_{\mathrm{LD}}(U(A))$ supported in degrees [0,2]:

$$\operatorname{Lie} U(A) \xrightarrow{d^1} (\operatorname{Lie} U(A))^{\oplus n+2} \xrightarrow{d^2} \operatorname{Lie} U(A),$$

where d^1 is defined by

$$d^1(v) = \left(-v + x_i \cdot v + \tfrac{1}{2}[-v, x_i \cdot v]\right)_{i=0,\dots,n+1}.$$

We need some preparations before we define d^2. An element $c = (\alpha_0, \dots, \alpha_{n+1}) \in C^1_{\mathrm{LD}}(U(A))$ can be regarded as a function on the free group with $(n+2)$ generators

$$c : \langle x_0, \dots, x_{n+1} \rangle \to \operatorname{Lie} U(A)$$

by setting $c(x_i) = \alpha_i$ for each i and extending it to the whole free group by

$$c(gh) := c(g) + g \cdot c(h) + \tfrac{1}{2}[c(g), g \cdot c(h)]$$

We define d^2 as

$$d^2(c) := c(R) = c(x_0^q(x_0, x_1)(x_2, x_3)\cdots(x_n, x_{n+1})).$$

Remark 2.3.4. (1) When U is an abelian group, we recover the definition in the previous section for the cohomology of the abelian $U(A)$.

(2) The main reason we define $C^\bullet_{\mathrm{LD}}(U(A))$ this way is because we want to compare it with $C^\bullet_{\mathrm{LD}}(\operatorname{Lie} U(A))$. Note that $C^\bullet_{\mathrm{LD}}(\operatorname{Lie} U(A))$ and $C^\bullet_{\mathrm{LD}}(U(A))$ have the same underlying group, but their differential $d^\bullet$ is different.

(3) Note that $d^2(c) = 0$ if and only if c defines a crossed homomorphism $\mathfrak{c} : G_K \to \operatorname{Lie} U(A)$ in the sense of (2-2). See the proof of Proposition 2.3.6.

(4) The differential maps are generally nonlinear.

Definition 2.3.5. We define $Z^i_{\mathrm{LD}} := (d^{i+1})^{-1}(0)$, and $B^i_{\mathrm{LD}} := d^i(C^{i-1}_{\mathrm{LD}})$ for $i = 0, 1, 2$.

Proposition 2.3.6. *We have*

$$H^0(G_K, U(A)) \cong Z^0_{\mathrm{LD}}(U(A))$$

and a surjection of pointed sets

$$Z^1_{\mathrm{LD}}(U(A)) \to H^1(G_K, U(A)).$$

Proof. $H^0(G_K, U(A))$ is by definition the G_K-fixed point subset of $U(A)$, while $Z^0_{\mathrm{LD}}(U(A))$ is the subset of $U(A)$ whose elements are fixed by the $x_0,\dots, x_{n+1}$: if $u \in U(A)$ is fixed by x_i, then $u^{-1}(x_i \cdot u) = 1$ and taking truncated log of both sides we get $d^1(\log u) = 0$.

$H^1(G_K, U(A))$ is by definition the set of equivalence classes of crossed homomorphisms, and $Z^1_{\mathrm{LD}}(U(A))$ is the set of crossed homomorphisms. □

$\operatorname{Lie} U$ has a lower central series filtration. Let $Z(U)$ be the center of U. Write U^{ad} for $U/Z(U)$. Since U is unipotent of class 2, $\operatorname{Lie} U$ is isomorphic to its graded Lie algebra $\operatorname{Lie} U \cong \operatorname{gr}^\bullet(\operatorname{Lie} U)$. We will fix a grading $\operatorname{Lie} U \cong Z(U) \oplus U^{\mathrm{ad}}$ of the Lie algebra $\operatorname{Lie} U$ once for all. In particular, we fix a projection $\operatorname{pr} : \operatorname{Lie} U \to Z(U)$.

2.3.7. *Cup products.* Let $c \in C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A))$. Let $\tilde{c} \in C^1_{\mathrm{LD}}(U(A))$ be the (unique) lift of c such that $\operatorname{pr}(\tilde{c}(x_0)) = \cdots = \operatorname{pr}(\tilde{c}(x_{n+1})) = 0$. Define

$$Q(c) := \operatorname{pr}(d^2(\tilde{c})) = \operatorname{pr}(\tilde{c}(R)) \in C^2_{\mathrm{LD}}(Z(U)(A)).$$

Lemma. *$Q(-)$ is a quadratic form, that is, $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form.*

Proof. In Definition 2.3.3, we defined it so that $\tilde{c}(gh) := \tilde{c}(g) + g \cdot \tilde{c}(h) + \frac{1}{2}[\tilde{c}(g), g \cdot \tilde{c}(h)]$. So after fully expanding the expression, $\tilde{c}(R) = \sum_i \alpha_i c(x_i) + \sum_{i<j} [\beta_i c(x_i), \gamma_i c(x_j)]$, where $\alpha_i, \beta_i, \gamma_j \in \langle x_0, \dots, x_{n+1}\rangle$. It follows that

$$Q(c) = \operatorname{pr}\biggl(\sum_i \alpha_i c(x_i) + \sum_{i<j} [\beta_i c(x_i), \gamma_i c(x_j)]\biggr) = \sum_{i<j} \operatorname{pr}([\beta_i c(x_i), \gamma_i c(x_j)]),$$

which is clearly a quadratic form. □

We define

$$C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \times C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \xrightarrow{\cup} C^2_{\mathrm{LD}}(Z(U)(A)), \quad x \cup y := \tfrac{1}{2}(Q(x + y) - Q(x) - Q(y)),$$

which is a symmetric bilinear form.

Remark. Alternatively, we can choose an arbitrary lift $\tilde{c}$ of c. Now $\operatorname{pr}(d^2(\tilde{c}))$ is an inhomogeneous polynomial of degree two. We recover Q by taking the homogeneous part of degree two.

Lemma 2.3.8. *Under the identification $C^1_{\mathrm{LD}}(U(A)) = C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \oplus C^1_{\mathrm{LD}}(Z(U)(A))$, we have*

$$Z^1_{\mathrm{LD}}(U(A)) = \{(x, y) \in C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \oplus C^1_{\mathrm{LD}}(Z(U)(A)) \mid d^2x = 0,\ x \cup x + d^2y = 0\}.$$

Proof. This is obvious from the definition of d^2 and Q. The projection of $d^2(x, y)$ to $C^2_{\mathrm{LD}}(U^{\mathrm{ad}}(A))$ is d^2x; and the projection of $d^2(x, y)$ to $C^2_{\mathrm{LD}}(Z(U)(A))$ is $x \cup x + d^2y$. □

Write $H^i_{\mathrm{LD}}(U^{\mathrm{ad}}(A))$ for

$$Z^i_{\mathrm{LD}}(U^{\mathrm{ad}}(A))/B^i_{\mathrm{LD}}(U^{\mathrm{ad}}(A))$$

and write $H^i_{\mathrm{LD}}(Z(U)(A))$ for

$$Z^i_{\mathrm{LD}}(Z(U)(A))/B^i_{\mathrm{LD}}(Z(U)(A)).$$

Lemma 2.3.9. *The pairing $\cup$ on the cochain level induces a symmetric pairing on the cohomology level*

$$H^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \times H^1_{\mathrm{LD}}(U^{\mathrm{ad}}(A)) \xrightarrow{\cup} H^2_{\mathrm{LD}}(Z(U)(A)).$$

Proof. It suffices to show, for all $x \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}})(A)$ and $y \in B^1_{\mathrm{LD}}(U^{\mathrm{ad}})(A)$, that

$$Q(x + y) - Q(x) \in B^2_{\mathrm{LD}}(Z(U)(A)).$$

Let $\tilde{x} \in C^1_{\mathrm{LD}}(U(A))$ be the unique extension of x such that $\mathrm{pr}\,\tilde{x} = 0$. The cochain $\tilde{x}$ represents a group homomorphism $\rho_{\tilde{x}} : \langle x_0, \ldots, x_{n+1}\rangle \to U(A) \rtimes \langle x_0, \ldots, x_{n+1} | R\rangle$ such that $\rho_{\tilde{x}}(R) = 1 \bmod Z(U)(A)$. More explicitly, we define $\rho_{\tilde{x}}(x_i) = (\exp(\tilde{x}(x_i)), x_i)$ where exp is the truncated exponential map (the inverse to the truncated log map). Since y is a coboundary, there exists $n \in U(A)$ such that $n\rho_{\tilde{x}}n^{-1}$ is represented by a cocycle $(x + y, f)$ extending $x + y$ (we are exploiting the abelian coefficients here). We have $n\rho_{\tilde{x}}(R)n^{-1}\rho_{\tilde{x}}(R)^{-1} = 1 \in U(A) \rtimes \langle x_0, \ldots, x_{n+1} | R\rangle$ since $\rho_{\tilde{x}}(R)$ lies in the center of $U(A)$. Since $Q(x+y)-d^2(f) = n\rho_{\tilde{x}}(R)n^{-1}$ and $Q(x) = \rho_{\tilde{x}}(R)$, we have $Q(x+y)-Q(x) = d^2 f \in B^2_{\mathrm{LD}}(Z(U)(A))$. □

Recall $Z^1_{\mathrm{LD}}(U(A))$ and $Z^1_{\mathrm{LD}}(\mathrm{Lie}\, U(A))$ are both subsets of $C^1_{\mathrm{LD}}(U(A))$.

Lemma 2.3.10. *If $Z(U)(\mathbb{F}) \cong \mathbb{F}$, then*

$$Z^1_{\mathrm{LD}}(U(\mathbb{F})) \subset Z^1_{\mathrm{LD}}(\mathrm{Lie}\, U(\mathbb{F})),$$

that is, the nonabelian cocycles with $U(\mathbb{F})$-coefficients are automatically abelian cocycles with $(\mathrm{Lie}\, U(\mathbb{F}))$*-coefficients.*

Proof. We have noted in Remark 2.3.4(2) that $C^1_{\mathrm{LD}}(U(\mathbb{F}))$ and $C^1_{\mathrm{LD}}(\mathrm{Lie}\, U(\mathbb{F}))$ have the same underlying space. By Lemma 2.3.8, an element of $Z^1_{\mathrm{LD}}(U(\mathbb{F}))$ is a pair (x, y) such that $d^2x = 0$ and $x \cup x + d^2y = 0$. By our assumption, $C^2_{\mathrm{LD}}(Z(U)(\mathbb{F})) = H^2(G_K, Z(U)(\mathbb{F}))$ (Corollary 2.2.2) and thus $B^2_{\mathrm{LD}}(Z(U)(\mathbb{F})) = 0$ and $d^2 = 0$. So $d^2y = 0$ automatically, and (x, y) defines an element of $Z^1_{\mathrm{LD}}(\mathrm{Lie}\, U(\mathbb{F}))$. □

3. An analysis of cup products

Let E be a p-adic field with ring of integers $\mathcal{O}_E$, residue field $\mathbb{F}$ and uniformizer ϖ.

Let U be a smooth connected unipotent group of class 2 over $\operatorname{Spec}\mathcal{O}_E$, with center $Z(U)\cong\mathbb{G}_a$. Write U^{ad} for $U/Z(U)$. Assume $U^{\mathrm{ad}}\cong\mathbb{G}_a^{\oplus s}$ is a vector group.

Definition 3.0.1. Let K' be a p-adic field. A Lyndon–Demushkin action $G_{K'}\to\operatorname{Aut}(U)(\mathcal{O}_E)$ is said to be *mildly regular* if the following are satisfied:

(MR1) $H^0(G_{K'},U^{\mathrm{ad}}(E))=0$.

(MR2) The bilinear pairing

$$\cup_{\mathbb{F}}:C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))\times C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))\to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

is nondegenerate.

Remark 3.0.2. In practice U is the unipotent radical of a parabolic subgroup of a reductive group and (MR2) is equivalent to "p being not too small". We worked out the G_2-case in Appendix A, and showed that if $p>5$, (MR2) always holds. The same proof but with more complicated notation should work for general reductive groups.

In general, (MR2) can be checked by computer algebra systems because it is a finite field vector space question for a finite number of small p's. We include an algorithm (written in SageMath) in Appendix B.

The following proposition is a summary of Appendix A:

Proposition 3.0.3. *If U is the unipotent radical of the short root parabolic of G_2 or the quotient of the unipotent radical of the long root parabolic of G_2 by its center, then* (*MR*2) *is true when $p\geq 5$.*

Definition 3.0.4. Given a tuple of labeled Hodge–Tate weights (see [Emerton and Gee 2023, Subsection 1.12] for the definition) $\underline{\lambda}$, we say $\underline{\lambda}$ is slightly less than 0 if for each $\sigma:K'\hookrightarrow\overline{\mathbb{Q}}_p$, λ_σ consists of nonpositive integers, and for at least one σ, λ_σ consists of negative integers. (The cyclotomic character has Hodge–Tate weight -1.)

Proposition 3.0.5. *Assume $p\geq 5$. If U is the unipotent radical of the short root parabolic of G_2 or the quotient of the unipotent radical of the long root parabolic of G_2 by its center, then $G_{K'}\to\operatorname{Aut}(U)(\mathcal{O}_E)$ is mildly regular if $U^{\mathrm{ad}}(E)$ is Hodge–Tate of labeled Hodge–Tate weights slightly less than* 0.

Proof. If $H^0(G_{K'},U^{\mathrm{ad}}(E))\neq 0$, then for all embeddings $\sigma:K\hookrightarrow\overline{\mathbb{Q}}_p$, $0\in\lambda_\sigma$. The proposition now follows from Proposition 3.0.3 and Appendix A. □

3.1. *Cup products mod ϖ.*

Lemma 3.1.1. *The image of $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))\to C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))$ has codimension at most* $\dim_E U^{\mathrm{ad}}(E)$.

Proof. Say $\dim_{\mathbb{F}}C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))=\operatorname{rank}_{\mathcal{O}_E}C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))=N$. Since $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$ is the kernel of $C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))\to C^2_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$, and $\operatorname{rank}_{\mathcal{O}_E}C^2_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))=\dim_E U^{\mathrm{ad}}(E)$, we have

$$\operatorname{rank}_{\mathcal{O}_E}Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))\geq N-\dim_E U^{\mathrm{ad}}(E).$$

Since $C^2_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$ is torsion-free, $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$ is saturated in $C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$, and is thus a direct summand. In particular, the image of $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$ in $C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))$ has dimension $\geq N-\dim_E U^{\mathrm{ad}}(E)$. □

Lemma 3.1.2. *If*

$$\cup_{\mathbb{F}} : C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \times C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

is nondegenerate, then the kernel of

$$\cup_{\mathbb{F}} : Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \times Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

has dimension at most $\dim_E U^{\mathrm{ad}}(E)$.

Remark. Note that $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \neq Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi$ in general.

The kernel of a bilinear pairing is also called the annihilator.

Proof. For ease of notation, write C for $C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))$, and write Z for the image of $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$ in C. Note that $Z \cong Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi$ by the proof of the above lemma.

Let $K \subset Z$ be the kernel of $\cup_{\mathbb{F}}$. Since the cup product on C is nondegenerate, there exists a subspace $F \subset C$ of dimension equal to that of K, such that the restriction of the cup product to $(F+K)$ is also nondegenerate. Since $F \cap Z = 0$, $\dim C \geq \dim(F+Z) = \dim Z + \dim F = \dim Z + \dim K$. The lemma now follows from the previous lemma. □

We also record the following lemma whose proof is similar.

Lemma 3.1.3. (1) *The image of* $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))$ *has codimension at most* $\dim_E U^{\mathrm{ad}}(E)$.

(2) *If*

$$\cup_{\mathbb{F}} : C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \times C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

is nondegenerate, then the kernel of

$$\cup_{\mathbb{F}} : Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \times Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

has dimension at most $\dim_E U^{\mathrm{ad}}(E)$.

3.2. *General cup products in group cohomology.*

In this subsection, we give a reinterpretation of Section 2.3.7, which is convenient for theoretic applications.

Let V be a unipotent algebraic group of class 2 over $\mathcal{O}_E$. Let Γ be an abstract group, together with a homomorphism $\theta : \Gamma \to \mathrm{Aut}(V)(\mathcal{O}_E)$. By the Lie correspondence, $\mathrm{Aut}(\mathrm{Lie}\, V) \cong \mathrm{Aut}(V)$, and thus θ induces a $\mathcal{O}_E$-linear Γ-action on $\mathrm{Lie}\, V$ which respects Lie brackets.

We fix a grading $\mathrm{Lie}\, V = V_1 \oplus V_2$ such that $[V_1, V_1] \subset V_2$, and $[V, V_2] = 0$. We will write V for $V(\mathcal{O}_E)$ for simplicity.

Let $f:\Gamma\to V$ be a crossed homomorphism. By definition, for any $g_1, g_2\in\Gamma$, $f(g_1g_2)=f(g_1)g_1f(g_2)$. Write $c=c_1+c_2$ for $\log(f)$, where c_1 values in V_1 and c_2 values in V_2. By the Baker–Campbell–Hausdorff formula, we have

$$\begin{aligned} c(gh) &= c(g)+gc(h)+[c(g), gc(h)]/2 \\ &= (c_1(g)+gc_1(h))+(c_2(g)+gc_2(h))+[c_1(g), gc_1(h)]/2 \end{aligned} \tag{3-1}$$

Lemma 3.2.1. *Let $a, b\in H^1(\Gamma, V_1)$ be two crossed homomorphisms. The 2-cochain $B(a, b):(g, h)\mapsto [a(g), gb(h)]$ is a 2-cocycle.*

Proof. By definition, we have

$$\begin{aligned} &d^2(B(a,b))(g_1, g_2, g_3) \\ &\quad = g_1[a(g_2), g_2b(g_3)]-[d^1a(g_1, g_2), g_1g_2b(g_3)]+[a(g_1), g_1d^1b(g_2, g_3)]+[a(g_1), g_1b(g_2)] \\ &\quad = g_1[a(g_2), g_2b(g_3)]-[a(g_1)+g_1a(g_2), g_1g_2b(g_3)]+[a(g_1), g_1b(g_2)+g_1g_2b(g_3)]+[a(g_1), g_1b(g_2)] \\ &\quad = 0. \end{aligned}$$

□

For crossed homomorphisms $a\in H^1(\Gamma, V_1)$, define $Q(a):=B(a, a)$. By comparing (3-1) and Section 2.3.7, it is not hard to see the $Q(-)$ defined in this subsection coincides with that of Section 2.3.7 for 1-cocycles when Γ is the discrete Demushkin group.

Since $a\cup b:=(Q(a+b, a+b)-Q(a)-Q(b))/2=(B(a, b)+B(b, a))/2$, we have $a\cup b\in H^2(\Gamma, V_2)$. Again the cup product defined in this subsection coincides with that of Section 2.3.7 when the settings overlap.

Lemma 3.2.2. *Let $\Gamma'\subset\Gamma$ be a normal subgroup of finite index. Write Δ for Γ/Γ'. The cup product $\cup: H^1(\Gamma', V_1)\times H^1(\Gamma', V_1)\to H^2(\Gamma', V_2)$ is Δ-equivariant.*

Proof. Let $a, b\in H^1(\Gamma^1, V_1)$, and let $\sigma\in\Gamma$. We have by definition $\sigma\cdot a(g)=\sigma a(\sigma^{-1}g\sigma)$, and $\sigma\cdot B(a, b)(g, h)=\sigma B(a, b)(\sigma^{-1}g\sigma, \sigma^{-1}h\sigma)$ (see [Serre 2002, Section I.5.8]). We immediately have $\sigma\cdot B(a, b)=B(\sigma\cdot a, \sigma\cdot b)$. □

Example 3.2.3 (the completely split case). In this paragraph we analyze the special case where the $G_{K'}$ action on $U^{\mathrm{ad}}(\mathbb{F})\cong\operatorname{Lie}U^{\mathrm{ad}}(\mathbb{F})$ is trivial and $H^2(G_{K'}, Z(U)(\mathbb{F}))=Z(U)(\mathbb{F})=\mathbb{F}$. It will be used in the proof of Theorem 3.3.1.

Since the center of $\operatorname{Lie}U$ is one-dimensional, the Lie bracket

$$\operatorname{Lie}U^{\mathrm{ad}}(\mathbb{F})\times\operatorname{Lie}U^{\mathrm{ad}}(\mathbb{F})\xrightarrow{[-,-]} Z(U)(\mathbb{F})$$

is a nondegenerate, alternating pairing. Choose a basis $\{e_1, \dots, e_k, e'_1, \dots, e'_k\}$ of $\operatorname{Lie}U^{\mathrm{ad}}(\mathbb{F})$ such that $[e'_i, e'_j]=[e_i, e_j]=0$ and $[e_i, e'_j]=-[e'_i, e_j]=\delta_{i,j}$. Since by assumption the $G_{K'}$-action on $U^{\mathrm{ad}}(\mathbb{F})$ is trivial, the cup product

$$\cup: H^1(G_{K'}, U^{\mathrm{ad}}(\mathbb{F}))\times H^1(G_{K'}, U^{\mathrm{ad}}(\mathbb{F}))\to H^2(G_{K'}, Z(U)(\mathbb{F}))$$

is isomorphic to the (exterior) direct sum of cup products

$$\cup_i : H^1(G_{K'}, \mathbb{F}e_i \oplus \mathbb{F}e'_i) \times H^1(G_{K'}, \mathbb{F}e_i \oplus \mathbb{F}e'_i) \to H^1(G_{K'}, \mathbb{F}).$$

Write $\wedge$ for the usual cup product $H^1(G_{K'}, \mathbb{F}) \times H^1(G_{K'}, \mathbb{F}) \to H^2(G_{K'}, \mathbb{F})$ which appears in local Tate duality. By definition, for $a, b \in H^1(G_{K'}, \mathbb{F})$ we have

$$\begin{aligned} Q(ae_i + be'_i) &= B(ae_i + be'_i, ae_i + be'_i) \\ &= ((g, h) \mapsto [a(g)e_i + b(g)e'_i, a(h)e_i + b(h)e'_i]) \\ &= ((g, h) \mapsto (a(g)b(h) - b(g)a(h))) \\ &= a \wedge b - b \wedge a \\ &= 2a \wedge b \end{aligned}$$

and thus, for $a_1, b_1, a_2, b_2 \in H^1(G_{K'}, \mathbb{F})$,

$$B(a_1e_i + b_1e'_i, a_2e_i + b_2e'_i) = 2(a_1 \wedge b_2 + a_2 \wedge b_1).$$

Since $\wedge$ is a nondegenerate pairing, B is also a nondegenerate pairing.

3.3. *Nontriviality of cup products.*

Theorem 3.3.1. *Let K'/K be a finite Galois extension of p-adic fields of prime-to-p degree. Let $r : G_K \to \mathrm{Aut}(U)(\mathcal{O}_E)$ be a continuous group homomorphism.*

If $r|_{G_{K'}}$ is Lyndon–Demushkin and mildly regular, then either

(i) $H^2(G_K, Z(U)(\mathbb{F})) = 0$, *or*

(ii) *the symmetric bilinear pairing*

$$H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \times H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \to H^2(G_K, Z(U)(\mathcal{O}_E)) \otimes \mathbb{F}$$

is nontrivial.

Remark. Notice that

$$H^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \cong H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E)) \quad \text{and} \quad H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))^{G_K} = H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)).$$

The symmetric pairing in the theorem is the restriction to $H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))$ of the symmetric pairing defined in Lemma 2.3.9.

Proof. Assume $H^2(G_K, Z(U)(\mathbb{F})) \neq 0$. Consider the diagram

$$\begin{tikzcd} H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \times H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \arrow[r] \arrow[d, hook] & H^2(G_K, Z(U)(\mathcal{O}_E)) \arrow[d, "\cong"] \\ H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E)) \times H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E)) \arrow[r] & H^2(G_{K'}, Z(U)(\mathcal{O}_E)) \\ Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \times Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \arrow[r] \arrow[u] & C^2(Z(U)(\mathcal{O}_E)) \arrow[u] \end{tikzcd}$$

By Lemma 3.1.2, the kernel of

$$H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \times H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \to H^2(G_{K'}, Z(U)(\mathbb{F}))$$

has $\mathbb{F}$-dimension at most $\dim_E U^{\mathrm{ad}}(E)$. Write Δ for $G_K/G_{K'}$, which acts on $H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))$ with fixed-point subspace $H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))$.

By an averaging argument (explained below), the kernel of

$$H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \times H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \to H^2(G_K, Z(U)(\mathbb{F}))$$

is contained in the kernel of

$$H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \times H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \to H^2(G_{K'}, Z(U)(\mathbb{F}))$$

and thus has $\mathbb{F}$-dimension at most $\dim_E U^{\mathrm{ad}}(E)$. (Let $[c] \in H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi$ and suppose $[c] \cup [d] = 0$ for all $[d] \in H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi$. Let $[c'] \in H^1(G_{K'}, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi$. Then $\sum_{\sigma\in\Delta} \sigma([c] \cup [c']) = [c] \cup \sum_{\sigma\in\Delta}[c'] = 0$. Since $H^2(G_K, Z(U)(\mathbb{F})) \neq 0$, we have $H^2(G_K, Z(U)(\mathbb{F})) = H^2(G_{K'}, Z(U)(\mathbb{F}))$ and thus $\sum_{\sigma\in\Delta} \sigma([c] \cup [c']) = \#\Delta\sigma([c] \cup [c'])$.)

We remark that as a finitely generated module over a DVR, $H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))$ is the direct sum of its torsion-free part and its torsion part; and $H^1(G_K, U^{\mathrm{ad}}(E)) = H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))_{\text{torsion-free}} \otimes_{\mathcal{O}_E} E$.

By the local Euler characteristic,

$$\begin{aligned}\dim_E H^1(G_K, U^{\mathrm{ad}}(E)) &= \dim_E H^2(G_K, U^{\mathrm{ad}}(E)) + \dim_E H^0(G_K, U^{\mathrm{ad}}(E)) + \dim_E U^{\mathrm{ad}}(E)[K:\mathbb{Q}_p] \\ &\geq \dim_E H^2(G_K, U^{\mathrm{ad}}(E)) + \dim_E U^{\mathrm{ad}}(E).\end{aligned}$$

We will now consider two possibilities: $H^2(G_K, U^{\mathrm{ad}}(\mathbb{F})) \neq 0$ and $H^2(G_K, U^{\mathrm{ad}}(\mathbb{F})) = 0$.

Case $H^2(G_K, U^{\mathrm{ad}}(\mathbb{F})) \neq 0$. Since $H^2(G_K, U^{\mathrm{ad}}(\mathbb{F})) \neq 0$, $H^2(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))$ is nontrivial. So either we have $\dim_E H^2(G_K, U^{\mathrm{ad}}(E)) > 0$, or $H^2(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))$ has nontrivial torsion. If $H^2(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))$ has nontrivial torsion, then again by the local Euler characteristic (mod ϖ version), $H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))$ also has nontrivial torsion. In either case, $\dim_{\mathbb{F}} H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi \geq \dim_E U^{\mathrm{ad}}(E) + 1$. So the kernel of the cup product is a proper subspace of $H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))/\varpi$.

Case $H^2(G_K, U^{\mathrm{ad}}(\mathbb{F})) = 0$. By Nakayama's lemma, $H^2(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) = 0$. By [Emerton and Gee 2023], there exists a perfect $\mathcal{O}_E$-complex $[C^0 \to C^1 \to C^2]$ concentrated in degrees [0, 2] which computes $H^\bullet(G_K, U^{\mathrm{ad}}(\mathcal{O}_E))$. By the universal coefficient theorem, there exists a short exact sequence

$$0 \to H^1(C^\bullet) \otimes \mathbb{F} \to H^1(C^\bullet \otimes \mathbb{F}) \to \mathrm{Tor}_1^{\mathcal{O}_E}(H^2(C^\bullet), \mathbb{F}) \to 0.$$

So $H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \otimes_{\mathcal{O}_E} \mathbb{F} = H^1(G_K, U^{\mathrm{ad}}(\mathbb{F}))$. We assume (i) and (ii) are false, and try to get a contradiction. The kernel of

$$H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \times H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \to H^2(G_K, Z(U)(\mathcal{O}_E)) \otimes \mathbb{F}$$

has dimension $h^1 := \dim_{\mathbb{F}} H^1(G_K, U^{\mathrm{ad}}(\mathbb{F}))$. By the local Euler characteristic,

$$h^1 = \dim_E U^{\mathrm{ad}}(E)[K:\mathbb{Q}_p] + \dim_{\mathbb{F}} H^0(G_K, U^{\mathrm{ad}}(\mathbb{F})). \tag{3-2}$$

By Lemma 3.1.3, the kernel k_Z of

$$Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \times Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to H^2(G_{K'}, Z(U)(\mathbb{F}))$$

has dimension at most $\dim_E U^{\mathrm{ad}}(E)$. Since the cup product is trivial on $H^1(G_K, U^{\mathrm{ad}}(\mathbb{F}))$, we have

$$\dim k_Z \geq \dim H^1(G_K, U^{\mathrm{ad}}(\mathbb{F})) + \dim B^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) = h^1 + \dim B^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})). \tag{3-3}$$

Combining (3-2) and (3-3), we have

$$\dim_E U^{\mathrm{ad}}(E) \geq \dim_{\mathbb{F}} k_Z \geq \dim_E U^{\mathrm{ad}}(E)[K : \mathbb{Q}_p] + \dim_{\mathbb{F}} H^0(G_K, U^{\mathrm{ad}}(\mathbb{F})) + \dim B^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))$$

So we conclude that

$$1 = [K : \mathbb{Q}_p], \quad 0 = H^0(G_K, U^{\mathrm{ad}}(\mathbb{F})), \quad 0 = B^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})).$$

In particular, we have $H^0(G_{K'}, U^{\mathrm{ad}}(\mathbb{F})) = U^{\mathrm{ad}}(\mathbb{F})$, and the kernel of the cup product on $H^1(G_{K'}, U^{\mathrm{ad}}(\mathbb{F}))$ has dimension exactly $\dim_E U^{\mathrm{ad}}(E)$. However, by Example 3.2.3, the cup product on $H^1(G_{K'}, U^{\mathrm{ad}}(\mathbb{F}))$ is nondegenerate by local Tate duality. □

Theorem 3.3.1 is used in the following scenario.

Lemma 3.3.2. *Let L be a split reductive group over $\mathbb{F}$. Let $r : G_K \to L(\mathbb{F})$ be a Galois representation valued in L. Let r^{ss} be the semisimplification of r. Write $G_{K'}$ for the kernel of r^{ss}. Then the degree $[K' : K]$ divides $(q-1)^r \# W_L$, where*

- *r is the rank of L,*
- *q is a power of p, and*
- *$\# W_L$ is the cardinality of the Weyl group of L.*

Proof. By [Lin 2022], r^{ss} is tamely ramified and factors through the normalizer of a maximal torus of L (after possibly extending the base field). □

In particular, if $L = G_2$ and $p > 3$, the kernel of r^{ss} defines a Galois extension K'/K of prime-to-p degree, and $r|_{G_{K'}}$ is Lyndon–Demushkin since it has trivial semisimplification.

4. Nonabelian obstruction theory via the Lyndon–Demushkin cocycle group with external Galois action

Let $K/\mathbb{Q}_p$ be a p-adic field. Let $E/\mathbb{Q}_p$ be a finite extension with ring of integers $\mathcal{O}_E$, residue field $\mathbb{F}$, and uniformizer ϖ.

Let L be a split reductive group over $\mathcal{O}_E$. Fix a Galois representation

$$r^\circ : G_K \to L(\mathcal{O}_E)$$

throughout this section.

Let U be a unipotent group over $\mathcal{O}_E$ whose adjoint group is abelian. Let $Z(U)$ be the center of U. The adjoint group U^{ad} is defined to be $U/Z(U)$.

Fix a group scheme homomorphism $\phi : L \to \mathrm{Aut}(U)$ throughout this section. In particular, there is a Galois action $\phi(r^\circ) : G_K \xrightarrow{r^\circ} L(\mathcal{O}_E) \xrightarrow{\phi(\mathcal{O}_E)} \mathrm{Aut}(U)(\mathcal{O}_E)$. We will talk about nonabelian Galois cohomology $H^\bullet(G_K, U(\mathcal{O}_E))$ and $H^\bullet(G_K, U(\mathbb{F}))$ using this Galois action throughout this section.

Let K'/K be a prime-to-p, finite Galois extension of K containing the group of p-th root of unity, such that $r^\circ(G_{K'}) \subset L(\mathcal{O}_E)$ is a pro-p group. Write Δ for $\mathrm{Gal}(K'/K)$. Set $\Gamma := G_K$, and $H := G_{K'}$.

4.1. *Nonabelian inflation-restriction.*

Nonabelian Galois cohomology. We recall a few facts about the nonabelian version of Galois cohomology. Let

$$0 \to A \to B \to C \to 0$$

be a short exact sequence of groups with continuous Γ-action. If $A \to B$ is *central*, that is, A is contained in the center of B, then we have a long exact sequence of pointed sets (see [Serre 2002, Proposition 43, 5.7])

$$1 \to A^\Gamma \to B^\Gamma \to C^\Gamma \to H^1(\Gamma, A) \to H^1(\Gamma, B) \to H^1(\Gamma, C) \xrightarrow{\delta} H^2(\Gamma, A).$$

Let $H \subset \Gamma$ be a closed normal subgroup. Then there is an exact sequence (see [Serre 2002, 5.8])

$$1 \to H^1(\Gamma/H, A^H) \to H^1(\Gamma, A) \to H^1(H, A)^{\Gamma/H}. \tag{4-1}$$

If A is an abelian group, then the sequence above can be upgraded to the inflation-restriction exact sequence:

$$1 \to H^1(\Gamma/H, A^H) \to H^1(\Gamma, A) \to H^1(H, A)^{\Gamma/H} \to H^2(\Gamma, A^H).$$

Theorem 4.1.1 [Koch 2002, Theorem 3.15]. *Let Γ be a profinite group, H a normal subgroup of finite index, and A an* (*abelian*) *G-module whose elements have finite order coprime to* $(\Gamma : H)$. *Then*

$$H^n(\Gamma/H, A^H) = 0$$

for all $n \geq 1$, and the restriction

$$H^n(\Gamma, A) \to H^n(H, A)^{\Gamma/H}$$

is an isomorphism.

Let R be either $\mathcal{O}_E$ or $\mathbb{F}$. For ease of notation, write U for $U(R)$ in this paragraph. The fact above implies the following diagram commutes, with exact columns:

$$\begin{tikzcd}
H^1(\Gamma, Z(U)) \arrow[r, "\cong", "\mathrm{res}"'] \arrow[d] & H^1(H, Z(U))^\Delta \arrow[d] \\
H^1(\Gamma, U) \arrow[r, hook, "\mathrm{res}"'] \arrow[d, "\alpha_1"] & H^1(H, U)^\Delta \arrow[d, "\alpha_2"] \\
H^1(\Gamma, U^{\mathrm{ad}}) \arrow[r, "\cong", "\mathrm{res}"'] \arrow[d, "\delta_1"] & H^1(H, U^{\mathrm{ad}})^\Delta \arrow[d, "\delta_2"] \\
H^2(\Gamma, Z(U)) \arrow[r, hook] & H^2(H, Z(U))
\end{tikzcd}$$

The injectivity of the second line follows from (4-1).

Proposition 4.1.2. *The restriction map of nonabelian* 1*-cocycles*

$$H^1(\Gamma, U) \to H^1(H, U)^{\Delta}$$

is a bijection.

Proof. This follows from diagram chasing: Let $[c] \in H^1(H, U)^{\Delta}$. Since $\delta_1(\mathrm{res}^{-1}(\alpha_2[c])) = \delta_2(\alpha_2[c]) = 0$, there exists $[b] \in H^1(\Gamma, U)$ such that $\alpha_1(\mathrm{res}([b])) = \alpha_2([c])$. Since $\alpha_2^{-1}(\alpha_2([c]))$ is a $H^1(H, Z(U))^{\Delta}$-torsor, we can twist $[b]$ to make $\mathrm{res}([b]) = [c]$. □

4.1.3. *Representation-theoretic interpretation of nonabelian* 1*-cocycles.* Let $\mathfrak{P}$ be a group which is a semidirect product $\mathfrak{L} \ltimes \mathfrak{U}$. Let $q_{\mathfrak{L}} : \mathfrak{P} \to \mathfrak{L}$ be the quotient map. Fix a section $\mathfrak{L} \to \mathfrak{P}$ of $q_{\mathfrak{L}}$, which allows us to identify (set-theoretically) $\mathfrak{P}$ with $\mathfrak{U} \times \mathfrak{L}$, and write $q_{\mathfrak{U}} : \mathfrak{P} \to \mathfrak{U}$ be the projection map. For $g \in \mathfrak{P}$, write $g = g_{\mathfrak{U}} g_{\mathfrak{L}}$ such that $g_{\mathfrak{U}} \in \mathfrak{U} \times \{1\}$ and $g_L \in \{1\} \times \mathfrak{L}$. Let $\bar{\tau} : \Gamma \to \mathfrak{L}$ be a group homomorphism. Let $\tau : \Gamma \to \mathfrak{P}$ be a lifting of $\bar{\tau}$. Set $c := q_{\mathfrak{U}} \circ \tau : \Gamma \to \mathfrak{U}$. Then

$$\begin{aligned} c(gh) &= q_{\mathfrak{U}}(\tau(g)\tau(h)) = q_{\mathfrak{U}}(\tau(g)_{\mathfrak{U}}\tau(g)_{\mathfrak{L}}\tau(h)_{\mathfrak{U}}\tau(h)_{\mathfrak{L}}) \\ &= q_{\mathfrak{U}}(\tau(g)_{\mathfrak{U}}\tau(g)_{\mathfrak{L}}\tau(h)_{\mathfrak{U}}\tau(g)_{\mathfrak{L}}^{-1}\tau(gh)_{\mathfrak{L}}) = c(g)(\tau(g)_{\mathfrak{L}}c(h)\tau(g)_{\mathfrak{L}}^{-1}) \\ &=: c(g)(\tau(g)_{\mathfrak{L}} \cdot c(h)) \end{aligned}$$

is a (nonabelian) crossed homomorphism. Two liftings τ_1 and τ_2 are equivalent if there exists an element $n \in \mathfrak{U}$ such that $\tau_1 = n\tau_2 n^{-1}$. So $H^1(\Gamma, \mathfrak{U})$ classifies liftings τ of $\bar{\tau}$ up to equivalence.

4.1.4. *Lifting characteristic-p cocycles via inflation-restriction.* Let $[\bar{c}] \in H^1(\Gamma, U(\mathbb{F}))$ be a characteristic-p cocycle. Assume the restriction $[\bar{c}|_H] \in H^1(H, U(\mathbb{F}))$ has a characteristic-0 lift $[c_h] \in H^1(H, U(\mathcal{O}_E))$. We want to build a lift $[c] \in H^1(\Gamma, U(\mathcal{O}_E))$ of $[\bar{c}]$ using $[c_h]$.

Note that when U is an abelian group, this can be easily achieved by taking the average

$$[c] := \frac{1}{\#\Delta} \sum_{g \in \Delta} g \cdot [c_h].$$

Here we identify $H^1(\Gamma, U(\mathcal{O}_E))$ with a subset of $H^1(H, U(\mathcal{O}_E))$ via Proposition 4.1.2.

Such a trick does not work anymore when U is nonabelian. Nonetheless, we have the following:

Lemma 4.1.5. *If there exists $[c_h] \in H^1(H, U(\mathcal{O}_E))$ and $[d] \in H^1(\Gamma, U^{\mathrm{ad}}(\mathcal{O}_E))$ such that $\alpha_2([c_h]) = \mathrm{res}([d])$ and $[c_h]$ mod $\varpi = [\bar{c}|_H]$, then there exists $[c] \in H^1(\Gamma, U(\mathcal{O}_E))$ which is a lifting of $[\bar{c}]$.*

$$\begin{tikzcd}
H^1(\Gamma, Z(U)(\mathcal{O}_E)) \arrow[r, hook, "\mathrm{res}"'] \arrow[d] & H^1(H, Z(U)(\mathcal{O}_E)) \arrow[d] \\
H^1(\Gamma, U(\mathcal{O}_E)) \arrow[r, hook, "\mathrm{res}"'] \arrow[d, "\alpha_1"] & H^1(H, U(\mathcal{O}_E)) \ni [c_h] \arrow[d, "\alpha_2"] \\
{[d] \in H^1(\Gamma, U^{\mathrm{ad}}(\mathcal{O}_E))} \arrow[r, "\mathrm{res}"'] \arrow[d, "\delta_1"] & H^1(H, U^{\mathrm{ad}}(\mathcal{O}_E)) \arrow[d, "\delta_2"] \\
H^2(\Gamma, Z(U)(\mathcal{O}_E)) \arrow[r, hook] & H^2(H, Z(U)(\mathcal{O}_E))
\end{tikzcd}$$

Proof. Since

$$\delta_1([d]) = \delta_2(\alpha_2([c_h])) = 0,$$

we have $[d] = \alpha_1([c'])$ for some $[c'] \in H^1(\Gamma, U(\mathcal{O}_E))$. Since $\operatorname{res}([c'])$ and $[c_h] \in H^1(H, U(\mathcal{O}_E))$ have the same image in $H^1(H, U^{\mathrm{ad}}(\mathcal{O}_E))$ (via α_2), it makes sense to talk about the difference $\operatorname{res}([c']) - [c_h] \in H^1(H, Z(U)(\mathcal{O}_E))$.[1] Consider the diagram

$$\begin{tikzcd}
H^1(\Gamma, Z(U)(\mathcal{O}_E)) \arrow[r] \arrow[d, hook, "\mathrm{res}"] & H^1(\Gamma, Z(U)(\mathbb{F})) \arrow[r, "\delta"] \arrow[d, hook, "\mathrm{res}"] & H^2(\Gamma, Z(U)(\mathcal{O}_E)) \arrow[d, hook] \\
H^1(H, Z(U)(\mathcal{O}_E)) \arrow[r] & H^1(H, Z(U)(\mathbb{F})) \arrow[r, "\delta"] & H^2(H, Z(U)(\mathcal{O}_E))
\end{tikzcd}$$

Let $[\bar{c}'] \in H^1(\Gamma, Z(U)(\mathbb{F}))$ be the reduction mod ϖ of $[c']$. Since $\operatorname{res}([\bar{c}']) - [\bar{c}_h]$ has a lift,

$$\delta(\operatorname{res}([\bar{c}'] - [\bar{c}_h])) = 0 \in H^2(H, Z(U)(\mathbb{F}))$$

by the exactness of the second row of the diagram above. Therefore

$$\delta([\bar{c}'] - [\bar{c}]) = \delta(\operatorname{res}([\bar{c}'] - [\bar{c}])) = \delta(\operatorname{res}([\bar{c}'] - [\bar{c}_h])) = 0$$

and $[\bar{c}'] - [\bar{c}] \in H^1(\Gamma, Z(U)(\mathbb{F}))$ has a characteristic-0 lift $[x]$, and $[c] := [c'] - [x]$ is a lift of $[\bar{c}]$. □

The purpose of the whole Section 4 is to prove Theorem 4.3.2, which extends the above lemma.

4.2. ***External Galois action on the Lyndon–Demushkin cocycle group.*** The earlier subsection shows there is an identification

$$H^1(\Gamma, U(\mathcal{O}_E)) \cong H^1(H, U(\mathcal{O}_E))^{\Delta}.$$

The goal of this subsection is to upgrade this identification to the cochain level.

Since the Galois action

$$\phi(r^\circ)|_{G_{K'}} : G_{K'} \to U(\mathcal{O}_E)$$

is Lyndon–Demushkin, we have a Lyndon–Demushkin complex $C^\bullet_{\mathrm{LD}}(U(\mathcal{O}_E))$ computing $H^\bullet(H, U(\mathcal{O}_E))$. Recall from Section 2.3.2 that a 1-cochain $c \in C^1_{\mathrm{LD}}(U(\mathcal{O}_E))$ is the same as a function

$$\mathfrak{c} : \langle x_0, \dots, x_{n+1} \rangle \to (\operatorname{Lie} U)(\mathcal{O}_E)$$

such that

$$\mathfrak{c}(gh) = \mathfrak{c}(g) + g \cdot \mathfrak{c}(h) + \tfrac{1}{2}[\mathfrak{c}(g), g \cdot \mathfrak{c}(h)]$$

for all g, h; or, equivalently, a function

$$c : \langle x_0, \dots, x_{n+1} \rangle \to U(\mathcal{O}_E)$$

such that

$$c(gh) = c(g)(g \cdot c(h))$$

for all g, h.

[1] $H^1(H, U(\mathcal{O}_E))$ is a $H^1(H, Z(U)(\mathcal{O}_E))$-principle homogeneous space.

A cochain $c : \langle x_0, \dots, x_{n+1}\rangle \to U(\mathcal{O}_E)$ lies in $Z^1_{\mathrm{LD}}(U(\mathcal{O}_E))$ if and only if it factors through the (discrete) Demushkin group $\langle x_0, \dots, x_{n+1}|R\rangle$ (see the proof of Proposition 2.3.6).

Let $c \in Z^1_{\mathrm{LD}}(\mathcal{O}_E)$, regarded as a function $\langle x_0, \dots, x_{n+1}|R\rangle \to U(\mathcal{O}_E)$. Since $U(\mathcal{O}_E)$ is a pro-p group, the crossed homomorphism necessarily factors through the pro-p completion, that is, we have a commutative diagram

$$\begin{tikzcd}
 & \langle x_0, \dots, x_{n+1}|R\rangle \arrow[r, "c"] \arrow[d, "\pi"] & U(\mathcal{O}_E) \\
G_{K'}(p) \arrow[r, equal] & \widehat{\langle x_0, \dots, x_{n+1}\,|\,R\rangle}^{p} \arrow[ur, "\hat{c}"] &
\end{tikzcd}$$

Since we have identified the pro-p quotient of $G_{K'}$ with the pro-p completion of $\langle x_0, \dots, x_{n+1}\,|\,R\rangle$, we can define, for each $g \in G_K$, an automorphism α_g of $Z^1_{\mathrm{LD}}(U(\mathcal{O}_E))$ via

$$\alpha_g(c) := (h \mapsto g \cdot \hat{c}(g^{-1}\pi(h)g)).$$

So we defined an action of G_K on $Z^1_{\mathrm{LD}}(U(\mathcal{O}_E))$.

For ease of notation, write $g \cdot c$ for $\alpha_g(c)$. Note that $(g \cdot c)(h) = (\alpha_g(c))(h)$ is different from $g \cdot c(h)$. We apologize for the confusing notation.

Remark 4.2.1. We don't know whether or not we can define a G_K-action on the whole cochain group $C^1_{\mathrm{LD}}(U(\mathcal{O}_E))$. It seems to involve some subtle combinatorial group theory.

Digression. It is curious to know if the cup product

$$\cup : Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \times Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \to C^2_{\mathrm{LD}}(Z(U(\mathcal{O}_E)))$$

is compatible with the G_K-action.

This answer would be affirmative if, for example, for each $g \in G_K$, the conjugation by g,

$$\phi_g : G_{K'} \to G_{K'},$$

can be lifted to an automorphism of free pro-p groups on $(n+2)$-generators,

$$\phi_g : \langle x_0, \dots, x_{n+1}\rangle \to \langle x_0, \dots, x_{n+1}\rangle.$$

This is closely related to the so-called *Dehn–Nielsen* theorem. Classically, Dehn–Nielsen is saying all automorphism of the fundamental group of the genus g closed surface M_g are induced by a homeomorphism. The algebraic version of Dehn–Nielsen can be formulated as, under the usual presentation of $F = \langle a_1, b_1, \dots, a_g, b_g\rangle \to \langle a_1, b_1, \dots, a_g, b_g|[a_1, b_1] \cdots [a_g, b_g]\rangle \cong \pi_1(M_g)$, all automorphism of $\pi_1(M_g)$ are induced from an automorphism of the free group F.

Conjecture (pro-p Dehn–Nielsen). *All automorphisms of the pro-p completion of $\langle x_0, \dots, x_{n+1}|R\rangle$ are induced by an automorphism of the pro-p completion of $\langle x_0, \dots, x_{n+1}\rangle$.*

4.3. ***Constructing nonabelian cocycles.*** Recall that $H^1(H, U^{\mathrm{ad}})^\Delta = H^1(G_K, U^{\mathrm{ad}})$, where $H = G_{K'}$ and K'/K is a normal extension of prime-to-p degree. Define

$$\begin{aligned}(Z^1_{LD})^\Delta &:= \{x \in Z^1_{\mathrm{LD}} \mid \text{image of } x \text{ in } H^1 \text{ is contained in } (H^1)^\Delta\}\\ &= \{x \in Z^1_{\mathrm{LD}} \mid g\cdot x - x \in B^1_{\mathrm{LD}} \text{ for all } g \in G_K\}.\end{aligned}$$

Since $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))^\Delta$ is a submodule of a finite flat $\mathcal{O}_E$-module, it is finite $\mathcal{O}_E$-flat.

We keep all notation from the previous subsections.

Assume $Z(U)(\mathcal{O}_E) = \mathcal{O}_E$ from now on. We fix some notation. The quotient $U \to U/Z(U) = U^{\mathrm{ad}}$ induces maps $\mathrm{ad} : Z^1_{\mathrm{LD}}(U(\mathcal{O}_E)) \to Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))$.

Lemma 4.3.1. *Assume that $p \neq 2$ and that the cup product*

$$\cup : H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \times H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \to H^2(G_K, Z(U)(\mathbb{F})) \tag{4-2}$$

is nontrivial.

Let $(\bar{c}, \bar{f}) \in Z^1_{\mathrm{LD}}(U(\mathbb{F}))$ (using Lemma 2.3.8). Assume $\bar{c} \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))^\Delta$. If $\bar{c}$ admits a characteristic-0 lift $c' \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}})(\mathcal{O}_E)$, then $(\bar{c}, \bar{f})$ admits a lift $(c, f) \in Z^1_{\mathrm{LD}}(U(\overline{\mathbb{Z}}_p))$ such that $c \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))^\Delta$.

Proof. Pick an arbitrary lift $f \in C^1_{\mathrm{LD}}(Z(U)(\mathcal{O}_E))$ of $\bar{f}$. Choose a system of representatives $\{g_i\} \subset G_K$ of Δ. By replacing c' by the Δ-average $\frac{1}{\#\Delta}\sum g_i \cdot c'$ + some coboundary (which is also a lift of $[\bar{c}]$), we assume $c' \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))^\Delta$.

Let $\lambda \in \overline{\mathbb{Z}}_p^\times$ be a scalar.

Since the symmetric bilinear pairing (4-2) is nontrivial, there exists $y \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E))^\Delta$ such that $y \cup y \neq 0 \bmod \varpi$. Consider

$$(c' + \lambda y) \cup (c' + \lambda y) + d^2(f) = c' \cup c' + d^2(f) + 2\lambda c' \cup y + \lambda^2 y \cup y \in C^2(Z(U)(\mathcal{O}_E)) \cong \mathcal{O}_E,$$

which is a degree two polynomial in λ whose Newton polygon has vertices $(0, +)$, $(1, +$ or $0)$, $(2, 0)$ and thus has at least one solution λ_0 with positive p-adic valuation; here "$+$" means a positive number. Set $(c, f) := (c' + \lambda_0 y, f)$.

We have $(c, f) \in Z^1_{\mathrm{LD}}(U(\overline{\mathbb{Z}}_p))$ by Lemma 2.3.8 and $c \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))^\Delta$. □

Theorem 4.3.2. *Assume that $p \neq 2$ and that the cup product*

$$\cup : H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \times H^1(G_K, U^{\mathrm{ad}}(\mathcal{O}_E)) \otimes \mathbb{F} \to H^2(G_K, Z(U)(\mathbb{F}))$$

is nontrivial.

Let $[(\bar{c}, \bar{f})] \in H^1(G_K, U(\mathbb{F}))$ be a characteristic-p cocycle. If $[\bar{c}|_{G_{K'}}] \in H^1(G_{K'}, U^{\mathrm{ad}}(\mathbb{F}))$ admits a characteristic-0 lift in $H^1(G_{K'}, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))$, then $[(\bar{c}, \bar{f})]$ admits a characteristic-0 lift $[(c, f)] \in H^1(G_K, U(\overline{\mathbb{Z}}_p))$.

Proof. We choose a cocycle $(\bar{c}, \bar{f}) \in Z^1_{\mathrm{LD}}(U(\mathbb{F}))$ which defines the cohomology class $[(\bar{c}, \bar{f})]$. Clearly $\bar{c} \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))^\Delta$. Say $[d] \in H^1(G_{K'}, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))$ is a lift of $[\bar{c}]$, which is defined by $d \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))$. Write $\bar{d}$ for the image of d in $Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\overline{\mathbb{F}}_p))$. By changing d by a coboundary, we can assume $\bar{d} = \bar{c}$.

Lemma 4.3.1 produces $(c, f) \in Z^1_{\mathrm{LD}}(U(\overline{\mathbb{Z}}_p))$ such that $c \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))^\Delta$. Now the theorem follows from Lemma 4.1.5. □

Theorem 4.3.2 is saying that when U is a unipotent group of class 2 with one-dimensional center, there exists a short exact sequence of pointed sets

$$H^1(G_K, U(\overline{\mathbb{Z}}_p)) \to H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{\delta} H^2(G_{K'}, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))$$

under technical assumptions.

Combining Theorems 4.3.2 and 3.3.1, we have very nice obstruction theory for lifting mod ϖ cohomology classes in the mildly regular case.

Theorem 4.3.3. *Assume $p \neq 2$ and $Z(U)(\mathcal{O}_E) = \mathcal{O}_E$. Let $r : G_K \to L(\mathcal{O}_E)$ be a fixed continuous group homomorphism and equip $U(\overline{\mathbb{Z}}_p)$ with the G_K-action $G_K \xrightarrow{r} L(\overline{\mathbb{Z}}_p) \to \mathrm{Aut}(U(\overline{\mathbb{Z}}_p))$. Let K'/K be a finite Galois extension of prime-to-p degree such that $r|_{G_{K'}}$ is Lyndon–Demushkin and mildly regular.*

There is a short exact sequence of pointed sets

$$H^1(G_K, U(\overline{\mathbb{Z}}_p)) \to H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{\delta} H^2(G_{K'}, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p)),$$

where δ has a factorization $H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{z} H^1(G_K, U^{\mathrm{ad}}(\overline{\mathbb{F}}_p)) \to H^2(G_{K'}, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))$.

Proof. Write Δ for $G_K/G_{K'}$. By the moreover part of Theorem 3.3.1, there are two cases to consider.

Case I: the cup product (4-2), $H^1(G_K, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p)) \otimes \mathbb{F} \times H^1(G_K, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p)) \otimes \mathbb{F} \to H^2(G_K, Z(U)(\overline{\mathbb{Z}}_p)) \otimes \mathbb{F}$, is nontrivial. This is a corollary of Theorem 4.3.2.

Case II: $H^2(G_K, Z(U)(\mathbb{F})) = 0$. The short exact sequence $0 \to Z(U)(\mathcal{O}_E) \to Z(U)(\mathcal{O}_E) \to Z(U)(\mathbb{F}) \to 0$ induces a long exact sequence $H^2(G_K, Z(U)(\mathcal{O}_E)) \to H^2(G_K, Z(U)(\mathbb{F})) \to 0$. By Nakayama's lemma, $H^2(G_K, Z(U)(\mathcal{O}_E)) = 0$, and thus $H^2(G_K, Z(U)(\overline{\mathbb{Z}}_p)) = 0$ by flat base change.

Let $[(\bar{c}, \bar{f})] \in H^1(G_K, U(\overline{\mathbb{F}}_p))$ be a cohomology class defined by $(\bar{c}, \bar{f}) \in Z^1_{\mathrm{LD}}(U(\overline{\mathbb{F}}_p))$.

Set $\delta : H^1(G_K, U(\overline{\mathbb{F}}_p)) \to H^2(G_{K'}, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))$ to be the composite

$$H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{[(\bar{c}, \bar{f})] \mapsto [\bar{c}]} H^1(G_K, U^{\mathrm{ad}}(\overline{\mathbb{F}}_p)) \to H^2(G_{K'}, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p)).$$

If $\delta([(\bar{c}, \bar{f})]) = 0$, then there exists a lift $c \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))$ of $\bar{c}$. By replacing c by the Δ-average of c, we assume $c \in Z^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))^\Delta$. Since $H^2(G_K, Z(U)(\overline{\mathbb{Z}}_p)) = 0$, $[c \cup c] = 0$ and thus there exists $g \in C^1_{\mathrm{LD}}(Z(U)(\overline{\mathbb{Z}}_p))^\Delta$ such that $c \cup c = -d^2(g)$. Write $\bar{g}$ for the image of g in $C^1_{\mathrm{LD}}(Z(U)(\overline{\mathbb{F}}_p))$. We have $\bar{g} - \bar{f} \in Z^1_{\mathrm{LD}}(Z(U)(\overline{\mathbb{F}}_p))^\Delta$. Since $H^2(G_K, Z(U)(\overline{\mathbb{Z}}_p)) = 0$, there exists a lift $h \in Z^1_{\mathrm{LD}}(Z(U)(\overline{\mathbb{Z}}_p))^\Delta$ of $\bar{f} - \bar{g}$. It is clear that $[(c, g + h)] \in H^1(G_K, U(\overline{\mathbb{Z}}_p))$ is a lift of $[(\bar{c}, \bar{f})]$. □

Corollary 4.3.4. *Assume $p \neq 2$ and $Z(U)(\mathcal{O}_E) = \mathcal{O}_E$. Let $r : G_K \to L(\mathcal{O}_E)$ be a continuous group homomorphism.*

If there exists a finite Galois extension K'/K of prime-to-p degree such that $r|_{G_{K'}}$ is Lyndon–Demushkin and mildly regular, then there is a short exact sequence of pointed sets

$$H^1(G_K, U(\overline{\mathbb{Z}}_p)) \to H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{\delta} H^2(G_K, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))$$

where δ has a factorization $H^1(G_K, U(\overline{\mathbb{F}}_p)) \xrightarrow{z} H^1(G_K, U^{\mathrm{ad}}(\overline{\mathbb{F}}_p)) \to H^2(G_K, U^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))$.

Proof. This is an immediate consequence of Theorem 4.3.3. □

5. The machinery for lifting nonabelian cocycles

Let $K/\mathbb{Q}_p$ be a p-adic field. Let $E/\mathbb{Q}_p$ be the coefficient field with ring of integers $\mathcal{O}_E$, residue field $\mathbb{F}$ and uniformizer ϖ.

5.0.1. *Emerton–Gee stacks.* Let H be a connected reductive group over K which splits over a tame extension K_H/K. Denote by ${}^LH$ the Langlands dual group $\widehat{H} \rtimes \mathrm{Gal}(K_H/H)$ where $\widehat{H}$ is the split connected reductive group over $\mathbb{Z}$ whose root datum is dual to that of H. The reduced Emerton–Gee stack $\mathcal{X}_{{}^LH,\mathrm{red}}$ is a reduced algebraic stack defined over $\mathbb{F}_p$ (see [Lin 2023b, Theorem 1]).

Moreover, it is proved in many cases that $\mathcal{X}_{K,{}^LH,\mathrm{red}}$ is equidimensional of dimension $[K:\mathbb{Q}_p]\dim \widehat{H}/B_{\widehat{H}}$, where $B_{\widehat{H}}$ is a Borel of $\widehat{H}$ (see [Lin 2023b]).

5.0.2. *Potentially semistable lifting rings.* Write $L := {}^LH$ for simplicity. Let $\bar{r} : G_K \to L(\mathbb{F})$ be a mod ϖ Langlands parameter, that is, a continuous group homomorphism such that the composite $G_K \to {}^LH(\overline{\mathbb{F}}_p) \to \mathrm{Gal}(K_H/K)$ is the canonical quotient map. Let $\underline{\lambda}$ be a Hodge type and let τ be a inertial Galois type (see [Lin 2023c] for the definitions). The potentially semistable deformation ring $R_{\bar{r}}^{\underline{\lambda},\tau,\mathcal{O}}$ of $\bar{r}$ of p-adic Hodge type $\underline{\lambda}$ is constructed in [Bellovin and Gee 2019, Theorem 3.3.8]. It is an $\mathcal{O}$-flat quotient of the universal lifting ring, and is equidimensional of dimension $(1 + \dim \widehat{H} + [K : \mathbb{Q}_p] \dim \widehat{H}/B_{\widehat{H}})$ when $\underline{\lambda}$ is a regular Hodge type.

5.1. *A geometric argument of Emerton–Gee.*

Definition 5.1.1. Let $\mathcal{F}$ be a coherent sheaf over a scheme $X = \operatorname{Spec} R$. We say $\mathcal{F}$ is *sufficiently generically regular* (SGR) if for each $s \geq 1$, the locus

$$X_s := \{x \in \operatorname{Spec} R \mid \dim \kappa(x) \otimes_R \mathcal{F} \geq s\}$$

has codimension $\geq s + 1$ in $\operatorname{Spec} R$.

Theorem 5.1.2. *Let $X = \operatorname{Spec} R$ with R a complete reduced, $\mathbb{Z}_p$-flat local ring that is equidimensional of dimension $(1 + \dim L + \dim \mathcal{X}_{L,\mathrm{red}})$. Let $r^{\mathrm{univ}} : G_K \to L(R)$ be a family of L-parameters on X. Assume $X[1/p] \neq \varnothing$. Let $F : L \to \mathrm{GL}(V)$ be an algebraic representation where V is a vector space scheme over $\mathcal{O}_E$.*

Assume $H^2(G_K, F(r^{\mathrm{univ}}))$ is SGR over X and is supported on $X \otimes_{\mathbb{Z}_p} \mathbb{F}_p$. Given any $[\bar{c}] \in H^1(G_K, F(\bar{r}))$, there exists a $\overline{\mathbb{Z}}_p$-point of X giving rise to a Galois representation $r^\circ : G_K \to L(\overline{\mathbb{Z}}_p)$, such that the 1-cocycle $[\bar{c}]$ admits a lift $[c] \in H^1(G_K, F(r^\circ))$.

Remark 5.1.3. Since $H^2(G_K, -)$ (abelian coefficients) is the highest degree cohomology ($H^i(G_K, -) = 0$ for $i > 2$), $H^2(G_K, -)$ commutes with base change. Thus we may view $H^2(G_K, F(r^{\mathrm{univ}}))$ as a coherent sheaf over X.

The proof is almost identical to that of [Emerton and Gee 2023, Theorem 6.3.2].

We would like to explain the main ideas behind the proof, and why we need the sufficiently generically regular condition.

We have a complex of finitely generated projective modules over R concentrated on degree [0, 2]

$$C^0 \to C^1 \xrightarrow{d} C^2$$

which computes the Galois cohomology $H^\bullet(G_K, F(r^{\mathrm{univ}}))$. Let $Z^1 := \ker(d)$ and $B^2 := \mathrm{Im}(d)$. A mod ϖ cocycle $[\bar{c}]$ is represented by an element $\bar{c}$ in the kernel of $C^1/\varpi \to C^2/\varpi$. We fix an arbitrary lift $\tilde{c} \in C^1$ of $\bar{c}$. We can do a formal blowup $\operatorname{Spec} \widetilde{R} \to \operatorname{Spec} R$, so that the pullback of B^2 on $\operatorname{Spec} \widetilde{R}$ a locally free sheaf. To make the exposition short, we simply assume B^2 is locally free over $\operatorname{Spec} R$, but we should not think of $\operatorname{Spec} R$ as a local ring anymore, because after formal blow-up, there are more closed points in the special fiber. Now we have a sequence of locally free sheaves of modules

$$C^1 \to B^2 \to C^2.$$

The key here is we want to regard this as a sequence of vector bundles instead of sheaves of modules. Write $\mathscr{V}(\mathcal{F})$ for $\underline{\mathrm{Spec}}(\mathrm{Sym}\,\mathcal{F}^\vee)$, the vector bundle associated to the coherent sheaf $\mathcal{F}$. So we have a sequence of scheme morphisms

$$\begin{tikzcd}
\mathscr{V}(C^1) \arrow[r, "f"] \arrow[rr, bend left, "d"] & \mathscr{V}(B^2) \arrow[r] & \mathscr{V}(C^2) \\
& \operatorname{Spec} R \arrow[ul, "s"] \arrow[u, "f\circ s"] \arrow[ur, "d\circ s"'] &
\end{tikzcd}$$

The element $\tilde{c}$ of C^1 defines a section $s : \operatorname{Spec} R \to \mathscr{V}(C^1)$ such that the section $d \circ s : \operatorname{Spec} R \to \mathscr{V}(C^2)$ intersects with the identity section $e_{\mathscr{V}(C^2)} : \operatorname{Spec} R \to \mathscr{V}(C^2)$.

It turns out $\bar{c} \in \ker(C^1/\varpi \to C^2/\varpi)$ admits a lift in Z^1, as long as the section $f \circ s$ intersects with the identity section $e_{\mathscr{V}(B^2)}$ of $\mathscr{V}(B^2)$. The intersection $(d \circ s) \cap e_{\mathscr{V}(C^2)}$ should occur above a codimension 1 locus of $\operatorname{Spec} R$. If the support of $H^2 = C^2/B^2$ is small (that is, has big codimension), then the intersection should happen at some point $x \in \operatorname{Spec} R$ outside of the support of H^2, and we are done.

We include a formal proof here, as suggested by a referee.

Proof. We follow the notation of [Emerton and Gee 2023, Theorem 6.3.2] closely. The Herr complex $C^\bullet$ (supported in degrees [0, 2]) computes $H^\bullet(G_K, F(r^{\mathrm{univ}}))$. Since B^2 equals to C^2 over the generic fiber $U = X[1/p]$, by [Stacks, Tag 0815], there exists a U-admissible blowup $\pi : \widetilde{X} \to X$ such that $\pi^* B^2$ is locally free. Let $\widetilde{C}^\bullet$ be the pullback complex $\pi^*(C^\bullet)$. The corresponding 2-coboundaries $\widetilde{B}^2 = \pi^* B^2$ (since it is the highest degree coboundary). Thus the 1-cocycles $\widetilde{Z}^1$ is locally free and $[\widetilde{C}^0 \to \widetilde{Z}^1]$ is a good complex.

Lifting the class $[\bar{c}]$ to an element of $\kappa \otimes C^1$ (where κ is the residue field of R) and then to an element c of C^1. c can be thought of as a homomorphism $R \to C^1$ whose image under the coboundary lies in $m_R C^2$. The composite $b : R \xrightarrow{c} C^1 \to B^2$ pulls back to a section $\tilde{b} : \mathcal{O}_{\widetilde{X}} \to \widetilde{B}^2$. By [Emerton and Gee 2023, Lemma 6.2.7] and the SGR property, $\tilde{b}$ has nonempty zero locus, which contain a point $\tilde{x}$ lying over the closed point $x \in X$. The section c pulls back to a section $\tilde{c} : \mathcal{O}_{\widetilde{X}} \to \widetilde{C}^1$, whose valued at the point $\tilde{x}$ lies in the fiber of $\widetilde{Z}^1$. In other words, the fiber of $\tilde{c}$ at $\tilde{x}$ defines a 1-cocycle in the complex $\kappa(\tilde{x}) \otimes [\widetilde{C}^0 \to \widetilde{Z}^1]$, giving rise to a class $\bar{e} \in H^1(\kappa(\tilde{x}) \otimes [\widetilde{C}^0 \to \widetilde{Z}^1])$ lifting the original class $[\bar{c}]$.

Since $\widetilde{X}$ is $\mathbb{Z}_p$-flat, there exists a morphism $\tilde{f} : \operatorname{Spec} \overline{\mathbb{Z}}_p \to \widetilde{X}$ lifting $\tilde{x}$. The composite $f : \operatorname{Spec} \overline{\mathbb{Z}}_p \xrightarrow{\tilde{f}} \widetilde{X} \to X$ lifts the closed point $x \in X$, and determines an L-parameter $r^\circ : G_K \to L(\overline{\mathbb{Z}}_p)$. Since $H^2(\widetilde{C}^\bullet)$ is the kernel of the homomorphism of locally free sheaves $\widetilde{B}^2 \hookrightarrow \widetilde{C}^2$ and is torsion, by [Emerton and Gee 2023, Lemma 6.2.1] there is an effective Cartier divisor D contained in the special fiber of $\widetilde{X}$ with the property that for any morphism to $\widetilde{X}$ that meets D properly, the higher derived pullbacks of $H^2(\widetilde{C}^\bullet)$ under this morphism vanish. Since $\tilde{f}$ meets the special fiber of $\widetilde{X}$ properly and thus meets D properly, $\boldsymbol{L}_i \tilde{f}^* H^2(\widetilde{C}^\bullet) = 0$ for $i > 0$. Thus

$$H^1(G_K, F(r^\circ)) = H^1(\tilde{f}^* \widetilde{C}^\bullet) = \tilde{f}^* H^1(\widetilde{C}^\bullet) = H^1(\tilde{f}^*[\widetilde{C}^0 \to \widetilde{Z}^1]).$$

(See the last two paragraphs of the proof [Emerton and Gee 2023, Theorem 6.3.2] for explanations). Choose a class $e \in H^1(\tilde{f}^*[\widetilde{C}^0 \to \widetilde{Z}^1])$ lifting $\bar{e}$, which corresponds to a 1-cocycle c lifting $\bar{e}$ by the identifications above. □

5.2. *A nonabelian lifting theorem.*

Theorem 5.2.1. *Let U be a unipotent linear algebraic group of class 2 whose center is isomorphic to $\mathbb{G}_a$. Write $Z(U)$ for the center of U and U^{ad} for $U/Z(U)$. Fix an algebraic group homomorphism $\phi : L \to \operatorname{Aut}(U)$ with graded pieces $\phi^{\mathrm{ad}} : L \to \operatorname{GL}(U^{\mathrm{ad}})$ and $\phi^{z} : L \to \operatorname{GL}(Z(U))$.*

Fix a mod ϖ representation $\bar{r} : G_K \to L(\mathbb{F})$. Let $[\bar{c}] \in H^1(G_K, U(\mathbb{F}))$ be a characteristic-p cocycle. Let Spec R *be an irreducible component of a crystalline lifting ring of $\bar{r}$. Assume*

(1) $H^2(G_K, \phi^{\mathrm{ad}}(r^{\mathrm{univ}}))$ *is SGR and is supported on the special fiber of* Spec R;

(2) $p \neq 2$;

(3) *there exists a finite Galois extension K'/K of prime-to-p degree such that $\phi(\bar{r})|_{G_{K'}}$ is Lyndon–Demushkin*; *and*

(4) *there exists a $\overline{\mathbb{Z}}_p$-point of* Spec R *which is mildly regular when restricted to $G_{K'}$*. (*In particular*, Spec $R[1/p] \neq 0$.)

Then there exists a $\overline{\mathbb{Z}}_p$-point of Spec R *which gives rise to a Galois representation $r^\circ : G_K \to L(\overline{\mathbb{Z}}_p)$ such that if we endow $U(\overline{\mathbb{Z}}_p)$ with the G_K-action $G_K \xrightarrow{r^\circ} L(\overline{\mathbb{Z}}_p) \xrightarrow{\phi} \operatorname{Aut}(U)(\overline{\mathbb{Z}}_p)$, the cocycle $[\bar{c}]$ has a characteristic-0 lift $[c] \in H^1(G_K, U(\overline{\mathbb{Z}}_p))$.*

Proof. Take $F = \phi^{\mathrm{ad}}$ in Theorem 5.1.2. The theorem follows from Corollary 4.3.4. □

We explain how the above theorem will be used. Let G be a connected reductive group over $\mathcal{O}_E$. Let $\bar{\rho} : G_K \to G(\mathbb{F})$ be a mod ϖ representation. Assume $\bar{\rho}$ factors through a parabolic $P \subset G$, with Levi decomposition $P = L \ltimes U$. Denote by $\phi : L \to \operatorname{Aut}(U)$ the conjugation action. We assume U is unipotent of class 2, so U^{ad} is an abelian group. Write $\bar{r}$ for the Levi factor of $\bar{\rho}$.

$$\begin{tikzcd} & P(\overline{\mathbb{F}}_p) \arrow[d] \\ G_K \arrow[ur, "\bar{\rho}"] \arrow[r, "\bar{r}"] & L(\overline{\mathbb{F}}_p) \end{tikzcd}$$

Then $\bar{\rho}$ defines a cohomology class $[\bar{c}] \in H^1(G_K, \phi(\bar{r}))$, and the theorem above can be used to lift $[\bar{c}]$.

5.3. ***An unobstructed lifting theorem.*** The following result will be used in the proof of the main theorem.

Proposition 5.3.1. *Let V be a unipotent linear algebraic group such that $V(\overline{\mathbb{Z}}_p)$ is equipped with a continuous G_K-action. Let $[\bar{c}] \in H^1(G_K, V(\overline{\mathbb{F}}_p))$ be a characteristic-p cocycle. Let $Z(V)$ be the center of V, and write V^{ad} for $V/Z(V)$. The quotient $V \to V^{\mathrm{ad}}$ induces a map* $\mathrm{ad} : H^1(G_K, V) \to H^1(G_K, V^{\mathrm{ad}})$. *Assume $H^2(G_K, Z(V)(\overline{\mathbb{F}}_p)) = 0$.*

If $\mathrm{ad}([\bar{c}])$ *admits a lift in $H^1(G_K, V^{\mathrm{ad}}(\overline{\mathbb{Z}}_p))$, then $[\bar{c}]$ admits a lift in $H^1(G_K, V(\overline{\mathbb{Z}}_p))$.*

Proof. By [Serre 2002, Proposition 43], since $Z(V)$ is a central normal subgroup of V, there exists a long exact sequence of pointed sets

$$\begin{tikzcd} H^1(G_K, V(\overline{\mathbb{Z}}_p)) \arrow[r, "\mathrm{ad}"] \arrow[d] & H^1(G_K, V^{\mathrm{ad}}(\overline{\mathbb{Z}}_p)) \arrow[r, "\delta"] \arrow[d] & H^2(G_K, Z(V)(\overline{\mathbb{Z}}_p)) \arrow[d] \\ H^1(G_K, V(\overline{\mathbb{F}}_p)) \arrow[r, "\mathrm{ad}"] & H^1(G_K, V^{\mathrm{ad}}(\overline{\mathbb{F}}_p)) \arrow[r] & H^2(G_K, Z(V)(\overline{\mathbb{F}}_p)) \end{tikzcd}$$

By Nakayama's lemma, we have $H^2(G_K, Z(V)(\overline{\mathbb{Z}}_p)) = 0$. In particular, there exists $[c'] \in H^1(G_K, V(\overline{\mathbb{Z}}_p))$ such that $\mathrm{ad}([\bar{c}]) = \mathrm{ad}([c'])$ mod ϖ. Write $[\bar{c}']$ for $[c']$ mod ϖ. Say $[\bar{c}] = [\bar{c}'] + [\bar{f}]$ for some $[\bar{f}] \in H^1(G_K, Z(V)(\overline{\mathbb{F}}_p))$ (recall that $H^1(G_K, V)$ is a $H^1(G_K, Z(V))$-torsor). Since $H^1(G_K, Z(V)(\overline{\mathbb{Z}}_p)) = 0$, there exists a lift $[f]$ of $\bar{f}$. The cocycle $[c] := [c'] + [f]$ is a lift of $[\bar{c}]$. □

6. Codimension estimates of loci cut out by H^2

Assume $p > 3$. Let $K/\mathbb{Q}_p$ be a finite extension. Let $E/\mathbb{Q}_p$ be a finite extension with ring of integers $\mathcal{O}_E$, uniformizer ϖ, and residue field $\mathbb{F}$.

6.1. ***The Emerton–Gee stack.*** We follow the notation of [Emerton and Gee 2023]. For each $d > 0$, Emerton and Gee [2023] constructed the moduli stack $\mathcal{X}_d = \mathcal{X}_{K,d}$ of projective étale (ϕ, Γ_K)-modules of rank d, which is a finite-type algebraic stack over $\mathbb{F}$.

We prove a mild generalization of [Emerton and Gee 2023, Proposition 5.4.4(1)].

Let T be a reduced finite-type $\overline{\mathbb{F}}_p$-scheme. Let $f : T \to (\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p}$ be a morphism. There is a morphism

$$\eta : (\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p} \to (\mathcal{X}_{ad,\mathrm{red}})_{\overline{\mathbb{F}}_p}$$

sending a pair of (ϕ, Γ)-modules M, N to their hom module $\mathrm{Hom}_{\phi,\Gamma}(M, N)$, by the moduli interpretation. The morphism $\eta(f)$ corresponds to a family $\bar{\rho}_T$ of rank ad Galois representations over T. We assume $H^2(G_K, \bar{\rho}_{\eta(t)})$ is of constant rank for all $t \in T(\overline{\mathbb{F}}_p)$. By [Emerton and Gee 2023, Lemma 5.4.1], the coherent sheaf $H^2(G_K, \bar{\rho}_T)$ is locally free of rank r as an $\mathcal{O}_E$-module.

By [Emerton and Gee 2023, Theorem 5.1.22], we can choose a complex of finite rank locally free $\mathcal{O}_E$-modules

$$C_T^0 \to C_T^1 \to C_T^2$$

computing $H^\bullet(G_K, \bar{\rho}_T)$. Since $H^2(G_K, \bar{\rho}_T)$ is a locally free sheaf, the truncated complex

$$C_T^0 \to Z_T^1$$

is again a complex of locally free $\mathcal{O}_T$-modules. The vector bundle $\mathscr{V}(Z_T^1) := \underline{\mathrm{Spec}}(\mathrm{Sym}(Z_T^1)^\vee)$ associated to the locally free sheaf Z_T^1 parametrizes all extensions

$$0 \to \bar{\rho}_{\eta(t)} \to ? \to \overline{\mathbb{F}}_p \to 0, \quad t \in T(\overline{\mathbb{F}}_p)$$

of the trivial G_K-representation $\overline{\mathbb{F}}_p$ by $\bar{\rho}_{\eta(t)}$. There are two projection morphisms

$$(\,)_1 : (\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p} \to (\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p} \quad \text{and} \quad (\,)_2 : (\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p} \to (\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p}.$$

For each $t \in T(\overline{\mathbb{F}}_p)$, $f(t)_1 \in (\mathcal{X}_{a,\mathrm{red}})(\overline{\mathbb{F}}_p)$ corresponds to a rank-a Galois representation $\bar{\rho}_{t_1}$, and $f(t)_2 \in (\mathcal{X}_{d,\mathrm{red}})(\overline{\mathbb{F}}_p)$ corresponds to a rank-d Galois representation $\bar{\rho}_{t_2}$. We have $\bar{\rho}_{\eta(t)} = \mathrm{Hom}_{G_K}(\bar{\rho}_{t_1}, \bar{\rho}_{t_2})$. So we can also regard $\mathscr{V}(Z_T^1)$ is a scheme parametrizing all extensions

$$0 \to \bar{\rho}_{t_1} \to ? \to \bar{\rho}_{t_2} \to 0, \quad t \in T(\overline{\mathbb{F}}_p)$$

and we have a morphism sending extension classes to equivalence classes of G_K-representations,

$$g : \mathscr{V}(Z_T^1) \to (\mathcal{X}_{a+d,\mathrm{red}})_{\overline{\mathbb{F}}_p}.$$

Lemma 6.1.1. *Let e denote the dimension of the scheme-theoretic image of T in $(\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p}$. Then the scheme-theoretic image of $V = \mathscr{V}(Z_T^1)$ in $(\mathcal{X}_{a+d,\mathrm{red}})_{\overline{\mathbb{F}}_p}$ has dimension at most*

$$e + r + ad[K : \mathbb{Q}_p].$$

Proof. Without loss of generality, we assume T (and hence V) is irreducible. The proof is a routine calculation using stacks. We follow the proof of [Emerton and Gee 2023, Proposition 5.4.4] closely.

Let $v \in V(\overline{\mathbb{F}}_p)$. Write t for the composite $\operatorname{Spec}\overline{\mathbb{F}}_p \xrightarrow{v} V \to T$. Write $f(t)$ for the composite $f \circ t$ Write $g(v)$ for the composite $g \circ v$. Define

$$\begin{aligned} T_{f(t)} &:= T \underset{f,(\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p}\times(\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p},f(t)}{\times} \operatorname{Spec}\overline{\mathbb{F}}_p, \\ V_{g(v)} &:= V \underset{g,(\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p}\times(\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p},g(v)}{\times} \operatorname{Spec}\overline{\mathbb{F}}_p, \\ V_{f(t),g(v)} &:= V_{g(v)} \underset{(\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p}\times(\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p},f(t)}{\times} \operatorname{Spec}\overline{\mathbb{F}}_p. \end{aligned}$$

Note that $V_{f(t),g(v)} \cong T_{f(t)} \times_T V_{g(v)}$.

By [Stacks, Tag 0DS4], it suffices to show, for v lying in some dense open subset of V,

$$\dim V_{f(t),g(v)} \geq \dim V - (e + r + ad[K:\mathbb{Q}_p]).$$

Let $\bar{\rho}_{f(t)_1}$ denote the Galois representation corresponding to $f(t)_1 : \operatorname{Spec}\overline{\mathbb{F}}_p \to (\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p}$. Let $\bar{\rho}_{f(t)_2}$ denote the Galois representation corresponding to $f(t)_2 : \operatorname{Spec}\overline{\mathbb{F}}_p \to (\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p}$. Say $G_{t_1} := \operatorname{Aut}(\bar{\rho}_{f(t)_1})$, and $G_{t_2} := \operatorname{Aut}(\bar{\rho}_{f(t)_2})$. The morphism $f(t)$ factors through a monomorphism

$$[\operatorname{Spec}\overline{\mathbb{F}}_p/G_{t_1}] \times [\operatorname{Spec}\overline{\mathbb{F}}_p/G_{t_2}] \hookrightarrow (\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p} \times (\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p}$$

which induces a monomorphism

$$([\operatorname{Spec}\overline{\mathbb{F}}_p/G_{t_1}] \times [\operatorname{Spec}\overline{\mathbb{F}}_p/G_{t_2}]) \underset{(\mathcal{X}_{a,\mathrm{red}})_{\overline{\mathbb{F}}_p}\times(\mathcal{X}_{d,\mathrm{red}})_{\overline{\mathbb{F}}_p}}{\times} V_{g(v)} \hookrightarrow V_{g(v)}.$$

So it suffices to show

$$\dim V_{f(t),g(v)} \geq \dim V - (e + r + ad[K:\mathbb{Q}_p]) + \dim G_{t_1} + \dim G_{t_2} \tag{6-1}$$

for v lying in a dense open of V.

There exists an étale cover S of $(T_{f(t)})_{\mathrm{red}}$ such that the pullback family $\bar{\rho}_S$ is a trivial family with fiber $\bar{\rho}_t$.

Let $C^0_S \to Z^1_S$ denote the pullback family of $C^0_T \to Z^1_T$ to S. $C^0_S \to Z^1_S$ is also the pullback family of the fiber $C^0_t \to Z^1_t$ to S. Write W for the affine scheme associated to $H^1(G_K, \bar{\rho}^\vee_{f(t)_1} \otimes \bar{\rho}_{f(t)_2})$. By the isomorphism

$$H^1(G_K, \bar{\rho}^\vee_{f(t)_1} \otimes \bar{\rho}_{f(t)_2}) \cong \operatorname{Ext}_{G_K}(\bar{\rho}_{f(t)_1}, \bar{\rho}_{f(t)_2})$$

there is a morphism $W \to (\mathcal{X}_{a+d,\mathrm{red}})_{\overline{\mathbb{F}}_p}$. Denote by w the image of v in w. We have

$$S \times_T V_{g(v)} = S \times_T V \times_W W_{h(w)}.$$

Let V' be the kernel of $S \times_T V \to S \times_{\overline{\mathbb{F}}_p} W$, which is a trivial vector bundle over S. We have

$$\begin{aligned} \dim V_{f(t),g(v)} &= \dim S \times_T V_{g(v)} \\ &= \operatorname{rank} V' + \dim S + \dim W_{h(w)} \\ &= \operatorname{rank} Z^1_T - \dim H^1(G_K, \bar{\rho}^\vee_{f(t)_1} \otimes \bar{\rho}_{f(t)_2}) + \dim S + \dim W_{h(w)}. \end{aligned}$$

Note that $\dim V - \dim T = \operatorname{rank} Z^1_T$, and, by the local Euler characteristic,

$$H^0(G_K, \bar\rho^\vee_{f(t)_1} \otimes \bar\rho_{f(t)_2}) - H^1(G_K, \bar\rho^\vee_{f(t)_1} \otimes \bar\rho_{f(t)_2}) + r = -ad[K : \mathbb{Q}_p].$$

We can replace T by a dense open of T where $e = \dim T - \dim T_{f(t)} = \dim T - \dim S$. Combining all these equalities, (6-1) becomes

$$\dim W_{h(w)} \geq \dim H^0(G_K, \bar\rho^\vee_{f(t)_1} \otimes \bar\rho_{f(t)_2}) + \dim G_{t_1} + \dim G_{t_2}$$

which follows from the fact that

$$H^0(G_K, \bar\rho^\vee_{f(t)_1} \otimes \bar\rho_{f(t)_2}) \rtimes (G_{t_1} \times G_{t_2}) \subset \operatorname{Aut}(\bar\rho_w)$$

and $\dim W_{h(w)} \geq \dim \operatorname{Aut}(\bar\rho_w)$. □

We recall some terminology from [Emerton and Gee 2023]. Denote by $\mathrm{ur}_x : \mathbb{G}_m \to \mathcal{X}_1$ the family of unramified characters of G_K. Let T be a reduced finite-type $\mathbb{F}$-scheme. Let $T \to \mathcal{X}$ be a morphism, corresponding to a family $\bar\rho_T$ of G_K-representations over T. We can construct the family of unramified twisting $\bar\rho_T \boxtimes \mathrm{ur}_x$ over $T \times \mathbb{G}_m$. $\bar\rho_T$ is said to be *twistable* if whenever $\bar\rho_t \cong \bar\rho_{t'} \otimes \mathrm{ur}_a$ for $t, t' \in T(\overline{\mathbb{F}}_p)$ and $a \in \overline{\mathbb{F}}_p^\times$, we have $a = 1$. $\bar\rho_T$ is said to be *essentially twistable* if for each $t \in T(\overline{\mathbb{F}}_p)$, the set of $a \neq 1$ for which $\bar\rho_t \cong \bar\rho_{t'} \otimes \mathrm{ur}_a$ is finite.

We say $\bar\rho_T$ is *untwistable* if $\bar\rho$ is not essentially twistable.

From now on, write $\mathcal{X} = (\mathcal{X}_{2,\mathrm{red}})_{\overline{\mathbb{F}}_p}$ for the moduli stack parametrizing (ϕ, Γ)-modules of rank 2.

Let $\bar r^{\mathrm{univ}}$ be the universal family of (ϕ, Γ)-modules over $\mathcal{X}$.

6.1.2. *Remarks on the word use "locus".* Let (P) be a property that can be written as

$$(\mathrm{P}) = (\mathrm{P1}) - (\mathrm{P2})$$

where both (P1) and (P2) are closed conditions.

If $\mathcal{X}$ be a moduli stack of finite type over $\overline{\mathbb{F}}_p$, the *locus of objects satisfying property* (Pi) is by definition the scheme-theoretic of a finite-type morphism $Y \to \mathcal{X}$ such that all objects of $\mathcal{X}(\overline{\mathbb{F}}_p)$ satisfying property (Pi) are in the image of $Y(\overline{\mathbb{F}}_p)$, $i = 1, 2$.

The *locus of objects satisfying property* (P) is by definition the locus of objects satisfying (P1) − locus of objects satisfying (P2).

6.2. *Loci cut out by $H^2(G_K, \mathrm{sym}^3 / \det^2)$.*

Write H^2 for $H^2(G_K, \mathrm{sym}^3(\bar r^{\mathrm{univ}})/\det(\bar r^{\mathrm{univ}})^2)$. Let $x \in \mathcal{X}(\overline{\mathbb{F}}_p)$ with corresponding Galois representation $\bar r_x : G_K \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$.

We are interested in $H^2(G_K, \mathrm{sym}^3 / \det^2)$ because it is a composition factor of the unipotent radical of the short root parabolic of the exceptional group G_2, regarded as a representation of the corresponding Levi factor.

Lemma 6.2.1. *If $\bar r_x$ is irreducible, then*

$$h^2_x := \dim_{\overline{\mathbb{F}}_p} H^2\left(G_K, \frac{\mathrm{sym}^3(\bar r_x)}{\det(\bar r_x)^2}\right) \leq 2.$$

Proof. An irreducible mod ϖ representation is of the shape $\operatorname{Ind}_{G_{K_2}}^{G_K} \bar{\chi}$ for some character $\bar{\chi}$ of the degree 2 unramified extension K_2 of K. A direct computation shows

$$\operatorname{sym}^3(\bar{r}_x) = \operatorname{Ind}(\bar{\chi}^3) \oplus \operatorname{Ind}(\bar{\chi} \det \bar{r}_x).$$

Both

$$H^2\left(G_K, \frac{\operatorname{Ind}(\bar{\chi}^3)}{\det(\bar{r}_x)^2}\right) \quad \text{and} \quad H^2\left(G_K, \frac{\operatorname{Ind}(\bar{\chi} \det \bar{r}_x)}{\det(\bar{r}_x)^2}\right)$$

have dimension at most 1. This is because the induction of a character can't be a direct sum of two isomorphic characters (when $p \neq 2$), by Shapiro's lemma and local Tate duality. □

Corollary 6.2.2. *H^2 is SGR when restricted to the irreducible locus.*

Proof. Up to unramified twist, there are only finitely many irreducible representations. By Lemma 6.2.1, we have $h_x^2 \leq 2$ when $\bar{r}_x$ is irreducible.

We first consider the sublocus where $h_x^2 = 2$. This sublocus consists of finitely many irreducible G_K-representations. Thus the sublocus in question is the scheme-theoretic union of the scheme-theoretic images of finitely many morphisms $\operatorname{Spec} \bar{\mathbb{F}}_p \to \mathcal{X}$ corresponding to the finitely many irreducibles. The automorphism group of such an irreducible representation is $\mathbb{G}_m$ and the morphisms $\operatorname{Spec} \bar{\mathbb{F}}_p \to \mathcal{X}$ factor through $[\operatorname{Spec} \bar{\mathbb{F}}_p/\mathbb{G}_m] \to \mathcal{X}$. The sublocus has dimension at most -1.

Then we consider the locus where $h_x^2 \leq 1$. This sublocus consists of the unramified twists of finitely many irreducible G_K-representations. Thus the sublocus in question is the scheme-theoretic union of the scheme-theoretic images of finitely many morphisms $\mathbb{G}_m \to [\mathbb{G}_m/\mathbb{G}_m] \to \mathcal{X}$ corresponding to the finitely many irreducibles, and has dimension at most $\dim[\mathbb{G}_m/\mathbb{G}_m] = 0$.

In either case, the dimension of the locus is at most $[K : \mathbb{Q}_p] - h_x^2$. □

Lemma 6.2.3. *If $\bar{r}_x$ is a nontrivial extension of two characters, then*

$$h_x^2 := \dim H^2\left(G_K, \frac{\operatorname{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}\right) \leq 1$$

and when the equality holds, the quotient character of $\bar{r}_x$ is a character whose third power is $\bar{\mathbb{F}}_p(1)$.

Proof. This is where we make use of the assumption $p > 3$. Say $\bar{r}_x \sim \left[\begin{smallmatrix} \bar{\chi}_1 & \bar{c} \\ & \bar{\chi}_2 \end{smallmatrix}\right]$. We claim

$$\operatorname{sym}^3(\bar{r}_x) \sim \begin{bmatrix} \bar{\chi}_1^3 & \bar{\chi}_1^2\bar{c} & * & * \\ & \bar{\chi}_1^2\bar{\chi}_2 & 2\bar{\chi}_1\bar{\chi}_2\bar{c} & * \\ & & \bar{\chi}_1\bar{\chi}_2^2 & 3\bar{\chi}_2^2\bar{c} \\ & & & \bar{\chi}_2^3 \end{bmatrix},$$

which has a unique G_K-invariant quotient line. Let $\{e_1, e_2\}$ be a basis of the representation space of $\bar{r}_x$ such that e_1 is an invariant line. Then $\{e_1^3, e_1^2e_2, e_1e_2^2, e_2^3\}$ is a basis of the representation space of $\operatorname{sym}^3(\bar{r}_x)$. By duality, we only need to show $\operatorname{sym}^3(\bar{r}_x)$ has a unique invariant line. Clearly $\{e_1^3\}$ defines an invariant line. Assume there is another invariant line $\operatorname{span}(v)$. We quotient $\operatorname{sym}^3(\bar{r}_x)$ by $\operatorname{span}(e_1^3)$. The quotient representation has a unique invariant line generated by the image of $e_1^2e_2$ (we postpone the explanation to the next paragraph). So $v \in \operatorname{span}(e_1^3, e_1^2e_2)$. But then we must have $v \in \operatorname{span}(e_1^3)$, since $[\bar{c}]$ is a nontrivial extension class.

The quotient representation $\operatorname{sym}^3(\bar{r}_x)/\operatorname{span}(e_1^3)$ has a G_K-invariant line spanned by the image of $e_1^2e_2$. Say $\operatorname{span}(u)$ is another invariant line of $\operatorname{sym}^3(\bar{r}_x)/\operatorname{span}(e_1^3)$. We have $u \in \operatorname{span}(e_1^2e_2, e_1e_2^2) \cong \bar{\chi}_1\bar{\chi}_2 \otimes \bar{r}_x$. Thus $u \in \operatorname{span}(e_1^2e_2)$ since $\bar{c}$ is a nontrivial extension. □

Corollary 6.2.4. *H^2 is SGR when restricted to the locus where $\bar{r}_x$ is a nontrivial extension of two characters.*

Proof. Say $\bar{r}_x$ is the extension of $\bar{\beta}$ by $\bar{\alpha}$. By Lemma 6.2.3, we have $h_x^2 \leq 1$ when $\bar{r}_x$ is a nontrivial extension of characters. So the locus where $\bar{r}_x$ is a nontrivial extension of characters consists of four subloci:

(i) $h_x^2 = 1$ and $\operatorname{Ext}^2(\beta, \alpha) = 0$;

(ii) $h_x^2 = 1$ and $\operatorname{Ext}^2(\beta, \alpha) \neq 0$;

(iii) $h_x^2 = 0$ and $\operatorname{Ext}^2(\beta, \alpha) = 0$; and

(iv) $h_x^2 = 0$ and $\operatorname{Ext}^2(\beta, \alpha) \neq 0$.

Let $T \subset (\mathcal{X}_{1,\mathrm{red}})_{\bar{\mathbb{F}}_p} \times (\mathcal{X}_{1,\mathrm{red}})_{\bar{\mathbb{F}}_p}$ be the locus of the pair (α, β), $\alpha, \beta \in \mathcal{X}_{1,\mathrm{red}}(\bar{\mathbb{F}}_p)$; say $\dim T = e$, and $\dim \operatorname{Ext}^2(\beta, \alpha) = r$. By Lemma 6.1.1, each sublocus has dimension at most

$$e + r + [K : \mathbb{Q}_p].$$

In sublocus (i), β has only finitely many choices once α is chosen, so $e = -1$, $r = 0$; in sublocus (ii), both β and α have only finitely many choices, so $e = -2$, $r = 1$; in sublocus (iii), both β and α can vary in a dense open of $(\mathcal{X}_{1,\mathrm{red}})_{\bar{\mathbb{F}}_p}$, so $e = 2\dim(\mathcal{X}_{1,\mathrm{red}})_{\bar{\mathbb{F}}_p} = 0$, $r = 0$; in sublocus (iv), when α is chosen, β has only finitely many choices, so $e = -1$, $r = 1$. We can verify that in each case $e + r + [K : \mathbb{Q}_p] \leq \dim \mathcal{X} - h_x^2 = [K : \mathbb{Q}_p] - h_x^2$. □

Lemma 6.2.5. *If $\bar{r}_x$ is a direct sum of distinct characters, then*

$$H^2\left(G_K, \frac{\operatorname{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}\right) \leq 2.$$

Proof. Say $\bar{r}_x \sim \left[\begin{smallmatrix}\bar{\chi}_1 & \\ & \bar{\chi}_2\end{smallmatrix}\right]$. We have

$$\frac{\operatorname{sym}^3(\bar{r}_x)}{\det(\bar{r})^2} \cong \bar{\chi}_1\bar{\chi}_2^{-2} \oplus \bar{\chi}_2^{-1} \oplus \bar{\chi}_1^{-1} \oplus \bar{\chi}_2\bar{\chi}_1^{-2}.$$

If $\bar{\chi}_1 \neq \bar{\chi}_2$, then the multiset $\{\bar{\chi}_1\bar{\chi}_2^{-2}, \bar{\chi}_2^{-1}, \bar{\chi}_1^{-1}, \bar{\chi}_1^{-2}\bar{\chi}_2\}$ contains at most 2 isomorphic characters. □

Corollary 6.2.6. *H^2 is SGR when restricted to the locus where $\bar{r}_x$ is a direct sum of distinct characters.*

Proof. By Lemma 6.2.5, we have $h_x^2 \leq 2$ when $\bar{x} = \alpha \oplus \beta$ is a direct sum of distinct characters.

In the sublocus where $h_x^2 = 2$, we must have $\pm\alpha = \pm\beta = \mathbb{F}(-1)$. The sublocus is the scheme-theoretic union of the scheme-theoretic image of finitely many $\operatorname{Spec} \overline{\mathbb{F}}_p \times \operatorname{Spec} \overline{\mathbb{F}}_p \to \mathcal{X}$ and has dimension $0 - 2 = -2$.

In the locus where $h_x^2 = 1$, we have one of the following:

$$\begin{aligned} &\text{(i)} \quad \alpha = \mathbb{F}(-1), &&\text{(ii)} \quad \beta = \mathbb{F}(-1), \\ &\text{(iii)} \quad \alpha = \beta^2(-1), &&\text{(iv)} \quad \beta = \alpha^2(-1). \end{aligned}$$

In each of these cases, the locus has dimension $\dim \mathbb{G}_m - \dim \operatorname{Aut}(\bar{r}_x) = 1 - 2 = -1$.

In the locus where $h_x^2 = 0$, both α and β lives in an untwistable family, and the locus has dimension $2 \dim \mathbb{G}_m - \dim \operatorname{Aut}(\bar{r}_x) = 2 - 2 = 0$. □

Lemma 6.2.7. *If $\bar{r}_x$ is a direct sum of isomorphic characters, then*

$$H^2\left(G_K, \frac{\operatorname{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}\right) \leq 4.$$

Proof. This is trivial because the underlying $\overline{\mathbb{F}}_p$-vector space is four-dimensional. □

Corollary 6.2.8. *H^2 is SGR when restricted to the locus where $\bar{r}_x$ is a direct sum of isomorphic characters.*

Proof. The automorphism group is four-dimensional. So the locus in the moduli stack has dimension $\dim \mathbb{G}_m - \dim \operatorname{Aut}(\bar{r}_x) = 1 - 4 = -3$. □

Theorem 6.2.9. *The locus of $\bar{r}_x$ in $\mathcal{X}$ for which*

$$H^2\left(G_K, \frac{\operatorname{sym}^3(\bar{r}_x)}{\det(\bar{r}_x)^2}\right) \geq r$$

is of dimension at most $[K : \mathbb{Q}_p] - r$.

Proof. This theorem follows immediately from Lemmas 6.2.1, 6.2.3, 6.2.5, 6.2.7, and their corollaries. □

Fix a mod ϖ representation $\bar{r} : G_K \to GL_2(\mathbb{F})$. Let $\underline{\lambda}$ be a Hodge type. Let R be an irreducible component of the crystalline lifting ring $R_{\bar{r}}^{\mathrm{crys}, \underline{\lambda}, \mathcal{O}_E}$. Assume $\operatorname{Spec} R[1/p] \neq \varnothing$. Let r^{univ} be the universal family of Galois representations on R.

Since $H^2(G_K, \operatorname{sym}^3(r^{\mathrm{univ}})/\det(r^{\mathrm{univ}})^2)$ is a coherent sheaf, by the semicontinuity theorem, the locus $X_s := \{x \in \operatorname{Spec} R \mid \dim \kappa(x) \otimes_R H^2 \geq s\}$ is locally closed, and has a reduced induced scheme structure.

Theorem 6.2.10. *Let R be an irreducible component of the crystalline lifting ring of regular labeled Hodge–Tate weights. If $H^2(G_K, \operatorname{sym}^3(r^{\mathrm{univ}})/\det(r^{\mathrm{univ}})^2)$ is ϖ-torsion, the locus*

$$\left\{x \in \operatorname{Spec} R \mid \dim \kappa(x) \otimes_R H^2\left(G_K, \frac{\operatorname{sym}^3(r^{\mathrm{univ}})}{\det(r^{\mathrm{univ}})^2}\right) \geq s\right\}$$

has codimension $\geq s + 1$ in $\operatorname{Spec} R$ *for $s \geq 1$.*

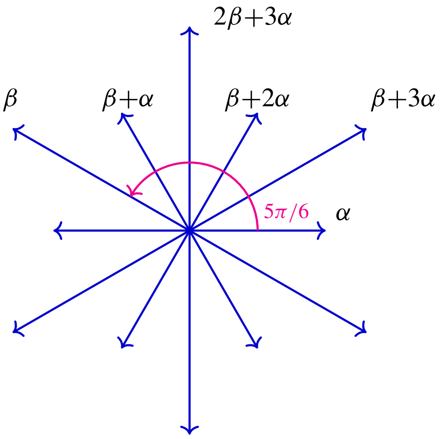
Proof. The proof is identical to that of [Emerton and Gee 2023, Theorem 6.1.1] if we use Theorem 6.2.9 instead of [Emerton and Gee 2023, Theorem 5.5.12]. □

7. The existence of crystalline lifts for the exceptional group G_2

7.1. ***Parabolics of G_2.*** Let G_2 be the Chevalley group over $\mathcal{O}_E$ of type G_2.

Let $E/\mathbb{Q}_p$ be a finite extension with ring of integers $\mathcal{O}_E$, residue field $\mathbb{F}$ and uniformizer ϖ.

We remind the reader of the root system of G_2:



7.1.1. *The short root parabolic.* Let $P \subset G_2$ be the short root parabolic, which admits a Levi decomposition $P = L \ltimes U$. The Levi factor L is a copy of GL_2 and the unipotent radical U is a unipotent group of class 2. Write U^{ad} for $U/Z(U)$.

Fix an isomorphism $\mathrm{std} : L \cong \mathrm{GL}_2$. We have

- $Z(U) \cong \mathbb{G}_a$; and
- $U^{\mathrm{ad}} \cong \mathbb{G}_a^{\oplus 4}$.

Write $\operatorname{Lie} U = Z(U) \oplus U^{\mathrm{ad}}$. The Levi factor acts on U by conjugation. We have an isomorphism of L-modules

$$\operatorname{Lie} U \cong \frac{1}{\det^2} \operatorname{sym}^3(\mathrm{std}) \oplus \frac{1}{\det} \tag{7-1}$$

where $\det : L \to \mathbb{G}_m$ is the determinant character, and $\mathrm{std} : L \xrightarrow{\cong} \mathrm{GL}_2$ is the fixed isomorphism. The above short exact sequence can be upgraded to a short exact sequence of groups with L-actions

$$0 \to \frac{1}{\det} \to U \to \frac{1}{\det^2} \operatorname{sym}^3(\mathrm{std}) \to 0.$$

For lack of reference, we explain how to get (7-1). By inspecting the root system for G_2, we find that the roots whose root group is contained in U^{ad} lie in a single line. Therefore U^{ad} is an irreducible L-module, and is thus isomorphic to $\operatorname{sym}^3(\mathrm{std})$ up to an algebraic character; then computation shows the character is $1/\det^2$ (also see the SageMath code on my homepage).

7.1.2. *The long root parabolic.* Let $Q \subset G_2$ be the long root parabolic, which admits a Levi decomposition $Q = L' \ltimes V$ where $L' \cong \mathrm{GL}_2$ and V is a unipotent group of class 3. Fix an isomorphism $\mathrm{std} : L' \xrightarrow{\cong} \mathrm{GL}_2$. Write $\det$ for the composition $L' \xrightarrow{\mathrm{std}} \mathrm{GL}_2 \xrightarrow{\det} \mathrm{GL}_1$.

Write U' for $V/Z(V)$. Then U' is a unipotent group of class 2 whose center is isomorphic to $\mathbb{G}_a$. The conjugation action of L' on U' is given by $U'/Z(U') \cong \mathrm{std}$, and $Z(U') \cong \det$, as L'-modules.

Theorem 7.1.3. *Assume $p > 3$. Let $K/\mathbb{Q}_p$ be a p-adic field. Let $\bar{\rho} : G_K \to G_2(\overline{\mathbb{F}}_p)$ be a mod ϖ Galois representation. Then $\bar{\rho}$ admits a crystalline lift $\rho^\circ : G_K \to G_2(\overline{\mathbb{Z}}_p)$ of $\bar{\rho}$.*

Moreover, if $\bar{\rho}$ factors through a maximal parabolic and the Levi factor $\bar{r} := \bar{r}_{\bar{\rho}}$ of $\bar{\rho}$ admits a Hodge–Tate regular and crystalline lift r_1 such that the adjoint representation $\phi^{\mathrm{Lie}}(r_1)$ has Hodge–Tate weights slightly less than $\underline{0}$, then ρ° can be chosen such that it factors through the same maximal parabolic and its Levi factor r_{ρ° lies on the same irreducible component of the spectrum of the crystalline lifting ring that r_1 does.

Proof. If $\bar{\rho}$ is irreducible, then $\bar{\rho}$ admits a crystalline lift by [Lin 2022].

The exceptional group G_2 has two maximal parabolic subgroups: the short root parabolic, and the long root parabolic.

If $\bar{\rho}$ is reducible, then it factors through either parabolic subgroups.

7.1.4. *The short root parabolic case.* Let $P \subset G_2$ be the short root parabolic. Recall that P has a Levi decomposition $P = L \ltimes U$. Fix an isomorphism $L \cong \mathrm{GL}_2$.

By Lemma 3.3.2, there exists a finite Galois extension K'/K, of prime-to-p degree such that $\bar{r}|_{K'}$ is Lyndon–Demushkin.

Write $Z(U)$ for center of U, and write U^{ad} for $U/Z(U)$. Write $\phi : L \to \mathrm{Aut}(U)$ for the conjugation action, with graded pieces $\phi^{\mathrm{ad}} : L \to \mathrm{GL}(U^{\mathrm{ad}})$ and $\phi^z : L \to \mathrm{GL}(Z(U))$. Write ϕ^{Lie} for $\phi^{\mathrm{ad}} \oplus \phi^z$.

Lemma 7.1.5. *Assume $p > 2$. There exists a Hodge–Tate regular crystalline lifting $r^\circ : G_K \to L(\overline{\mathbb{Z}}_p)$ of the Levi factor $\bar{r}$, such that the adjoint representation $\phi^{\mathrm{Lie}}(r^\circ) : G_K \xrightarrow{r^\circ} L(\overline{\mathbb{Z}}_p) \to \mathrm{GL}(\mathrm{Lie}\, U(\overline{\mathbb{Z}}_p))$ has labeled Hodge–Tate weights slightly less than $\underline{0}$.*

Proof. It is well known Hodge–Tate regular crystalline lifts of $\bar{r}$ exists since $L \cong \mathrm{GL}_2$. We have

$$\phi^{\mathrm{Lie}}(r^\circ) = \frac{1}{\det r^{\circ 2}} \mathrm{sym}^3(r^\circ) \oplus \frac{1}{\det r^\circ}.$$

So by replacing r° by a Tate twist, we can ensure $\phi^{\mathrm{Lie}}(r^\circ)$ has labeled Hodge–Tate weights slightly less than $\underline{0}$. □

Let Spec R be an irreducible component (with nonempty generic fiber) of a crystalline lifting ring $R_{\bar{r}}^{\mathrm{crys},\underline{\lambda}}$ of regular labeled Hodge–Tate weights $\underline{\lambda}$ such that the labeled Hodge–Tate weights $\phi^{\mathrm{Lie}}(\underline{\lambda})$ are slightly less than 0. By the lemma above, such a Spec R exists.

Let $r^{\mathrm{univ}} : G_K \to L(R)$ be the universal Galois representation.

The mod ϖ Galois representation $\bar{r}$ defines a Galois action $\phi(\bar{r}) : G_K \to \mathrm{Aut}(U(\overline{\mathbb{F}}_p))$ on $U(\overline{\mathbb{F}}_p)$. By Section 4.1.3, the datum of $\bar{\rho} : G_K \to G_2(\overline{\mathbb{F}}_p)$ is encoded in a nonabelian cocycle $[\bar{c}] \in H^1(G_K, U(\overline{\mathbb{F}}_p))$.

The strategy for lifting $\bar{\rho}$ is as follows. We choose a suitable $\overline{\mathbb{Z}}_p$-point x of Spec R which defines a lift $r_x : G_K \to L(\overline{\mathbb{Z}}_p)$ of $\bar{r}$, and endow $U(\overline{\mathbb{Z}}_p)$ with the Galois action $\phi(r_x) : G_K \xrightarrow{r_x} L(\overline{\mathbb{Z}}_p) \to \mathrm{Aut}(U(\overline{\mathbb{Z}}_p))$. There is a map of pointed set $H^1(G_K, U(\overline{\mathbb{Z}}_p)) \to H^1(G_K, U(\overline{\mathbb{F}}_p))$. If the cohomology class $[\bar{c}]$ admits a lift $[c] \in H^1(G_K, U(\overline{\mathbb{Z}}_p))$, then $\bar{\rho}$ admits a lift $\rho : G_K \to G_2(\overline{\mathbb{Z}}_p)$ whose datum is encoded in $[c]$. Such a lift ρ is crystalline by the main result of [Lin 2019], since $\phi^{\mathrm{Lie}}(r^\circ)$ has labeled Hodge–Tate weights slightly less than $\underline{0}$.

By Theorem 5.2.1, to lift the nonabelian 1-cocycle $[\bar{c}]$, it suffices to verify the following:

(1) $H^2(G_K, \operatorname{sym}^3(r^{\mathrm{univ}})/\det^2(r^{\mathrm{univ}}))$ is SGR and supported on the special fiber of $\operatorname{Spec} R$.

(2) $p \neq 2$.

(3) There exists a finite Galois extension K'/K of prime-to-p degree such that $\phi(\bar{r})|_{G_{K'}}$ is Lyndon–Demushkin.

(4) There exists a $\overline{\mathbb{Z}}_p$-point of $\operatorname{Spec} R$ which is mildly regular when restricted to $G_{K'}$.

Item (1) is verified by Theorem 6.2.10. Note that since the Hodge type of $\operatorname{Spec} R$ is chosen so that $\operatorname{sym}^3(r_x)/\det(r_x)^2$ has labeled Hodge–Tate weights slightly less than $\underline{0}$, $H^2(G_K, \operatorname{sym}^3(r_x)/\det(r_x)^2)$ is torsion for any characteristic-0 point x of $\operatorname{Spec} R$. Item (3) follows from Lemma 3.3.2, and (4) follows from Proposition 3.0.5.

7.1.6. *The long root parabolic case.* Let $Q \subset G_2$ be the long root parabolic. Q has a Levi decomposition $Q = L' \ltimes V$. Fix an isomorphism $\mathrm{std} : L' \xrightarrow{\cong} \mathrm{GL}_2$. Write det for the composition $L' \xrightarrow{\mathrm{std}} \mathrm{GL}_2 \xrightarrow{\det} \mathrm{GL}_1$.

Let $\{1\} = V_0 \subset V_1 \subset V_2 \subset V_3 = V$ be the upper central series of V. Then the conjugation action of L' on each graded piece is given by

- $V_3/V_2 \cong \det \otimes \mathrm{std}$;
- $V_2/V_1 \cong \det$;
- $V_1 \cong \mathrm{std}$.

Suppose $\bar{\rho}$ factors through the long root parabolic Q, but not the short root parabolic P. Then the Levi factor

$$\bar{r} : G_K \xrightarrow{\bar{\rho}} Q(\overline{\mathbb{F}}_p) \to L'(\overline{\mathbb{F}}_p)$$

is necessarily an irreducible representation. If we endow each graded piece of $V(\overline{\mathbb{F}}_p)$ with the Galois action $G_K \xrightarrow{\bar{r}} L(\overline{\mathbb{Z}}_p) \to \mathrm{GL}(V_{i+1}(\overline{\mathbb{F}}_p)/V_i(\overline{\mathbb{F}}_p))$, then we have, by local Tate duality,

$$H^2(G_K, V_3(\overline{\mathbb{F}}_p)/V_2(\overline{\mathbb{F}}_p)) = H^2(G_K, \bar{r} \otimes \det \bar{r}) = 0,$$
$$H^2(G_K, V_1(\overline{\mathbb{F}}_p)) = H^2(G_K, \bar{r}) = 0.$$

So the only cohomological obstruction occurs in the second graded piece.

The datum of $\bar{\rho}$ is encoded in a nonabelian cocycle $[\bar{c}] \in H^1(G_K, V(\overline{\mathbb{F}}_p))$. Just as is done in the short root parabolic case, it suffices to lift the cocycle $[\bar{c}]$. By Proposition 5.3.1, since the only cohomological obstruction lies in the second graded piece, it suffices to lift $\operatorname{ad}([\bar{c}]) \in H^1(G_K, (V/V_1)(\overline{\mathbb{F}}_p))$.

Write U' for V/V_1. Recall that U' is a unipotent group of class 2 with rank-1 center, and we can directly appeal to Theorem 5.2.1. We repeat the procedure worked out in the short root case 7.1.4.

Let r° be a lift of $\bar{r}$ such that r° is Hodge–Tate regular and crystalline and the Hodge–Tate weights of r° are strictly less than $\underline{0}$.

Let Spec R be the irreducible component of the crystalline lifting ring of $\bar{r}$ containing r°. Write $r^{\mathrm{univ}} : G_K \to \mathrm{GL}_2(R)$ for the universal family.

Write $Z(U')$ for the center of U', and write $U'^{\,\mathrm{ad}}$ for $U'/Z(U')$. Write ϕ^{ad} for the conjugate action $L' \to \mathrm{Aut}(U'^{\,\mathrm{ad}})$ and write ϕ^{z} for the conjugate action $L' \to \mathrm{Aut}(Z(U'))$.

Note that $\phi^{\mathrm{ad}}(r^{\mathrm{univ}}) = r^{\mathrm{univ}}$ and $\phi^{z}(r^{\mathrm{univ}}) = \det r^{\mathrm{univ}}$.

We have the following checklist:

(1) $H^2(G_K, \det(r^{\mathrm{univ}})r^{\mathrm{univ}})$ is SGR.

(2) $p \neq 2$.

(3) There exists a finite Galois extension K'/K of prime-to-p degree such that $\phi(\bar{r})|_{G_{K'}}$ is Lyndon–Demushkin.

(4) There exists a $\overline{\mathbb{Z}}_p$-point of Spec R which is mildly regular when restricted to $G_{K'}$.

By the assumption $H^2(G_K, \det(r^{\mathrm{univ}})r^{\mathrm{univ}}) = 0$. (3) follows from Lemma 3.3.2, and (4) follows from Proposition 3.0.5. □

Appendix A: Nondegeneracy of mod ϖ cup product for G_2

Let $\mathbb{F}$ be a finite field of characteristic $p > 3$. Write G_2 for the Chevalley group over $\mathbb{F}$ of type G_2.

Let P be the short root parabolic of G_2. Let $P = L \ltimes U$ be the Levi decomposition. Let $\bar{r} : G_K \to L(\mathbb{F})$ be a Galois representation which is Lyndon–Demushkin. Since $L \cong \mathrm{GL}_2$, $\bar{r}$ is the extension of two trivial characters. Denote by $\phi : L \to \mathrm{Aut}(U)$ the conjugation action. G_K acts on U via the conjugate action $G_K \xrightarrow{r^\circ} L \xrightarrow{\phi} \mathrm{Aut}(U)$.

We set up a computational framework to prove various claims. Let $\{x_0, \dots, x_n, x_{n+1}\}$ be the Demushkin generators.

Let $\{e_1, e_2\}$ be a basis of the representation space of $\bar{r}$ such that r° is upper-triangular with respect to this basis. Without loss of generality, assume $e_1 = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$, $e_2 = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$. Say for $i = 0, \dots, n+1$, $\bar{r}(x_i) = \left[\begin{smallmatrix}1 & l_i\\ & 1\end{smallmatrix}\right]$.

The set $\{e_1^3, e_1^2e_2, e_1e_2^2, e_2^3\}$ is a basis of the representation space $\mathrm{sym}^3(\bar{r})$, which is identified with $U^{\mathrm{ad}}(\mathbb{F})$.

The root system of G_2 can be found in Section 7.1. In the diagram, α is the short root, and β is the short root. Each root x generates a root group $U_x \subset U$. The short root parabolic P has seven root groups: the five root groups

$$\{U_\beta, U_{\beta+\alpha}, U_{\beta+2\alpha}, U_{\beta+3\alpha}, U_{2\beta+3\alpha}\}$$

lying above the x-axis generates the unipotent radical U, the two root groups $\{U_\alpha, U_{-\alpha}\}$ lying on the x-axis are the root groups of the Levi factor group L. Say under the identification std : $L \cong \mathrm{GL}_2$, the matrices $\left[\begin{smallmatrix}0 & *\\ 0 & 0\end{smallmatrix}\right]$ are identified with the root group U_α. Now we have identifications

$$\operatorname{span} e_1^3 \sim U_\beta, \quad \operatorname{span} e_1^2e_2 \sim U_{\beta+\alpha}, \quad \operatorname{span} e_1e_2^2 \sim U_{\beta+2\alpha}, \quad \operatorname{span} e_2^3 \sim U_{\beta+3\alpha}.$$

For ease of notation, write $E_0 := e_1^3$, $E_1 := e_1^2e_2$, $E_2 := e_1e_2^2$, $E_3 := e_2^3$. A basis of

$$C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathcal{O}_E)) \cong \{\langle x_0, \dots, x_{n+1}\rangle \to U_\beta(\mathcal{O}_E) \oplus U_{\beta+\alpha}(\mathcal{O}_E) \oplus U_{\beta+2\alpha}(\mathcal{O}_E) \oplus U_{\beta+3\alpha}(\mathcal{O}_E)\}$$

is given by

$$\mathscr{B} = \begin{Bmatrix} x_0^* E_0, x_1^* E_0, & \dots, & x_{n+1}^* E_0, \\ x_0^* E_1, x_1^* E_1, & \dots, & x_{n+1}^* E_1, \\ x_0^* E_2, x_1^* E_2, & \dots, & x_{n+1}^* E_2, \\ x_0^* E_3, x_1^* E_3, & \dots, & x_{n+1}^* E_3 \end{Bmatrix},$$

where $x_i^* E_j$ is the cochain $c : \langle x_0, \dots, x_{n+1} \rangle$ such that $c(x_k) = \delta_{ik} E_j$, where δ_{ik} is the Kronecker delta. For any $c \in C^1_{\mathrm{LD}}(U^{\mathrm{ad}})$, we can write down the $\mathscr{B}$-coordinates $[c]_{\mathscr{B}} := (c_v)_{v \in \mathscr{B}}$ of c.

Lemma A.0.1. *The cup products on cochains*

$$\cup_{\mathbb{F}} : C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \times C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \to C^2_{\mathrm{LD}}(Z(U)(\mathbb{F}))$$

is nondegenerate.

Ideas. We compute the cup products $v \cup w$ for $v, w \in \mathscr{B}$. The matrix $[\cup_{\mathbb{F}}]_{\mathscr{B}}$ is anti-lower-triangular, (that is, of the shape

$$\begin{bmatrix} 0 & 0 & 0 & * \\ 0 & 0 & * & * \\ 0 & * & * & * \\ * & * & * & * \end{bmatrix}$$

whose antidiagonal blocks are constant invertible matrices), and thus nondegenerate.

To help the reader better understand what's going on, we attached SageMath code in Appendix B.

Proof. Recall the relator of the Lyndon–Demushkin group is

$$R = x_0^q (x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1}).$$

Since we are working mod ϖ, we have for any $p > 5$, any $g \in G_{K'}$, $\phi(\bar{r}(g))^p \equiv \mathrm{id} \bmod \varpi$ (See Appendix B for the verification). In particular, the relator R reduces to

$$(x_0, x_1) \dots (x_n, x_{n+1})$$

when we compute mod ϖ. (When $p = 5$, things are still good, and can be confirmed by running the SageMath code in Appendix B.)

We regard cochains in $C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F}))$ as a $(U^{\mathrm{ad}}(\mathbb{F}))$-valued function on the free group with generators $\{x_0, \dots, x_{n+1}\}$,

Now we let c be the "universal" mod ϖ 1-cochain. That is, we let

$$\begin{Bmatrix} \lambda_{0,0}, & \lambda_{1,0}, & \dots, & \lambda_{n+1,0}, \\ \lambda_{0,1}, & \lambda_{1,1}, & \dots, & \lambda_{n+1,1}, \\ \lambda_{0,2}, & \lambda_{1,2}, & \dots, & \lambda_{n+1,2}, \\ \lambda_{0,3}, & \lambda_{1,3}, & \dots, & \lambda_{n+1,3} \end{Bmatrix}$$

be indeterminants, and set

$$c := \sum \lambda_{i,j} x_i^* E_j \in C^1_{\mathrm{LD}}(U^{\mathrm{ad}}(\mathbb{F})) \otimes \mathbb{Z}[\lambda_{i,j}].$$

The cup product

$$c \cup c = Q(c) \in C^2_{\mathrm{LD}}(Z(U)(\mathbb{F})) \otimes \mathbb{Z}[\lambda_{i,j}] = Z(U)(\mathbb{F}) \otimes \mathbb{Z}[\lambda_{i,j}] \cong \mathbb{F}[\lambda_{i,j}]$$

will be a quadratic form in variables $\{\lambda_{i,j}\}$, and the matrix of this quadratic form is nothing but the matrix $[\cup_{\mathbb{F}}]_{\mathscr{B}}$. Recall that $c \cup c = Q(c)$ is defined to be the projection of $\tilde{c}(R)$ onto the center of the Lie algebra Lie U, where $\tilde{c} \in C^1_{\mathrm{LD}}(U(\mathbb{F}))$ is the unique extension of c to a $U(\mathbb{F})$-valued cochain as is explained in Section 2.

Write $[\cup_{\mathbb{F}}]_{\mathscr{B}}$ as a block matrix

$$[\cup_{\mathbb{F}}]_{\mathscr{B}} = \begin{array}{c|c|c|c|c} & \beta & \beta+\alpha & \beta+2\alpha & \beta+3\alpha \\ \hline \beta & M_{11} & M_{12} & M_{13} & M_{14} \\ \hline \beta+\alpha & M_{21} & M_{22} & M_{23} & M_{24} \\ \hline \beta+2\alpha & M_{31} & M_{32} & M_{33} & M_{34} \\ \hline \beta+3\alpha & M_{41} & M_{42} & M_{43} & M_{44} \end{array},$$

where each M_{ij} is an $(n+2)\times(n+2)$ matrix. We say the blocks M_{24}, M_{33}, M_{34}, M_{42}, M_{43}, M_{44} are *strictly below the antidiagonal*, and we call M_{41}, M_{32}, M_{23} and M_{14} the antidiagonal blocks:

$$\begin{array}{c|c|c|c|c} & \beta & \beta+\alpha & \beta+2\alpha & \beta+3\alpha \\ \hline \beta & & & & \\ \hline \beta+\alpha & & & & M_{24} \\ \hline \beta+2\alpha & & & M_{33} & M_{34} \\ \hline \beta+3\alpha & & M_{42} & M_{43} & M_{44} \end{array} \qquad \begin{array}{c|c|c|c|c} & \beta & \beta+\alpha & \beta+2\alpha & \beta+3\alpha \\ \hline \beta & & & & M_{14} \\ \hline \beta+\alpha & & & M_{23} & \\ \hline \beta+2\alpha & & M_{32} & & \\ \hline \beta+3\alpha & M_{41} & & & \end{array}$$

strictly below antidiagonal   antidiagonal blocks

Sublemma. *Let $g = g_1 g_2 \dots g_s$. Write ϕ_i for $\phi(\bar{r}(g_1, \dots, g_{i-1}))$. We have*

$$\tilde{c}(g) = \sum \phi_i \tilde{c}(g_i) + \tfrac{1}{2} \sum_{i<j} [\phi_i \tilde{c}(g_i), \phi_j \tilde{c}(g_j)].$$

Proof. This is an immediate consequence of the Baker–Campbell–Hausdorff formula. □

Note that $\phi(\bar{r}((x_i, x_j))) = \mathrm{id}$, so

$$\begin{aligned} \tilde{c}(R) &= \tilde{c}(x_0^q (x_0, x_1)(x_2, x_3) \cdots (x_n, x_{n+1})) \\ &= \sum \tilde{c}((x_{2k}, x_{2k+1})) + \tfrac{1}{2} \sum_{j<k} [\tilde{c}((x_{2j}, x_{2j+1})), \tilde{c}((x_{2k}, x_{2k+1}))]. \end{aligned}$$

We have

$$\tilde{c}((x_{2k}, x_{2k+1})) = -\phi(x_{2k}^{-1})(\phi(x_{2k+1}) - 1)\tilde{c}(x_{2k}) + \phi(x_{2k}^{-1} x_{2k+1}^{-1})(\phi(x_{2k}) - 1)\tilde{c}(x_{2k+1}) + Z_k = Y_k + Z_k,$$

where Z_k is a sum of Lie brackets (see below), and lies in the center of the Lie U. Note that $[Y_j, Y_k]$ only contributes to the part of $[\cup_{\mathbb{F}}]_{\mathscr{B}}$ which lies strictly below the antidiagonal, because $(\phi(x_{2k}) - 1)$ and $(\phi(x_{2k+1}) - 1)$ moved the appearance of the indeterminant $\lambda_{i,j}$ from the root group $U_{\beta+j\alpha}$ to the root group $U_{\beta+(j+1)\alpha}$.

So it remains to analyze $\sum Z_k$. We have

$$\begin{aligned} 2Z_k = {} & [-\phi(x_{2k}^{-1})\tilde{c}(x_{2k}), -\phi(x_{2k}^{-1} x_{2k+1}^{-1})\tilde{c}(x_{2k+1})] + [-\phi(x_{2k}^{-1})\tilde{c}(x_{2k}), +\phi(x_{2k}^{-1} x_{2k+1}^{-1})\tilde{c}(x_{2k})] \\ & + [-\phi(x_{2k}^{-1})\tilde{c}(x_{2k}), +\phi(x_{2k}^{-1} x_{2k+1}^{-1} x_{2k})\tilde{c}(x_{2k+1})] + [-\phi(x_{2k}^{-1} x_{2k+1}^{-1})\tilde{c}(x_{2k+1}), +\phi(x_{2k}^{-1} x_{2k+1}^{-1})\tilde{c}(x_{2k})] \\ & + [-\phi(x_{2k}^{-1} x_{2k+1}^{-1})\tilde{c}(x_{2k+1}), +\phi(x_{2k}^{-1} x_{2k+1}^{-1} x_{2k})\tilde{c}(x_{2k+1})] \\ & + [\phi(x_{2k}^{-1} x_{2k+1}^{-1})\tilde{c}(x_{2k}), +\phi(x_{2k}^{-1} x_{2k+1}^{-1} x_{2k})\tilde{c}(x_{2k+1})] \end{aligned}$$

Write

$$2Z'_k := [-\tilde{c}(x_{2k}), -\tilde{c}(x_{2k+1})] + [-\tilde{c}(x_{2k}), \tilde{c}(x_{2k})] + [-\tilde{c}(x_{2k}), \tilde{c}(x_{2k+1})] + [-\tilde{c}(x_{2k+1}), \tilde{c}(x_{2k})] \\ + [-\tilde{c}(x_{2k+1}), \tilde{c}(x_{2k+1})] + [\tilde{c}(x_{2k}), \tilde{c}(x_{2k+1})].$$

Z'_k is obtained by replacing all Galois action in Z_k by the trivial action. $Z_k - Z'_k$ only contributes to the part of $[\cup_{\mathbb{F}}]_{\mathscr{B}}$ with lies strictly below the antidiagonal for a similar reason (a "shifting" effect). It is easy to see that

$$Z'_k = [\tilde{c}(x_{2k}), \tilde{c}(x_{2k+1})] = \pm\lambda_{2k,0}\lambda_{2k+1,3} \pm \lambda_{2k+1,0}\lambda_{2k,3} \pm 3\lambda_{2k,1}\lambda_{2k+1,2} \pm 3\lambda_{2k+1,2}\lambda_{2k,1}.$$

As a consequence of these computations, we see that each of the antidiagonal blocks of $[\cup]_{\mathscr{B}}$ are constant matrices:

$$\pm M_{41} = \pm M_{14} = \begin{bmatrix} \begin{bmatrix} & -1/2 \\ 1/2 & \end{bmatrix} & & & \\ & \begin{bmatrix} & -1/2 \\ 1/2 & \end{bmatrix} & & \\ & & \ddots & \\ & & & \begin{bmatrix} & -1/2 \\ 1/2 & \end{bmatrix} \end{bmatrix},$$

$$\pm M_{32} = \pm M_{23} = \begin{bmatrix} \begin{bmatrix} & -3/2 \\ 3/2 & \end{bmatrix} & & & \\ & \begin{bmatrix} & -3/2 \\ 3/2 & \end{bmatrix} & & \\ & & \ddots & \\ & & & \begin{bmatrix} & -1/2 \\ 1/2 & \end{bmatrix} \end{bmatrix}.$$

So $[\cup_{\mathbb{F}}]_{\mathscr{B}}$ is an invertible matrix. □

The long root parabolic case is much simpler.

Appendix B: Sagemath code

Proposition B.0.1. *Let $V \subset B$ be the unipotent radical of the Borel of G_2. Let $g \in V(\overline{\mathbb{Z}}_p)$. If $p > 5$, then $g^p = \mathrm{id} \bmod \varpi$.*

Proof. Let $P \supset B$ be the short root parabolic. Let $P = L \ltimes U$ be the Levi decomposition. Let $\pi : P \to L$ be the quotient. Say $\pi(g) = \left[\begin{smallmatrix} 1 & l \\ 0 & 1 \end{smallmatrix}\right]$. Fix a projection $P \to U$. Also fix a projection $U \to Z(U)$. Say the projection of g onto $U/Z(U) \cong \mathbb{A}^4$ via $P \to U \to U/Z(U)$ is (u_0, u_1, u_2, u_3). Say the projection of g onto $Z(U) \cong \mathbb{A}^1$ via $P \to U \to Z(U)$ is u_4.

For simplicity, we write $g = (l; u_0, u_1, u_2, u_3; u_4)$. We have, for any integer q,

$$g^q = \Big(ql; qu_0, -\tfrac{1}{2}q(q-1)u_0 l + qu_1, -\tfrac{1}{6}q(q-1)(2q-1)u_0 l^2 + q(q-1)u_1 l + qu_2, \\ -\tfrac{1}{4}q^2(q-1)^2 u_0 l^3 + \tfrac{1}{2}q(q-1)(2q-1)u_1 l^2 + \tfrac{3}{2}q(q-1)u_2 l + qu_3, qu_4; \\ \tfrac{1}{120}(q-1)q(q+1)(3q^2-2)u_0^2 l^3 - \tfrac{1}{2}(q-1)q(q+1)(u_1^2 + u_0 u_2)l\Big).$$

This can be computed by hand, and can be verified by a computer algebra system. The proposition follows from the above computation immediately. □

The SageMath source code for computing is on the website sharkoko.space.

If we compute `cup_product_mod_p(5,4,4)` in SageMath notebook, we'll get an anti-lower-triangular matrix in the sense of Lemma A.0.1.

Acknowledgement

I would like to thank David Savitt, for suggesting to me the project of constructing crystalline lifts of Galois representations valued in general reductive groups, and for his excellent advisoring. I would like to thank Matthew Emerton for teaching me his work [Emerton and Gee 2023]. I also want to thank the referees for very careful reading and thank Joel Specter and Xiyuan Wang for helpful discussions.

References

[Bellovin and Gee 2019] R. Bellovin and T. Gee, "G-valued local deformation rings and global lifts", *Algebra Number Theory* **13**:2 (2019), 333–378. MR Zbl

[Böckle 2003] G. Böckle, "Lifting mod p representations to characteristics p^2", *J. Number Theory* **101**:2 (2003), 310–337. MR Zbl

[Caruso and Liu 2011] X. Caruso and T. Liu, "Some bounds for ramification of p^n-torsion semi-stable representations", *J. Algebra* **325** (2011), 70–96. MR Zbl

[Emerton and Gee 2023] M. Emerton and T. Gee, *Moduli stacks of étale (φ, Γ)-modules and the existence of crystalline lifts*, Ann. of Math. Stud. **215**, Princeton Univ. Press, 2023. MR Zbl

[Fakhruddin et al. 2018] N. Fakhruddin, C. Khare, and S. Patrikis, "Lifting irreducible Galois representations", preprint, 2018. arXiv 1810.05803

[Gee et al. 2018] T. Gee, F. Herzig, and D. Savitt, "General Serre weight conjectures", *J. Eur. Math. Soc.* **20**:12 (2018), 2859–2949. MR Zbl

[Koch 2002] H. Koch, *Galois theory of p-extensions*, Springer, 2002. MR Zbl

[Lin 2019] Z. Lin, "Extensions of crystalline representations valued in general reductive groups", preprint, 2019, available at https://sharkoko.space/pdf/unobs.pdf.

[Lin 2022] Z. Lin, "Crystalline lifts and a variant of the Steinberg–Winter theorem", *Doc. Math.* **27** (2022), 2441–2468. MR Zbl

[Lin 2023a] Z. Lin, "A Deligne–Lusztig type correspondence for tame p-adic groups", preprint, 2023. arXiv 2306.02093

[Lin 2023b] Z. Lin, "The Emerton–Gee stacks for tame groups, I", preprint, 2023. arXiv 2304.05317

[Lin 2023c] Z. Lin, "The Emerton–Gee stacks for tame groups, II", preprint, 2023. arXiv 2309.05773

[Lyndon 1950] R. C. Lyndon, "Cohomology theory of groups with a single defining relation", *Ann. of Math.* (2) **52**:3 (1950), 650–665. MR Zbl

[Muller 2013] A. Muller, *Relèvements cristallins de représentations galoisiennes*, Ph.D. thesis, Université de Strasbourg, 2013, available at https://theses.hal.science/tel-00873407.

[Serre 2002] J.-P. Serre, *Galois cohomology*, Springer, 2002. MR Zbl

[Stacks] "The Stacks project", electronic reference, available at http://stacks.math.columbia.edu.

Communicated by Frank Calegari
Received 2021-08-25 Revised 2023-12-25 Accepted 2024-03-05

ygwcpoi@gmail.com *Northwestern University, Evanston, IL, United States*

ALGEBRA AND NUMBER THEORY 19:3 (2025)
https://doi.org/10.2140/ant.2025.19.457

Fermat's last theorem over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Maleeha Khawaja and Frazer Jarvis

Dedicated to Iffat (Zaman) Khawaja
January 1936 – January 2022

In this paper, we begin the study of the Fermat equation $x^n + y^n = z^n$ over real biquadratic fields. In particular, we prove that there are no nontrivial solutions to the Fermat equation over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ for $n \geq 4$.

1. Introduction

Since the groundbreaking work of Wiles [1995] on the resolution of the Fermat equation over $\mathbb{Q}$, the Fermat equation has been studied extensively over various number fields. Let K be a number field and let $n \geq 3$ be an integer. The Fermat equation over K with exponent n is the equation

$$x^n + y^n = z^n, \quad x, y, z \in K. \tag{1}$$

We say a solution (a, b, c) to (1) over K is trivial if $abc = 0$ and nontrivial otherwise.

Wiles' method of resolving (1) over $\mathbb{Q}$ became known as the modular approach. Thereafter, Jarvis and Meekin [2004] extended this method to prove that there are no nontrivial solutions to (1) over $\mathbb{Q}(\sqrt{2})$ for $n \geq 4$. This was followed by work of Freitas and Siksek [2015a; 2015b] who established a framework on how to resolve (1) (and more general Diophantine equations) over totally real number fields. Furthermore, Freitas and Siksek [2015b] proved that there are no nontrivial solutions to (1) over $\mathbb{Q}(\sqrt{d})$ for $n \geq 4$, where $3 \leq d \leq 23,\ d \neq 5, 17$ is a squarefree integer. When approaching real quadratic fields with a larger discriminant, they encountered the obstacle of demonstrating the irreducibility of certain Galois representations and eliminating the number of Hilbert newforms that arose as a result of level lowering. Michaud-Jacobs [2022] worked around these obstacles by studying quadratic points on certain modular curves and working directly with Hecke operators. He proved, for most squarefree d in the range $26 \leq d \leq 97$, that there are no nontrivial solutions to (1) over $\mathbb{Q}(\sqrt{d})$ for $n \geq 4$. Kraus [2019] provided a partial resolution of (1) over various totally real number fields of degrees ≤ 8. By a partial resolution we mean for all prime exponents $n = p > B_K$, where B_K is a constant depending only on K. For example if K is a real cubic field with discriminant 148, 404 or 564, or if K is the cyclic quartic field $\mathbb{Q}(\zeta_{16})^+$ then $B_K = 5$. It is a natural problem then to study (1) over real biquadratic fields. Freitas and Siksek [2015a] initiated the study of looking at (1) "asymptotically". As in [Freitas and Siksek 2015a], we say the

MSC2020: 11D41, 14G05, 14H52.
Keywords: Fermat equation, modularity, Galois representations, rational points, elliptic curves.

asymptotic Fermat's last theorem holds over K if there is a constant B_K such that there are no nontrivial solutions to (1) over K for primes $p > B_K$. Freitas, Kraus and Siksek [Freitas et al. 2020] studied the solutions to certain S-unit equations to prove that the asymptotic Fermat's last theorem holds for several infinite families of number fields — including some real biquadratic fields. In this paper, we will prove the following result and discuss some obstacles that arise over more general real biquadratic fields.

Theorem 1.1. *Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. There are no nontrivial solutions to* (1) *over K for $n \geq 4$.*

We give a brief outline of the paper. In Section 2, we apply and give a brief overview of the modular approach found in [Freitas and Siksek 2015a; 2015b]. In Section 3, we determine the conductor of the Frey curve using techniques outlined in [Freitas and Siksek 2015b], as well as Tate's algorithm [Silverman 1994, pp. 364–368]. In Section 4, we prove that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$. For $p = 13$ and 17, we prove this by studying the explicit modular parametrisation. For $p \geq 19$, we use work of Derickx, Kamienny, Stein and Stoll [Derickx et al. 2023] and David [2011] to get a contradiction if $\bar{\rho}_{E,p}$ is reducible. In Section 6, we rule out solutions for certain small integer exponents. To treat $n = 9$ and $n = 6$, we study the hyperelliptic curves obtained from the Fermat curve of degree n. We also extend work of Mordell [1968] to determine all quartic points on the Fermat quartic lying in a quadratic extension of $\mathbb{Q}(\sqrt{2})$. In Section 7, we give a brief overview of some obstacles that arise when extending our method to more general real biquadratic fields. All supporting computations were performed in Magma; the scripts are available within the GitHub repository https://github.com/MaleehaKhawaja/Fermat.

2. The modular approach

Let K be a totally real field (until otherwise specified) and let $\mathcal{O}_K$ denote its ring of integers. Let $p \geq 5$ be a prime. Suppose (a, b, c) is a nontrivial solution to (1) over K with exponent p. The traditional Frey curve associated to (a, b, c) is given by

$$y^2 = x(x - a^p)(x + b^p).$$

Our Frey curve will be a quadratic twist of this elliptic curve by a well-chosen unit $\varepsilon \in \mathcal{O}_K^*$. We write

$$E = E_{a,b,c,\varepsilon} : y^2 = x(x - \varepsilon a^p)(x + \varepsilon b^p). \tag{2}$$

The reason for allowing twists by units is to reduce the number of possibilities for the conductor of the Frey curve. Write $\mathcal{N}_\varepsilon$ for the conductor of the Frey curve E above. We denote by $\bar{\rho}_{E,p}$ the mod p Galois representation associated to E.

The following theorem of Freitas and Siksek is formulated from the combination of the works of Fujiwara [2006], Jarvis [1999a; 1999b], and Rajaei [2001].

Theorem 2.1 [Freitas and Siksek 2015a, Theorem 7]. *Let K be a totally real field. Let $p \geq 5$ be a prime. Suppose $\mathbb{Q}(\zeta_p)^+ \not\subseteq K$. Let E be an elliptic curve over K with conductor $\mathcal{N}$. Suppose E is modular and $\bar{\rho}_{E,p}$ is irreducible. Denote by $\Delta_\mathfrak{q}$ the discriminant for a local minimal model of E at a prime ideal $\mathfrak{q}$*

of K. Let

$$\mathcal{M}_p := \prod_{\mathfrak{q} \| \mathcal{N},\, p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})} \mathfrak{q}, \quad \mathcal{N}_p := \frac{\mathcal{N}}{M_p}.$$

Suppose the following conditions are satisfied for all prime ideals $\mathfrak{q} \mid p$:

(i) *E is semistable at $\mathfrak{q}$.*

(ii) *$p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$.*

(iii) *The ramification index satisfies $e(\mathfrak{q}/p) < p - 1$.*

Then, $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\varpi}$, where $\mathfrak{f}$ is a Hilbert eigenform of parallel weight 2 that is new at level $\mathcal{N}_p$ and ϖ is a prime ideal of $\mathbb{Q}_{\mathfrak{f}}$ that lies above p.

We apply Theorem 2.1 to the Frey curve (2) in order to contradict the existence of the putative solution (a, b, c).

Several advances have been made in the direction of establishing the modularity of elliptic curves over totally real number fields. For example, the modularity of elliptic curves over real quadratic fields [Freitas et al. 2015] and totally real cubic fields [Derickx et al. 2020] has been established. Moreover, thanks to the following result of Box, we now know elliptic curves over most totally real quartic fields are modular.

Theorem 2.2 [Box 2022, Theorem 1.1]. *Let K be a totally real quartic field not containing $\sqrt{5}$. Every elliptic curve over K is modular.*

We turn to the question of how to show that conditions (i) and (ii) of Theorem 2.1 are satisfied. Let $\mathcal{H} = \mathrm{Cl}(K)/\mathrm{Cl}(K)^2$, where $\mathrm{Cl}(K)$ denotes the class group of K. We can assume, without loss of generality, that any nontrivial solution (a, b, c) to (1) is integral. By Lemma 3.3 of [Freitas and Siksek 2015b], a, b, c are coprime away from a small set of primes, i.e., $\gcd(a, b, c) = \mathfrak{m} \cdot \tau^2$ for some $\mathfrak{m} \in \mathcal{H}$ and odd prime ideal $\tau \neq \mathfrak{m}$. The following result addresses conditions (i) and (ii) above.

Lemma 2.3 [Freitas and Siksek 2015b, Lemma 3.3]. *Let K be a totally real field. Let S denote the set of primes of K above 2. Let $\mathfrak{q}$ be a prime ideal of K such that $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$. Then E is semistable at $\mathfrak{q}$ and $p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$.*

We remark that our Frey curve is a quadratic twist of the usual Frey curve by a unit and thus the set of primes dividing the conductor remains unchanged away from 2.

The Jacobian of the Fermat curve of degree 5, 7 or 11 has finitely many rational points. Since the divisor obtained from the formal sum of a point and its Galois conjugates gives a rational divisor, this allows the study of points on these Fermat curves over fields of low degree. Klassen and Tzermias [1997] have classified all points on the Fermat quintic defined over number fields of degree at most 6. Building on this work, Kraus [2018] has provided an algebraic description of the quartic points on the Fermat quintic. Tzermias [1998] has determined all points on the Fermat septic defined over number fields of degree at most 5. Gross and Rohrlich [1978] have determined all points on (1) with exponent $p = 11$ over fields of degree at most 5. We can thus suppose that $n = 4, 6, 9$, or $n = p \geq 13$ is a prime.

Throughout, unless otherwise specified, let $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$ and let $\mathcal{O}_K$ denote its ring of integers. Let $p\geq 13$ be a prime. Suppose there is a nontrivial solution (a,b,c) to (1) over K with exponent p. Let E be the Frey curve (2) associated to this solution. By Theorem 2.2, E is modular. We note that K has class number 1 and thus $\mathfrak{m}=1\cdot\mathcal{O}_K$. Suppose $\mathfrak{q}\mid p$ is a prime ideal of K. By Lemma 2.3, assumptions (i) and (ii) of Theorem 2.1 are satisfied for $\mathfrak{q}$. In particular, E is semistable away from 2. Thus, in order to prove Theorem 1.1, it remains to

(1) determine the reduction type of E at $\mathfrak{P}$, where $\mathfrak{P}$ is the unique prime above 2,

(2) prove that $\bar{\rho}_{E,p}$ is irreducible for $p\geq 13$,

(3) eliminate the Hilbert newforms arising as a result of level lowering (Theorem 2.1),

(4) rule out solutions to (1) for $n=4$, 6 and 9.

3. Computing the lowered level

Write $\mathcal{N}_\varepsilon$ for the conductor of the Frey curve E above. We note that $2\mathcal{O}_K=\mathfrak{P}^4$ and $\mathcal{O}_K/\mathfrak{P}=\mathbb{F}_2$. Thus $\mathfrak{P}$ divides exactly one of $a,\ b,\ c$, since $\gcd(a,b,c)=1$. Without loss of generality, we suppose $\mathfrak{P}\mid b$.

Lemma 3.1. *Suppose that either $p\geq 17$, or $p=13$ and $\operatorname{ord}_{\mathfrak{P}}(b)\geq 2$. There is some $\varepsilon\in\mathcal{O}_K^*$ such that one of the following holds*:

(i) *Either E has multiplicative reduction at $\mathfrak{P}$, or*

(ii) *E has additive potentially multiplicative reduction at $\mathfrak{P}$ and $\operatorname{ord}_{\mathfrak{P}}(\mathcal{N}_\varepsilon)=4$.*

Proof. Write $c_4,\ c_6,\ \Delta$ and j for the usual invariants attached to the model (2). A straightforward computation shows that

$$c_4=\varepsilon^2\cdot 16\cdot(c^{2p}-a^pb^p),\qquad \Delta=\varepsilon^6\cdot 16\cdot(abc)^{2p},\qquad j=c_4^3/\Delta.$$

We recall that $\mathfrak{P}\mid b$. Write $t=\operatorname{ord}_{\mathfrak{P}}(b)$. Then,

$$\operatorname{ord}_{\mathfrak{P}}(j)=3\operatorname{ord}_{\mathfrak{P}}(c_4)-\operatorname{ord}_{\mathfrak{P}}(\Delta)=32-2pt. \tag{3}$$

Under the assumptions of the lemma, we have $\operatorname{ord}_{\mathfrak{P}}(j)<0$; thus we have potentially multiplicative reduction at $\mathfrak{P}$ (irrespective of the choice of ε).

The rest of the lemma is a consequence of [Freitas and Siksek 2015b, Lemma 4.4]. We give some of the details. Let

$$\mathfrak{b}=\mathfrak{P}^{2\operatorname{ord}_{\mathfrak{P}}(2)+1}=\mathfrak{P}^9.$$

Consider the natural map

$$\Phi:\mathcal{O}_K^*\to(\mathcal{O}_K/\mathfrak{b})^*/((\mathcal{O}_K/\mathfrak{b})^*)^2.$$

By an explicit computation in Magma, we find that the image of Φ has index 2 in the codomain, and that $\lambda_1=1$ and $\lambda_2=-1+2\mu$ are elements of $\mathcal{O}_K$ which represent the cokernel, where $\mu=\sqrt{2}+\sqrt{3}$. Let $n_i=\operatorname{ord}_{\mathfrak{P}}(\Delta(L_i/K))$, where $L_i=K(\sqrt{\lambda_i})$ and $\Delta(L_i/K)$ is the relative discriminant ideal for the extension L_i/K. We find that $n_1 = 0$ and $n_2 = 2$. By the aforementioned lemma, there is a unit $\varepsilon \in \mathcal{O}_K^*$ such that $\operatorname{ord}_{\mathfrak{P}}(\mathcal{N}_\varepsilon) = 1$ or 4. □

In Lemma 3.1, we determined the conductor of the Frey curve E for all primes $p \geq 17$ and a suitable choice of $\varepsilon \in \mathcal{O}_K^*$. In particular, we prove that E either has multiplicative reduction or additive potentially multiplicative reduction at $\mathfrak{P}$. This proof fails for $p = 13$ in the case that $\operatorname{ord}_{\mathfrak{P}}(b) = 1$, and we treat this case separately in the rest of the section.

Lemma 3.2. *Suppose $p = 13$ and $\operatorname{ord}_{\mathfrak{P}}(b) = 1$. Then there is a unit $\varepsilon \in \mathcal{O}_K^*$ and $\alpha \in \mathcal{O}_K$ such that*

$$\mathfrak{P}^6 \mid (\varepsilon b^{13} - \varepsilon a^{13} - \alpha^2),$$

where $\mathfrak{P} \nmid \alpha$.

Proof. Let

$$\theta : \mathcal{O}_K^* \to U/U^2,$$

where $U = (\mathcal{O}_K/\mathfrak{P}^6)^*$. We checked that θ is surjective using a straightforward computation in Magma. Let $\beta = b^{13} - a^{13}$. Note that $\mathfrak{P} \nmid \beta$. As θ is surjective, there is some $\gamma \in \mathcal{O}_K^*$ such that $\theta(\gamma) = \beta U^2$. Thus $\beta \equiv \gamma\alpha^2 \pmod{\mathfrak{P}^6}$ for some $\alpha \in \mathcal{O}_K \setminus \mathfrak{P}$. Let $\varepsilon = \gamma^{-1} \in \mathcal{O}_K^*$. Then $\varepsilon\beta \equiv \alpha^2 \pmod{\mathfrak{P}^6}$, which proves the lemma. □

Let $\varepsilon \in \mathcal{O}_K^*$ be as in Lemma 3.2. We begin by working with the Frey curve

$$E_{13,\varepsilon} : y^2 = x(x - \varepsilon a^{13})(x + \varepsilon b^{13}). \tag{4}$$

We recall that, by Lemma 2.3, $E_{13,\varepsilon}$ is semistable away from $\mathfrak{P}$. Thus, in order to determine the conductor of $E_{13,\varepsilon}$, it remains to determine the reduction type of $E_{13,\varepsilon}$ at $\mathfrak{P}$.

Lemma 3.3. *Suppose $\operatorname{ord}_{\mathfrak{P}}(b) = 1$. The Frey curve $E_{13,\varepsilon}$ has additive potentially good reduction at $\mathfrak{P}$. Moreover, $\operatorname{ord}_{\mathfrak{P}}(\mathcal{N}) = 5$, where $\mathcal{N}$ is the conductor of $E_{13,\varepsilon}$.*

Proof. Let $\alpha \in \mathcal{O}_K$ be as in Lemma 3.2. Recall that K has class number 1, and therefore every ideal is principal. Let π be a generator for $\mathfrak{P}$. For example, we can take

$$\pi = \frac{\mu^3 + \mu^2 - 9\mu - 9}{4},$$

where $\mu = \sqrt{2} + \sqrt{3}$. We make the substitutions

$$x \mapsto \pi^6 x, \quad y \mapsto \alpha\pi^6 x + \pi^9 y.$$

This yields the model

$$W : y^2 + \frac{2\alpha}{\pi^3}xy = x^3 + \frac{(\varepsilon b^{13} - \varepsilon a^{13} - \alpha^2)}{\pi^6}x^2 - \frac{\varepsilon^2 a^{13} b^{13}}{\pi^{12}}x,$$

which is integral by Lemma 3.2 and has discriminant

$$\Delta(W) = \frac{\Delta(E_{13,\varepsilon})}{\pi^{36}} = \frac{16\varepsilon^6 a^{26} b^{26} c^{26}}{\pi^{36}}.$$

Note that $\mathrm{ord}_{\mathfrak{P}}(\Delta(W)) = 6$. Thus W is minimal at $\mathfrak{P}$. We use Tate's algorithm [Silverman 1994, pp. 364–368] to compute the valuation of the conductor for W. Let $a_1, \dots, a_6$ be the usual a-invariants for W given in the above model, and let $b_2, \dots, b_8$ be the corresponding b-invariants

$$b_2 = \frac{4\alpha^2}{\pi^6}, \quad b_4 = -\frac{2\varepsilon^2 a^{13} b^{13}}{\pi^{12}}, \quad b_6 = 0, \quad b_8 = -\frac{\varepsilon^4 a^{26} b^{26}}{\pi^{24}}.$$

In particular, $\mathfrak{P} \mid a_3$, a_4, b_2 and $\mathfrak{P}^2 \mid a_6$, and $\mathrm{ord}_{\mathfrak{P}}(b_8) = 2$. Thus, by Step 4 of Tate's algorithm, the reduction type for W at $\mathfrak{P}$ is III, and the valuation of the conductor at $\mathfrak{P}$ is

$$\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}) = \mathrm{ord}_{\mathfrak{P}}(\Delta(W)) - 1 = 5. \qquad \square$$

4. Proving irreducibility of $\bar{\rho}_{E,p}$

We prove that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$. In particular, we show that a possible consequence of $\bar{\rho}_{E,p}$ being reducible is that E has a K-rational point of order p. In this instance, by [Derickx et al. 2023, Theorem 1.2], we obtain a contradiction if $p \geq 19$. We thus treat the primes $p = 13$ and 17 separately.

Since the Frey curve E has full 2-torsion over K, it is sufficient to show that there are no noncuspidal K-rational points on one of the modular curves $X_0(p)$, $X_0(2p)$ or $X_0(4p)$. We find it convenient to work with the modular curves $X_0(26)$ and $X_0(34)$. In particular, we show that $X_0(26)(K) = X_0(26)(\mathbb{Q})$ and $X_0(34)(K) = X_0(34)(\mathbb{Q})$. All points in $X_0(26)(\mathbb{Q})$ and $X_0(34)(\mathbb{Q})$ are cuspidal, thus proving the irreducibility of $\bar{\rho}_{E,p}$ for $p = 13$ and 17.

4.1. $p = 13$. Using the explicit modular parametrisation, we prove that if $P \in X_0(26)(K)$ then either $P \in X_0(26)(\mathbb{Q}(\sqrt{3}))$ or $C(\mathbb{Q}(\sqrt{3}))$ is nonempty, where C is a genus 2 hyperelliptic curve. In the first case, by [Bruin and Najman 2015], $P \in X_0(26)(\mathbb{Q})$. In the second case, we show that $C(\mathbb{Q}(\sqrt{3}))$ is empty.

Lemma 4.1. *$\bar{\rho}_{E,13}$ is irreducible.*

Proof. We prove that $X_0(26)(K) = X_0(26)(\mathbb{Q})$. We work with the model

$$X_0(26) : y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1 \tag{5}$$

given in Magma. Let

$$E' : y^2 + xy + y = x^3 - x^2 - 3x + 3.$$

Then E' is the elliptic curve with Cremona label `26b1`. Suppose $P = (a, b) \in X_0(26)(K)$. Note that if $a = 1$ then $b^2 = -16$, i.e., $P \notin X_0(26)(K)$. Suppose from now on that $a \neq 1$. Using Magma, we find the explicit parametrisation

$$\pi : X_0(26) \to E', \quad (a, b) \mapsto \left(-\frac{(a+1)^2}{(a-1)^2}, \frac{-2b + 2a(a-1)}{(a-1)^3} \right).$$

Let $L = \mathbb{Q}(\sqrt{3})$. We checked using Magma that $E'(K) = E'(L)$. It immediately follows that

$$\left(\frac{a+1}{a-1} \right)^2 \in L.$$

Let

$$\sigma : K \to K, \quad \sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}.$$

Then

$$\sigma\left(\frac{a+1}{a-1}\right) = \frac{a+1}{a-1} \quad \text{or} \quad \sigma\left(\frac{a+1}{a-1}\right) = -\frac{a+1}{a-1}.$$

Thus there are two cases to consider:

(1) $(a+1)/(a-1) \in L$.

(2) $(a+1)/(a-1) \in \sqrt{2} \cdot L$.

Case (1). In this case $a \in L$, and it immediately follows from the parametrisation of π that $b \in L$. Observe that $X_0(26)$ has infinitely many quadratic points of the form $(r, \sqrt{f(r)})$, where $r \in \mathbb{Q}$. Such points are called *nonexceptional* and all other quadratic points are called *exceptional*.

Case (1.1). If $a \in L \setminus \mathbb{Q}$ then P is an exceptional quadratic point on $X_0(26)$. Bruin and Najman [2015, Table 3] have given an explicit description of all quadratic points on $X_0(26)$. They find that all exceptional quadratic points are defined over $\mathbb{Q}(\sqrt{d})$ for $d = -1, -3, -11$ and -23.

Case (1.2). If $a \in \mathbb{Q}$ then $b^2 \in \mathbb{Q}$. Then P is a nonexceptional quadratic point on $X_0(26)$ defined over L. Moreover, P corresponds to a rational point on the quadratic twist of $X_0(26)$ over $\mathbb{Q}(\sqrt{3})$. We denote this quadratic twist by X_3. We checked using Magma that X_3 has no points defined over $\mathbb{Q}_3$. Thus $X_3(\mathbb{Q})$ is empty.

Case (2). In this case we have $(a+1)/(a-1) \in \sqrt{2} \cdot L$, i.e.,

$$\frac{a+1}{a-1} = \sqrt{2}\alpha \quad \text{for some } \alpha \in L. \tag{6}$$

Note the identity

$$\left(\frac{a+1}{a-1}\right)^2 - 1 = \frac{(a+1)^2 - (a-1)^2}{(a-1)^2} = \frac{4a}{(a-1)^2} = \frac{4a(a-1)}{(a-1)^3}. \tag{7}$$

From the parametrisation of π and (7), we see that

$$\frac{b}{(a-1)^3} \in L.$$

Note the identity

$$16\left(\frac{a^6 - 8a^5 + 8a^4 - 18a^3 + 8a^2 - 8a + 1}{(a-1)^6}\right) = -4\left(\frac{a+1}{a-1}\right)^6 - 3\left(\frac{a+1}{a-1}\right)^4 + 10\left(\frac{a+1}{a-1}\right)^2 + 13. \tag{8}$$

By combining (5) and (8), we obtain

$$\left(\frac{4b}{(a-1)^3}\right)^2 = -4\left(\frac{a+1}{a-1}\right)^6 - 3\left(\frac{a+1}{a-1}\right)^4 + 10\left(\frac{a+1}{a-1}\right)^2 + 13.$$

After making the substitutions $\beta = 4b/(a-1)^3$ and (6), we obtain

$$\beta^2 = -32\alpha^6 - 12\alpha^4 + 20\alpha^2 + 13.$$

Thus (α, β) is a L-rational point on the curve

$$C : y^2 = -32x^6 - 12x^4 + 20x^2 + 13.$$

Write $\mathcal{O}_L$ for the ring of integers of L. Then $13\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$. We checked using Magma that there are no points on C defined over the completion of L at $\mathfrak{p}_1$. Thus $C(L)$ is empty. □

4.2. $p = 17$. Using the explicit modular parametrisation, we show that if $P \in X_0(34)(K)$ then either $P \in X_0(34)(\mathbb{Q}(\sqrt{2}))$ or $C(\mathbb{Q}(\sqrt{2}))$ is nonempty, where C is the quadratic twist of $X_0(34)$ over $\mathbb{Q}(\sqrt{3})$. In the first case, by [Ozman and Siksek 2019], $P \in X_0(34)(\mathbb{Q})$. In the second case, we show that $C(\mathbb{Q}(\sqrt{2}))$ is empty.

Lemma 4.2. *$\bar{\rho}_{E,17}$ is irreducible.*

Proof. We prove that $X_0(34)(K) = X_0(34)(\mathbb{Q})$. We work with the model

$$X_0(34) : x^4 - y^4 + x^3 + 3xy^2 - 2x^2 + x + 1 = 0 \tag{9}$$

given in Magma. Making the change of variables $x \mapsto x,\ y \mapsto y^2$ yields the curve

$$C' : x^4 - y^2 + x^3 + 3xy - 2x^2 + x + 1 = 0.$$

Since C' has genus 1, we can transform it to an elliptic curve:

$$C' \to E', \quad (x, y) \mapsto (2(x^2 - 2x + y), 4x(x^2 - 2x + y)), \tag{10}$$

where

$$E' : y^2 + xy + 2y = x^3 - 4x$$

is the elliptic curve with Cremona label 34a1. We deduce the explicit modular parametrisation

$$\pi : X_0(34) \to E', \quad (x, y) \mapsto (2(x^2 - 2x + y^2), 4x(x^2 - 2x + y^2)).$$

Let $L = \mathbb{Q}(\sqrt{2})$. Using Magma we find that $E'(K) = E'(L)$. Suppose $P = (a, b) \in X_0(34)(K)$. Since

$$2(a^2 - 2a + b^2),\ 4a(a^2 - 2a + b^2) \in L,$$

it follows that either $a^2 - 2a + b^2 = 0$ or $a \in L$. Suppose the former is true, i.e.,

$$b^2 = 2a - a^2. \tag{11}$$

We substitute (11) into (9) to find that

$$2a^3 + a + 1 = 0$$

and $a \notin K$. Thus $a \in L$, and hence $b^2 \in L$. Either $b \in L$ or $b = \sqrt{3}\beta$ for some $\beta \in L$. If $b \in L$ then $P \in X_0(34)(L)$. Ozman and Siksek [2019] have determined the quadratic points on $X_0(34)$, and they found that there are no real quadratic points on $X_0(34)$. Thus $P \in X_0(34)(\mathbb{Q})$.

Suppose $b = \sqrt{3}\beta$ for some $\beta \in L$. Thus (a, β) is an L-rational point on the curve

$$C : x^4 - 9y^4 + x^3 + 9xy^2 - 2x^2 + x + 1 = 0,$$

where C is the quadratic twist of $X_0(34)$ over $\mathbb{Q}(\sqrt{3})$. Note that 3 is inert in L. We checked using Magma that there are no points on C defined over the completion of L at $3\mathcal{O}_L$. Thus $C(L)$ is empty. □

4.3. $\boldsymbol{p \geq 19}$. We let $E = E_{a,b,c,\varepsilon}$, where $\varepsilon \in \mathcal{O}_K^*$ is chosen so that one of the two possibilities in Lemma 3.1 hold. Suppose $\bar{\rho}_{E,p}$ is reducible. Then

$$\bar{\rho}_{E,p} \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix},$$

where θ and θ' are characters $G_K \to \mathbb{F}_p^*$. Recall that $\chi_p = \det(\bar{\rho}_{E,p}) = \theta\theta'$, where χ_p denotes the mod p cyclotomic character. We let $\mathcal{N}_\theta$ and $\mathcal{N}_{\theta'}$ denote the conductors of θ and θ', respectively. We shall require the following result of Freitas and Siksek.

Lemma 4.3 [Freitas and Siksek 2015b, Lemma 6.3]. *Let E be an elliptic curve defined over a number field K with conductor $\mathcal{N}$. Let $p \geq 5$ be a prime, and let $\mathfrak{q} \nmid p$ be a prime. Let θ and θ' be as above. If $\bar{\rho}_{E,p}$ is reducible then*

$$\operatorname{ord}_{\mathfrak{q}}(\mathcal{N}_\theta) = \operatorname{ord}_{\mathfrak{q}}(\mathcal{N}_{\theta'}) = \begin{cases} 0 & \textit{if } E \textit{ has good or multiplicative reduction at } \mathfrak{q}, \\ \frac{1}{2}\operatorname{ord}_{\mathfrak{q}}(\mathcal{N}) \in \mathbb{Z} & \textit{if } E \textit{ has additive reduction at } \mathfrak{q}. \end{cases}$$

Lemma 4.4. *Let $p \geq 19$. Then $\bar{\rho}_{E,p}$ is irreducible.*

Proof. Suppose $\bar{\rho}_{E,p}$ is reducible. Since p is unramified in K and E has good or multiplicative reduction at $\mathfrak{p} \mid p$, we have that, for any $\mathfrak{p} \mid p$, precisely one of θ, θ' is ramified at $\mathfrak{p}$; see [Kraus 1996, Lemma 1].

First suppose that either of θ, θ' is unramified at all $\mathfrak{p} \mid p$ (and thus the other is ramified at all $\mathfrak{p} \mid p$). We note that replacing E by a p-isogenous elliptic curve, if necessary, allows us to swap θ and θ'. Thus we may suppose that θ is unramified at all the primes above p, and hence θ is unramified away from $\mathfrak{P}$.

We shall use Lemma 4.3 to determine $\mathcal{N}_\theta$. Suppose we are in case (i) of Lemma 3.1 and E has multiplicative reduction at $\mathfrak{P}$. Then, by Lemma 4.3, we have $\operatorname{ord}_{\mathfrak{P}}(\mathcal{N}_{\theta'}) = \operatorname{ord}_{\mathfrak{P}}(\mathcal{N}_\theta) = 0$. Suppose now that we are in case (ii) of Lemma 3.1 and E has additive reduction at $\mathfrak{P}$. Then, by Lemma 4.3, we have

$$\operatorname{ord}_{\mathfrak{P}}(\mathcal{N}_\theta) = \operatorname{ord}_{\mathfrak{p}}(\mathcal{N}_{\theta'}) = \tfrac{1}{2}\operatorname{ord}_{\mathfrak{P}}(\mathcal{N}_\varepsilon) = 2.$$

Hence either $\mathcal{N}_\theta = 1$ or $\mathfrak{P}^2$. Let $\infty_1, \dots, \infty_4$ denote the four real places of K. Then θ is a character for the ray class group of the modulus $\infty_1 \cdots \infty_4$ in the first case, and of the modulus $\mathfrak{P}^2 \cdot \infty_1 \cdots \infty_4$ in the second case. Using Magma we find that this ray class group is $\mathbb{Z}/2\mathbb{Z}$ in either case. Thus the order of θ divides 2, and θ is either trivial or a quadratic character. In the first case, when θ is trivial, E has a K-rational point of order p. In the second case, let E' be the quadratic twist of E by θ. Then

$$\bar{\rho}_{E',p} \sim \begin{pmatrix} \theta^2 & * \\ 0 & \theta\theta' \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & \chi_p \end{pmatrix}.$$

Thus E' has a K-rational point of order p. In both cases, we obtain an elliptic curve with a point of order p defined over K (a quartic field). By [Derickx et al. 2023, Theorem 1.2], $p \leq 17$. We obtain a contradiction since $p \geq 19$.

Fix $\mathfrak{p}_0$ a prime ideal of $\mathcal{O}_K$ above p. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Then G acts transitively on the primes $\mathfrak{p} \mid p$. Let S be the set of $\tau \in G$ such that θ is ramified at $\tau(\mathfrak{p}_0)$. We know from above that S is a proper subset of G, i.e., $S \neq \varnothing$ and $S \neq G$. For a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$, we write $I_\mathfrak{q}$ for an inertia subgroup of G_K corresponding to $\mathfrak{q}$. Thus $\theta|_{I_\mathfrak{q}} = 1$ for all

$$\mathfrak{q} \notin \{\mathfrak{P}\} \cup \{\tau(\mathfrak{p}_0) : \tau \in S\}.$$

By Lemma 3.1, E has potentially multiplicative reduction at $\mathfrak{P}$. By the theory of the Tate curve [David 2011, Proposition 1.2], $\theta^2|_{I_\mathfrak{P}} = 1$. Let $\phi = \theta^2$. Then $\phi|_{I_\mathfrak{q}} = 1$ for all

$$\mathfrak{q} \notin \{\tau(\mathfrak{p}_0) : \tau \in S\}.$$

Recall that θ' is unramified at $\mathfrak{q} \in \{\tau(\mathfrak{p}_0) : \tau \in S\}$. Since $\theta\theta' = \chi_p$, we conclude that

$$\phi|_{I_\mathfrak{q}} = \begin{cases} \chi_p^2|_{I_\mathfrak{q}}, & \mathfrak{q} \in \{\tau(\mathfrak{p}_0) : \tau \in S\}, \\ 1 & \text{otherwise.} \end{cases} \tag{12}$$

Let $u \in \mathcal{O}_K^*$. We define the twisted norm of u attached to S to be

$$\mathfrak{N}_S(u) = \prod_{\tau \in S} (\tau(u))^2.$$

By the proof of [David 2011, Proposition 2.6], the existence of ϕ satisfying (12) ensures that

$$\mathfrak{p}_0 \mid (\mathfrak{N}_S(u) - 1).$$

Let $\mu = \sqrt{2} + \sqrt{3}$, and let

$$u_1 = \mu, \quad u_2 = \tfrac{1}{2}(-\mu^3 + 9\mu + 2), \quad u_3 = \tfrac{1}{4}(\mu^3 - \mu^2 - 9\mu + 5);$$

this is a basis for $\mathcal{O}_K^*/\{\pm 1\}$. Then $p \mid B_S$, where

$$B_S = \mathrm{Norm}\biggl(\sum_{i=1}^{3} (\mathfrak{N}_S(u_i) - 1) \cdot \mathcal{O}_K\biggr).$$

We used Magma to compute B_S for all nonempty proper subsets S of $G = \mathrm{Gal}(K/\mathbb{Q})$. In all cases we found that if $p \mid B_S$ then $p = 2$ or 3. Thus we obtain a contradiction. □

5. Eliminating Hilbert newforms

Let

$$\mathcal{N}_0 = \begin{cases} \mathfrak{P} & \text{if we are in case (i) of Lemma 3.1,} \\ \mathfrak{P}^4 & \text{if we are in case (ii) of Lemma 3.1,} \\ \mathfrak{P}^5 & \text{if } p = 13 \text{ and } \mathrm{ord}_\mathfrak{P}(b) = 1. \end{cases}$$

Applying level lowering (i.e., Theorem 2.1), we obtain

$$\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\mathfrak{p}},$$

where $\mathfrak{f}$ is a Hilbert newform of parallel weight 2 and level $\mathcal{N}_0$, and $\mathfrak{p}$ is some prime above p in $\mathbb{Q}_{\mathfrak{f}}$, the Hecke eigenvalue field of $\mathfrak{f}$. Using Magma we find that there are no newforms with parallel weight 2 and level $\mathfrak{P}$ or level $\mathfrak{P}^5$, obtaining a contradiction in these cases.

We thus suppose we are in case (ii) of Lemma 3.1. For the level $\mathfrak{P}^4$, we find that there are two newforms $\mathfrak{f}_1$ and $\mathfrak{f}_2$ and for both the corresponding Hecke eigenvalue field is $\mathbb{Q}$. Let E_1/K and E_2/K be the following elliptic curves:

$$E_1 : y^2 + (\mu+1)xy = x^3 + \tfrac{1}{4}(-\mu^3 - \mu^2 - 3\mu + 5)x^2 + \tfrac{1}{2}(-\mu^3 - 5\mu)x + \tfrac{1}{4}(\mu^3 + 7\mu^2 - 9\mu - 3),$$
$$E_2 : y^2 + \tfrac{1}{4}(\mu^3 + \mu^2 + 3\mu + 3)y = x^3 + \tfrac{1}{2}(-\mu^2 - 1)x^2 + \mu^2 x + \tfrac{1}{4}(-3\mu^3 - 17\mu^2 - \mu + 1),$$

where $\mu = \sqrt{2}+\sqrt{3}$. These elliptic curves have conductors $\mathfrak{P}^4$ and were found using the Magma command EllipticCurveSearch. These are nonisogenous, as $a_{\mathfrak{q}}(E_1) = 6$ and $a_{\mathfrak{q}}(E_2) = -6$, where $3\mathcal{O}_K = \mathfrak{q}^2$. By the work of Box [2022], E_1 and E_2 are modular and thus correspond to the two Hilbert newforms $\mathfrak{f}_1$ and $\mathfrak{f}_2$ of parallel weight 2 and level $\mathfrak{P}^4$. Thus $\bar{\rho}_{E,p} \sim \bar{\rho}_{E_i,p}$, where $i = 1$ or 2. To obtain a contradiction, we shall use a standard image of inertia argument; see [Freitas and Siksek 2015a, Lemma 3.5].

Let j be the j-invariant of the Frey curve E. By (3) we have $\operatorname{ord}_{\mathfrak{P}}(j) < 0$ and $p \nmid \operatorname{ord}_{\mathfrak{P}}(j)$. Thus, $p \mid \#\bar{\rho}_{E,p}(I_{\mathfrak{P}})$ [Silverman 1994, Proposition 6.1, Chapter 5]. However, we find that E_1 and E_2 have j-invariants

$$j_1 = 0 \quad \text{and} \quad j_2 = -853632\mu^3 + 7682688\mu + 2417472,$$

respectively. As $\operatorname{ord}_{\mathfrak{P}}(j_i) \geq 0$, we have that E_1 and E_2 have potentially good reduction at $\mathfrak{P}$. It follows that $\#\bar{\rho}_{E_i,p}(I_{\mathfrak{P}}) \mid 24$ from [Kraus 1990, Introduction]. As $\bar{\rho}_{E,p} \sim \bar{\rho}_{E_i,p}$ for $i = 1$ or 2, we obtain $p \mid 24$ giving a contradiction.

6. Small integer exponents

We have thus far shown that there are no solutions to (1) over K for primes $p \geq 5$. In order to complete the proof of Theorem 1.1, it remains to rule out solutions to (1) for $n = 4, 6, 9$. We note in passing that there are nontrivial solutions to the Fermat cubic over $\mathbb{Q}(\sqrt{2})$; see [Jarvis and Meekin 2004, p. 184].

6.1. $n = 9$.

We are very grateful to Samir Siksek for the lengthy discussions and ideas that resulted in this proof. We first convert the problem of finding K-points on the Fermat curve of degree 9 to finding the $\mathbb{Q}(\sqrt{3})$-points on a certain hyperelliptic curve C. We then study the Jacobian of C to show that $C(\mathbb{Q}(\sqrt{3})) = \{\infty\}$, where ∞ denotes the point at infinity on C.

Theorem 6.1. *There are no nontrivial solutions to* (1) *over K for $n = 9$.*

We find it convenient to let

$$F_9 : x^9 + y^9 + z^9 = 0.$$

That is, F_9 is the Fermat curve of degree 9. We recall that $2\mathcal{O}_K = \mathfrak{P}^4$ and that K has class number 1. We will prove that $F_9(K) = \{(1 : -1 : 0), (1 : 0 : -1), (0 : 1 : -1)\}$, i.e, $F_9(K)$ consists only of trivial solutions. Suppose $(\alpha : \beta : \gamma) \in F_9(K)$ is a nontrivial solution. We may suppose that $\alpha, \beta, \gamma \in \mathcal{O}_K$ and that they are coprime. We recall that $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$ and

$$F_9(\mathbb{F}_2) = \{(1:1:0),\ (1:0:1),\ (0:1:1)\}.$$

Hence, by permuting α, β, γ appropriately, we may suppose $(\alpha : \beta : \gamma) \equiv (1:1:0) \pmod{\mathfrak{P}}$. Thus

$$\mathfrak{P} \mid \gamma, \quad \mathfrak{P} \nmid \alpha\beta. \tag{13}$$

Observe

$$\gamma^{18} - (\alpha^9 - \beta^9)^2 = (\alpha^9 + \beta^9)^2 - (\alpha^9 - \beta^9)^2 = 4(\alpha\beta)^9.$$

After making the substitutions

$$u = \frac{\alpha\beta}{\gamma^2}, \quad v = \frac{\alpha^9 - \beta^9}{\gamma^9}, \tag{14}$$

we see that $Q_1 = (u, v) \in C_1(K)$, where

$$C_1 : y^2 = -4x^9 + 1.$$

Let

$$E_1 : y^2 = 4x^3 + 1.$$

This is an elliptic curve. Let

$$\pi_1 : C_1 \to E_1, \quad (x, y) \mapsto (-x^3, y).$$

The elliptic curve E_1 has minimal Weierstrass model

$$E_1' : z^2 + z = x^3,$$

which is obtained from E_1 by the substitution $y = 2z + 1$. This has Cremona label 27a3. In particular, E_1' has good reduction away from 3. Let $R_1 = \pi_1(Q_1) = (-u^3, v) \in E_1(K)$. Then R_1 corresponds to the point

$$S_1 = \left(-u^3, \tfrac{1}{2}(v-1)\right) \in E_1'(K).$$

Let $\sigma : K \to K$ be the automorphism satisfying

$$\sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}.$$

We note that the fixed field of σ is $L = \mathbb{Q}(\sqrt{3})$. Thus $S_1 + S_1^\sigma \in E_1'(L)$. We checked using Magma that E_1' has rank 0 over L, and indeed

$$E_1'(L) = \{\mathcal{O},\ (0,0),\ (0,-1)\} \cong \mathbb{Z}/3\mathbb{Z}. \tag{15}$$

Thus $S_1 + S_1^\sigma$ is one of these three points. However, $\operatorname{ord}_{\mathfrak{P}}(u) < 0$ by (13) and (14). It follows that

$$S_1 \equiv \mathcal{O} \pmod{\mathfrak{P}}.$$

Hence

$$S_1^\sigma \equiv \mathcal{O}^\sigma = \mathcal{O} \pmod{\mathfrak{P}^\sigma}.$$

However, $\mathfrak{P}$ is a totally ramified prime, so $\mathfrak{P}^\sigma = \mathfrak{P}$. Thus $S_1^\sigma \equiv \mathcal{O} \pmod{\mathfrak{P}}$, and

$$S_1 + S_1^\sigma \equiv \mathcal{O} \pmod{\mathfrak{P}}.$$

By (15) and the injectivity of torsion upon reduction modulo primes of good reduction (see [Katz 1981, Appendix]), we conclude that

$$S_1 + S_1^\sigma = \mathcal{O}.$$

Hence

$$R_1 + R_1^\sigma = \mathcal{O}.$$

Hence

$$(-u^3)^\sigma = -u^3, \quad v^\sigma = -v.$$

As the only cube root of 1 in K is 1, we have $u^\sigma = u$ and so $u \in L$. Moreover, $v^2 = -4u^9 + 1 \in L$ and $v^\sigma = -v$, so $v = w/\sqrt{2}$, where $w \in L$. Hence $(u, w) \in C(L)$, where

$$C : y^2 = 2(-4x^9 + 1).$$

Lemma 6.2. *$C(L) = \{\infty\}$.*

Since $u = \alpha\beta/\gamma^2$, Theorem 6.1 follows from Lemma 6.2. We now prove Lemma 6.2 by studying $J(\mathbb{Q})$, where J is the Jacobian of C.

Proof. Let

$$E : y^2 = x^3 + 2,$$

which is the elliptic curve with Cremona label `1728a1`. Let

$$\pi : C \to E, \quad (x, y) \mapsto (-2x^3, y). \tag{16}$$

Using Magma we find that E has zero torsion and rank 1 over $\mathbb{Q}$ and that, in fact,

$$E(\mathbb{Q}) = \mathbb{Z} \cdot (-1, 1).$$

We write $\mathrm{Pic}^0(E)$ for the group of rational degree 0 divisors on $E/\mathbb{Q}$ modulo linear equivalence and $\mathrm{Pic}^0(C)$ for the group of rational degree 0 divisors on $C/\mathbb{Q}$ modulo linear equivalence. We recall the standard isomorphism [Silverman 2009, Proposition III.3.4]

$$E(\mathbb{Q}) \cong \mathrm{Pic}^0(E), \quad P \mapsto [P - \infty], \tag{17}$$

where $[D]$ denotes the linear equivalence class of a divisor D. Thus

$$\mathrm{Pic}^0(E) = \mathbb{Z} \cdot \mathcal{Q}, \quad \mathcal{Q} = [(-1, 1) - \infty].$$

We also recall the standard isomorphism $J(\mathbb{Q}) \cong \mathrm{Pic}^0(C)$, and we will represent elements of the Mordell–Weil group $J(\mathbb{Q})$ as elements of $\mathrm{Pic}^0(C)$. Using Magma we find that J has good reduction away from the primes 2 and 3. Moreover, a straightforward calculation in Magma returns

$$J(\mathbb{F}_5) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/126\mathbb{Z}, \quad J(\mathbb{F}_{13}) \cong \mathbb{Z}/42997\mathbb{Z}.$$

As these two groups have coprime orders, we conclude that J has trivial torsion over $\mathbb{Q}$. Moreover, using Magma, we find that J has 2-Selmer rank 1 over $\mathbb{Q}$, so J has rank at most 1 over $\mathbb{Q}$. The morphism π in (16) has degree 3 and induces homomorphisms (see [Silverman 2009, Section II.3])

$$\pi_* : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(E), \quad \left[\sum a_i P_i\right] \mapsto \left[\sum a_i \pi(P_i)\right]$$

and

$$\pi^* : \mathrm{Pic}^0(E) \to \mathrm{Pic}^0(C), \quad \left[\sum b_j Q_j\right] \mapsto \left[\sum b_j \sum_{P \in \pi^{-1}(Q_j)} e_\pi(P) \cdot P\right],$$

where $e_\pi(P)$ denotes the ramification degree of π at P.

Let

$$\mathcal{P} = \pi^*(\mathcal{Q}) = [(1/\sqrt[3]{2}, 1) + (\omega/\sqrt[3]{2}, 1) + (\omega^2/\sqrt[3]{2}, 1) - 3\infty] \in \mathrm{Pic}^0(C) \cong J(\mathbb{Q}),$$

where ω is a primitive cube root of 1. The point $\mathcal{P}$ has infinite order on $J(\mathbb{Q})$. Thus J has rank exactly 1 over $\mathbb{Q}$ and no torsion. Therefore $J(\mathbb{Q}) = \mathbb{Z} \cdot \mathcal{P}'$ for some $\mathcal{P}' \in J(\mathbb{Q}) = \mathrm{Pic}^0(C)$. Hence

$$\mathcal{P} = k\mathcal{P}',$$

where k is a nonzero integer. Applying π_* to both sides, we obtain

$$k\pi_*(\mathcal{P}') = \pi_*(\mathcal{P}) = 3\mathcal{Q}.$$

However, $\pi_*(\mathcal{P}') \in \mathrm{Pic}^0(E) = \mathbb{Z}\mathcal{Q}$, so

$$\pi_*(\mathcal{P}') = \ell \cdot \mathcal{Q}$$

for some $\ell \in \mathbb{Z}$. Hence $k\ell = 3$, so $k = \pm 1$ or ± 3. Using Magma we checked that the image of $\mathcal{P}$ under the composition

$$J(\mathbb{Q}) \to J(\mathbb{F}_5) \to J(\mathbb{F}_5)/3J(\mathbb{F}_5)$$

is nonzero. Thus $k \neq \pm 3$, so $k = \pm 1$; hence

$$J(\mathbb{Q}) = \mathrm{Pic}^0(C) = \mathbb{Z} \cdot \mathcal{P}.$$

Suppose $P \in C(L)$. Let $\tau : L \to L$ be the nontrivial automorphism. Then $[P + P^\tau - 2\infty] \in \mathrm{Pic}^0(C)$. Thus

$$[P + P^\tau - 2\infty] = n \cdot \mathcal{P} = n \cdot \pi^*(\mathcal{Q}) = \pi^*(n \cdot \mathcal{Q})$$

for some integer n. We claim that $n = 0$. Suppose otherwise; then $n \cdot \mathcal{Q} \in \mathrm{Pic}^0(E) \setminus \{0\}$ and by the isomorphism in (17) we have $n \cdot \mathcal{Q} = [Q - \infty]$, where $Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Write $Q = (a, b) \in E(\mathbb{Q})$ with $a, b \in \mathbb{Q}$. Then

$$[P + P^\tau - 2\infty] = \pi^*([(a, b) - \infty]) = [D - 3\infty],$$

where

$$D = P_1 + P_2 + P_3, \quad P_j = (-\omega^{j-1}\sqrt[3]{a/2}, b), \quad j = 1, 2, 3.$$

Hence

$$D \sim D', \quad D' = P + P^\tau + \infty,$$

where $\sim$ denotes linear equivalence on C. Write $|D|$ for the complete linear system of effective divisors of C linearly equivalent to D. Let $r(D) = \dim|D|$. Note that $D' \in |D|$ and $D' \neq D$; therefore $r(D) \geq 1$. By Riemann–Roch [Arbarello et al. 1985, p. 13],

$$r(D) - i(D) = \deg(D) - g = -1,$$

where $i(D) \geq 0$ is the so-called index of speciality of D and $g = 4$ is the genus of C. It follows that $i(D) > 0$ and therefore that D is a special divisor. By Clifford's theorem [Hartshorne 1977, Theorem IV.5.4],

$$r(D) \leq \tfrac{1}{2}\deg(D) = \tfrac{3}{2}.$$

Hence $r(D) = 1$. Thus the complete linear system $|D|$ is a g^1_3. As C is hyperelliptic, by [Arbarello et al. 1985, p. 13], $|D| = g^1_2 + p$, where p is a fixed base point of the linear system. In particular, every divisor in $|D|$ is the sum of p and two points interchanged by the hyperelliptic involution. We apply this to D itself. Thus two of the points P_1, P_2, P_3 are interchanged by the hyperelliptic involution. However, they all have the same y-coordinate b, so $b = 0$. But $(a, b) \in E(\mathbb{Q})$, so $a \in \mathbb{Q}$ and $a^3 = -2$, giving a contradiction. Hence $n = 0$, and so

$$P + P^\tau \sim 2\infty.$$

Thus P and P^τ are interchanged by the hyperelliptic involution. We recall that we want to show that $P = \infty$. Suppose otherwise. Then we can write $P = (c, d)$, where $c, d \in L$ and $c^\tau = c$, $d^\tau = -d$. Thus $c \in \mathbb{Q}$ and $d = e/\sqrt{3}$ with $e \in \mathbb{Q}$. Thus $P' = (c, e) \in C'(\mathbb{Q})$, where

$$C' : y^2 = 6(-4x^9 + 1).$$

Let J' be the Jacobian of C' and

$$E' : y^2 = 6(4x^3 + 1).$$

Using Magma, we find that $E'(\mathbb{Q}) = \mathbb{Z} \cdot \left(\frac{1}{2}, 3\right)$. Let $\mathcal{Q}' = \left[\left(\frac{1}{2}, 3\right) - \infty\right] \in \mathrm{Pic}^0(E')$, so $\mathrm{Pic}^0(E') = \mathbb{Z} \cdot \mathcal{Q}$. Let

$$\pi' : C' \to E', \quad (x, y) \mapsto (-x^3, y).$$

Using Magma, we find that J' has trivial torsion and 2-Selmer rank 1, and, following the same steps as before, we show that $J'(\mathbb{Q}) = \mathrm{Pic}^0(C) = \mathbb{Z} \cdot \mathcal{P}'$, where $\mathcal{P}' = (\pi')^*(\mathcal{Q})$. Now $[P' - \infty]$ equals $n\mathcal{P}'$, where n is an integer, and must be nonzero as $P' \neq \infty$. Let $(f, g) = n \cdot \left(\frac{1}{2}, 3\right) \in E'(\mathbb{Q}) \setminus \{\mathcal{O}\}$. As before, we find that

$$P' + 2\infty \sim P'_1 + P'_2 + P'_3, \quad P'_j = (-\omega^{j-1} \cdot \sqrt[3]{f}, g).$$

Continuing as before, it follows that $g = 0$, so $f^3 = -\frac{1}{4}$, contradicting $f \in \mathbb{Q}$. We can thus conclude that if $P \in C(L)$ then $P = \infty$. This completes the proof of Lemma 6.2 and therefore Theorem 6.1. □

6.2. $n = 6$. We show that a K-point on the Fermat curve of degree 6 induces a K-point P on a certain hyperelliptic curve C. Let E be the elliptic curve obtained by taking the quotient of C by a certain automorphism of C. We find that $E(K) = E(\mathbb{Q}) = \mathbb{Z}$ and use this to show that P is defined over a quadratic subfield of K. This leads to the search of $\mathbb{Q}$-rational points on the twists of C over the quadratic subfields of K.

Theorem 6.3. *There are no nontrivial solutions to* (1) *over K for $n = 6$.*

Proof. We find it convenient to let

$$F_6 : x^6 + y^6 = z^6.$$

That is, F_6 is the Fermat curve of degree 6. We will prove that

$$F_6(K) = \{(0 : -1 : 1),\ (-1 : 0 : 1),\ (0 : 1 : 1),\ (1 : 0 : 1)\},$$

i.e., $F_6(K)$ consists only of trivial solutions. Suppose $(\alpha : \beta : \gamma) \in F_6(K)$ is a nontrivial solution. We can assume without loss of generality that $\alpha,\ \beta,\ \gamma$ are integral and coprime. Similar to the proof of Theorem 6.1, observe

$$\gamma^{12} - (\alpha^6 - \beta^6)^2 = (\alpha^6 + \beta^6)^2 - (\alpha^6 - \beta^6)^2 = 4(\alpha\beta)^6.$$

Let

$$a = \frac{\alpha\beta}{\gamma^2}, \quad b = \frac{\alpha^6 - \beta^6}{\gamma^6}.$$

Then $P = (a, b) \in C(K)$, where

$$C : y^2 = -4x^6 + 1.$$

Let

$$E : y^2 = x^3 - 4.$$

This is the elliptic curve with Cremona label `432b1`. Let

$$\pi : C \to E, \quad (x, y) \mapsto \left(\frac{1}{x^2}, \frac{y}{x^3}\right), \quad (0, \pm 1) \mapsto 0_E.$$

We checked using Magma that E has rank 1 over K (and $\mathbb{Q}$) and that

$$E(K) = E(\mathbb{Q}) \cong \mathbb{Z}.$$

Since $\pi(P) \in E(\mathbb{Q})$, it follows that $a^2 \in \mathbb{Q}$ and hence $b^2 \in \mathbb{Q}$. If $a = 0$ then it's clear that $(\alpha : \beta : \gamma)$ is a trivial solution. Observe that a and b are necessarily defined over the same quadratic subfield of K since

$$\frac{b}{a} \in \mathbb{Q}.$$

Either $a \in \mathbb{Q}$ and hence $b \in \mathbb{Q}$, or

$$a = \frac{a'}{\sqrt{d}}, \quad b = \frac{b'}{\sqrt{d}}, \qquad \text{for } d \in \{2, 3, 6\},\ \ a', b' \in \mathbb{Q}.$$

If $a, b \in \mathbb{Q}$ then $P \in C(\mathbb{Q})$. The Jacobian of C has rank 1 over $\mathbb{Q}$. Using the Chabauty implementation in Magma, we find that

$$C(\mathbb{Q}) = \{(0, \pm 1)\},$$

and it immediately follows that $(\alpha : \beta : \gamma)$ is a trivial solution. Thus, $(a', b'd) \in C_d(\mathbb{Q})$ where

$$C_d : y^2 = -4x^6 + d^3,$$

where $d \in \{2, 3, 6\}$. Suppose $d = 3$ or 6. We checked using Magma that there are no points on C_d defined over $\mathbb{Q}_2$. Thus $C_3(\mathbb{Q}) = C_6(\mathbb{Q}) = \varnothing$. It remains to determine $C_2(\mathbb{Q})$. We will work with the model

$$C_2 : y^2 = -x^6 + 2. \tag{18}$$

We note that the curve C_2 has genus 2 and the rank of the Jacobian of C_2 over $\mathbb{Q}$ is 2. Thus, we are unable to determine $C_2(\mathbb{Q})$ using Chabauty. Instead, we used the elliptic curve Chabauty method of [Bruin 2003] to do so as we now demonstrate.

Let $\theta = \sqrt[6]{2}$, and note that θ is a root of the hyperelliptic polynomial for C_2 given in (18). Let $L = \mathbb{Q}(\theta)$. Consider the map

$$\varphi : C_2(\mathbb{Q}) \to L^*/(L^*)^2, \quad (x, y) \to (x - \theta) \cdot (L^*)^2.$$

The method of two-cover descent, due to Bruin and Stoll [2009], uses sieving information to determine a small finite set containing the image of φ. This is implemented in Magma, and applying it we find that

$$\varphi(C_2(\mathbb{Q})) \subseteq \{(1 + \theta) \cdot (L^*)^2, (1 - \theta) \cdot (L^*)^2\}.$$

Thus, for a rational point $(x, y) \in C_2(\mathbb{Q})$, we have

$$x - \theta = (1 \pm \theta)\beta^2 \tag{19}$$

with $\beta \in L^*$. Now let $F = \mathbb{Q}(\sqrt[3]{2})$, and note that $x^2 - \sqrt[3]{2} = \mathrm{Norm}_{L/F}(x - \theta)$. Observe that

$$\mathrm{Norm}_{L/F}(1 \pm \theta) = (1 - \theta)(1 + \theta) = 1 - \sqrt[3]{2}.$$

Taking norms in (19) gives

$$x^2 - \sqrt[3]{2} = (1 - \sqrt[3]{2})w^2, \quad w = \mathrm{Norm}_{L/F}(\beta) \in F^*.$$

Note the factorisation

$$C_2 : y^2 = -x^6 + 2 = -(x^2 - \sqrt[3]{2})(x^4 + \sqrt[3]{2}x^2 + \sqrt[3]{2}^2).$$

Thus, for $(x, y) \in C_2(\mathbb{Q})$, we have

$$x^4 + \sqrt[3]{2}x^2 + \sqrt[3]{2}^2 = \frac{-y^2}{x^2 - \sqrt[3]{2}} = \frac{-1}{(1 - \sqrt[3]{2})} \cdot \frac{y^2}{w^2}.$$

Let $\epsilon = -1/(1 - \sqrt[3]{2}) = 1 + \sqrt[3]{2} + \sqrt[3]{2}^2 \in F^*$ and $z = y/w \in F^*$. Then, for $(x, y) \in C_2(\mathbb{Q})$, we have

$$x^4 + \sqrt[3]{2}x^2 + \sqrt[3]{2}^2 = \epsilon z^2. \tag{20}$$

Let

$$X = \epsilon x^2 \quad \text{and} \quad Y = \epsilon^2 xz. \tag{21}$$

Then $(X, Y) \in E_2(F)$, where E_2/F is the elliptic curve

$$E_2 : Y^2 = X^3 + \epsilon\sqrt[3]{2}X^2 + \epsilon^2\sqrt[3]{2}^2 X.$$

Using Magma, we found that the Mordell–Weil group is given by

$$E_2(F) = (\mathbb{Z}/2\mathbb{Z}) \cdot (0, 0) \oplus \mathbb{Z} \cdot (1 + \sqrt[3]{2} + \sqrt[3]{2}^2, 5 + 4\sqrt[3]{2} + 3\sqrt[3]{2}^2).$$

We are interested in points $(X, Y) \in E_2(F)$ which satisfy (21), where $(x, y) \in C_2(\mathbb{Q})$. In particular, to determine $C_2(\mathbb{Q})$, it is enough to find all points $Q = (X, Y) \in E_2(F)$ such that $f(Q) \in \mathbb{Q}$, where $f(X, Y) = X/\epsilon$. The elliptic curve Chabauty method of [Bruin 2003] is one that can sometimes be used to provably determine all F-points Q on an elliptic curve E defined over a number field F such that $f(Q) \in \mathbb{Q}$ for a given nonconstant function $f \in F(E)$, provided the degree $[F : \mathbb{Q}]$ exceeds the rank of E over F. In our situation, the degree is $[F : \mathbb{Q}] = 3$ and the rank of E over F is 1. We applied the implementation of the elliptic curve Chabauty method available in Magma to our E_2/F and f. This succeeded in showing that the only $(X, Y) \in E_2(F)$ with $X/\varepsilon \in \mathbb{Q}$ are

$$(X, Y) = (0, 0),\ \ (1 + \sqrt[3]{2} + \sqrt[3]{2}^2, 5 + 4\sqrt[3]{2} + 3\sqrt[3]{2}^2),\ \ (1 + \sqrt[3]{2} + \sqrt[3]{2}^2, -5 - 4\sqrt[3]{2} - 3\sqrt[3]{2}^2).$$

Thus $X = 0$ or ϵ, and hence if $(x, y) \in C_2(\mathbb{Q})$ then $x = 0$ or ± 1. It immediately follows that

$$C_2(\mathbb{Q}) = \{(\pm 1, \pm 1)\}.$$

Thus, $(a', b') \in \{(\pm 1, \pm 1)\}$ and if $P = (a, b) \in C(K)$ then $P \in \{(\pm 1/\sqrt{2}, \pm 1/\sqrt{2})\}$. Recall that

$$b = \frac{\alpha^6 - \beta^6}{\gamma^6},$$

where $(\alpha : \beta : \gamma) \in F_6(K)$. It immediately follows that $\frac{1}{2}(b + 1)$ is a square in K. For each b, we check using Magma that $\frac{1}{2}(b + 1)$ is not a square in K. We have reached a contradiction. □

6.3. ***n* = 4.** Quadratic points on the Fermat quartic have been studied by Aigner [1934], Faddeev [1960] and Mordell [1968]. Mordell starts with the knowledge that there are no nontrivial points on the Fermat quartic over $\mathbb{Q}$ and studies points over all quadratic fields. We generalise his method, observing that we can also classify points over quadratic extensions of certain quadratic fields. More precisely, if L is any field for which there are no points on the Fermat quartic, and if the two elliptic curves with Cremona labels `32a1` and `64a1` have rank 0 over L, then we give a procedure to write down all the points on the Fermat quartic over quadratic extensions of L.

In an earlier version of this paper, we conjectured that there are no points on the Fermat quartic over any real biquadratic field. We thank Pedro José Cazorla Garcia for pointing out to us that the point $(\sqrt{3}, 2, \sqrt{5})$ lies on the Fermat quartic over $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

After the completion of this work, we were made aware that Ishitsuka, Ito and Ohshita [Ishitsuka et al. 2020, Theorem 7.3] have previously determined all points on the Fermat quartic lying in a quadratic extension of $\mathbb{Q}(\zeta_8)$. We thank the authors for making us aware of this. Since $\mathbb{Q}(\sqrt{2})$ is contained in $\mathbb{Q}(\zeta_8)$, this is indeed stronger than the statement of Theorem 6.4. We note that the authors of [Ishitsuka et al. 2020] study the Jacobian of the Fermat quartic over $\mathbb{Q}(\zeta_8)$ and that the proof of Theorem 6.4, extending work of Mordell [1968], makes use of a different strategy.

Theorem 6.4. *The points on the Fermat quartic lying in quadratic extensions of* $\mathbb{Q}(\sqrt{2})$ *lie in one of* $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt{2}, \sqrt{-7})$, $\mathbb{Q}(\sqrt[4]{2})$ *or* $\mathbb{Q}(\sqrt[4]{2}i)$.

Proof. Let $L = \mathbb{Q}(\sqrt{2})$, and let K be a quadratic extension of L. We will determine all points on the Fermat quartic $F_4 : x^4 + y^4 = 1$ in K, using the same strategy as Mordell (where, of course, Mordell works with a quadratic extension K of $L = \mathbb{Q}$). Let $t = (1 - x^2)/y^2$, so that $x^2 + ty^2 = 1$. This gives a parametrisation

$$x^2 = \frac{1-t^2}{1+t^2}, \quad y^2 = \frac{2t}{1+t^2}.$$

We point out that if $x, y \in K$ then $x^2, y^2 \in K$ and therefore so is t.

Suppose first that $t \in L$. Then $x^2, y^2 \in L$. In order for x and y to lie in the same quadratic extension K of L, either $x \in L$, $y \in L$ or $x/y \in L$. This means that one of

$$\frac{1-t^2}{1+t^2}, \quad \frac{2t}{1+t^2} \quad \text{or} \quad \frac{2t}{1-t^2}$$

is a square in L. Equivalently, $(1-t^2)(1+t^2)$, $2t(1+t^2)$ or $2t(1-t^2)$ is a square in L. These correspond to L-rational points of one of the curves

$$u^2 = (1-t^2)(1+t^2), \quad u^2 = 2t(1+t^2), \quad u^2 = 2t(1-t^2).$$

Both of the first two possibilities are isomorphic to $E_1 : y^2 = x^3 + 4x$ (the elliptic curve with Cremona label `32a1`) via the maps

$$(t, u) \mapsto \left(\frac{2t+2}{1-t}, \frac{u}{(1-t)^2}\right) \quad \text{and} \quad (t, u) \mapsto (2t, 2u),$$

respectively, and the third to $E_2 : y^2 = x^3 - 4x$ (the elliptic curve with Cremona label `64a1`) via the map $(t, u) \mapsto (-2t, 2u)$. We checked, using Magma, that E_1 and E_2 have rank 0 over L. We first consider E_1 and find

$$E_1(L) = E_1(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (2, \pm 4)\}.$$

We find that these points correspond on the first curve to $t = \pm 1$ and $t = 0$, and on the second to $t = 0$, $t = 1$ and $t = \infty$. These values of t correspond to

$$(x^2, y^2) = \{(1, 0), (-1, 0), (0, 1), (0, -1)\},$$

corresponding to points on F_4 defined over $\mathbb{Q}$ or $\mathbb{Q}(i)$. Similarly,

$$E_2(L) = \{\mathcal{O},\ (0,0),\ (\pm 2, 0)\} \cup \{(2+2\sqrt{2},\ \pm(4+4\sqrt{2}),\ (2-2\sqrt{2},\ \pm(4-4\sqrt{2})\},$$

and the rational points correspond to $t = \pm 1$ and $t = 0$, and the point at infinity to $t = \infty$, as before. The points in $E(L) \setminus E(\mathbb{Q})$ correspond to $t = -1 \pm \sqrt{2}$, and these give

$$(x^2, y^2) \in \left\{ \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right), \left(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}} \right) \right\},$$

corresponding to points on F_4 defined over $\mathbb{Q}(\sqrt[4]{2})$ or $\mathbb{Q}(\sqrt[4]{2}i)$.

We now suppose $t \in K,\ t \notin L$. We write $F(t) = t^2 + \beta t + \gamma$ for the minimal polynomial of t over L, so $\beta, \gamma \in L$. We let $A = (1+t^2)xy$ and $B = (1+t^2)y$, so that

$$A^2 = 2t(1-t^2), \quad B^2 = 2t(1+t^2).$$

Since $A^2, B^2 \in K$ and $K = L(t)$, we can write

$$A = \lambda + \mu t, \quad B = \lambda' + \mu' t, \quad \lambda, \mu, \lambda', \mu' \in L.$$

Comparing the two expressions for A yields

$$(\lambda + \mu t)^2 = 2t(1-t^2).$$

In particular, the equation

$$(\lambda + \mu z)^2 - 2z(1-z^2) = 0$$

has a root $z = t$. As the equation is defined over L, we see the left-hand side is divisible by the minimal polynomial $F(z)$, and, as this is a cubic, we have

$$(\lambda + \mu z)^2 - 2z(1-z^2) = F(z)(\rho + \sigma z), \tag{M1}$$

a factorisation over L (so $\rho, \sigma \in L$). Then $z = -\rho/\sigma$ is a solution to the left-hand side of (M1) defined over L. In particular, we have a solution with $z \in L$ to

$$Y^2 = 2z(1-z^2) = -2z^3 + 2z,$$

where $Y = \lambda + \mu z \in L$. Thus we get an L-point on the elliptic curve $Y^2 = -2X^3 + 2X$, which is isomorphic to the elliptic curve E_2, and the points in $E_2(L)$ correspond to $z = \pm 1,\ z = 0$ and $z = -1 \pm \sqrt{2}$. In exactly the same way, looking at B^2, we will get a solution over L to

$$(\lambda' + \mu' z)^2 - 2z(1+z^2) = F(z)(\rho' + \sigma' z), \tag{M2}$$

and therefore a solution over L to $Y^2 = 2z(1+z^2)$, which is isomorphic to E_1. The points in $E_2(L)$ correspond to $z = 0$ and $z = 1$.

We will now consider all these cases, as in Mordell. We write (z_1, z_2) for the situation where (M1) is solved by z_1 and (M2) is solved by z_2. We remark that these calculations are quite involved, and we therefore omit some details.

Case 1. $(-1, 1)$ This is Mordell's case (VI). If $z_1 = -1$ is a root of the left-hand side of (M1) then $\lambda + \mu = 0$ and, since -1 must then be a root of the right-hand side of (M1), it follows that $\rho + \sigma = 0$. Similarly, if $z_1 = 1$ is a root of the left-hand side of (M2) then $\lambda' + \mu' = 2,\ \rho' + \sigma' = 0$. Equation (M1) is

$$\lambda^2(1+z) - 2z(1-z) = \rho F(z)$$

(after dividing by $1 - z$). We can rewrite the left-hand side of (M2) as $(2 - \mu' + \mu' z)^2 - 2z - 2z^3 = \rho'(1-z)F(z)$. Thus, after dividing by $1 - z$, we get

$$(\mathrm{M2}) : 2(z^2 + z + 2) - 4\mu' + \mu'^2(1-z) = \rho' F(z).$$

Both (M1) and (M2) have the same coefficient of z^2, so $\rho = \rho'$. Comparing constant terms and z terms:

$$\lambda^2 = (2 - \mu')^2, \quad \lambda^2 - 2 = 2 - \mu'^2,$$

so either $(\lambda, \mu') = (0, 2)$ or $(\lambda, \mu') = (\pm 2, 0)$. In the first case, (M1) becomes $-2z(1-z) = \rho \cdot F(z)$, but this contradicts the irreducibility of $F(z)$. In the second case,

$$(\mathrm{M1}) : \rho F(z) = 4(1+z) - 2z(1-z) = 2(z^2 + z + 2),$$

so $F(z) = z^2 + z + 2$. Thus, $t = \frac{1}{2}(-1 \pm \sqrt{-7})$ and $K = L(\sqrt{-7})$.

Case 2. $(-1, 0)$ This is Mordell's case (III). In order for $z = -1$ to be a root of the left-hand side of (M1), we need $(\lambda - \mu)^2 = 0$. So $\lambda - \mu = 0$. Similarly, for $z = 0$ to be a root of the left-hand side of (M2), we need $\lambda' = 0$. Then for the left-hand side of (M1) to have -1 as a root, the same will be true of the right-hand side, so $\rho - \sigma = 0$. Equation (M1) is then divisible by $(1 + z)$, and dividing through, we get

$$(\mathrm{M1}) : \lambda^2(1+z) - 2z(1-z) = \rho \cdot F(z).$$

We rewrite this as

$$(\mathrm{M1}) : 2z^2 + (\lambda^2 - 2)z + \lambda^2 = \rho \cdot F(z).$$

In order for $z = 0$ to be a root of the left-hand side of (M2), it must be that $\lambda' = 0$, and thus

$$(\mathrm{M2}) : -2z^2 + \mu'^2 z - 2 = \sigma' F(z).$$

The right-hand sides of (M1) and (M2) differ by a constant, and upon comparing the z^2 coefficients on the left-hand sides, we see that they differ by a factor of -1. Then comparing the constant term, we get $\lambda^2 = 2$. Thus $\lambda = \mu = \pm\sqrt{2}$. The coefficient of z in the first equation is $\lambda^2 - 2$, and the coefficient of z in the second is μ'^2, so $\mu' = 0$. Then $Y = \lambda' + \mu' t = 0$. But $Y^2 = 2t(1+t^2)$, so this means that $t = 0$, contradicting $t \notin L$, or $(1 + t^2)$ in which case $t = i$ and $K = L(i)$.

For the remaining pairs (z_1, z_2), in each case, after performing a similar analysis, we reach a contradiction to the fact $\lambda, \mu, \lambda', \mu' \in L$, and thus no solutions are found in these cases. □

This completes the proof of Theorem 1.1.

7. More general real biquadratic fields

We give examples of obstacles that arise in generalising the proof of Theorem 1.1 to more general real biquadratic fields. As in the proof of Theorem 1.1, we apply level lowering (Theorem 2.1) to the Frey curve (2) for $p \geq 17$ and $E_{13,\epsilon}$ for $p = 13$.

7.1. $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. In order to apply level lowering (Theorem 2.1), one needs to demonstrate the modularity of the Frey curve over K. It has not yet been proven that elliptic curves over totally real quartic fields containing $\sqrt{5}$ are modular; see [Box 2022, Section 7.1] for a discussion concerning this problem. We remark however that establishing the modularity of the Frey curve over this particular field K may be possible through the use of [Freitas et al. 2015, Theorem 7].

7.2. $K = \mathbb{Q}(\sqrt{2}, \sqrt{7})$. Write $\mathcal{O}_K$ for the ring of integers of K. A straightforward computation in Magma returns that K has class number 1 and $2\mathcal{O}_K = \mathfrak{P}^4$. A straightforward generalisation of Lemmas 3.1, 3.2 and 3.3 returns that the lowered level is $\mathfrak{P}^t$, where $t = 1, 5, 8$ or 16. In particular, the dimension of Hilbert newforms of parallel weight 2 and level $\mathfrak{P}^{16}$ is 40960, making the elimination step currently computationally infeasible in this case.

7.3. $K = \mathbb{Q}(\sqrt{2}, \sqrt{11})$. Write $\mathcal{O}_K$ for the ring of integers of K. A straightforward computation in Magma returns that K has class number 1 and $2\mathcal{O}_K = \mathfrak{P}^4$. By a direct generalisation of the techniques outlined in Section 4, it is straightforward to see that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$.

A straightforward generalisation of Lemmas 3.1, 3.2 and 3.3 returns that the lowered level is $\mathfrak{P}^t$, where $t = 1, 4$ or 5. As is true for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, there are no Hilbert newforms of parallel weight 2 and level $\mathfrak{P}$ over K. There are 44 Hilbert newforms of parallel weight 2 and level $\mathfrak{P}^4$ and 76 Hilbert newforms of parallel weight 2 and level $\mathfrak{P}^5$ over K. In order to get a contradiction, we make use of the standard method of eliminating newforms given by the following lemma.

Lemma 7.1 [Freitas and Siksek 2015b, Lemma 7.1]. *Let K be a totally real field, and let $p \geq 5$ be a prime. Let E be an elliptic curve over K of conductor $\mathcal{N}$, and let $\mathfrak{f}$ be a newform of parallel weight 2 and level $\mathcal{N}_p$. Let t be a positive integer satisfying $t \mid \#E(K)_{\text{tors}}$. Let $\mathfrak{q} \nmid t\mathcal{N}_p$ be a prime ideal of $\mathcal{O}_K$, and let*

$$\mathcal{A}_{\mathfrak{q}} = \{a \in \mathbb{Z} : |a| \leq 2\sqrt{\text{Norm}(\mathfrak{q})},\ \text{Norm}(\mathfrak{q}) + 1 - a \equiv 0 \pmod{t}\}.$$

If $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\varpi}$ then ϖ divides the principal ideal

$$B_{\mathfrak{f},\mathfrak{q}} = \text{Norm}(\mathfrak{q})((\text{Norm}(\mathfrak{q}) + 1)^2 - a_{\mathfrak{q}}(\mathfrak{f})^2) \prod_{a \in \mathcal{A}_{\mathfrak{q}}} (a - a_{\mathfrak{q}}(\mathfrak{f})) \cdot \mathcal{O}_{\mathbb{Q}_{\mathfrak{f}}}.$$

We briefly explain how to apply Lemma 7.1. Namely let

$$B_{\mathfrak{f}} = \sum_{\mathfrak{q} \in T} B_{\mathfrak{f},\mathfrak{q}},$$

where T is a small set of primes $\mathfrak{q} \nmid t\mathcal{N}_p$. Let $C_{\mathfrak{f}} = \text{Norm}_{\mathbb{Q}_{\mathfrak{f}}/\mathbb{Q}}(B_{\mathfrak{f}})$. Then Lemma 7.1 asserts that $p \mid C_{\mathfrak{f}}$. We wrote a short program to implement Lemma 7.1 in Magma with $\mathcal{N}_p = \mathfrak{P}^4$ or $\mathfrak{P}^5$, with $t = 4$ and T

equal to the set of prime ideals $\mathfrak{q} \neq \mathfrak{P}$ of K with norm less than 90. From this implementation, we found that if $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\varpi}$, where E is our Frey curve and $\mathfrak{f}$ is a newform of level $\mathcal{N}_p$, then $p = 2$ or 3.

We remark that the proofs of Theorems 6.1 and 6.3 do not readily generalise to K. In combination with the remarks made in Section 2, this leads to the following result.

Theorem 7.2. *Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{11})$. There are no nontrivial solutions to* (1) *over K for all primes $n \geq 5$.*

Acknowledgements

We would like to thank Samir Siksek for several useful and enlightening discussions, particularly with regard to the contents of Section 4 and the proof of Theorem 6.1. We would also like to thank Philippe Michaud-Jacobs, Jeremy Rouse and Michael Stoll for helpful correspondence, and Pedro José Cazorla Garcia for a careful reading of an earlier version of this paper. We would like to thank the authors, Yasuhiro Ishitsuka, Tetsushi Ito and Tatsuya Ohshita, of [Ishitsuka et al. 2020] for making us aware of their work determining all points on the Fermat quartic lying in a quadratic extension of $\mathbb{Q}(\zeta_8)$. We would like to thank the referees for their careful reading of the paper as well as the invaluable comments and suggestions they provided. Khawaja thanks the University of Sheffield for their financial support via a doctoral training partnership scholarship (ESPRC grant no EP/T517835/1).

References

[Aigner 1934] A. Aigner, "Über die Möglichkeit von $x^4 + y^4 = z^4$ in quadratischen Körpern", *Jahresber. Dtsch. Math.-Ver.* **43** (1934), 226–229. Zbl

[Arbarello et al. 1985] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves, I*, Grundl. Math. Wissen. **267**, Springer, 1985. MR Zbl

[Box 2022] J. Box, "Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular", *Trans. Amer. Math. Soc.* **375**:5 (2022), 3129–3172. MR Zbl

[Bruin 2003] N. Bruin, "Chabauty methods using elliptic curves", *J. Reine Angew. Math.* **562** (2003), 27–49. MR Zbl

[Bruin and Najman 2015] P. Bruin and F. Najman, "Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields", *LMS J. Comput. Math.* **18**:1 (2015), 578–602. MR Zbl

[Bruin and Stoll 2009] N. Bruin and M. Stoll, "Two-cover descent on hyperelliptic curves", *Math. Comp.* **78**:268 (2009), 2347–2370. MR Zbl

[David 2011] A. David, "Caractère d'isogénie et critères d'irréductibilité", preprint, 2011. arXiv 1103.3892

[Derickx et al. 2020] M. Derickx, F. Najman, and S. Siksek, "Elliptic curves over totally real cubic fields are modular", *Algebra Number Theory* **14**:7 (2020), 1791–1800. MR Zbl

[Derickx et al. 2023] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, "Torsion points on elliptic curves over number fields of small degree", *Algebra Number Theory* **17**:2 (2023), 267–308. MR Zbl

[Faddeev 1960] D. K. Faddeev, "Group of divisor classes on the curve defined by the equation $x^4 + y^4 = 1$", *Soviet Math. Dokl.* **1** (1960), 1149–1151. Zbl

[Freitas and Siksek 2015a] N. Freitas and S. Siksek, "The asymptotic Fermat's last theorem for five-sixths of real quadratic fields", *Compos. Math.* **151**:8 (2015), 1395–1415. MR Zbl

[Freitas and Siksek 2015b] N. Freitas and S. Siksek, "Fermat's last theorem over some small real quadratic fields", *Algebra Number Theory* **9**:4 (2015), 875–895. MR Zbl

[Freitas et al. 2015] N. Freitas, B. V. Le Hung, and S. Siksek, "Elliptic curves over real quadratic fields are modular", *Invent. Math.* **201**:1 (2015), 159–206. MR Zbl

[Freitas et al. 2020] N. Freitas, A. Kraus, and S. Siksek, “Class field theory, Diophantine analysis and the asymptotic Fermat’s last theorem”, *Adv. Math.* **363** (2020), art. id. 106964. MR Zbl

[Fujiwara 2006] K. Fujiwara, “Level optimization in the totally real case”, preprint, 2006. arXiv math/0602586

[Gross and Rohrlich 1978] B. H. Gross and D. E. Rohrlich, “Some results on the Mordell–Weil group of the Jacobian of the Fermat curve”, *Invent. Math.* **44**:3 (1978), 201–224. MR Zbl

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math. **52**, Springer, 1977. MR Zbl

[Ishitsuka et al. 2020] Y. Ishitsuka, T. Ito, and T. Ohshita, “Explicit calculation of the mod 4 Galois representation associated with the Fermat quartic”, *Int. J. Number Theory* **16**:4 (2020), 881–905. MR Zbl

[Jarvis 1999a] F. Jarvis, “Level lowering for modular mod l representations over totally real fields”, *Math. Ann.* **313**:1 (1999), 141–160. MR Zbl

[Jarvis 1999b] F. Jarvis, “Mazur’s principle for totally real fields of odd degree”, *Compos. Math.* **116**:1 (1999), 39–79. MR Zbl

[Jarvis and Meekin 2004] F. Jarvis and P. Meekin, “The Fermat equation over $\mathbb{Q}(\sqrt{2})$”, *J. Number Theory* **109**:1 (2004), 182–196. MR Zbl

[Katz 1981] N. M. Katz, “Galois properties of torsion points on abelian varieties”, *Invent. Math.* **62**:3 (1981), 481–502. MR Zbl

[Klassen and Tzermias 1997] M. Klassen and P. Tzermias, “Algebraic points of low degree on the Fermat quintic”, *Acta Arith.* **82**:4 (1997), 393–401. MR Zbl

[Kraus 1990] A. Kraus, “Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive”, *Manuscripta Math.* **69**:4 (1990), 353–385. MR Zbl

[Kraus 1996] A. Kraus, “Courbes elliptiques semi-stables et corps quadratiques”, *J. Number Theory* **60**:2 (1996), 245–253. MR Zbl

[Kraus 2018] A. Kraus, “Quartic points on the Fermat quintic”, *Ann. Math. Blaise Pascal* **25**:1 (2018), 199–205. MR Zbl

[Kraus 2019] A. Kraus, “Le théorème de Fermat sur certains corps de nombres totalement réels”, *Algebra Number Theory* **13**:2 (2019), 301–332. MR Zbl

[Michaud-Jacobs 2022] P. Michaud-Jacobs, “Fermat’s last theorem and modular curves over real quadratic fields”, *Acta Arith.* **203**:4 (2022), 319–351. MR Zbl

[Mordell 1968] L. J. Mordell, “The Diophantine equation $x^4 + y^4 = 1$ in algebraic number fields”, *Acta Arith.* **14** (1968), 347–355. MR Zbl

[Ozman and Siksek 2019] E. Ozman and S. Siksek, “Quadratic points on modular curves”, *Math. Comp.* **88**:319 (2019), 2461–2484. MR Zbl

[Rajaei 2001] A. Rajaei, “On the levels of mod l Hilbert modular forms”, *J. Reine Angew. Math.* **537** (2001), 33–65. MR Zbl

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. **151**, Springer, 1994. MR Zbl

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math. **106**, Springer, 2009. MR Zbl

[Tzermias 1998] P. Tzermias, “Algebraic points of low degree on the Fermat curve of degree seven”, *Manuscripta Math.* **97**:4 (1998), 483–488. MR Zbl

[Wiles 1995] A. Wiles, “Modular elliptic curves and Fermat’s last theorem”, *Ann. of Math.* (2) **141**:3 (1995), 443–551. MR Zbl

Communicated by Bjorn Poonen
Received 2022-12-26 Revised 2024-03-14 Accepted 2024-04-29

maleehakhawaja@hotmail.com *School of Mathematics and Statistics, University of Sheffield, Sheffield, United Kingdom*

a.f.jarvis@sheffield.ac.uk *School of Mathematics and Statistics, University of Sheffield, Sheffield, United Kingdom*

ALGEBRA AND NUMBER THEORY 19:3 (2025)
https://doi.org/10.2140/ant.2025.19.481

Moments in the Chebotarev density theorem: general class functions

Régis de la Bretèche, Daniel Fiorilli and Florent Jouve

À la mémoire de Joël Bellaïche

We find lower bounds on higher moments of the error term in the Chebotarev density theorem. Inspired by the work of Bellaïche, we consider general class functions and prove bounds which depend on norms associated to these functions. Our bounds also involve the ramification and Galois theoretical information of the underlying extension L/K. Under a natural condition on class functions (which appeared in earlier work), we obtain that those moments are at least Gaussian. The key tools in our approach are the application of positivity in the explicit formula followed by combinatorics on zeros of Artin L-functions (which generalize previous work), as well as precise bounds on Artin conductors.

1. Introduction

The study of the error term in the Chebotarev density theorem has a long history and is critical in many applications. If L/K is a Galois extension of number fields, $G = \mathrm{Gal}(L/K)$ and $C \subset G$ is a conjugacy class, then this theorem states that as $x \to \infty$

$$\pi_C(x; L/K) := \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ \mathcal{N}\mathfrak{p} \leq x \\ \varphi_{\mathfrak{p}} = C}} 1 \sim \frac{|C|}{|G|} \mathrm{Li}(x),$$

where $\mathrm{Li}(x) := \int_2^x \mathrm{d}u/\log u$, and the sum extends to maximal ideals $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of K with associated Frobenius (resp. norm) denoted $\varphi_{\mathfrak{p}}$ (resp. $\mathcal{N}\mathfrak{p}$); see, e.g., [Martinet 1977, Section 4] for the general definition of the Frobenius substitution. Equivalently, if $t \colon G \to \mathbb{R}$ is a real-valued class function, then

$$\pi(x; L/K, t) := \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ \mathcal{N}\mathfrak{p} \leq x}} t(\varphi_{\mathfrak{p}}) \sim \hat{t}(1) \,\mathrm{Li}(x),$$

where $\hat{t}(1) = (1/|G|) \sum_{g \in G} t(g)$. Note that if $\mathbf{1}_C$ denotes the indicator function of a given conjugacy class C of G, then $\pi(x; L/K, \mathbf{1}_C) = \pi_C(x; L/K)$. As for the error term, which was first bounded effectively by Lagarias and Odlyzko [1977], Bellaïche [2016] has shown under GRH and Artin's conjecture

MSC2020: primary 11R42, 11R44, 11R45; secondary 11N64.
Keywords: Chebotarev density theorem, distribution of primes, moments computation.

(denoted by AC throughout the paper; see Section 4 for recollections on Artin L-functions), that in the case $K=\mathbb{Q}$ and for $x\geq 3$,

$$\pi(x;L/K,t)-\hat{t}(1)\operatorname{Li}(x)\ll\lambda_{1,1}(t)\sqrt{x}\log(xM|G|),$$

where M is the product of all primes ramified in L and $\lambda_{1,1}(t):=\sum_{\chi\in\operatorname{Irr}(G)}\chi(1)|\hat{t}(\chi)|$, with $\operatorname{Irr}(G)$ being the set of irreducible characters of G and

$$\hat{t}(\chi):=\langle t,\chi\rangle_G=\frac{1}{|G|}\sum_{g\in G}\overline{\chi(g)}t(g).$$

As an example, if $t=\mathbf{1}_C$ for some conjugacy class $C\subset G$, then $\hat{t}(\chi)=(|C|/|G|)\overline{\chi(C)}$.

Bellaïche's bound has been generalized and improved in the recent work [Fiorilli and Jouve 2024]. Moreover, [loc. cit.] studies the generic behavior of the error term, in particular its limiting distribution as $x\to\infty$. Using probabilistic tools, a sufficient condition is obtained for this error term to be Gaussian [loc. cit., Proposition 5.8]. This generalizes previous work on primes in arithmetic progressions [Hooley 1977; Rubinstein and Sarnak 1994; Fiorilli and Martin 2013]. For example, Hooley has shown that for $(a,q)=1$, the error term

$$E(x;q,a):=\sum_{\substack{n\leq x\\ n\equiv a \bmod q}}\Lambda(n)-\frac{1}{\phi(q)}\sum_{n\leq x}\Lambda(n)$$

is such that for any fixed $r\in\mathbb{N}$,

$$\lim_{q\to\infty}\lim_{X\to\infty}\frac{\phi(q)^{r/2}}{(\log q)^{r/2}}\frac{1}{\log X}\int_2^X\frac{(E(x;q,a))^r}{x^{r/2}}\frac{\mathrm{d}x}{x}=\mu_r,$$

where

$$\mu_r:=\begin{cases}(2n-1)\cdot(2n-3)\cdots 1 & \text{if } r=2n,\\ 0 & \text{otherwise}\end{cases}$$

is the r-th moment of the Gaussian. Hooley's theorem is conditional on GRH, as well as the assumption that the multiset of nonnegative nontrivial zeros of Dirichlet L-functions modulo q is linearly independent over the rationals.

The results which we just described (including a number of results in [Fiorilli and Jouve 2024]) apply to limiting distributions as $x\to\infty$, and thus do not give information on the behavior of the error term uniformly when q varies with x. In fact, to obtain such explicit information one would need to significantly strengthen the linear independence hypothesis, that is one would need to assume that integer linear combinations of L-function zeros are bounded away from zero as a function of q (in the spirit of [Montgomery and Vaughan 2007, Section 15.3]).

In [de la Bretèche and Fiorilli 2023], a lower bound is established on higher moments of primes in progressions in a certain range of q in terms of x, assuming only GRH. More precisely, the results of [loc. cit.] manage to circumvent the linear independence assumption by considering a weighted version of $E(x;q,1)$ and applying positivity in the explicit formula.

The goal of the present paper is to generalize these results in the context of the Chebotarev density theorem, that is to obtain lower bounds on moments of a weighted version of the error term $\pi(x; L/K, t) - \hat{t}(1)\,\mathrm{Li}(x)$ in certain ranges of x depending on the class function t and on invariants of the extension L/K such as the size of its Galois group and of the root discriminant of L. We stress that our results do not assume any form of linear independence of the L-function zeros involved.

Before we state our results, we need a few definitions. We let $\delta > 0$ and $\mathcal{S}_\delta \subset \mathcal{L}^1(\mathbb{R})$ be the set of all nontrivial differentiable even $\eta : \mathbb{R} \to \mathbb{R}$ such that, for all $t \in \mathbb{R}$,

$$\eta(t), \eta'(t) \ll \mathrm{e}^{-(1/2+\delta)|t|},$$

and moreover for all $\xi \in \mathbb{R}$, we have that[1]

$$0 \le \hat{\eta}(\xi) \ll (|\xi|+1)^{-1}(\log(|\xi|+2))^{-2-\delta}. \tag{1}$$

Here, the Fourier transform is defined by

$$\hat{\eta}(\xi) := \int_{\mathbb{R}} \mathrm{e}^{-2\pi i \xi u} \eta(u)\,\mathrm{d}u.$$

Finally for any $h \in \mathcal{L}^1(\mathbb{R})$ we define

$$\alpha(h) := \int_{\mathbb{R}} h(t)\,\mathrm{d}t.$$

In this notation, one of the goals of the paper [de la Bretèche and Fiorilli 2023] is to give lower bounds on moments of the error term

$$\sum_{\substack{n \ge 1 \\ n \equiv 1 \bmod q}} \frac{\Lambda(n)}{n^{1/2}} \eta(\log(n/x)) - \frac{1}{\phi(q)} \sum_{\substack{n \ge 1 \\ (n,q)=1}} \frac{\Lambda(n)}{n^{1/2}} \eta(\log(n/x)), \tag{2}$$

which is a weighted version of $\psi(x; q, 1) - (1/\phi(q))\psi(x, \chi_{0,q})$ where $\chi_{0,q}$ is the principal character modulo q.

In this paper we consider L/K a Galois extension of number fields of group $G = \mathrm{Gal}(L/K)$ and we fix a real-valued class function $t \colon G \to \mathbb{R}$.[2] Our goal will be to understand the moments of

$$\psi_\eta(x; L/K, t) := \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ m \ge 1}} t(\varphi_{\mathfrak{p}}^m) \frac{\log(\mathcal{N}\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{m/2}} \eta(\log(\mathcal{N}\mathfrak{p}^m/x)), \tag{3}$$

which is a direct generalization of (2) (where, disregarding ramified primes, $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_q)$ and $t = \mathbf{1}_{1 \bmod q} - 1/\phi(q)$). First, we notice that with this smooth weight, the Chebotarev density theorem

[1] The upper bound on $\hat{\eta}(\xi)$ is a quite mild condition given the differentiability of η; going through the proof of the Riemann–Lebesgue lemma we see for instance that a stronger bound holds as soon as η' is monotonous. (A stronger bound holds if η is twice differentiable.) As for the positivity condition, we can take for example $\eta = \eta_1 \star \eta_1$ for some smooth and rapidly decaying η_1.

[2] We will require later the condition $\hat{t} \ge 0$. In particular, the results of our paper also apply to class functions of the form $\mathrm{Re}(t)$, where $t \colon G \to \mathbb{C}$ is a class function of nonnegative real part such that $\hat{t} \ge 0$.

reads

$$\psi_\eta(x; L/K, t) \sim \hat{t}(1) x^{1/2} \mathcal{L}_\eta\big(\tfrac{1}{2}\big),$$

where

$$\mathcal{L}_\eta(u) := \int_{\mathbb{R}} \mathrm{e}^{ux} \eta(x) \mathrm{d}x$$

(note that $\mathcal{L}_\eta(u) = \mathcal{L}_\eta(-u)$). Secondly, it follows from an analysis as in [Fiorilli and Jouve 2024] (see, e.g., [loc. cit., Theorem 2.1]) that under GRH, the remainder term $\psi_\eta(x; L/K, t) - \hat{t}(1) x^{1/2} \mathcal{L}_\eta\big(\tfrac{1}{2}\big)$ has average value equal to $\hat{\eta}(0) z(L/K, t)$, where we define

$$z(L/K, t) := \sum_{\chi \in \mathrm{Irr}(G)} \hat{t}(\chi) \operatorname{ord}_{s=1/2} L(s, L/K, \chi).$$

With this in mind, we define $\mathcal{U}$ to be the set of even nontrivial integrable functions $\Phi\colon \mathbb{R} \to \mathbb{R}$ such that $\Phi, \widehat{\Phi} \geq 0$,[3] and we consider for $U > 0$, $\Phi \in \mathcal{U}$, $n \in \mathbb{Z}_{\geq 1}$, and $\eta \in \mathcal{S}_\delta$ the central moment

$$\widetilde{M}_n(U, L/K; t, \eta, \Phi) := \frac{1}{U \int_0^\infty \Phi} \int_0^\infty \Phi\Big(\frac{u}{U}\Big) \Big(\psi_\eta(\mathrm{e}^u; L/K, t) - \hat{t}(1) \mathrm{e}^{u/2} \mathcal{L}_\eta\Big(\frac{1}{2}\Big) - \hat{\eta}(0) z(L/K, t)\Big)^n \mathrm{d}u. \tag{4}$$

We will see that under GRH and AC, this integral converges.

Our main result is a lower bound on the even moments $\widetilde{M}_{2m}(U; L/K; t, \eta, \Phi)$, which is conditional on GRH as well as AC. More precisely, if AC holds for a Galois extension L/F where K/F is a subextension, then we obtain a bound which depends on F. For simplicity one can assume that $F = \mathbb{Q}$; in general, we expect to obtain the best possible (and in many families asymptotically optimal) bound with this choice. Our bounds will depend on the root discriminant

$$\mathrm{rd}_L := d_L^{1/[L:\mathbb{Q}]}, \tag{5}$$

where d_L is the absolute value of the discriminant of $L/\mathbb{Q}$. Our estimates will also involve various norms relative to the Galois groups G and G^+ of the extensions L/K and L/F respectively. For a finite group $\mathcal{G}$ and for a class function $t\colon \mathcal{G} \to \mathbb{C}$, these norms are defined as follows:

$$\lambda_{j,k}(t) := \sum_{\chi \in \mathrm{Irr}(\mathcal{G})} \chi(1)^j |\hat{t}(\chi)|^k \quad (j, k \geq 0). \tag{6}$$

Our main results (Theorems 1.1 and 1.4) show that the moments $\widetilde{M}_{2m}(U, L/K; t, \eta, \Phi)$ are asymptotically greater than or equal those of a Gaussian of expected variance. The implied variance will be expressed in terms of zeros of Artin L-functions of a Galois number field extension L/F. More precisely, denoting $t^+ := \mathrm{Ind}_G^{G^+} t$, this variance takes the shape

$$\nu(L/F, t^+; \eta) := \sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^2 b_0(\chi; \hat{\eta}^2), \tag{7}$$

[3] Note that those conditions imply that $\widehat{\Phi}(0) > 0$.

and where $\chi \in \mathrm{Irr}(\mathrm{Gal}(L/F))$,

$$b_0(\chi;\hat{\eta}^2) := \sum_{\rho_\chi \notin \mathbb{R}} \left| \hat{\eta}\left(\frac{\rho_\chi - \frac{1}{2}}{2\pi i}\right)\right|^2, \tag{8}$$

where ρ_χ is running over the nontrivial zeros of $L(s, L/F, \chi)$.

Theorem 1.1. *Let $L/K/F$ be a tower of number fields such that $L \neq \mathbb{Q}$, L/F is Galois, and assume GRH and AC for the extension L/F.[4] Define $G := \mathrm{Gal}(L/K)$, $G^+ := \mathrm{Gal}(L/F)$, let $\eta \in \mathcal{S}_\delta$, $\Phi \in \mathcal{U}$, and assume that $t\colon G \to \mathbb{R}$ is a nonzero class function such that $t^+ := \mathrm{Ind}_G^{G^+} t$, the class function on G^+ induced by t, satisfies $\widehat{t^+} \in \mathbb{R}_{\geq 0}$.[5] For $m \in \mathbb{N}$, we have the lower bound*

$$\begin{aligned}&\widetilde{M}_{2m}(U, L/K; t, \eta, \Phi)\\ &\quad \geq \mu_{2m}\nu(L/F, t^+;\eta)^m(1 + O_\eta(m^2 m!\, w_4(L/F, t^+;\eta))) + O\left(\frac{(\kappa_\eta[F:\mathbb{Q}]\lambda_{1,1}(t^+)\log(\mathrm{rd}_L))^{2m}}{U}\right),\end{aligned} \tag{9}$$

where $\kappa_\eta > 0$ is a constant which depends only on η and

$$w_4(L/F, t^+;\eta) := \frac{\sum_{\chi\in\mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^4 b_0(\chi;\hat{\eta}^2)}{\left(\sum_{\chi\in\mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^2 b_0(\chi;\hat{\eta}^2)\right)^2}. \tag{10}$$

In other words, the moments $\widetilde{M}_{2m}(U, L/K; t, \eta, \Phi)$ are at least Gaussian of variance $\nu(L/F, t^+;\eta)$. Our next main result is an estimation of this variance as well as an upper bound on the error term $w_4(L/F, t^+;\eta)$.

Remark 1.2. A version of the quantity $w_4(L/F, t^+;\eta)$ has already appeared in the probabilistic study of the error term in Chebotarev [Fiorilli and Jouve 2024, Section 5.2]. In particular, the condition $w_4(L/F, t^+;\eta) = o(1)$ was necessary in order to obtain the central limit theorem [loc. cit., Proposition 5.8]. However, there exists class functions for which this condition does not hold: taking for instance $t = 1$, we obtain a weighted version of the error term in the prime number theorem which under standard hypotheses is not Gaussian; this goes back to Wintner [1941]. Another instance of non-Gaussian moments is explored in [de la Bretèche et al. 2023].

In order to state our bounds on the variance $\nu(L/F, t^+;\eta)$, we define the following quantity attached to a nontrivial class function $t\colon G \to \mathbb{R}$:[6]

$$S_t := \max_{1\neq a\in G} \frac{\left|\sum_{\chi\in\mathrm{Irr}(G)} \chi(a)|\hat{t}(\chi)|^2\right|}{\sum_{\chi\in\mathrm{Irr}(G)} \chi(1)|\hat{t}(\chi)|^2} = \max_{1\neq a\in G} \frac{\left|\sum_{\chi\in\mathrm{Irr}(G)} \chi(a)|\hat{t}(\chi)|^2\right|}{\lambda_{1,2}(t)} \leq 1. \tag{11}$$

Remark 1.3. The quantity S_t is, in a sense, a measure of the size of the support of $\hat{t}$. For many groups, we expect S_t to be much smaller than 1 as soon as $\hat{t}$ has a "large" support in $\mathrm{Irr}(G)$ (see the example following Theorem 1.4 as well as Section 2).

[4] Note that AC for the extension L/F implies AC for the extension L/K.

[5] See the beginning of Section 4 for recollections on induction. Notice that the condition $\hat{t}^+ \geq 0$ is weaker than $\hat{t} \geq 0$. Indeed, by Frobenius reciprocity, we have that $\widehat{t^+}(\chi) = \hat{t}(\chi|_G)$, and moreover the character $\chi|_G$ is a sum of irreducible characters of G.

[6] Note that if $G = \{1\}$, then we define $S_t := 0$.

Here and throughout we denote by $\log_k$ the k-fold iterated logarithm.

Theorem 1.4. *With the same notations and assumptions as in Theorem 1.1, we have the following*:

- *Assume that the weight function η is such that* $\inf\{|z-z'| : z \neq z', \hat{\eta}(z) = \hat{\eta}(z') = 0\} > 0$.[7] *Then, we have the bounds*

$$\nu(L/F, t^+; \eta) \asymp_\eta \sum_{\chi \in \mathrm{Irr}(G^+)} |\widehat{t^+}(\chi)|^2 \log(A(\chi)+2),$$

$$w_4(L/F, t^+, \eta) \ll_\eta \frac{\sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^4 \log(A(\chi)+2)}{\left(\sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^2 \log(A(\chi)+2)\right)^2}.$$

Here, $A(\chi)$ is the Artin conductor which is defined in (18).

- *Assume that $S_{t^+} \leq 1 - \kappa_\eta (\log_2(\mathrm{rd}_L + 2))^{-1}$ where $\kappa_\eta > 0$ is a large enough constant which depends only on η. Then we have the more explicit bounds*

$$\begin{aligned} 1 - S_{t^+} - O_\eta\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right) &\leq \frac{\nu(L/F, t^+; \eta)}{\alpha(|\hat{\eta}|^2)[F:\mathbb{Q}] \log(\mathrm{rd}_L) \lambda_{1,2}(t^+)} \\ &\leq 1 + S_{t^+} + O_\eta\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right), \end{aligned} \tag{12}$$

as well as[8]

$$w_4(L/F, t^+; \eta)[F:\mathbb{Q}] \log(\mathrm{rd}_L) \ll_\eta \frac{\lambda_{1,4}(t^+)}{\lambda_{1,2}(t^+)^2} \left(1 - S_{t^+} - O_\eta\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right)\right)^{-2} \ll_\eta (\log_2 \mathrm{rd}_L)^2.$$

Remark 1.5. To see why the assumptions made in Theorem 1.4 are important, consider the case where $K = \mathbb{Q}$ and $t = t^+ = 1$, in which $S_{t^+} = 1$. Then we have that

$$\psi_\eta(x; L/K, t) - x^{1/2} \mathcal{L}_\eta\left(\tfrac{1}{2}\right) = \sum_{\substack{p \\ m \geq 1}} \frac{\log p}{p^{m/2}} \eta(\log(p^m/x)) - x^{1/2} \mathcal{L}_\eta\left(\tfrac{1}{2}\right),$$

and the moments of the limiting distribution of this function are much smaller than those of a Gaussian (in fact the limiting distribution has compact and uniformly bounded support, which does not depend on the extension L/K). This does not contradict Theorem 1.1, since in this case $w_4(L/F, t^+, \eta) \gg 1$ (hence we cannot extract any information from (9)).

Remark 1.6. The norms $\lambda_{j,k}(t) := \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^j |\hat{t}(\chi)|^k$ play a fundamental role in the analysis of the error term in the Chebotarev density theorem. Bellaïche [2016] coined the term "Littlewood norm" for $\lambda_{1,1}(t)$, which he thoroughly studied with applications to the sup norm of the error term in Chebotarev. The norm $\lambda_{1,2}(t)$ and its applications to the mean square of the error term in Chebotarev were studied in [Fiorilli and Jouve 2024].

[7] More generally, it is sufficient to assume that there exists an interval $[T_1, T_2]$ where $T_1 > \kappa$ and $T_2 - T_1 \geq \kappa(\log_2(T_1))^{-1}$ on which $\hat{\eta}$ does not vanish, where $\kappa > 0$ is a large enough absolute constant.

[8] Note that the second bound here shows that $w_4(L/F, t^+; \eta)$ is small as soon as the root discriminant is large. However, this bound is far from optimal, and we expect the quotient $\lambda_{1,4}(t^+)/\lambda_{1,2}(t^+)^2$ to also be small in many cases.

Remark 1.7. One can generalize the bound (12). If $\Xi \subset \mathrm{Irr}(G^+)$ is a set of irreducible characters, then one can drop the terms where $\chi \notin \Xi$ in the definition (7) of $\nu(L/F, t^+; \eta)$. Doing so, and assuming that

$$S_{t^+}(\Xi) := \max_{1\neq a\in G} \frac{\left|\sum_{\chi\in\Xi}\chi(a)|\hat{t}(\chi)|^2\right|}{\sum_{\chi\in\Xi}\chi(1)|\hat{t}(\chi)|^2} \le 1-\kappa_\eta(\log_2(\mathrm{rd}_L+2))^{-1},$$

where $\kappa_\eta > 0$ is a large enough constant which depends only on η, we deduce the bound

$$\frac{\nu(L/F, t^+; \eta)}{\alpha(|\hat{\eta}|^2)[F:\mathbb{Q}]\log(\mathrm{rd}_L)\lambda_{1,2}(t^+; \Xi)} \ge 1 - S_{t^+}(\Xi) - O_\eta\bigg(\frac{1}{\log_2(\mathrm{rd}_L+2)}\bigg),$$

where $\lambda_{1,2}(t^+; \Xi) := \sum_{\chi\in\Xi}\chi(1)|\hat{t}(\chi)|^2$. This generalized bound will be useful in the case $G^+ = S_n$ (see Section 2.5).

The following example illustrates the relevance of introducing the quantities S_t and S_{t^+} in the statement of Theorem 1.4.

Example. Fix an abelian extension L/K of number fields and let $G = \mathrm{Gal}(L/K)$. Let t be real-valued with nonnegative Fourier coefficients of constant modulus (e.g., $t = \mathbf{1}_g$, for any $g \in G$), then, since by orthogonality $\sum_{\chi\in\mathrm{Irr}(G)}\chi(a) = 0$ for every $a \in G\setminus\{1\}$, we have $S_t = 0$. In particular (12) combined with (9) generalizes the situation considered in [de la Bretèche and Fiorilli 2021, page 7] where $t = \mathbf{1}_{1 \bmod q}$ and $G \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ is the Galois group of the cyclotomic extension $\mathbb{Q}(\zeta_q)/\mathbb{Q}$. For further examples, including nonabelian extensions, see Section 2.

Remark 1.8. In Theorem 1.1, one might wonder whether it is possible to bound the more familiar moments

$$M_n(U, L/K; t, \eta, \Phi) := \frac{1}{U\int_0^\infty \Phi}\int_0^\infty \Phi\big(\tfrac{u}{U}\big)\big(\psi_\eta(\mathrm{e}^u; L/K, t) - \hat{t}(1)\mathrm{e}^{u/2}\mathcal{L}_\eta\big(\tfrac{1}{2}\big)\big)^n\,\mathrm{d}u,$$

rather than $\widetilde{M}_n(U, L/K; t, \eta, \Phi)$. This is indeed the case since in Theorem 1.1,

$$m_{L/K;t,\eta} := \hat{\eta}(0)z(L/K, t) = \hat{\eta}(0)z(L/F, t^+)$$

(this follows from [Fiorilli and Jouve 2024, Lemma 3.15]), which by our assumptions is nonnegative. Then, we have that

$$M_{2m}(U, L/K; t, \eta, \Phi) = \sum_{j=0}^{2m}\binom{2m}{j}\widetilde{M}_j(U; L/K, t)m_{L/K;t,\eta}^{2m-j} \ge \widetilde{M}_{2m}(U, L/K; t, \eta, \Phi).$$

Of course, if we can show that $m_{L/K;t,\eta} > 0$, then the last bound can be improved. As a result, we obtain the following corollary.

Corollary 1.9. *Under the assumptions of Theorem 1.1, the bound* (9) *holds with* $M_{2m}(U, L/K; t, \eta, \Phi)$ *in place of* $\widetilde{M}_{2m}(U, L/K; t, \eta, \Phi)$.

We end this section by noting that Theorems 1.1 and 1.4 imply Ω-results on the classical (unweighted) prime ideal counting functions

$$\psi(x;\, L/K, t) := \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ m \geq 1}} t(\varphi_{\mathfrak{p}}^m) \log(\mathcal{N}\mathfrak{p}). \tag{13}$$

Corollary 1.10. *Let L/K be a Galois extension of number fields for which GRH holds. Let F be any subfield of K (i.e., $F \subset K \subset L$) which is such that L/F is Galois and satisfies AC. Define $G := \mathrm{Gal}(L/K)$, $G^+ := \mathrm{Gal}(L/F)$, and assume that $t\colon G \to \mathbb{R}$ is a nonzero class function such that $t^+ := \mathrm{Ind}_G^{G^+} t$ satisfies $\widehat{t^+} \in \mathbb{R}_{\geq 0}$. Assume that $S_{t^+} \leq 1 - \kappa(\log_2(\mathrm{rd}_L + 2))^{-1}$ where $\kappa > 0$ is a large enough absolute constant. Then there exists a sequence of values $x = x_{j;L/K,t}$ tending to infinity such that*

$$|\psi(x;\, L/K, t) - \hat{t}(1)x| \gg x^{1/2}([F:\mathbb{Q}]\log(\mathrm{rd}_L)\lambda_{1,2}(t^+))^{1/2}\left(1 - S_{t^+} - O\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right)\right)^{1/2}, \tag{14}$$

where the implied constant is absolute. More precisely, there exists a large enough absolute constant $\kappa' > 0$ such that for any large enough $U > 0$ (in absolute terms), there exists $x > 1$ such that (14) holds with $\log x \in [U, U \cdot \beta_{L,F,K,t}]$ where

$$\beta_{L,F,K,t} := \kappa'[F:\mathbb{Q}]\lambda_{1,1}(t^+)^2 \log(\mathrm{rd}_L + 2)\log_2(\mathrm{rd}_L + 2)/\lambda_{1,2}(t^+).$$

Corollary 1.11. *Let L/K with $L \neq \mathbb{Q}$ be a Galois extension of number fields for which GRH holds, and define $G := \mathrm{Gal}(L/K)$. Then for any large enough $U > 0$, there exists $x > 1$ for which $\log x \in [U, \kappa' U \cdot \log(d_L + 2)]$ and such that*

$$|\psi(x;\, L/K, |G|\mathbf{1}_e) - x| \gg x^{1/2}(\log d_L)^{1/2}. \tag{15}$$

Here, κ' is a large enough absolute constant (in absolute terms).

The paper is organized as follows. In Section 2 we state applications of our main results to specific families of Galois extensions of number fields. The proofs of these statements are postponed to Section 6. Next, Sections 3 and 4 are dedicated to recollections and preparatory results concerning Artin conductors, and zeros of Artin L-functions, respectively. We prove our main results as well as Corollaries 1.10 and 1.11 in Section 5.

2. Explicit families of Galois extensions and class functions

In this section we study explicit infinite families of extensions for which Theorems 1.1 and 1.4 apply. The proofs of these results are contained in Section 6.

2.1. ***Abelian extensions: moments for prime ideals in ray classes.*** A natural way to generalize the questions addressed in [Hooley 1977; de la Bretèche and Fiorilli 2021; 2023] is to consider moments for the distribution of prime ideals in abelian number field extensions. Indeed, class field theory provides one with the exact transposition to any relative abelian extension of number fields of the classical approach to the study of primes in arithmetic progressions. Let $\mathfrak{m}$ be a nonzero ideal of the ring of integers $\mathcal{O}_K$ of a number field K, denote by $v_{\mathfrak{p}}$ the valuation on K with respect to a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, and consider

$$\begin{aligned}\mathrm{I}_{\mathfrak{m}}(K) &= \{\text{fractional ideals } \mathfrak{a} \text{ of } K : v_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ if } \mathfrak{p} \mid \mathfrak{m}\},\\ \mathrm{P}_{\mathfrak{m}}(K)^+ &= \{\gamma\mathcal{O}_K : \gamma \in K, \gamma \text{ totally positive and } \gamma \equiv 1 \bmod \mathfrak{m}\}.\end{aligned}$$

The (strict) ray class group attached to K and $\mathfrak{m}$ is defined as the quotient $\mathrm{Cl}_{\mathfrak{m}}(K) := \mathrm{I}_{\mathfrak{m}}(K)/\mathrm{P}_{\mathfrak{m}}(K)^+$. The quotient group $\mathrm{Cl}_{\mathfrak{m}}(K)$ is abelian and finite of order denoted $h_{K,\mathfrak{m}}$ (the strict ray class number attached to K and $\mathfrak{m}$). In the case $K = \mathbb{Q}$ and $\mathfrak{m} = m\mathbb{Z}$ for a positive integer m, we have

$$\mathrm{Cl}_{\mathfrak{m}}(K) = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times.$$

Class field theory asserts that, in general, there exists an (abelian) extension $L_{\mathfrak{m}}/K$ such that $G = \mathrm{Gal}(L_{\mathfrak{m}}/K) \simeq \mathrm{Cl}_{\mathfrak{m}}(K)$. In this setting, for any (class) function $t\colon \mathrm{Cl}_{\mathfrak{m}}(K) \to \mathbb{C}$, the prime counting function we are interested in takes the form

$$\psi_\eta(x; K, \mathfrak{m}, t) := \sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K\\ m \geq 1}} t([\mathfrak{p}]^m)\frac{\log(\mathcal{N}\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{m/2}}\eta(\log(\mathcal{N}\mathfrak{p}^m/x)),$$

where $[\mathfrak{p}]$ denotes the class of the prime ideal $\mathfrak{p}$ in $\mathrm{Cl}_{\mathfrak{m}}(K)$. Note that $\psi_\eta(x; K, \mathfrak{m}, t) = \psi_\eta(x; L_{\mathfrak{m}}/K, t)$, and thus this is a particular case of the setting in Theorem 1.1. The Chebotarev density theorem for $L_{\mathfrak{m}}/K$ and $t = h_{K,\mathfrak{m}}\mathbf{1}_{[\mathfrak{a}]}$, the (normalized) indicator function of a class $[\mathfrak{a}] \in \mathrm{Cl}_{\mathfrak{m}}(K)$, can be seen as a "prime number theorem in the ray class field of K corresponding to $\mathfrak{m}$". In this setting, applying Theorem 1.1 gives the following result.

Proposition 2.1. *For $\mathfrak{m}$ a nonzero ideal of the ring of integers $\mathcal{O}_K$ of a number field K, let $L_{\mathfrak{m}}/K$ be the corresponding ray class field extension, for which we assume that GRH holds. One has for the trivial class $[\mathfrak{e}] \in \mathrm{Cl}_{\mathfrak{m}}(K)$, any $m \geq 1$, any $\eta \in \mathcal{S}_\delta$ and any $\Phi \in \mathcal{U}$,*

$$\widetilde{M}_{2m}(U, L_{\mathfrak{m}}/K; h_{K,\mathfrak{m}}\mathbf{1}_{[\mathfrak{e}]}, \eta, \Phi) \geq \mu_{2m}(\alpha(|\hat{\eta}|^2)\log d_{L_{\mathfrak{m}}})^m(1 + o_{\mathrm{rd}_{L_{\mathfrak{m}}}\to\infty}(1)),$$

provided $(\log d_{L_{\mathfrak{m}}})^m/U \to 0$, where the implied constant in $o(\,\cdot\,)$ depends on $\mathfrak{m}$.

By analogy with the case of primes in arithmetic progressions (see [de la Bretèche and Fiorilli 2023, Theorem 1.3]), we expect that the dependency on the discriminant of $L_{\mathfrak{m}}$ can be made explicit in terms of the norm of $\mathfrak{m}$. This is indeed the case, as shown in [Cohen et al. 1998, Theorem 3.3(2)].

2.2. ***Dihedral extensions.*** A natural next step after analyzing the abelian case (see Remark 1.3) is to consider groups having an abelian subgroup of small index. Such is the case of dihedral groups. Let us start by recalling classical facts (see, e.g., [Serre 1977, Section 5.3]): for an odd integer $n \geq 3$, the dihedral group of order $2n$ is defined as follows,

$$D_n = \langle \sigma, \tau : \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1}\rangle.$$

The nontrivial conjugacy classes of D_n are

$$\{\sigma^j,\sigma^{-j}\}\bigl(1\le j\le \tfrac{1}{2}(n-1)\bigr),\quad \text{and}\quad \{\tau\sigma^k\colon 0\le k\le n-1\}.$$

Proposition 2.2. *One has the following table of values of S_t for various choices of central functions $t\colon D_n\to\mathbb{R}$:*

n	≥ 3	≥ 3	≥ 5
t	$\lvert D_n\rvert\mathbf{1}_e$	$\mathbf{1}_{\{\sigma,\sigma^{-1}\}}$	$2\mathbf{1}_e+\mathbf{1}_{\{\sigma,\sigma^{-1}\}}$
S_t	$\dfrac{1}{2n-1}$	$\dfrac{1-2/n}{2(1-1/n)}$	$<\frac{2}{3}$

The first column of the table is used to prove the following result.

Proposition 2.3. *For $n\ge 3$ odd, let $L/\mathbb{Q}$ be a D_n-extension of number fields for which GRH holds. One has for any $m\ge 1$, any $\eta\in\mathcal{S}_\delta$ and any $\Phi\in\mathcal{U}$,*

$$\widetilde{M}_{2m}(U,L/\mathbb{Q};\lvert D_n\rvert\mathbf{1}_e,\eta,\Phi)\ge\mu_{2m}\bigl(\alpha(\lvert\hat{\eta}\rvert^2)\bigl(2-\tfrac{1}{n}\bigr)\log d_L\bigr)^m(1+o_{\mathrm{rd}_L\to\infty}(1)),$$

provided $(\log d_L)^m/U\to 0$, *where the implied constant in $o(\cdot)$ depends on n.*

2.3. ***Radical extensions.*** We consider the following Galois extension studied in [Fiorilli and Jouve 2024, Section 9.2]. Let a, p be distinct prime numbers such that $p\ne 2$ and $a^{p-1}\not\equiv 1 \bmod p^2$ and let $K_{a,p}$ be the splitting field (inside $\mathbb{C}$) of $X^p-a\in\mathbb{Q}[X]$. The Galois group $G:=\mathrm{Gal}(K_{a,p}/\mathbb{Q})$ is isomorphic to the group of affine transformations of $\mathbb{A}^1_{\mathbb{F}_p}$. A convenient way to describe G is the following:

$$G\simeq\left\{\begin{pmatrix}c & d\\ 0 & 1\end{pmatrix}:c\in\mathbb{F}_p^*,d\in\mathbb{F}_p\right\}.\tag{16}$$

One has $\lvert G\rvert=p(p-1)$ and G admits a real irreducible character ϑ of degree $p-1$ (see Section 6.3).

Proposition 2.4. *Let G be as in* (16). *One has the following table of values for S_t for various choices of central functions $t\colon G\to\mathbb{R}$:*

t	$\lvert G\rvert\mathbf{1}_e$	ϑ
S_t	$\dfrac{1}{p(1-2/p+2/p^2)}$	$\dfrac{1}{p-1}$

We deduce the following result on the moments attached to the class functions considered in the table of Proposition 2.4.

Proposition 2.5. *Let a, p be distinct prime numbers such that $p\ne 2$ and $a^{p-1}\not\equiv 1 \bmod p^2$. Let $K_{a,p}/\mathbb{Q}$ be the Galois extension of group G defined by* (16). *Assuming that GRH holds for $K_{a,p}$, one has for any $m\ge 1$, any $\eta\in\mathcal{S}_\delta$ and any $\Phi\in\mathcal{U}$,*

$$\widetilde{M}_{2m}(U,K_{a,p}/\mathbb{Q};\lvert G\rvert\mathbf{1}_e,\eta,\Phi)\ge\mu_{2m}(\alpha(\lvert\hat{\eta}\rvert^2)p^3\log p)^m(1+o_{p\to\infty}(1)),$$
$$\widetilde{M}_{2m}(U,K_{a,p}/\mathbb{Q};\vartheta,\eta,\Phi)\ge\mu_{2m}(\alpha(\lvert\hat{\eta}\rvert^2)p\log p)^m(1+o_{p\to\infty}(1)),$$

provided $(p\log p)^m=o_{p\to\infty}(U)$.

Note that in this particular example of Galois extension $K_{a,p}/\mathbb{Q}$ the Artin conductors of the elements of $\mathrm{Irr}(G)$ can be explicitly computed (see [Fiorilli and Jouve 2024, Section 9.2] and [Viviani 2004]), therefore the last estimates of Theorem 1.4 can also be applied (yielding a weaker bound). Specific features of moments in the Chebotarev density theorem for Galois extensions of type generalizing the case of $K_{a,p}/\mathbb{Q}$ are studied in detail in [de la Bretèche et al. 2023].

2.4. ***Moments for irreducible characters.*** As already mentioned in Remark 1.3, choosing t such that $\hat{t}(\chi) = 0$ for many irreducible characters χ of G could lead to a value of S_t that is close to 1, however in a longer sum we can hope to have more cancellations (following, e.g., the philosophy of [Iwaniec and Kowalski 2004, Chapter 12], cancellations in character sums are believed to occur only when the sums are taken over a sufficiently large index set). However, in some cases where t is nontrivial but has a Fourier support of minimal size (e.g., when t is a nontrivial irreducible character of G, as in the case of $t = \vartheta$ in Section 2.3), one can still have $S_t < 1$ so that our main estimates in Theorem 1.1 and 1.4 apply. The following statement gives a setup where one can take t to be very close to an irreducible character and still apply our main results. This result covers the situation lying at the opposite of the generalization of the bound (12) discussed in Remark 1.7, where one discriminates the irreducible characters appearing in the Fourier support of the class function t according to the size of their degree.

Proposition 2.6. *Let $L/K/F$ be a tower of number fields such that $L \neq \mathbb{Q}$, L/F is Galois, and assume GRH and AC for the extension L/F. Define $G := \mathrm{Gal}(L/K)$ and $G^+ := \mathrm{Gal}(L/F)$. Let $t\colon G \to \mathbb{R}$ be a class function such that $t^+ = \frac{1}{2}(\chi + \overline{\chi})$ for some irreducible representation ρ of G^+ of character χ. Let $\eta \in \mathcal{S}_\delta$ and $\Phi \in \mathcal{U}$. Then $S_{t^+} < 1$ if and only if ρ is faithful and the center $Z(G^+)$ of G^+ has odd order.*[9] *In particular, if this last condition holds and if rd_L is large enough in terms of $1 - S_{t^+}$, then* (12) *applies.*

Finite groups admitting faithful irreducible characters are classified by a result of Gaschütz; see, e.g., [Huppert 1998, Theorem 42.7]. Finally note that even if ρ is not faithful or $2 \mid |Z(G^+)|$ then we may apply the first case in Theorem 1.4.

2.5. ***S_n-extensions.*** Perhaps what can be seen as the "generic" situation is when $L/\mathbb{Q}$ is Galois of group S_n the symmetric group on n letters. One can obtain explicit lower bounds for $\nu(L/F, t^+; \eta)$ by following the approach in [Fiorilli and Jouve 2024, Section 7], which involves Roichman's bound [1996]. For a large set of class functions t, one can show that S_t remains bounded away from 1 (where the distance to 1 is precisely evaluated as a function of n in [loc. cit.]). For instance this applies to the difference of normalized indicator functions

$$t_{C_1,C_2} = (|G|/|C_1|)\mathbf{1}_{C_1} - (|G|/|C_2|)\mathbf{1}_{C_2} \quad (\text{resp. } t_C = (|G|/|C|)\mathbf{1}_C)$$

as soon as C_1, C_2 are distinct conjugacy classes of S_n, one of which has size at most (resp. C is a conjugacy class of S_n of size at most) $n!^{1-(4+\varepsilon)/(\mathrm{e}\log n)}$. Using these ideas, we obtain the following result.

[9] Recall that a representation $\rho\colon G \to \mathrm{GL}(V)$ is said to be faithful if ρ is an injective group morphism.

Proposition 2.7. *Let n be large enough and assume that L/K is a Galois extension of number fields for which $L/\mathbb{Q}$ is Galois of group S_n and satisfies AC and GRH. Let C_1, C_2 be conjugacy classes of* $\mathrm{Gal}(L/K)$ *for which* $\min(|C_1^+|, |C_2^+|) \leq n!^{1-(4+\varepsilon)/(\mathrm{e}\log n)}$, *where* $\varepsilon > 0$ *is fixed. Then for all fixed* $m \geq 1$ *we have the bound*

$$\begin{aligned}&\widetilde{M}_{2m}(U, L/K; t_{C_1,C_2}, \eta, \Phi)\\ &\qquad\geq \mu_{2m}\biggl(c_\eta \frac{\log(n!/\min(|C_1^+|, |C_2^+|))}{\log n!} \frac{[K:\mathbb{Q}]\log(\mathrm{rd}_L) n!^{3/2}}{\min(|C_1^+|, |C_2^+|)^{3/2} p(n)^{1/2}}\biggr)^m (1 + o_{\mathrm{rd}_L\to\infty}(1)),\end{aligned}$$

provided $([K:\mathbb{Q}]\log(\mathrm{rd}_L)\min(|C_1^+|, |C_2^+|)^3 p(n)/n!^3)^{m/2}/U \to 0$, *where* $c_\eta > 0$ *depends only on* η. *The same bound holds for the class function* $t_{C_1} = (|G|/|C_1|)\mathbf{1}_{C_1}$, *with the convention that in this case,* $\min(|C_1^+|, |C_2^+|) = |C_1^+|$.

Note that the factor $\log(n!/\min(|C_1^+|, |C_2^+|))/\log n! \gg_\theta 1$ as soon as $\min(|C_1^+|, |C_2^+|) \leq n!^{1-\theta}$ for some $\theta > 0$.

3. Artin conductors

Let us first recall a few facts on Artin conductors. Consider a finite Galois extension of number fields L/K with Galois group G. For $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$, the higher ramification groups form a sequence $(G_i(\mathfrak{P}/\mathfrak{p}))_{i\geq 0}$ of subgroups of G (called filtration of the inertia group $\mathrm{I}(\mathfrak{P}/\mathfrak{p})$) defined as follows:

$$G_i(\mathfrak{P}/\mathfrak{p}) := \{\sigma \in G : \forall z \in \mathcal{O}_L, (\sigma z - z) \in \mathfrak{P}^{i+1}\}.$$

Each $G_i(\mathfrak{P}/\mathfrak{p})$ only depends on $\mathfrak{p}$ up to conjugation and $G_0(\mathfrak{P}/\mathfrak{p}) = \mathrm{I}(\mathfrak{P}/\mathfrak{p})$ (when conjugation is unimportant we will simply denote this group $I(\mathfrak{p})$). For clarity let us fix prime ideals $\mathfrak{p}$ and $\mathfrak{P}$ as above and write G_i for $G_i(\mathfrak{P}/\mathfrak{p})$. Given a representation $\rho\colon G \to \mathrm{GL}(V)$ on a complex vector space V, the subgroups G_i act on V through ρ and we denote by $V^{G_i} \subset V$ the subspace of G_i-invariant vectors. Let χ be the character of ρ and

$$n(\chi, \mathfrak{p}) := \sum_{i=0}^{\infty} \frac{|G_i|}{|G_0|} \operatorname{codim} V^{G_i}, \tag{17}$$

which was shown by Artin to be an integer. The *Artin conductor of* χ is the ideal of $\mathcal{O}_K$

$$\mathfrak{f}(L/K, \chi) := \prod_{\mathfrak{p}} \mathfrak{p}^{n(\chi,\mathfrak{p})}.$$

Note that the set indexing the above product is finite since only finitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ ramify in L/K. We set

$$A(\chi) := d_K^{\chi(1)} \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{f}(L/K, \chi)), \tag{18}$$

where d_K is the absolute value of the absolute discriminant of the number field K and $\mathcal{N}_{K/\mathbb{Q}}$ is the relative ideal norm with respect to $K/\mathbb{Q}$ (we will use the slight abuse of notation that identifies the value taken by this relative norm map with the positive generator of the corresponding ideal).

We recall the following pointwise bounds on the Artin conductor.

Lemma 3.1 [Fiorilli and Jouve 2024, Lemma 4.1]. *Let L/K be a finite Galois extension. For any nontrivial irreducible character χ of $G = \mathrm{Gal}(L/K)$, one has the bounds*

$$\max\bigl(1, \tfrac{1}{2}[K:\mathbb{Q}]\bigr)\chi(1) \le \log A(\chi) \le 2\chi(1)[K:\mathbb{Q}]\log(\mathrm{rd}_L),$$

where the root discriminant rd_L *is defined by* (5)*. The upper bound is unconditional. The lower bound is unconditional if $K/\mathbb{Q}$ is nontrivial and holds assuming AC for the Artin L-function $L(s, L/\mathbb{Q}, \chi)$.*[10]

We will also use the following average bounds, which generalize [Fiorilli and Jouve 2024, Lemma 4.2].

Lemma 3.2. *Let L/K be a Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. Let $\{c_\chi\}_{\chi\in\mathrm{Irr}(G)}$ be a family of nonnegative real numbers. Then we have the bounds*

$$(1-S(c))\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)c_\chi \le \sum_{\chi\in\mathrm{Irr}(G)}\frac{c_\chi\log A(\chi)}{[K:\mathbb{Q}]\log(\mathrm{rd}_L)} \le (1+S(c))\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)c_\chi,$$

where $S(c) := S_t$ (recall (11)*) for the choice $t = \sum_{\chi\in\mathrm{Irr}(G)} c_\chi\cdot\chi$.*

Proof. Denoting by χ_{reg} the character of the regular representation of G, we have the equality

$$\sum_{\chi\in\mathrm{Irr}(G)} c_\chi\left(\frac{\chi(1)}{|G|}n(\chi_{\mathrm{reg}},\mathfrak{p}) - n(\chi,\mathfrak{p})\right) = \frac{1}{|G_0|}\sum_{i\ge 0}\sum_{1\ne a\in G_i}\sum_{\chi\in\mathrm{Irr}(G)}\chi(a)c_\chi.$$

Summing over the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, we deduce that

$$\left|\sum_{\chi\in\mathrm{Irr}(G)}\frac{c_\chi\log A(\chi)}{[K:\mathbb{Q}]\log(\mathrm{rd}_L)} - \sum_{\chi\in\mathrm{Irr}(G)}\chi(1)c_\chi\right| \le S(c)\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)|c_\chi|,$$

from which the claimed bounds follow. □

We will also use the following bound.

Lemma 3.3. *Let L/K be a Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. For all $\chi\in\mathrm{Irr}(G)$, we have*

$$\frac{\log(A(\chi)+2)}{\log_2((A(\chi)+2)^{3/\chi(1)[K:\mathbb{Q}]})} \ll [K:\mathbb{Q}]\chi(1)\frac{\log(\mathrm{rd}_L+2)}{\log_2(\mathrm{rd}_L+2)}.$$

Proof. This follows form the fact that the function $\cdot/\log\cdot$ is eventually increasing, combined with the upper bound in Lemma 3.1. □

4. Sums over zeros of Artin L-functions

The goal of this section is to express the function $\psi_\eta(x; L/K, t)$ defined by (3) in terms of a sum over zeros of Artin L-functions, which will allow us to give a lower bound on the moments $\widetilde{M}_{2m}(U, L/K; t, \eta, \Phi)$ through an application of positivity. This lower bound will be expressed as a convergent sum over zeros, which we will evaluate explicitly.

[10] It actually also holds for the trivial character in this case.

First we recall a few facts about Artin L-functions. If χ is the character of an irreducible representation $\rho\colon G=\mathrm{Gal}(L/K)\to\mathrm{GL}(V)$, the corresponding Artin L-function is defined for $\mathrm{Re}(s)>1$ by the Euler product

$$L(s,L/K,\chi)=\prod_{\substack{\mathfrak{p}\lhd\mathcal{O}_K\\ \mathfrak{p}\text{ prime}}} L_{\mathfrak{p}}(s,\chi),\qquad \big(L_{\mathfrak{p}}(s,\chi)=\det(\mathrm{Id}-\mathcal{N}\mathfrak{p}^{-s}\rho(\varphi_{\mathfrak{p}})|_{V^{I_{\mathfrak{p}}}}),\ \mathfrak{p}\lhd\mathcal{O}_K\text{ prime}\big),$$

where $V^{I_{\mathfrak{p}}}$ is the subspace of V which is invariant under the inertia group $I_{\mathfrak{p}}$ (see Section 3). AC states that $L(s,L/K,\chi)$ can be extended to an entire function (except when χ is the trivial character, in which case there is a simple pole at $s=1$). Following [Artin 1931], we recall the definition of the archimedean part $L(s,\chi_\infty)$ of the completed L-function associated to the irreducible character χ. Let v be an infinite place of K (that is, v is a real embedding or a pair of conjugate complex embeddings). Let w be a place of L over v. For the couple (w,v), the analogue of the decomposition group is a subgroup $G_{w/v}$ of G which is trivial if v and w are both real or both complex, and which is the group of order two generated by complex conjugation otherwise. If we denote

$$\Gamma_{\mathbb{R}}(s)=\pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big),\qquad \Gamma_{\mathbb{C}}(s)=\Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1),$$

then the Euler factor at v is

$$\gamma_v(\chi,s)=\begin{cases}\Gamma_{\mathbb{R}}(s)^{\dim V^{G_{w/v}}}\,\Gamma_{\mathbb{R}}(s+1)^{\operatorname{codim} V^{G_{w/v}}} & \text{if } v \text{ is real},\\ \Gamma_{\mathbb{C}}(s)^{\chi(1)} & \text{if } v \text{ is complex}.\end{cases}$$

The Archimedean part of the completed L-function associated to χ is then defined by the formula (recall the definition (18) of the Artin conductor $A(\chi)$)

$$L(s,\chi_\infty)=A(\chi)^{s/2}\prod_{v}\gamma_v(\chi,s). \tag{19}$$

We are ready to prove the following explicit formula for the function

$$\psi_\eta(x;L/K,\chi):=\sum_{\substack{\mathfrak{p}\lhd\mathcal{O}_K\\ m\geq 1}}\chi(\varphi_{\mathfrak{p}}^m)\frac{\log(\mathcal{N}\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{m/2}}\eta(\log(\mathcal{N}\mathfrak{p}^m/x)).$$

Lemma 4.1. *Let L/K be a Galois extension of number fields, denote $G=\mathrm{Gal}(L/K)$, and let $\chi\in\mathrm{Irr}(G)$. Under AC for $L(s,L/K,\chi)$, for any $\eta\in\mathcal{S}_\delta$ and $x\geq 1$ we have the formula*

$$\psi_\eta(x;L/K,\chi)=x^{1/2}\mathcal{L}_\eta\big(\tfrac{1}{2}\big)\delta_{\chi=\chi_0}-\sum_{\rho_\chi}x^{\rho_\chi-\frac{1}{2}}\hat{\eta}\bigg(\frac{\rho_\chi-\frac{1}{2}}{2\pi i}\bigg)+O_\eta(x^{-1/2}\log(A(\chi)+2)),$$

where ρ_χ runs through the nontrivial zeros of $L(s,L/K,\chi)$.

Proof. Let

$$\gamma_\chi(s)=L(s,\chi_\infty)A(\chi)^{-s/2}.$$

Since we assume AC, we can use [Iwaniec and Kowalski 2004, Theorem 5.11] for the test function $\varphi\colon n\mapsto\eta(\log(n/x))/n^{1/2}$. Note that our assumptions are weaker than those in [loc. cit., Theorem 5.11], however going through the proof one sees that our hypotheses are sufficient for [loc. cit., (5.44)] to apply; see, e.g., [Montgomery and Vaughan 2007, Theorem 12.13] and [de la Bretèche and Fiorilli 2023]. Let us recall what is the relevant von Manglodt function Λ_χ in this case (it should satisfy [Iwaniec and Kowalski 2004, (5.25)]):

$$\Lambda_\chi(p^t)=\sum_{f\ell=t}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=f}}\log(p^f)\chi(\varphi_{\mathfrak{p}}^{\ell})\quad(p\text{ prime},\, t\in\mathbb{N}).$$

Indeed, by [Martinet 1977, page 11],

$$-\frac{L'(s,L/K,\chi)}{L(s,L/K,\chi)}=\sum_{\substack{\mathfrak{p}\lhd\mathcal{O}_K\\ \mathfrak{p}\text{ prime}}}\sum_{\ell\geq 1}\frac{\chi(\varphi_{\mathfrak{p}}^{\ell})\log\mathcal{N}\mathfrak{p}}{\mathcal{N}\mathfrak{p}^{s\ell}}=\sum_{p}\sum_{f,\ell\geq 1}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=f}}\frac{\chi(\varphi_{\mathfrak{p}}^{\ell})\log(p^f)}{p^{s\ell f}}=\sum_{p}\sum_{t\geq 1}\frac{\Lambda_\chi(p^t)}{p^{ts}}.$$

Then, the first term on the left-hand side of [Iwaniec and Kowalski 2004, (5.44)] is given by

$$\begin{aligned}\sum_{n\geq 1}\Lambda_\chi(n)\frac{\eta(\log(n/x))}{n^{1/2}}&=\sum_{p,t}\sum_{f\ell=m}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=f}}\frac{\log(p^f)\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(p^m/x))}{p^{m/2}}\\&=\sum_{p,m}\sum_{f\ell=m}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=f}}\frac{\log(\mathcal{N}\mathfrak{p})\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(\mathcal{N}\mathfrak{p}^{\ell}/x))}{\mathcal{N}\mathfrak{p}^{\ell/2}}\\&=\sum_{p,\ell}\sum_{m\equiv 0\bmod \ell}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=m/\ell}}\frac{\log(\mathcal{N}\mathfrak{p})\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(\mathcal{N}\mathfrak{p}^{\ell}/x))}{\mathcal{N}\mathfrak{p}^{\ell/2}}.\end{aligned}$$

Reindexing the sums, we obtain

$$\begin{aligned}\sum_{n\geq 1}\Lambda_\chi(n)\frac{\eta(\log(n/x))}{n^{1/2}}&=\sum_{p,\ell}\sum_{m'\geq 1}\sum_{\substack{\mathfrak{p}\mid p\\ f(\mathfrak{p}/p)=m'}}\frac{\log(\mathcal{N}\mathfrak{p})\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(\mathcal{N}\mathfrak{p}^{\ell}/x))}{\mathcal{N}\mathfrak{p}^{\ell/2}}\\&=\sum_{p,\ell}\sum_{\mathfrak{p}\mid p}\frac{\log(\mathcal{N}\mathfrak{p})\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(\mathcal{N}\mathfrak{p}^{\ell}/x))}{\mathcal{N}\mathfrak{p}^{\ell/2}}\\&=\sum_{\mathfrak{p},\ell}\frac{\log(\mathcal{N}\mathfrak{p})\chi(\varphi_{\mathfrak{p}}^{\ell})\eta(\log(\mathcal{N}\mathfrak{p}^{\ell}/x))}{\mathcal{N}\mathfrak{p}^{\ell/2}}=\psi_\eta(x;L/K,\chi).\end{aligned}$$

A similar calculation shows that the second term on the left-hand side of [Iwaniec and Kowalski 2004, (5.44)] is exactly $\psi_\eta(x^{-1};L/K,\overline{\chi})$. This translates into the formula

$$\begin{aligned}&\psi_\eta(x;L/K,\chi)+\psi_\eta(x^{-1};L/K,\overline{\chi})\\&\quad=\eta(\log(x))\log A(\chi)+\delta_{\chi=\chi_0}x^{1/2}\mathcal{L}_\eta\big(\tfrac{1}{2}\big)\\&\qquad+\tfrac{1}{2\pi}\int_{-\infty}^{\infty}\bigg(\frac{\gamma_\chi'\big(\frac12+it\big)}{\gamma_\chi\big(\frac12+it\big)}+\frac{\gamma_\chi'\big(\frac12-it\big)}{\gamma_\chi\big(\frac12-it\big)}\bigg)\widehat{\eta}\big(\tfrac{t}{2\pi}\big)x^{it}\,\mathrm{d}t-\sum_{\rho_\chi}x^{\rho_\chi-\frac12}\hat{\eta}\bigg(\frac{\rho_\chi-\frac12}{2\pi i}\bigg)+O_\eta(x^{-1/2}),\end{aligned}\tag{20}$$

where the error term accounts for possible trivial zeros of $L(s,L/K,\chi)$ at $s=0$.

To handle the contribution of the integral of γ-factors we use (19) as well as [Montgomery and Vaughan 2007, Lemma 12.14] that applies to our case with the choice $J(u) = \eta(2\pi(u - \log x))$. Up to the multiplicative constant $\chi(1)$ the contribution of any infinite place v of K is bounded by an analogous integral where the γ-factor appearing is the Euler Γ function. We can then combine [Montgomery and Vaughan 2007, Theorem 12.13 and Lemma 12.14] and [de la Bretèche and Fiorilli 2023, proof of Lemma 2.2] (note that we are using the assumption that η is differentiable here). To conclude, we use the upper bound $[K:\mathbb{Q}]\chi(1) \ll \log(A(\chi))$ from Lemma 3.1. □

In Section 5, we will apply Lemma 4.1 to approximate $\widetilde{M}_n(U, L/K; t, \eta, \Phi)$ (recall (4)). A positivity argument will then be applied to this approximation producing convergent sums over zeros of the form

$$b(\chi;h) := \sum_{\rho_\chi} h\biggl(\frac{\rho_\chi - \frac12}{2\pi i}\biggr), \quad b_0(\chi;h) := \sum_{\rho_\chi \notin \mathbb{R}} h\biggl(\frac{\rho_\chi - \frac12}{2\pi i}\biggr), \tag{21}$$

where ρ_χ runs through the nontrivial zeros of $L(s, L/K, \chi)$. Note that these sums take into account the multiplicities of zeros, by convention. As for the involved test function, we will work with $\mathcal{T}_\delta$, the set of nontrivial measurable functions $h\colon \mathbb{R} \to \mathbb{R}$ having the following properties. We require that $\xi \mapsto \xi h(\xi)$ is integrable, and that, for all $\xi \in \mathbb{R}$, we have the bounds

$$0 \le h(\xi) \ll (1+|\xi|)^{-1}(\log(2+|\xi|))^{-2-2\delta}.$$

Moreover, for all $t \in \mathbb{R}$, we have that[11]

$$\hat{h}(t), \hat{h}'(t) \ll \mathrm{e}^{-(1/2+\delta/2)|g|}.$$

Note that if $\eta \in \mathcal{S}_\delta$ is nontrivial, then $h_\eta := \hat{\eta}^2 \in \mathcal{T}_\delta$. We may extend h to the domain $\bigl\{s \in \mathbb{C}\colon |\Im\mathrm{m}(s)| \le \frac{1}{4\pi}\bigr\}$ by writing

$$h(s) := \int_{\mathbb{R}} \mathrm{e}^{2\pi i s\xi}\hat{h}(\xi)\,\mathrm{d}\xi. \tag{22}$$

Lemma 4.2. *Let L/K be a Galois extension of number fields of group G, and let $\chi \in \mathrm{Irr}(G)$. Assume AC for the extension L/K. Then for any $h \in \mathcal{T}_\delta$, we have the pointwise estimates*

$$\begin{aligned} &b(\chi;h) = \hat{h}(0)\log A(\chi) + O_h(\chi(1)[K:\mathbb{Q}]),\\ &b(\chi;h) \ll_h \log(A(\chi)+2). \end{aligned} \tag{23}$$

Proof. To estimate the sum $b(\chi;h)$ defined in (21), we set $x = 1$ and $\eta = \hat{h}$ in the explicit formula (20), resulting in the identity

$$\begin{aligned} b(\chi;h) = \mathcal{L}_\eta\bigl(\tfrac12\bigr)\delta_{\chi=\chi_0} + \hat{h}(0)\log A(\chi) + \tfrac{1}{2\pi}\int_{-\infty}^{\infty}\biggl(\frac{\gamma_\chi'\bigl(\frac12+it\bigr)}{\gamma_\chi\bigl(\frac12+it\bigr)} + \frac{\gamma_\chi'\bigl(\frac12-it\bigr)}{\gamma_\chi\bigl(\frac12-it\bigr)}\biggr)h\Bigl(\frac{t}{2\pi}\Bigr)\,\mathrm{d}t \\ - \psi_{\hat{h}}(1; L/K, \chi) - \psi_{\hat{h}}(1; L/K, \overline{\chi}) + O_h(1). \end{aligned} \tag{24}$$

[11] The integrability of $\xi \mapsto \xi h(\xi)$ implies that $\hat{h}$ is differentiable; see [Kolmogorov and Fomin 1989, page 430].

We have already seen in the proof of Lemma 4.1 that the contribution of the gamma factors is $\ll \chi(1)$. Moreover, we have the bound

$$\psi_{\hat{h}}(1; L/K, \chi) \ll_h \chi(1) \sum_{\substack{\mathfrak{p} \triangleleft \mathcal{O}_K \\ m \geq 1}} \frac{\log(\mathcal{N}\mathfrak{p})}{\mathcal{N}\mathfrak{p}^{(1+\delta/2)m}} \ll \chi(1) \sum_{p} \sum_{f \geq 1} \frac{\log(p^f)}{p^{f(1+\delta/2)}} \sum_{\substack{\mathfrak{p} \triangleleft \mathcal{O}_K \\ \mathfrak{p} \mid p \\ f(\mathfrak{p}/p) = f}} 1 \ll_\delta \chi(1)[K:\mathbb{Q}]. \tag{25}$$

The first claimed bound follows. As for the second, it is a consequence of Odlyzko type bounds; see, e.g., [Pizarro-Madariaga 2011, Theorem 3.2]. □

The next step will be to obtain an average bound on $b_0(\chi; \hat{\eta}^2)$. Precisely if $t\colon G \to \mathbb{C}$ is a class function and $\eta \in \mathcal{S}_\delta$ (recall the definition involving condition (1)) for some fixed $\delta > 0$, then we analyze in the following lemma the variance defined in (7).

Lemma 4.3. *Assume AC and GRH for the Galois extension of number fields L/K, and let $\eta \in \mathcal{S}_\delta$. Then we have the estimate*

$$\nu(L/K, t; \eta) = \alpha(|\hat{\eta}|^2) \sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 \log A(\chi) + E(L/K, t; \eta) + O_\eta([K:\mathbb{Q}]\lambda_{1,2}(t)), \tag{26}$$

where[12]

$$E(L/K, t; \eta) \ll_\eta \min\left\{ [K:\mathbb{Q}]\lambda_{1,2}(t) \frac{\log(\mathrm{rd}_L + 2)}{\log_2(\mathrm{rd}_L + 2)}, \left(\max_{\chi \in \mathrm{Irr}(G)} \frac{|\hat{t}(\chi)|^2}{\chi(1)} \right) \frac{\log(d_L + 2)}{\log_2(d_L + 2)} \right\}. \tag{27}$$

Moreover, we have the bounds

$$\begin{aligned} \alpha(|\hat{\eta}|^2)\lambda_{1,2}(t)\left(1 - S_t - O_\eta\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right)\right) &\leq \frac{\nu(L/K, t; \eta)}{[K:\mathbb{Q}]\log(\mathrm{rd}_L)} \\ &\leq \alpha(|\hat{\eta}|^2)\lambda_{1,2}(t)\left(1 + S_t + O_\eta\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right)\right). \end{aligned} \tag{28}$$

Proof. First observe that by (23), we have the estimate

$$\sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 b(\chi, |\hat{\eta}|^2) = \alpha(|\hat{\eta}|^2) \sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 \log A(\chi) + O_\eta([K:\mathbb{Q}]\lambda_{1,2}(t)).$$

Then, we remove the contribution of real zeros as follows:

$$\begin{aligned} \sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 (b(\chi, |\hat{\eta}|^2) - b_0(\chi, |\hat{\eta}|^2)) &\ll_\eta \sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 \operatorname{ord}_{s=1/2} L(s, L/K, \chi) \\ &\ll_\eta \sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 \frac{\log(A(\chi) + 2)}{\log_2(A(\chi) + 2)^{3/(\chi(1)[K:\mathbb{Q}])}}, \end{aligned}$$

[12] Note that only the first term of this minimum will be used in this paper — the second is present for future reference.

by [Iwaniec and Kowalski 2004, Proposition 5.21]. The first bound on $E(L/K, t; \eta)$ then follows directly from Lemma 3.3. As for the second, we have that

$$\sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 (b(\chi, |\hat{\eta}|^2) - b_0(\chi, |\hat{\eta}|^2)) \ll_\eta \left(\max_{\chi \in \mathrm{Irr}(G)} \frac{|\hat{t}(\chi)|^2}{\chi(1)} \right) \cdot \mathrm{ord}_{s=1/2}\, \zeta_L(s)$$

$$\ll_\eta \left(\max_{\chi \in \mathrm{Irr}(G)} \frac{|\hat{t}(\chi)|^2}{\chi(1)} \right) \frac{\log(d_L + 2)}{\log_2(d_L + 2)},$$

thanks to the decomposition $\zeta_L(s) = \prod_{\chi \in \mathrm{Irr}(G)} L(s, L/K, \chi)^{\chi(1)}$ and [Iwaniec and Kowalski 2004, Proposition 5.34]. Finally, (28) follows from combining (26) with the bounds in Lemma 3.2. □

In view of (28), one may wonder if we can still produce a lower bound if S_t is close to 1. In the next two lemmas we show that in this case we can still estimate $b_0(\chi, h)$ in terms of $\log A(\chi)$. The idea here is that if $\hat{\eta}$ does not vanish on an interval containing sufficiently many imaginary parts of L-function zeros then we can deduce the required estimate. For $\chi \in \mathrm{Irr}(\mathrm{Gal}(L/K))$ we will denote

$$N(T, \chi) = \{\rho \colon 0 < \Re\mathrm{e}(\rho) < 1, |\Im\mathrm{m}(\rho)| \le T, L(\rho, L/K, \chi) = 0\} \quad (T \ge 0).$$

Lemma 4.4. *Assume AC and GRH for the Galois extension of number fields L/K. Let $G = \mathrm{Gal}(L/K)$ and $\chi \in \mathrm{Irr}(G)$. For all $T > 0$ and all $0 < \varepsilon \le 1$ one has*

$$N(T + \varepsilon, \chi) - N(T, \chi)$$
$$= \frac{\varepsilon}{\pi} \log\left(A(\chi) \left(\frac{T + \varepsilon}{2\pi \mathrm{e}} \right)^{\chi(1)[K:\mathbb{Q}]} \right) + O\left(\frac{\log((A(\chi) + 2)(4T + 1)^{\chi(1)[K:\mathbb{Q}]})}{\log_2((A(\chi) + 2)^{3/(\chi(1)[K:\mathbb{Q}])}(4T + 1))} + [K : \mathbb{Q}]\chi(1) \right).$$

In particular, if $\varepsilon \ge \kappa(\log_2(T + 3))^{-1}$ and

$$(1 - S_t)^{-1} \le \kappa^{-1} \varepsilon \log_2(\mathrm{rd}_L + 2) \left(1 + \frac{[K : \mathbb{Q}] \log T}{\log(\mathrm{rd}_L + 2)} \right), \tag{29}$$

where $\kappa > 0$ is a large enough absolute constant, then we have the bound

$$\sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 (N(T + \varepsilon, \chi) - N(T, \chi)) \ge \frac{\varepsilon}{8\pi} \sum_{\chi \in \mathrm{Irr}(G)} |\hat{t}(\chi)|^2 \log\left(A(\chi) \left(\frac{T + \varepsilon}{2\pi \mathrm{e}} \right)^{\chi(1)[K:\mathbb{Q}]} \right).$$

In case $\mathrm{rd}_L \ll 1$, then the assumption $\varepsilon \gg \kappa(\log_2(T + 3))^{-1}$ is sufficient (i.e., (29) is not required).

Note that the condition $\varepsilon \gg \kappa(\log_2(T + 3))^{-1}$ implies that ε or T is large enough, which ensures that $N(T + \varepsilon, \chi) - N(T, \chi) \ne 0$.

Proof. Recalling the definition (19) of $L(s, \chi_\infty)$, we combine Theorem 5 and (4.1) of [Carneiro et al. 2015] to obtain

$$N(T+\varepsilon, \chi) - N(T, \chi) = \frac{1}{\pi} \int_{T<|g|<T+\varepsilon} \mathrm{Re}\left(\frac{L'}{L}\left(\frac{1}{2} + it, \chi_\infty \right) \right), \mathrm{d}t$$
$$+ O\left(\frac{\log((A(\chi)+2)(4T+1)^{\chi(1)[K:\mathbb{Q}]})}{\log_2((A(\chi)+2)^{3/(\chi(1)[K:\mathbb{Q}])}(4T+1))} \right) + O([K : \mathbb{Q}]\chi(1)). \tag{30}$$

To evaluate the main term we use the computations [Iwaniec and Kowalski 2004, (5.35) and (5.36)] in the context of [Carneiro et al. 2015, (4.1)]. Precisely the factors of $L(s, \chi_\infty)$ have the following contribution in the range $[T, T+\varepsilon]$ of imaginary parts of critical zeros:

$$\frac{\varepsilon}{\pi}\log\biggl(\frac{A(\chi)}{\pi^{[K:\mathbb{Q}]\chi(1)}}\biggr)+\frac{[K:\mathbb{Q}]\chi(1)}{\pi}\biggl((T+\varepsilon)\log\frac{T+\varepsilon}{2}-T\log\frac{T}{2}-\varepsilon\biggr)+O([K:\mathbb{Q}]\chi(1))$$
$$=\frac{\varepsilon}{\pi}\log\biggl(\frac{A(\chi)}{\pi^{[K:\mathbb{Q}]\chi(1)}}\biggr)+\frac{[K:\mathbb{Q}]\chi(1)}{\pi}\varepsilon\log\biggl(\frac{T+\varepsilon}{2\mathrm{e}}\biggr)+O([K:\mathbb{Q}]\chi(1)),$$

which leads to the first estimate. In order to prove the second part of the statement, note that

$$\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\frac{\log((A(\chi)+2)(4T+1)^{\chi(1)[K:\mathbb{Q}]})}{\log_2((A(\chi)+2)^{3/(\chi(1)[K:\mathbb{Q}])}(4T+1))}$$
$$\ll\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\frac{\log(A(\chi)+2)}{\log_2((A(\chi)+2)^{3/(\chi(1)[K:\mathbb{Q}])})}+[K:\mathbb{Q}]\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)|\hat{t}(\chi)|^2\frac{\log(4T+1)}{\log_2((A(\chi)+2)^{3/(\chi(1)[K:\mathbb{Q}])})}.$$

Moreover, Lemma 3.2 implies the bound (recall (11))

$$\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\log A(\chi)\geq(1-S_t)\log(\mathrm{rd}_L)\lambda_{1,2}(t)[K:\mathbb{Q}].$$

The stated lower bound then follows from (30) and from Lemmas 3.3 and 3.1. Indeed the main term is greater than twice the error term under the stated assumption. Finally note that if $2\leq\mathrm{rd}_L\ll 1$, then Lemma 3.1 implies that $\log(A(\chi)+2)\asymp[K:\mathbb{Q}]\chi(1)$ which is sufficient to obtain the stated lower bound. The only case not covered by this condition, which corresponds to $L=K=\mathbb{Q}$, can be trivially handled separately. □

Building on Lemma 4.4, we can now deduce an estimate on $b_0(\chi,\hat{\eta}^2)$ (recall (8)) in terms of $\log A(\chi)$ under a support condition on $\hat{\eta}$.

Lemma 4.5. *Assume AC and GRH for the Galois extension of number fields L/K. Let $G=\mathrm{Gal}(L/K)$ and let $\varepsilon, T>0$ be such that $T\geq\kappa$ and $\varepsilon\geq\kappa(\log_2(T+3))^{-1}$, where $\kappa>0$ is absolute and large enough. Assuming that $\hat{\eta}$ does not vanish on $[T,T+\varepsilon]$,*[13] *then we have*

$$\nu(L/K,t;\eta)\asymp_\eta\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\log(A(\chi)+2). \tag{31}$$

Proof. By definition, we have the lower bound

$$b_0(\chi;\hat{\eta}^2)\geq(N(T+\varepsilon,\chi)-N(T,\chi))\min_{|g|\in[T,T+\varepsilon]}|\hat{\eta}|^2\gg_\eta\log(A(\chi)+2),$$

by Lemma 4.4 and our hypotheses on ε and T, which imply that the main term in this lemma dominates the error term. As a result,

$$\nu(L/K,t;\eta)\gg_\eta\sum_{\chi\in\mathrm{Irr}(G)}|\hat{t}(\chi)|^2\log(A(\chi)+2).$$

The upper bound follows directly from (23). □

[13] Recall that in (29) the constant $\kappa>0$ is absolute. Note moreover that if $\hat{\eta}$ does not vanish, the condition on $\hat{\eta}$ is always fulfilled with $\varepsilon=\infty$.

5. Proof of Theorems 1.1 and 1.4: induction and positivity

In this section our main goal is to prove Theorems 1.1 and 1.4. This will be carried out through an application of positivity in the explicit formula obtained in Lemma 4.1 (positivity will circumvent the need for the LI hypothesis). Notice however that doing so directly with the Fourier decomposition (recall the definition (3))

$$\psi_\eta(x; L/K, t) = \sum_{\chi\in\mathrm{Irr}(G)} \hat{t}(\chi)\psi_\eta(x; L/K, \chi)$$

would yield bounds which we believe not to be optimal (unless $K = \mathbb{Q}$). To obtain conjecturally optimal bounds, we will first apply the inductive property of Artin L-functions. This is the purpose of Lemma 5.1. The following step, Lemma 5.2, will consist of approximating the moment we study $\widetilde{M}_n(U, L/K; t, \eta, \Phi)$ by the quantity $\widetilde{D}_n(U, L/K; t, \eta, \Phi)$ which involves zeros of Artin L-functions. A lower bound for $\widetilde{D}_n(U, L/K; t, \eta, \Phi)$ will be produced in Lemma 5.7 by combining two preparatory results: a combinatorial inequality which we believe is of intrinsic interest (Lemma 5.3) and a statement which is more representation theoretic in nature and deals with L-function zeros relevant to the moment $\widetilde{M}_n(U, L/K; t, \eta, \Phi)$ (Lemma 5.6).

We recall that L/K is a Galois extension of number fields of Galois group G, and $t\colon G \to \mathbb{C}$ is a class function. If F is a subfield of K such that L/F is Galois of group G^+, then we form the class function on G^+ induced by t in the following way:

$$t^+ = \mathrm{Ind}_G^{G^+}(t)\colon G^+ \to \mathbb{C}, \quad t^+(g) = \sum_{\substack{aG\in G^+/G:\\ a^{-1}ga\in G}} t(a^{-1}ga)(g \in G^+).$$

The property of invariance of Artin L-functions under induction (see [Artin 1931, (18)]) can be stated, in our situation, as the equality $L(s, L/K, t) = L(s, L/F, t^+)$: it is crucial to our analysis and implies in particular Lemma 5.1 below.

Through this section, one should keep in mind that if we assume AC for $L/\mathbb{Q}$, then we expect in most cases to obtain the best bounds by selecting $F = \mathbb{Q}$. On the other extreme, one may always take $F = K$ and obtain nontrivial bounds.

Lemma 5.1. *Let $L/K/F$ be a tower of number fields for which L/F is Galois, let $G = \mathrm{Gal}(L/K)$ and $G^+ = \mathrm{Gal}(L/F)$. For $\eta \in \mathcal{S}_\delta$ and for any class function $t\colon G \to \mathbb{C}$, we have the identity*

$$\psi_\eta(x; L/K, t) = \psi_\eta(x; L/F, t^+). \tag{32}$$

As a consequence, for any $\Phi \in \mathcal{U}$ we have the identity

$$\widetilde{M}_n(U, L/K; t, \eta, \Phi) = \widetilde{M}_n(U, L/F; t^+, \eta, \Phi). \tag{33}$$

Proof. The equality (32) is stated and proved in [Fiorilli and Jouve 2024, Proposition 3.11]. As for (33), it is a consequence of (32) combined with [loc. cit., Lemma 3.15], which asserts that $z(L/K, t) = z(L/\mathbb{Q}, t^+)$

(the limiting expectation involved in (4)), and the equality $\widehat{t^+}(1) = \hat{t}(1)$, which is a straightforward application of Frobenius reciprocity. □

We now approximate the moment $\widetilde{M}_n(U, L/K; t, \eta, \Phi)$ by a sum over zeros of Artin L-functions. If L/F is a Galois extension of group G^+, then we define for every integer $n \geq 1$

$$\widetilde{D}_n(U, L/F; t, \eta, \Phi) := \frac{(-1)^n}{2\int_0^\infty \Phi} \sum_{\chi_1,\dots,\chi_n \in \mathrm{Irr}(G^+)} \Bigl(\prod_{j=1}^n \hat{t}(\chi_j)\Bigr) \sum_{\gamma_{\chi_1},\dots,\gamma_{\chi_n} \neq 0} \widehat{\Phi}\Bigl(\frac{U}{2\pi}(\gamma_{\chi_1} + \cdots + \gamma_{\chi_n})\Bigr) \prod_{j=1}^n \hat{\eta}\Bigl(\frac{\gamma_{\chi_j}}{2\pi}\Bigr), \tag{34}$$

where $\gamma_{\chi_1}, \dots, \gamma_{\chi_n}$ run over the imaginary parts of the nontrivial zeros of the Artin L-functions

$$L(s, L/F, \chi_1), \dots, L(s, L/F, \chi_n).$$

Lemma 5.2. *Let $L/K/F$ be a tower of number fields in which L/F is a Galois extension satisfying AC and GRH. Let $t\colon \mathrm{Gal}(L/K) \to \mathbb{C}$ be a class function and let $t^+ := \mathrm{Ind}_{\mathrm{Gal}(L/K)}^{\mathrm{Gal}(L/F)} t$. Then for $\eta \in \mathcal{S}_\delta$, $\Phi \in \mathcal{U}$, and $n \in \mathbb{Z}_{\geq 1}$ we have the estimate*

$$\widetilde{M}_n(U, L/K; t, \eta, \Phi) = \widetilde{D}_n(U, L/F; t^+, \eta, \Phi) + O\biggl(\frac{(\kappa_\eta[F:\mathbb{Q}]\lambda_{1,1}(t^+)\log(\mathrm{rd}_L + 2))^n}{U}\biggr),$$

where $\kappa_\eta > 0$ is a constant which depends only on η.

Proof. Let $G^+ = \mathrm{Gal}(L/F)$, and recall that by Lemma 5.1, one has

$$\widetilde{M}_n(U, L/K; t, \eta, \Phi) = \widetilde{M}_n(U, L/F; t^+, \eta, \Phi).$$

Combining the Fourier decomposition

$$\psi_\eta(\mathrm{e}^u; L/F, t^+) = \sum_{\chi \in \mathrm{Irr}(G^+)} \widehat{t^+}(\chi)\psi_\eta(\mathrm{e}^u; L/F, \chi)$$

and Lemma 4.1 results in the estimate (recall that Frobenius reciprocity implies $\widehat{t^+}(1) = \hat{t}(1)$)

$$\psi_\eta(\mathrm{e}^u; L/F, t^+) = \hat{t}(1)x^{1/2}\mathcal{L}_\eta\Bigl(\frac{1}{2}\Bigr) - \sum_{\chi \in \mathrm{Irr}(G^+)} \widehat{t^+}(\chi) \sum_{\gamma_\chi} \mathrm{e}^{i\gamma_\chi u}\hat{\eta}\Bigl(\frac{\gamma_\chi}{2\pi}\Bigr) + O_\eta\Bigl(\mathrm{e}^{-u/2} \sum_{\chi \in \mathrm{Irr}(G^+)} |\widehat{t^+}(\chi)| \log(A(\chi)+2)\Bigr). \tag{35}$$

By Lemma 3.1, the error term is $\ll_\eta \mathrm{e}^{-u/2}[F:\mathbb{Q}]\log(\mathrm{rd}_L)\lambda_{1,1}(t^+)$. The claimed estimate follows from substituting this expression in the definition (4) and applying the bound

$$\sum_{\gamma_\chi} \mathrm{e}^{i\gamma_\chi u}\hat{\eta}\Bigl(\frac{\gamma_\chi}{2\pi}\Bigr) \ll_\eta \log(A(\chi) + 2),$$

which is a direct consequence of the Riemann-von Mangoldt formula; see, e.g., [Iwaniec and Kowalski 2004, Theorem 5.8]. □

Our goal will be to apply positivity on the right-hand side of (34). The idea here is that by our conditions on $\widehat{\Phi}$, $\widehat{t^+}$ and $\hat{\eta}$, the quantity $\widetilde{D}_n(U, L/F; t^+, \eta, \Phi)$ is a sum of positive terms. The rapid decay of $\widehat{\Phi}$ should imply that only the terms where $\gamma_{\chi_1} + \cdots + \gamma_{\chi_n}$ is very small contribute substantially to the inner sum in (34). However, if the zeros enjoy on average the diophantine properties of "random" real numbers, then we expect this to be the case only when the ρ_{χ_j} come in conjugate pairs, that is for each j there exists $\pi(j)$ such that $\gamma_{\chi_j} = -\gamma_{\chi_{\pi(j)}}$. Moreover, we also believe that this should force $\chi_j = \overline{\chi_{\pi(j)}}$. Those two facts follow from an effective version of the linear independence hypothesis for Artin L-functions; see [Fiorilli and Jouve 2024, Introduction] for the precise statement. The positivity condition will allow us to circumvent this hypothesis.

Let us first establish the following combinatorial result.

Lemma 5.3. *Let $\Gamma \subset \mathbb{R}_{>0}$ be a countable multiset, and let $\boldsymbol{a} = \{a_\gamma\}_{\gamma \in \Gamma \cup -\Gamma}$ be a sequence of complex numbers such that $a_{-\gamma} = \overline{a_\gamma}$ and moreover $\sum_{\gamma \in \Gamma} |a_\gamma|^2 < \infty$, where by convention sums over $\gamma \in \Gamma$ take multiplicities into account. Define*

$$S_{2\ell}(\boldsymbol{a}) := \sum_{\substack{\gamma_1,\dots,\gamma_\ell \in \Gamma, \gamma'_1,\dots,\gamma'_\ell \in -\Gamma \\ \forall \gamma \in \mathbb{R}, \#\{j : \gamma_j = \gamma\} = \#\{j : \gamma'_j = -\gamma\}}} \prod_{j=1}^{\ell} a_{\gamma_j} a_{\gamma'_j}.$$

Then, $S_{2\ell}(\boldsymbol{a}) \in \mathbb{R}$, and moreover for every positive integer ℓ, we have the inequality

$$S_{2\ell}(\boldsymbol{a}) \geq \ell! \biggl(\sum_{\gamma \in \Gamma} |a_\gamma|^2 \biggr)^{\ell - 1} \max\biggl\{ \sum_{\gamma \in \Gamma} |a_\gamma|^2 - \ell!\, \ell(\ell - 1) M^2 \mathrm{e}^{1/\ell}, 0 \biggr\}, \tag{36}$$

where $M := \sup\{|a_\gamma| : \gamma \in \Gamma\}$.

Remark 5.4. For $\ell = 1$, note that $\ell!\, \ell(\ell - 1) M^2 \mathrm{e}^{1/\ell} = 0$. In fact, in this case we have

$$S_2(\boldsymbol{a}) = \sum_{\gamma \in \Gamma} m_\gamma |a_\gamma|^2 \geq \sum_{\gamma \in \Gamma} |a_\gamma|^2,$$

where m_γ is the multiplicity of γ in Γ. Indeed, by definition $m_{-\gamma} = m_\gamma$.

Proof of Lemma 5.3. By Remark 5.4, we may assume that $\ell \geq 2$. For any integer $r \geq 1$ and any r-tuple $\boldsymbol{n} = (n_1, \dots, n_r) \in \mathbb{N}^r$, which is a partition of ℓ in the sense that $n_i \leq n_{i+1}$ for all i, and $\sum_i n_i = \ell$, we denote by s_1 the number of indices $i \geq 1$ such that $n_i = n_1$, and inductively by s_j the number of indices i such that $n_i = n_{s_{j-1}+1}$. Note that if k is the "number of distinct parts" in the partition $(n_1, \dots, n_r)$ of ℓ, in particular $s_k = \#\{i : n_i = n_r\}$, then one has $s_1 + \dots + s_k = r$. We set

$$c(\boldsymbol{n}) = c(n_1, \dots, n_r) = \binom{\ell}{n_1, \dots, n_r} \frac{1}{s_1! \cdots s_k!}.$$

where we recall the definition of the multinomial coefficient

$$\binom{\ell}{n_1, \dots, n_r} = \frac{\ell!}{n_1! \cdots n_r!}.$$

In particular $c(1, \dots, 1) = 1$ since in this case $k = 1$ and $s_1 = r = \ell$.

For every $\gamma \in \Gamma$, let m_γ be the multiplicity of γ in Γ. On one hand we have the following expansion (here we use the notation $\sum^*$ to denote a sum "without multiplicity")

$$\biggl(\sum_{\gamma \in \Gamma} |a_\gamma|^2 \biggr)^{\ell} = \biggl(\sideset{}{^*}\sum_{\gamma \in \Gamma} m_\gamma |a_\gamma|^2 \biggr)^{\ell} = \sum_{\substack{n_1 + \dots + n_r = \ell \\ n_1 \leq n_2 \leq \dots \leq n_r}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1, \dots, \gamma_r \in \Gamma \\ \forall i \neq j, \gamma_i \neq \gamma_j}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} |a_{\gamma_j}|^{2n_j}. \tag{37}$$

Here, we have used the fact that for a given $(n_1,\dots,n_r)\in\mathbb{N}^r$ such that $n_1+\cdots+n_r=\ell$, the number of permutations of the n_j such that $n_1\le n_2\le\cdots\le n_r$ is exactly $s_1!\cdots s_k!$.

On the other hand we have

$$\begin{aligned} S_{2\ell}(\boldsymbol{a}) &= \sum_{\substack{n_1+\cdots+n_r=\ell\\ n_1\le n_2\le\cdots\le n_r}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma\\ \forall i\neq j,\gamma_i\neq\gamma_j}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} a_{\gamma_j}^{n_j} \sideset{}{^*}\sum_{\substack{\gamma'_1,\dots,\gamma'_\ell\in\Gamma\\ \forall i,\#\{j\le\ell:\gamma'_j=-\gamma_i\}=n_i}} \prod_{j=1}^{\ell} m_{\gamma_j}^{n_j} a_{-\gamma_j}^{n_j},\\ &= \sum_{\substack{n_1+\cdots+n_r=\ell\\ n_1\le n_2\le\cdots\le n_r}} c(\boldsymbol{n}) \binom{\ell}{n_1,\dots,n_r} \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma\\ \forall i\neq j,\gamma_i\neq\gamma_j}} \prod_{j=1}^{r} m_{\gamma_j}^{2n_j} |a_{\gamma_j}|^{2n_j} \end{aligned} \tag{38}$$

which is a real number. The additional factor $\binom{\ell}{n_1,\dots,n_r}$ comes from the number of the sets $\#\{j\le\ell:\gamma'_j=-\gamma_i\}=n_i$. Since the multiplicities m_γ are positive integers, the contribution of $\boldsymbol{n}=(1,\dots,1)$ to the right-hand side of (38) admits the lower bound

$$\ell! \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_\ell\in\Gamma\\ \forall i\neq j,\gamma_i\neq\gamma_j}} \prod_{j=1}^{\ell} m_{\gamma_j}^{2} |a_{\gamma_j}|^2 \ge \ell! \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_\ell\in\Gamma\\ \forall i\neq j,\gamma_i\neq\gamma_j}} \prod_{j=1}^{\ell} m_{\gamma_j} |a_{\gamma_j}|^2. \tag{39}$$

Using (37) we see that the lower bound in (39) equals

$$\ell!\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell} - \ell! \sum_{\substack{n_1+\cdots+n_r=\ell\\ n_1\le n_2\le\cdots\le n_r\\ n_r>1}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma\\ \forall i\neq j,\gamma_i\neq\gamma_j}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} |a_{\gamma_j}|^{2n_j},$$

and therefore we deduce from (38) and (39) that

$$\begin{aligned} S_{2\ell}(\boldsymbol{a}) &\ge \ell!\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell} + \sum_{\substack{n_1+\cdots+n_r=\ell\\ n_1\le n_2\le\cdots\le n_r\\ n_r\ge2}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma\\ \forall i\neq j,\gamma_i\neq\gamma_j}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} |a_{\gamma_j}|^{2n_j} \Big(\binom{\ell}{n_1,\dots,n_r}\prod_{j=1}^{r} m_{\gamma_j}^{n_j} - \ell!\Big)\\ &\ge \ell!\Big(\sum_{\gamma\in\Gamma}|a_\gamma|^2\Big)^{\ell} - \ell!\, S'_{2\ell}(\boldsymbol{a}), \end{aligned} \tag{40}$$

where we denote

$$S'_{2\ell}(\boldsymbol{a}) := \sum_{\substack{n_1+\cdots+n_r=\ell\\ n_1\le n_2\le\cdots\le n_r\\ n_r\ge2}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma\\ \forall i\neq j,\gamma_i\neq\gamma_j\\ \prod_{j=1}^r m_{\gamma_j}^{n_j}\le n_1!\cdots n_r!}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} |a_{\gamma_j}|^{2n_j}.$$

Here we emphasize the extra condition $\prod_{j=1}^r m_{\gamma_j}^{n_j}\le n_1!\cdots n_r!$ appearing in the index set of the inner sum. This is explained by the fact that r-tuples $\boldsymbol{n}$ such that $\prod_{j=1}^r m_{\gamma_j}^{n_j}> n_1!\cdots n_r!$ contribute a positive term to the second summand in (40).

To obtain an upper bound for $S'_{2\ell}(\boldsymbol{a})$, we write

$$S'_{2\ell}(\boldsymbol{a}) = \sum_{2\le n_r\le\ell} \sum_{\substack{(n_1,\dots,n_{r-1}):\\ n_1+\cdots+n_{r-1}=\ell-n_r\\ n_1\le n_2\le\cdots\le n_r}} c(\boldsymbol{n}) \sideset{}{^*}\sum_{\substack{\gamma_1,\dots,\gamma_r\in\Gamma\\ \forall i\neq j,\gamma_i\neq\gamma_j\\ \prod_{j=1}^r m_{\gamma_j}^{n_j}\le n_1!\cdots n_r!}} \prod_{j=1}^{r} m_{\gamma_j}^{n_j} |a_{\gamma_j}|^{2n_j}.$$

Note that (37) can then be used for the partition $(n_1, \dots, n_{r-1})$ of $\ell - n_r$ since we have

$$c(\boldsymbol{n}) = c(n_1, \dots, n_r) = \binom{\ell}{n_1, \dots, n_r} \frac{1}{s_1! \cdots s_t!} \le c(n_1, \dots, n_{r-1}) \binom{\ell}{n_r}.$$

We deduce that

$$S'_{2\ell}(\boldsymbol{a}) \le \sum_{2 \le n_r \le \ell} \binom{\ell}{n_r} \Big(\sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big)^{\ell - n_r} \Big(\sideset{}{^*}\sum_{\substack{\gamma \in \Gamma \\ m_\gamma^{n_r} \le \ell!}} m_\gamma^{n_r} |a_\gamma|^{2n_r} \Big). \tag{41}$$

Next we use the condition $m_\gamma^{n_r} \le \ell!$ in the index set of the innermost sum of (41) as well as the inequality

$$\binom{\ell}{n_r} \le \ell(\ell-1) \binom{\ell-2}{n_r-2},$$

to compute

$$\begin{aligned} S'_{2\ell}(\boldsymbol{a}) &\le \ell! \sum_{2 \le n_r \le \ell} \binom{\ell}{n_r} \Big(\sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big)^{\ell - n_r} \Big(\sum_{\gamma \in \Gamma} |a_\gamma|^{2n_r} \Big) \\ &\le \ell!\, \ell(\ell-1) M^2 \sum_{2 \le n_r \le \ell} \binom{\ell-2}{n_r-2} \Big(\sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big)^{\ell - n_r} M^{2(n_r-2)} \Big(\sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big) \\ &\le \ell!\, \ell(\ell-1) M^2 \Big(M^2 + \sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big)^{\ell-1}, \end{aligned}$$

where we have used the upper bound $|a_\gamma|^{2n_r} \le M^{2n_r-2} |a_\gamma|^2$ and the binomial formula for the last step. Plugging this into (40) we deduce that

$$\frac{S_{2\ell}(\boldsymbol{a})}{\ell!} \ge \Big(\sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big)^{\ell} - \ell!\, \ell(\ell-1) M^2 \Big(M^2 + \sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big)^{\ell-1}. \tag{42}$$

To conclude, note that if $\sum_{\gamma \in \Gamma} |a_\gamma|^2 \le \ell(\ell-1)\ell!\, M^2$ then we have obtained a trivial lower bound since $S_{2\ell}(\boldsymbol{a}) \ge 0$ by (38). However if $\sum_{\gamma \in \Gamma} |a_\gamma|^2 > \ell(\ell-1)\ell!\, M^2$ then we have

$$\Big(M^2 + \sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big)^{\ell-1} \le \Big(\sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big)^{\ell-1} \Big(1 + \frac{1}{\ell(\ell-1)} \Big)^{\ell-1} \le \Big(\sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big)^{\ell-1} \mathrm{e}^{1/\ell} \tag{43}$$

and therefore (42) yields in both cases the asserted lower bound

$$\frac{S_{2\ell}(\boldsymbol{a})}{\ell!} \ge \Big(\sum_{\gamma \in \Gamma} |a_\gamma|^2 \Big)^{\ell-1} \max\Big\{ \sum_{\gamma \in \Gamma} |a_\gamma|^2 - \ell!\, \ell(\ell-1) M^2 \mathrm{e}^{1/\ell}, 0 \Big\}. \qquad \square$$

Next we state and prove Lemma 5.6 below, which is an application of Lemma 5.3. It makes use of the classification of irreducible characters χ of G according to their *Frobenius–Schur indicator* $\epsilon_2(\chi)$. In view of its importance, we first recall the definition and properties of this invariant. If χ denotes the character of a representation ρ of G, the number

$$\epsilon_2(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2)$$

is called the *Frobenius–Schur indicator* of χ. If χ is irreducible, then $\epsilon_2(\chi) \in \{-1, 0, 1\}$ (see [Huppert 1998, Theorem 8.7]), and each of these three possible values has a precise meaning in terms of the $\mathbb{R}$-rationality of χ and ρ, as we now recall; see, e.g., [Huppert 1998, Theorem 13.1] for a proof.

Theorem 5.5 (Frobenius, Schur). *Let G be a finite group, and let $\chi \in \mathrm{Irr}(G)$ be the character of an irreducible complex representation $\rho \colon G \to \mathrm{GL}(V)$:*

(1) *If $\epsilon_2(\chi) = 0$, then $\chi \neq \overline{\chi}$, χ is not the character of an $\mathbb{R}[G]$-module, and there does not exist a G-invariant, $\mathbb{C}$-bilinear form $\neq 0$ on V. We say that ρ is a unitary representation.*

(2) *If $\epsilon_2(\chi) = 1$, then $\chi = \overline{\chi}$ is the character of some $\mathbb{R}[G]$-module, and there exists a G-invariant, $\mathbb{C}$-bilinear form which is symmetric and nonsingular, unique up to factors in $\mathbb{C}$. We say that ρ is an orthogonal representation.*

(3) *If $\epsilon_2(\chi) = -1$, then $\chi = \overline{\chi}$ is not the character of any $\mathbb{R}[G]$-module, and there exists a G-invariant, $\mathbb{C}$-bilinear form which is skew-symmetric and nonsingular, unique up to factors in $\mathbb{C}$. We say that ρ is a symplectic (or quaternionic) representation.*

In the sequel, we will say that a character is unitary (resp. orthogonal, symplectic) if it is the character of a unitary (resp. orthogonal, symplectic) representation.

Lemma 5.6. *Let L/F be a Galois extension of number fields for which AC and GRH hold. Define $G^+ := \mathrm{Gal}(L/F)$, and let $t^+ \colon G^+ \to \mathbb{R}$ be a class function. For $\ell \in \mathbb{N}$, let $\eta \in \mathcal{S}_\delta$, $\psi \in \mathrm{Irr}(G^+)$, and let $\chi_1, \dots, \chi_{2\ell} \in \{\psi, \overline{\psi}\}$. If ψ is unitary then we have the estimate*

$$\sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_\ell}>0 \\ \gamma_{\chi_{\ell+1}},\dots,\gamma_{\chi_{2\ell}}<0 \\ \forall\gamma\in\mathbb{R}, \\ \#\{k\le 2\ell:\chi_k\in\{\psi,\overline{\psi}\},\gamma_{\chi_k}=\gamma\}=\#\{k\le 2\ell:\chi_k\in\{\psi,\overline{\psi}\},\gamma_{\chi_k}=-\gamma\}}} \prod_{k=1}^{2\ell} \hat{\eta}\left(\frac{\gamma_{\chi_k}}{2\pi}\right) \ge \max\bigl\{\ell!\, b_0(\psi; |\hat{\eta}|^2)^\ell - O_\eta(\ell!^2\ell(\ell-1)b_0(\psi; |\hat{\eta}|^2)^{\ell-1}), 0\bigr\}, \tag{44}$$

where the γ_{χ_j} run through the multiset of imaginary parts of the zeros of $L(s, L/F, \psi)L(s, L/F, \overline{\psi})$ (with multiplicity).

If ψ is either orthogonal or symplectic then we have

$$\sum_{\substack{\gamma_1,\dots,\gamma_\ell>0 \\ \gamma'_1,\dots,\gamma'_\ell<0 \\ \forall\gamma\in\mathbb{R}, \\ \#\{k\le\ell:\gamma_k=\gamma\}=\#\{k\le\ell:\gamma'_k=-\gamma\}}} \prod_{k=1}^{\ell} \hat{\eta}\left(\frac{\gamma_k}{2\pi}\right)\hat{\eta}\left(\frac{\gamma'_k}{2\pi}\right) \ge \max\bigl\{2^{-\ell}\ell!\, b_0(\psi; |\hat{\eta}|^2)^\ell - O_\eta(2^{-\ell}\ell!^2\ell(\ell-1)b_0(\psi; |\hat{\eta}|^2)^{\ell-1}), 0\bigr\},$$

where the $\gamma_1, \dots, \gamma_\ell, \gamma'_1, \dots, \gamma'_\ell$ run through the imaginary parts of the zeros of $L(s, L/F, \psi)$ (with multiplicity).

Proof. We will split the proof into two cases, depending on whether ψ is real-valued (orthogonal or symplectic) or not (unitary). Because of the symmetry properties of zeros of $L(s, L/F, \psi)$, this will lead to two distinct combinatorial approaches.

Let us start with the case where ψ is unitary. In this case ψ and $\overline{\psi}$ are distinct irreducible characters of G. One of the difficulties comes from the fact that some γ may satisfy $L\big(\frac{1}{2}+i\gamma, L/F, \psi\big) = L\big(\frac{1}{2}+i\gamma, L/F, \overline{\psi}\big) = 0$. We have

$$\#\{k \leq 2\ell : \chi_k \in \{\psi, \overline{\psi}\}, \gamma_{\chi_k} = \gamma\} = \#\{k \leq 2\ell : \chi_k \in \{\psi, \overline{\psi}\}, \gamma_{\chi_k} = -\gamma\}.$$

We define the multisets

$$\Gamma_1(\psi) := \big\{\gamma > 0\colon L\big(\tfrac{1}{2}+i\gamma, L/F, \psi\big) = L\big(\tfrac{1}{2}-i\gamma, L/F, \psi\big) = 0\big\}$$

and

$$\Gamma_2(\psi) := \big\{\gamma > 0\colon L\big(\tfrac{1}{2}+i\gamma, L/F, \psi\big) = 0, \quad L\big(\tfrac{1}{2}-i\gamma, L/F, \psi\big) \neq 0\big\},$$

so that $\Gamma_1(\psi) \cap \Gamma_2(\psi) = \varnothing$, $\Gamma_2(\psi) \cap \Gamma_2(\overline{\psi}) = \varnothing$, and $\Gamma_1(\psi) \cup \Gamma_2(\psi)$ (respectively $\Gamma_1(\psi) \cup \Gamma_2(\overline{\psi})$) is a multiset whose elements are the positive imaginary parts of the nontrivial zeros of $L(s, L/F, \psi)$ (respectively $L(s, L/F, \overline{\psi})$). In the multiset $\Gamma_1(\psi)$, we define the multiplicity associated to γ as the sum of the multiplicity of $\frac{1}{2}+i\gamma$ for $L(s, L/F, \psi)$ and the multiplicity of $\frac{1}{2}-i\gamma$ for $L(s, L/F, \psi)$. Note that $\Gamma_1(\psi) = \Gamma_1(\overline{\psi})$. Now, among the γ_{χ_k} in the sum on the left-hand side of (44), there are $2r$ elements in $\Gamma_1(\psi)$ where $0 \leq r \leq \ell$. Thus we can write

$$\sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_\ell} > 0 \\ \gamma_{\chi_{\ell+1}},\dots,\gamma_{\chi_{2\ell}} < 0 \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \leq 2\ell : \chi_k \in \{\psi, \overline{\psi}\}, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \leq 2\ell : \chi_k \in \{\psi, \overline{\psi}\}, \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2\ell} \hat{\eta}\bigg(\frac{\gamma_{\chi_k}}{2\pi}\bigg)$$

$$= \sum_{r=0}^{\ell} \binom{\ell}{r}^2 \Bigg(\sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_r} \in \Gamma_1(\psi) \\ \gamma_{\chi_{r+1}},\dots,\gamma_{\chi_{2r}} \in -\Gamma_1(\psi) \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \leq 2r : \gamma_{\chi_k} = \gamma\} = \\ \#\{k \leq 2r : \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2r} \hat{\eta}\bigg(\frac{\gamma_{\chi_k}}{2\pi}\bigg)\Bigg) \Bigg(\sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{\ell-r}} \in \Gamma_2(\psi) \cup \Gamma_2(\overline{\psi}) \\ \gamma_{\chi_{\ell-r+1}},\dots,\gamma_{\chi_{2\ell-2r}} \in -(\Gamma_2(\psi) \cup \Gamma_2(\overline{\psi})) \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \leq 2\ell-2r : \chi_k = \psi, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \leq 2\ell-2r : \chi_k = \overline{\psi}, \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2\ell-2r} \hat{\eta}\bigg(\frac{\gamma_{\chi_k}}{2\pi}\bigg)\Bigg). \tag{45}$$

Here, we use the convention that when $r = 0$, the first sum is equal to 1 whereas when $r = \ell$, the second sum is equal to 1.

Reindexing the innermost sum in (45), we see that

$$\sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{\ell-r}} \in \Gamma_2(\psi) \cup \Gamma_2(\overline{\psi}) \\ \gamma_{\chi_{\ell-r+1}},\dots,\gamma_{\chi_{2\ell-2r}} \in -(\Gamma_2(\psi) \cup \Gamma_2(\overline{\psi})) \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \leq 2\ell-2r : \chi_k = \psi, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \leq 2\ell-2r : \chi_k = \overline{\psi}, \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2\ell-2r} \hat{\eta}\bigg(\frac{\gamma_{\chi_k}}{2\pi}\bigg) = S_{2\ell-2r}(\boldsymbol{a}),$$

where $S_{2\ell-2r}(\boldsymbol{a})$ is defined in Lemma 5.3, with the choices

$$\Gamma := \Gamma_2(\psi) \cup \Gamma_2(\overline{\psi}), \quad a_\gamma := \hat{\eta}\bigg(\frac{\gamma}{2\pi}\bigg).$$

By Lemma 5.3, it is

$$\ge \max\big\{(\ell-r)!\, b_2(\psi;\, |\hat\eta|^2)^{\ell-r} - O_\eta((\ell-r)!^2(\ell-r)(\ell-r-1) b_2(\psi;\, |\hat\eta|^2)^{\ell-r-1}), 0\big\},$$

where $b_2(\psi;\, |\hat\eta|^2)$ is the contribution of $\gamma \in \Gamma_2(\psi) \cup \Gamma_2(\overline{\psi})$ in $b_0(\psi;\, |\hat\eta|^2)$ so that

$$b_0(\psi;\, |\hat\eta|^2) + b_0(\overline{\psi};\, |\hat\eta|^2) = b_1(\psi;\, |\hat\eta|^2) + b_2(\psi;\, |\hat\eta|^2),$$

with

$$b_1(\psi;\, |\hat\eta|^2) = 2 \sum_{\gamma \in \Gamma_1(\psi)} \left| \hat\eta\left(\frac{\gamma}{2\pi}\right)\right|^2, \quad b_2(\psi;\, |\hat\eta|^2) = 2 \sum_{\gamma \in \Gamma_2(\psi) \cup \Gamma_2(\overline{\psi})} \left| \hat\eta\left(\frac{\gamma}{2\pi}\right)\right|^2.$$

In the same fashion, we may estimate the first bracketed sum on the right-hand side of (45) using Lemma 5.3, with the choices

$$\Gamma := \Gamma_1(\psi), \quad a_\gamma := \hat\eta\left(\frac{\gamma}{2\pi}\right).$$

By the same argument, the first sum is

$$\ge \max\{r!\, b_1(\psi;\, |\hat\eta|^2)^r - O_\eta(r!^2 r(r-1) b_1(\psi;\, |\hat\eta|^2)^{r-1}), 0\}.$$

Summing over r yields the claimed estimate.

If ψ is either orthogonal or symplectic, then it is real-valued and thus the combinatorics are simpler in this case. Indeed, the claimed bound follows at once from Lemma 5.3 with the choices

$$\Gamma := \big\{\gamma > 0 : L\big(\tfrac{1}{2} + i\gamma, L/F, \psi\big) = 0\big\}, \quad a_\gamma := \hat\eta\left(\frac{\gamma}{2\pi}\right). \qquad \square$$

Lemma 5.7. *Let L/F be a Galois extension of number fields for which AC and GRH hold. Define $G^+ := \mathrm{Gal}(L/F)$, and let $t^+ \colon G^+ \to \mathbb{R}$ be a class function. Assume that $\hat t^+ \in \mathbb{R}_{\ge 0}$ and let $\eta \in \mathcal{S}_\delta$, $\Phi \in \mathcal{U}$. For $m \in \mathbb{N}$, we have the lower bound*

$$\widetilde{D}_{2m}(U, L/F;\, t^+, \eta, \Phi) \ge \mu_{2m} \nu(L/F, t^+;\, \eta)^m \big(1 + O_\eta(m^2 m!\, w_4(L/F, t^+;\, \eta))\big),$$

where we recall (7) *and*

$$w_4(L/F, t^+;\, \eta) := \frac{\sum_{\chi \in \mathrm{Irr}(G^+)} |\hat t^+(\chi)|^4 b_0(\chi;\, \hat\eta^2)}{\big(\sum_{\chi \in \mathrm{Irr}(G^+)} |\hat t^+(\chi)|^2 b_0(\chi;\, \hat\eta^2)\big)^2}. \tag{46}$$

Proof. Firstly, in (34), we may replace $\mathrm{Irr}(G^+)$ by $C_t := \mathrm{supp}(\widehat{t^+}) \subset \mathrm{Irr}(G^+)$. For simplicity, let us write (since t is real-valued)

$$C_t = \{\psi_1, \psi_2, \dots, \psi_{r_1}, \psi_{r_1+1}, \overline{\psi_{r_1+1}}, \psi_{r_1+2}, \dots, \psi_{r_1+r_2}, \overline{\psi_{r_1+r_2}}\},$$

where $\psi_1, \dots \psi_{r_1}$ are real and $\psi_{r_1+1}, \dots, \psi_{r_1+r_2}$ are complex. Note that C_t depends only on G and t, and $r_1 + 2r_2 = |C_t|$. Given a vector $\boldsymbol{\chi} = (\chi_1, \dots \chi_{2m}) \in (C_t)^{2m}$, define

$$E_j(\boldsymbol{\chi}) := \{1 \le k \le 2m \colon \chi_k \in \{\psi_j, \overline{\psi_j}\}\} \quad (1 \le j \le r_1 + r_2),$$

$\ell_j(\boldsymbol{\chi}) := |E_j(\boldsymbol{\chi})|$. Note that $\sum_{j=1}^{r_1+r_2} \ell_j(\boldsymbol{\chi}) = 2m$.

Secondly, by positivity of $\widehat{t^+}$ and $\hat{\eta}$, we may obtain a lower bound on $\widetilde{D}_{2m}(U, L/F; t^+, \eta, \Phi)$ by restricting the sum over characters to those $\boldsymbol{\chi} = (\chi_1, \dots, \chi_{2m})$ that are elements of $(C_t)^{2m}$ and $(\gamma_{\chi_1}, \dots, \gamma_{\chi_{2m}})$ for which for any $j \leq r_1 + r_2$ and $\gamma \in \mathbb{R}$ we have

$$|\{k \in E_j(\boldsymbol{\chi})\colon \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = \gamma\}| = |\{k \in E_j(\boldsymbol{\chi})\colon \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = -\gamma\}|.$$

Finally, we may further impose that $k_j(\boldsymbol{\chi}) := \frac{1}{2}\ell_j(\boldsymbol{\chi}) \in \mathbb{N}$, and we may restrict the sum over characters to the subset $\mathcal{C}_{t,2m}$ of vectors of characters $\boldsymbol{\chi} = (\chi_1, \dots, \chi_{2m}) \in C_t^{2m}$ which satisfy $|\{\ell \leq 2m : \chi_\ell = \psi_j\}| = |\{\ell \leq 2m : \chi_\ell = \overline{\psi_j}\}|$, for every $r_1 + 1 \leq j \leq r_1 + r_2$. We will also use the fact that for any $j \leq r_1 + r_2$ and for all $(\chi_1, \dots, \chi_{2k_j})$ and $(\gamma_{\chi_1}, \dots, \gamma_{\chi_{2k_j}})$ appearing in the index set of the double sum (34), we have that

$$\begin{aligned}\#\{\ell \in E_j(\boldsymbol{\chi})\} &= \sum_{\gamma \in \mathbb{R}_{>0}} \#\{\ell\colon \chi_\ell \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_\ell} = \gamma\} + \sum_{\gamma \in \mathbb{R}_{<0}} \#\{\ell\colon \chi_\ell \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_\ell} = \gamma\} \\ &= 2 \sum_{\gamma \in \mathbb{R}_{>0}} \#\{\ell\colon \chi_\ell \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_\ell} = \gamma\}.\end{aligned}$$

As a result, one deduces the following lower bound:

$$\begin{aligned}\widetilde{D}_{2m}(U, L/F; t^+, \eta, \Phi) \geq \frac{1}{2\int_0^\infty \Phi} &\sum_{\substack{\boldsymbol{\chi} = (\chi_1, \dots, \chi_{2m}) \in \mathcal{C}_{t,2m} \\ \forall j, k_j(\boldsymbol{\chi}) \in \mathbb{N}}} \biggl(\prod_{j=1}^{2m} \hat{t}^+(\chi_j)\biggr) \\ &\times \sum_{\substack{\gamma_{\chi_1}, \dots, \gamma_{\chi_{2m}} \neq 0 \\ \#\{k \in E_j(\boldsymbol{\chi}): \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \in E_j(\boldsymbol{\chi}): \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = -\gamma\}}} \widehat{\Phi}\Bigl(\frac{U}{2\pi}(\gamma_{\chi_1} + \cdots + \gamma_{\chi_{2m}})\Bigr) \prod_{j=1}^{2m} \hat{\eta}\Bigl(\frac{\gamma_{\chi_j}}{2\pi}\Bigr).\end{aligned}$$

At this point, we notice that the conditions in the inner sum automatically imply that $\gamma_{\chi_1} + \cdots + \gamma_{\chi_n} = 0$, resulting in the bound

$$\widetilde{D}_{2m}(U, L/F; t^+, \eta, \Phi) \geq \sum_{\substack{\boldsymbol{\chi} = (\chi_1, \dots, \chi_{2m}) \in \mathcal{C}_{t,2m} \\ \forall j, k_j(\boldsymbol{\chi}) \in \mathbb{N}}} \biggl(\prod_{j=1}^{2m} \hat{t}^+(\chi_j)\biggr) \sum_{\substack{\gamma_{\chi_1}, \dots, \gamma_{\chi_{2m}} \neq 0 \\ \forall j \leq r_1 + r_2, \forall \gamma \in \mathbb{R}, \\ \#\{k \in E_j(\boldsymbol{\chi}): \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \in E_j(\boldsymbol{\chi}): \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = -\gamma\}}} \prod_{j=1}^{2m} \hat{\eta}\Bigl(\frac{\gamma_{\chi_j}}{2\pi}\Bigr).$$

Next we stratify the first sum according to the values assumed by $k_j(\boldsymbol{\chi})$. Given a vector $\boldsymbol{k} = (k_1, \dots, k_{r_1+r_2}) \in \mathbb{N}^{r_1+r_2}$ such that $k_1 + \cdots + k_{r_1+r_2} = m$, we need to evaluate the sum

$$D(\boldsymbol{k}) := \sum_{\substack{\boldsymbol{\chi} = (\chi_1, \dots, \chi_{2m}) \in \mathcal{C}_{t,2m} \\ \forall j, k_j(\boldsymbol{\chi}) = k_j}} \biggl(\prod_{j=1}^{2m} \hat{t}^+(\chi_j)\biggr) \sum_{\substack{\gamma_{\chi_1}, \dots, \gamma_{\chi_{2m}} \neq 0 \\ \forall j \leq r_1 + r_2, \forall \gamma \in \mathbb{R}, \\ \#\{k \in E_j(\boldsymbol{\chi}): \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \in E_j(\boldsymbol{\chi}): \chi_k \in \{\psi_j, \overline{\psi_j}\}, \gamma_{\chi_k} = -\gamma\}}} \prod_{j=1}^{2m} \hat{\eta}\Bigl(\frac{\gamma_{\chi_j}}{2\pi}\Bigr).$$

Now, note that since t^+ and $\hat{t}^+$ are real-valued, we have that

$$\hat{t}^+(\chi)\hat{t}^+(\overline{\chi}) = \hat{t}^+(\chi)\overline{\hat{\bar{t}}(\chi)} = (\hat{t}^+(\chi))^2.$$

Hence, after reindexing we obtain the identity

$$D(\boldsymbol{k}) = \binom{2m}{2k_1, \dots, 2k_{r_1+r_2}} \prod_{j=1}^{r_1+r_2} \Bigg((\hat{t}^+(\psi_j))^{2k_j} \sum_{\substack{(\chi_1,\dots,\chi_{2k_j}) \in \mathcal{C}_{t,2k_j} \\ \forall \ell \leq 2k_j, \chi_\ell \in \{\psi_j, \overline{\psi_j}\}}} \sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{2k_j}} \neq 0 \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \leq 2k_j : \gamma_{\chi_k} = \gamma\} = \\ \#\{k \leq 2k_j : \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2k_j} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big)\Bigg).$$

Let us now evaluate the inner sum

$$\sigma_j(k_j) := \sum_{\substack{(\chi_1,\dots,\chi_{2k_j}) \in \mathcal{C}_{t,2k_j} \\ \forall \ell \leq 2k_j, \chi_\ell \in \{\psi_j, \overline{\psi_j}\}}} \sum_{\substack{\gamma_{\chi_1},\dots,\gamma_{\chi_{2k_j}} \neq 0 \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \leq 2k_j :\, \gamma_{\chi_k} = \gamma\} = \\ \#\{k \leq 2k_j :\, \gamma_{\chi_k} = -\gamma\}}} \prod_{k=1}^{2k_j} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big).$$

Reindexing, we obtain the identity

$$\sigma_j(k_j) = \binom{2k_j}{k_j} \sum_{\substack{\gamma_1,\dots,\gamma_{k_j} > 0, \gamma'_1,\dots,\gamma'_{k_j} < 0 \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \leq k_j : \gamma_k = \gamma\} = \#\{k_j < k \leq 2k_j : \gamma'_k = -\gamma\}}} \prod_{k=1}^{k_j} \hat{\eta}\Big(\frac{\gamma_k}{2\pi}\Big) \eta\Big(\frac{\gamma'_k}{2\pi}\Big),$$

where the γ_j and the γ'_j are running over the positive (respectively negative) imaginary parts of the zeros of $L(s, L/K, \psi_j)L(s, L/K, \overline{\psi_j})$. Applying Lemma 5.6, we deduce that for $j \geq r_1 + 1$ (i.e., ψ_j is unitary),

$$\sigma_j(k_j) \geq 2^{k_j} \mu_{2k_j} b_0(\psi_j; |\hat{\eta}|^2)^{k_j} \max\bigg\{1 - O_\eta\bigg(\frac{k_j!\, k_j(k_j - 1)}{b_0(\psi_j; |\hat{\eta}|^2)}\bigg), 0\bigg\},$$

since

$$\binom{2k_j}{k_j} k_j! = 2^{k_j} \mu_{2k_j}.$$

Now, if ψ_j is either orthogonal or symplectic (i.e., $j \leq r_1$), then we may fix the sign of the imaginary parts γ_{χ_j} and deduce that

$$\sigma_j(k_j) = \binom{2k_j}{k_j} \sum_{\substack{\gamma_1,\dots,\gamma_{k_j} > 0, \gamma'_1,\dots,\gamma'_{k_j} < 0 \\ \forall \gamma \in \mathbb{R}, \\ \#\{k \leq k_j : \gamma_k = \gamma\} = \#\{k_j < k \leq 2k_j : \gamma'_k = -\gamma\}}} \prod_{k=1}^{2k_j} \hat{\eta}\Big(\frac{\gamma_{\chi_k}}{2\pi}\Big).$$

We invoke Lemma 5.6 once more and deduce the bound

$$\sigma_j(k_j) \geq \mu_{2k_j} b_0(\psi_j; |\hat{\eta}|^2)^{k_j} \max\bigg\{1 - O_\eta\bigg(\frac{k_j!\, k_j(k_j - 1)}{b_0(\psi_j; |\hat{\eta}|^2)}\bigg), 0\bigg\}.$$

Putting everything together, we deduce the overall bound

$$\widetilde{D}_{2m}(U, L/F; t^+, \eta, \Phi) \geq \sum_{\substack{k_1,\dots,k_{r_1+r_2} \in \mathbb{N} \\ k_1 + \cdots + k_{r_1+r_2} = m}} \binom{2m}{2k_1, \dots, 2k_{r_1+r_2}} \prod_{\ell=1}^{r_1} (\mu_{2k_\ell} \hat{t}^+(\psi_j)^{2k_\ell} b_0(\psi_\ell; |\hat{\eta}|^2)^{k_\ell})$$
$$\times \prod_{\ell=r_1+1}^{r_1+r_2} (2^{k_\ell} \mu_{2k_\ell} \hat{t}^+(\psi_\ell)^{2k_\ell} b_0(\psi_\ell; |\hat{\eta}|^2)^{k_\ell}) \prod_{\ell=1}^{r_1+r_2} \max\bigg\{1 - O_\eta\bigg(\frac{k_\ell!\, k_\ell(k_\ell - 1)}{b_0(\psi_\ell; |\hat{\eta}|^2)}\bigg), 0\bigg\}. \quad (47)$$

Let us first evaluate the main term in this expression. By the identity

$$\binom{2m}{2k_1,\dots,2k_{r_1+r_2}}\prod_{j=1}^{r_1+r_2}\mu_{2k_j}=\binom{m}{k_1,\dots,k_{r_1+r_2}}\mu_{2m}$$

and the multinomial theorem, the main term is equal to

$$\mu_{2m}\biggl(\sum_{\ell=1}^{r_1}\hat{t}^+(\psi_\ell)^2 b_0(\psi_\ell;|\hat{\eta}|^2)+2\sum_{\ell=r_1}^{r_1+r_2}\hat{t}^+(\psi_\ell)^2 b_0(\psi_\ell;|\hat{\eta}|^2)\biggr)^m=\mu_{2m}\nu(L/F,t^+;\eta)^m,$$

which is equal to the claimed main term.

As for the error terms in (47), recall first that they vanish whenever $k_\ell\in\{0,1\}$ (see Remark 5.4). Next we handle the contribution of indices $k_j\geq 2$ to the error terms. Using the identity

$$\prod_{\ell=1}^{r_1+r_2}\max\{1-x_\ell,0\}\geq 1-\sum_{j=1}^{r_1+r_2}x_j\quad(x_\ell\geq 0),$$

we see that we need to multiply the main term in (47) by

$$\prod_{\ell=1}^{r_1+r_2}\max\biggl\{1+O\biggl(\frac{k_\ell!\,k_\ell(k_\ell-1)}{b_0(\psi_\ell;|\hat{\eta}|^2)}\biggr),0\biggr\}\geq 1+O\biggl(\sum_{\substack{j=1\\k_j\geq 2}}^{r_1+r_2}\frac{k_j!\,k_j(k_j-1)}{b_0(\psi_j;|\hat{\eta}|^2)}\biggr).$$

We obtain an error term which is

$$\ll\mu_{2m}\sum_{j=1}^{r_1+r_2}\frac{1}{b_0(\psi_j,|\hat{\eta}|^2)}\sum_{\substack{k_1,\dots,k_{r_1+r_2}\in\mathbb{N}\\k_1+\cdots+k_{r_1+r_2}=m\\k_j\geq 2}}k_j!\,k_j(k_j-1)\binom{m}{k_1,\dots,k_{r_1+r_2}}$$
$$\times\prod_{\ell=1}^{r_1}(\hat{t}^+(\psi_\ell)^{2k_\ell}b_0(\psi_\ell;|\hat{\eta}|^2)^{k_\ell})\prod_{\ell=r_1+1}^{r_1+r_2}(2^{k_\ell}\hat{t}^+(\psi_\ell)^{2k_\ell}b_0(\psi_\ell;|\hat{\eta}|^2)^{k_\ell}).$$

Finally, notice that

$$k_j(k_j-1)\binom{m}{k_1,\dots,k_{r_1+r_2}}=m(m-1)\binom{m-2}{k_1,\dots,k_j-2,\dots,k_{r_1+r_2}},$$

and hence the error term above is

$$\ll m^2m!\,\mu_{2m}\biggl(\sum_{j=1}^{r_1+r_2}\hat{t}^+(\psi_j)^4 b_0(\psi_j;|\hat{\eta}|^2)\biggr)\biggl(\sum_{\ell=1}^{r_1}\hat{t}^+(\psi_\ell)^2 b_0(\psi_\ell;|\hat{\eta}|^2)+2\sum_{\ell=r_1}^{r_1+r_2}\hat{t}^+(\psi_\ell)^2 b_0(\psi_\ell;|\hat{\eta}|^2)\biggr)^{m-2}$$
$$\ll\mu_{2m}\nu(L/F,t^+;\eta)^{m-2}m^2m!\biggl(\sum_{j=1}^{r_1+r_2}\hat{t}^+(\psi_j)^4 b_0(\psi_j;|\hat{\eta}|^2)\biggr).\qquad\square$$

Proof of Theorem 1.1. The claimed bound (9) follows from combining Lemmas 5.2 and 5.7. □

Proof of Theorem 1.4. The first part follows from Lemmas 4.2 and 4.5. More precisely, the bound

$$\sum_{\chi\in\mathrm{Irr}(G^+)}|\hat{t}^+(\chi)|^4 b_0(\chi;\hat{\eta}^2)\ll_\eta\sum_{\chi\in\mathrm{Irr}(G^+)}|\hat{t}(\chi)|^4\log(A(\chi)+2)$$

follows directly from Lemma 4.2.

Next (12) follows from Lemma 4.3. We will also apply this lemma to prove the last claimed bound on $w_4(L/F, t^+; \eta)$. Note that by Lemmas 3.2 and 4.2 we have the upper bound

$$\sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}^+(\chi)|^4 b_0(\chi; \hat{\eta}^2) \ll_\eta \lambda_{1,4}(t^+)[F : \mathbb{Q}] \log(\mathrm{rd}_L + 2).$$

Lemma 4.3 then implies that

$$w_4(L/F, t^+; \eta) \ll_\eta \frac{1}{[F : \mathbb{Q}] \log(\mathrm{rd}_L + 2)} \frac{\lambda_{1,4}(t^+)}{\lambda_{1,2}(t^+)^2} \left(1 - S_{t^+} - O\left(\frac{1}{\log_2(\mathrm{rd}_L + 2)}\right)\right)^{-2}.$$

Moreover, we have the trivial bound

$$\frac{\lambda_{1,4}(t^+)}{\lambda_{1,2}(t^+)^2} \le \frac{\lambda_{2,4}(t^+)}{\lambda_{1,2}(t^+)^2} \le 1.$$

The result follows. □

Finally, we prove Corollaries 1.10 and 1.11.

Proof of Corollary 1.10. We will argue by contradiction. Assume otherwise that for all large enough x,

$$|\psi(x; L/K, t) - \hat{t}(1)x| \le \varepsilon(x) x^{1/2} C_{F,L,t^+}^{1/2},$$

where

$$C_{F,L,t^+} = [F : \mathbb{Q}] \log(\mathrm{rd}_L) \lambda_{1,2}(t^+) \left(1 - S_{t^+} - \frac{A}{\log_2(\mathrm{rd}_L + 2)}\right),$$

$A > 0$ is an absolute and large enough constant and $\varepsilon(x)$ monotonically tends to zero as x tends to ∞. Let $\eta = \eta_0 \star \eta_0$, where η_0 is a nontrivial smooth even function supported in $[-1, 1]$. We then have that for large enough x,

$$\begin{aligned}\psi_\eta(x; L/K, t) - \hat{t}(1) x^{1/2} \mathcal{L}_\eta\left(\tfrac{1}{2}\right) &= \int_0^\infty \frac{\eta(\log(y/x))}{y^{1/2}} \mathrm{d}(\psi(y; L/K, t) - \hat{t}(1)y) \\ &= -\int_{\mathrm{e}^{-2}x}^{\mathrm{e}^2 x} \frac{\eta'(\log(y/x)) - \frac{1}{2}\eta(\log(y/x))}{y^{3/2}} (\psi(y; L/K, t) - \hat{t}(1)y)\, \mathrm{d}y \\ &\ll \varepsilon(\mathrm{e}^{-2}x) C_{F,L,t^+}^{1/2}.\end{aligned}$$

Now, for any large enough $0 < U_1 < U_2$, this implies the bound

$$\int_{U_1}^{U_2} \left(\psi_\eta(\mathrm{e}^u; L/K, t) - \hat{t}(1)\mathrm{e}^{u/2}\mathcal{L}_\eta\left(\tfrac{1}{2}\right)\right)^2 \mathrm{d}u \ll \varepsilon(\mathrm{e}^{-2}\mathrm{e}^{U_1})^2 (U_2 - U_1) C_{F,L,t^+}.$$

Moreover, (32) implies that

$$\psi_\eta(\mathrm{e}^u; L/K, t) = \psi_\eta(\mathrm{e}^u; L/F, t^+) = \sum_{\chi \in \mathrm{Irr}(G^+)} \hat{t}^+(\chi) \psi_\eta(\mathrm{e}^u; L/F, \chi).$$

We may apply Lemma 4.1 in which we can bound the second term on the right-hand side trivially (under GRH), resulting in the overall bound (recall that $\hat{t}(1) = \widehat{t^+}(1)$)

$$\psi_\eta(\mathrm{e}^u; L/K, t) - \hat{t}(1)\mathrm{e}^{u/2}\mathcal{L}_\eta(\tfrac{1}{2}) \ll \sum_{\chi \in \mathrm{Irr}(G^+)} |\hat{t}^+(\chi)| \log(A(\chi)+2) \ll \lambda_{1,1}(t^+)[F:\mathbb{Q}]\log(\mathrm{rd}_L+2).$$

This then implies that

$$\int_0^{U_1} \big(\psi_\eta(\mathrm{e}^u; L/K, t) - \hat{t}(1)\mathrm{e}^{u/2}\mathcal{L}_\eta\big(\tfrac{1}{2}\big)\big)^2\,\mathrm{d}u \ll U_1(\lambda_{1,1}(t^+)[F:\mathbb{Q}]\log(\mathrm{rd}_L+2))^2.$$

As a result, picking any even integrable function Φ supported in $[-1, 1]$, we deduce that

$$M_2(U_2, L/K, t, \eta, \Phi) \ll \frac{U_1}{U_2}(\lambda_{1,1}(t^+)[F:\mathbb{Q}]\log(\mathrm{rd}_L))^2 + \varepsilon(\mathrm{e}^{-2}\mathrm{e}^{U_1})^2\frac{U_2-U_1}{U_2}C_{F,L,t^+}.$$

Picking for instance $U_2 = U_1^2$, this will eventually contradict the lower bound in Corollary 1.9 (combined with Theorem 1.4). Indeed, the bound $S_{t^+} \le 1-\kappa(\log_2(\mathrm{rd}_L+2))^{-1}$ implies that rd_L is large enough (since κ itself is large enough), which in turns implies that $w_4(L/F, t^+, \eta)$ is small enough by Theorem 1.4.

We now show that there exists a value $\mathrm{e}^{U_1} \le x \le \mathrm{e}^{U_2}$ such that

$$|\psi(x; L/K, t) - \hat{t}(1)x| \gg x^{1/2}C_{F,L,t^+}^{1/2},$$

where $U_1 = U$ and $U_2 = \beta_{L,F,K,t}U$. Assume otherwise that for all $\varepsilon > 0$ and for all extensions L/K and class functions t, there exists arbitrarily large values of U (depending on ε, L/K and t) for which for all $x \in [\mathrm{e}^{U_1}, \mathrm{e}^{U_2}]$,

$$|\psi(x; L/K, t) - \hat{t}(1)x| \le \varepsilon x^{1/2}C_{F,L,t^+}^{1/2}.$$

One can deduce following the lines above that

$$M_2(\mathrm{e}^{-2}U_2, L/K, t^+, \eta, \Phi) \ll \frac{U_1}{U_2}(\lambda_{1,1}(t^+)[F:\mathbb{Q}]\log(\mathrm{rd}_L))^2 + \varepsilon C_{F,L,t^+}.$$

Once more, this will contradict Corollary 1.9 if

$$\begin{aligned} &U_2 > \kappa_2[F:\mathbb{Q}]\log(\mathrm{rd}_L+2)\log_2(\mathrm{rd}_L+2)\lambda_{1,1}(t^+)^2/\lambda_{1,2}(t^+),\\ &U_1 = \kappa_1 U_2\lambda_{1,2}(t^+)/([F:\mathbb{Q}]\lambda_{1,1}(t^+)^2\log(\mathrm{rd}_L+2)\log_2(\mathrm{rd}_L+2)),\end{aligned}$$

where $\kappa_2 > 0$ is large enough and $\kappa_1 > 0$ is small enough (both in absolute terms). □

Proof of Corollary 1.11. The proof goes along the lines of that of Corollary 1.10. By Lemma 5.1 applied to the tower $L/L/K$ and Lemma 5.2 applied to the trivial tower $L/L/L$,

$$\begin{aligned}\widetilde{M}_n(U, L/K; |G|\mathbf{1}_e, \eta, \Phi) &= \widetilde{M}_n(U, L/L; \mathbf{1}_e, \eta, \Phi)\\ &= \widetilde{D}_n(U, L/L; \mathbf{1}_e, \eta, \Phi) + O\bigg(\frac{(\kappa_\eta[K:\mathbb{Q}]\log(\mathrm{rd}_L+2))^n}{U}\bigg).\end{aligned}$$

Moreover, by Lemma 5.7,

$$\widetilde{D}_{2m}(U, L/L; \mathbf{1}_e, \eta, \Phi) \ge \mu_{2m}\nu(L/L, \mathbf{1}_e; \eta)^m(1 + O_\eta(m^2 m!\, w_4(L/L, \mathbf{1}_e; \eta))),$$

where

$$\nu(L/L, \mathbf{1}_e; \eta) = b_0(\chi_0; \hat{\eta}^2), \quad w_4(L/L, \mathbf{1}_e; \eta) = \frac{1}{b_0(\chi_0; \hat{\eta}^2)}.$$

Now, Lemma 4.2 implies that

$$b(\chi; \hat{\eta}^2) = \hat{h}(0) \log d_L + O_\eta([L:\mathbb{Q}]) = \hat{h}(0) \log d_L \left(1 + O\left(\frac{1}{\log(\mathrm{rd}_L + 2)}\right)\right), \tag{48}$$

resulting in the overall bound

$$\begin{aligned}\widetilde{M}_{2m}&(U, L/K; |G|\mathbf{1}_e, \eta, \Phi)\\ &\geq \mu_{2m}(\hat{h}(0) \log d_L)^m \left(1 + O_\eta\left(\frac{m}{\log(\mathrm{rd}_L + 2)} + \frac{m^2 m!}{\log(d_L + 2)}\right)\right) + O\left(\frac{(\kappa_\eta \log(d_L + 2))^{2m}}{U}\right).\end{aligned}$$

The rest of the proof is similar. □

6. Application to specific extensions and class functions: proofs

This section is dedicated to the proofs of our results for specific Galois extensions, which were stated in Section 2. The statements and their proofs make use of the terminology coming from the classical representation theory of finite groups and we refer the reader, e.g., to [Huppert 1998] or [Serre 1977] for recollections on the necessary background.

6.1. ***Moments for prime ideals in ray class groups.*** We prove Proposition 2.1.

Proof of Proposition 2.1. We apply Theorem 1.1 for $K = F$, and $L = L_{\mathfrak{m}}$. In particular we have $G = G^+ \simeq \mathrm{Cl}_{\mathfrak{m}}(K)$. For the choice $t = h_{K,\mathfrak{m}} \mathbf{1}_{[\mathfrak{a}]}$, where $[\mathfrak{a}]$ is any fixed class in $\mathrm{Cl}_{\mathfrak{m}}(K)$, one computes the norms (6) for all positive integers i, j:

$$\lambda_{i,j}(t) = h_{K,\mathfrak{m}},$$

since $\hat{t}(\chi) = \overline{\chi([\mathfrak{a}])}$ for every irreducible character (all of which have degree 1) of $\mathrm{Cl}_{\mathfrak{m}}(K)$. For the same reason, one has $S_t = 0$ (recall (11)), and if $[\mathfrak{a}] = [\mathfrak{e}]$, then $\hat{t}(\chi)$ is positive (and constant, equal to 1) for every character χ. Therefore applying Theorem 1.4 yields the upper bound

$$w_4(L_{\mathfrak{m}}/K, t; \eta) \ll \frac{1}{\log d_{L_{\mathfrak{m}}}}.$$

As for the variance, Theorem 1.4 gives

$$\left| \frac{\nu(L_{\mathfrak{m}}/K, t; \eta)}{\alpha(|\hat{\eta}|^2) \log d_{L_{\mathfrak{m}}}} - 1 \right| \ll \frac{1}{\log_2(\mathrm{rd}_{L_{\mathfrak{m}}} + 2)}.$$

Putting this together, Theorem 1.1 gives that for fixed $m \in \mathbb{N}$,

$$\begin{aligned}\widetilde{M}_{2m}(U, L_{\mathfrak{m}}/K; t, \eta, \Phi) &\geq \mu_{2m} \nu(L_{\mathfrak{m}}/K, t; \eta)^m (1 + o_{\mathrm{rd}_{L_{\mathfrak{m}}} \to \infty}(1))\\ &\geq \mu_{2m}(\alpha(|\hat{\eta}|^2) \log d_{L_{\mathfrak{m}}})^m (1 + o_{\mathrm{rd}_{L_{\mathfrak{m}}} \to \infty}(1)),\end{aligned}$$

provided $((\log d_{L_{\mathfrak{m}}})^m / U) \to 0$ as $d_{L_{\mathfrak{m}}} \to \infty$. □

6.2. ***D_n*-*examples.*** In this section, we prove Propositions 2.2 and 2.3. With notation as in these statements, we recall that among the $\frac{1}{2}(n+3)$ isomorphism classes of irreducible representations of D_n, exactly two have degree 1: the trivial representation and the lift of the nontrivial character of $D_n/\langle\sigma\rangle$ which is defined by

$$\psi(\sigma^j)=1, \quad \psi(\tau\sigma^k)=-1.$$

The remaining $\frac{1}{2}(n-1)$ irreducible representations of D_n have degree 2; the associated characters are given by

$$\chi_h(\sigma^j)=2\cos(2\pi hj/n), \quad \chi_h(\tau\sigma^k)=0, \quad \big(h\in\big\{1,\dots,\tfrac{1}{2}(n-1)\big\}\big).$$

Proof of Proposition 2.2. First note the following useful fact: for any integer j such that $n\nmid j$ we have

$$\frac{1}{2}\sum_{h=1}^{(n-1)/2}\chi_h(\sigma^j)=\sum_{h=1}^{(n-1)/2}\cos\frac{2\pi hj}{n}=\frac{\sin(\pi j/2-\pi j/(2n))}{\sin(\pi j/n)}\cos\Big(\frac{\pi j}{2}+\frac{\pi j}{2n}\Big)=-\frac{1}{2}. \tag{49}$$

(1) If one considers $t=|D_n|\mathbf{1}_e$, the indicator function of the neutral element of D_n, then $\hat{t}(\chi)=\chi(1)$ for any $\chi\in\mathrm{Irr}(D_n)$ and thus one computes for any $a\in D_n$

$$\sum_{\chi\in\mathrm{Irr}(D_n)}\chi(a)|\hat{t}(\chi)|^2=1+\psi(a)+4\sum_{h=1}^{(n-1)/2}\chi_h(a).$$

If $a=e$, this sum equals $\lambda_{1,2}(t)=2+4(n-1)=4n-2$. If a is in the conjugacy class of τ, then this sum vanishes, and finally if $a=\sigma^j$, then the sum equals -2 by (49). Therefore $S_t=1/(2n-1)$.

(2) Consider the class function $t=\mathbf{1}_{\{\sigma,\sigma^{-1}\}}$ (for which $\hat{t}(\chi)=\chi(\sigma)/n$ for any $\chi\in\mathrm{Irr}(D_n)$). One has for any $a\in D_n$,

$$\sum_{\chi\in\mathrm{Irr}(D_n)}\chi(a)|\hat{t}(\chi)|^2=\frac{1+\psi(a)}{n^2}+\frac{4}{n^2}\sum_{h=1}^{(n-1)/2}\chi_h(a)\Big(\cos\frac{2\pi h}{n}\Big)^2.$$

If a is conjugate to τ then this quantity vanishes. Also, for any $j'\in\big\{1,\dots,\frac{1}{2}(n-1)\big\}$, one has

$$\sum_{\chi\in\mathrm{Irr}(D_n)}\chi(\sigma^{j'})|\hat{t}(\chi)|^2=\frac{2}{n^2}+\frac{8}{n^2}\sum_{h=1}^{(n-1)/2}\cos\frac{2\pi hj'}{n}\Big(\cos\frac{2\pi h}{n}\Big)^2.$$

By linearizing the product on the right-hand side, we see that the maximal value of the left-hand side is attained at $j'=2$. Using (49) we can compute

$$\sum_{\chi\in\mathrm{Irr}(D_n)}\chi(\sigma^2)|\hat{t}(\chi)|^2=\frac{2}{n^2}+\frac{4}{n^2}\sum_{h=1}^{(n-1)/2}\Big(\cos\frac{4\pi h}{n}+\Big(\cos\frac{4\pi h}{n}\Big)^2\Big)=\frac{n-2}{n^2}.$$

Moreover one has

$$\lambda_{1,2}(t)=\sum_{\chi\in\mathrm{Irr}(D_n)}\chi(1)|\hat{t}(\chi)|^2=\frac{2}{n^2}+\frac{4}{n^2}\sum_{h=1}^{(n-1)/2}\Big(1+\cos\frac{4\pi h}{n}\Big)=\frac{2(n-1)}{n^2}.$$

We conclude that $S_t=(1-2/n)/(2(1-1/n))$.

(3) Finally consider $t = 2\mathbf{1}_e + \mathbf{1}_{\{\sigma,\sigma^{-1}\}}$. Unlike $\mathbf{1}_{\{\sigma,\sigma^{-1}\}}$, this class function has nonnegative Fourier coefficients. Indeed one has

$$\hat{t}(1) = \hat{t}(\psi) = \frac{2}{n}, \quad \hat{t}(\chi_h) = \frac{2}{n}\Big(1 + \cos\frac{2\pi h}{n}\Big) = \frac{4}{n}\Big(\cos\frac{4\pi h}{n}\Big)^2 \quad \big(1 \le h \le \tfrac{1}{2}(n-1)\big).$$

Therefore one has for any $a \in D_n$,

$$\sum_{\chi\in\mathrm{Irr}(D_n)} \chi(a)|\hat{t}(\chi)|^2 = \frac{4(1+\psi(a))}{n^2} + \frac{16}{n^2}\sum_{h=1}^{(n-1)/2} \chi_h(a)\Big(\cos\frac{4\pi h}{n}\Big)^4.$$

Using (49), one finds that this sum equals $(2/n)(3-4/n)$ if $a = e$. If a is in the conjugacy class of τ, the sum vanishes. If $a = \sigma^j$ and assuming $n \ge 5$, applying standard trigonometric identities as well as (49), we see that this sum is equal to

$$\frac{2}{n^2} + \frac{32}{n^2}\bigg\{\frac{1}{4}\Big(-\frac{1}{2}\cdot\mathbf{1}_{j\not\equiv -4 \bmod n} + \frac{n-1}{2}\cdot\mathbf{1}_{j\equiv -4 \bmod n}\Big) + \frac{1}{4}\Big(-\frac{1}{2}\cdot\mathbf{1}_{j\not\equiv 4 \bmod n} + \frac{n-1}{2}\cdot\mathbf{1}_{j\equiv 4 \bmod n}\Big)$$
$$+ \frac{1}{16}\Big(-\frac{1}{2}\cdot\mathbf{1}_{j\not\equiv -8 \bmod n} + \frac{n-1}{2}\cdot\mathbf{1}_{j\equiv -8 \bmod n}\Big) + \frac{1}{16}\Big(-\frac{1}{2}\cdot\mathbf{1}_{j\not\equiv 8 \bmod n} + \frac{n-1}{2}\cdot\mathbf{1}_{j\equiv 8 \bmod n}\Big)\bigg\}.$$

Clearly, this quantity is maximized when $j = \pm 4 \bmod n$, in which case it is equal to $(2/n)(2-4/n)$. Overall one concludes that $S_t \le (2-4/n)/(3-4/n) < \frac{2}{3}$. □

Proof of Proposition 2.3. Set $t = |D_n|\mathbf{1}_e$. One has

$$\lambda_{1,1}(t) = \sum_{\chi\in\mathrm{Irr}(D_n)} \chi(1)^2 = |D_n| = 2n, \quad \lambda_{1,4}(t) = \sum_{\chi\in\mathrm{Irr}(D_n)} \chi(1)^5 = 2 + \tfrac{1}{2}(32(n-1)) = 2(8n-7).$$

We apply Theorem 1.4 for $K = F = \mathbb{Q}$ and $L/\mathbb{Q}$ a D_n-extension. Therefore $G^+ = G$ and $t^+ = t$. Moreover AC holds for L since it is a supersolvable extension of $\mathbb{Q}$. Therefore applying Theorem 1.4 we deduce

$$w_4(L/\mathbb{Q}, t; \eta) \ll \frac{1}{n\log \mathrm{rd}_L}.$$

As for the variance, Theorem 1.4 gives

$$\bigg|\frac{\nu(L/\mathbb{Q}, t; \eta)}{\alpha(|\hat{\eta}|^2)(4n-2)\log \mathrm{rd}_L} - 1\bigg| \le \frac{1}{2n-1} + O\Big(\frac{1}{\log_2(\mathrm{rd}_L+2)}\Big).$$

Putting this together, Theorem 1.1 gives that for fixed $m \in \mathbb{N}$,

$$\begin{aligned}\widetilde{M}_{2m}(U, L/\mathbb{Q}; t, \eta, \Phi) &\ge \mu_{2m}\nu(L/K, t; \eta)^m(1 + o_{\mathrm{rd}_L\to\infty}(1))\\ &\ge \mu_{2m}\Big(\alpha(|\hat{\eta}|^2)\Big(2 - \frac{1}{n}\Big)\log d_L\Big)^m(1 + o_{\mathrm{rd}_L\to\infty}(1)),\end{aligned}$$

as soon as $((\log d_L)^m/U) \to 0$ as $d_L \to \infty$. □

6.3. ***Example of a radical extension.*** In this section we prove Propositions 2.4 and 2.5.

Notation is as in Section 2.3. The nontrivial conjugacy classes of G are

$$U := \left\{ \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} : \star \neq 0 \right\}, \quad T_c := \left\{ \begin{pmatrix} c & \star \\ 0 & 1 \end{pmatrix} \star \in \mathbb{F}_p \right\} \quad (c \neq 1).$$

One has $|U| = p - 1$ and $|T_c| = p$ for every $c \in \mathbb{F}_p \setminus \{0, 1\}$. As for the characters of G, exactly $p - 1$ of them have degree 1: these are the lifts of Dirichlet characters χ modulo p

$$\psi_\chi : \left\{ \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} : c \in \mathbb{F}_p^\times, d \in \mathbb{F}_p \right\} \to (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times, \quad \psi_\chi\left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \right) = \chi(c).$$

Finally G has a unique irreducible character ϑ of degree > 1. The character table of G summarizes the information:

	$\{\mathrm{Id}\}$	U	$T_c, c \neq 1$
ψ_χ	1	1	$\chi(c)$
ϑ	$p-1$	-1	0

Proof of Proposition 2.4. Take $t = |G|\mathbf{1}_e$, so that $\hat{t}(\chi) = \chi(1)$ for all $\chi \in \mathrm{Irr}(G)$. Then for any $a \in G$, we have

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(a) |\hat{t}(\chi)^2| = \sum_{\chi \bmod p} \chi(a_{1,1}) + (p-1)^2 \vartheta(a).$$

(Here $a_{1,1}$ denotes the coefficients in position $(1, 1)$ of the matrix $a \in G$.) This sum vanishes at $a \in T_c$ for any c. The value of the sum at $a \in U$ is $-p(p-1)$ and finally, at $a = 1$, the sum is $(p-1) + (p-1)^3$. Therefore

$$S_t = \frac{1}{p(1 - 2/p + 2/p^2)}.$$

Take $t = \vartheta$ which is real-valued with $\hat{t}$ nonnegative. Then

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(a) |\widehat{\vartheta}(\chi)|^2 = \vartheta(a) \quad (a \in G).$$

Therefore $S_\vartheta = 1/(p-1)$. □

Proof of Proposition 2.5. One has

$$\lambda_{1,1}(|G|\mathbf{1}_e) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = p(p-1), \quad \lambda_{1,1}(\vartheta) = \vartheta(1) = p - 1.$$

Moreover in the course of the proof of Proposition 2.4, we have shown that

$$\lambda_{1,2}(|G|\mathbf{1}_e) = (p-1)(1 + (p-1)^2), \quad \lambda_{1,2}(\vartheta) = p - 1.$$

Finally one computes

$$\lambda_{1,4}(|G|\mathbf{1}_e) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^5 = (p-1)(1 + (p-1)^4), \quad \lambda_{1,4}(\vartheta) = \vartheta(1) = p - 1.$$

Let t be either $|G|\mathbf{1}_e$ or ϑ. We apply Theorem 1.4 for $K = F = \mathbb{Q}$, and $L = K_{a,p}$. Therefore $G^+ = G$ and $t^+ = t$. Moreover AC holds for $K_{a,p}$ since it is a supersolvable extension of $\mathbb{Q}$. Finally one has $d_L = |\mathrm{disc}(K_{a,p}/\mathbb{Q})| = p^{p^2-2}a^{(p-1)^2}$; see [Komatsu 1976, end of the proof of the Theorem] and [Westlund 1910, Section 3.I]. Therefore

$$\log d_L = p^2 \log p(1+o_{p\to\infty}(1)), \quad \log \mathrm{rd}_L = (1+o_{p\to\infty}(1))\log p.$$

For every $\eta \in \mathcal{S}_\delta$, the last bound of Theorem 1.4 gives

$$w_4(K_{a,p}/\mathbb{Q}, t; \eta) \ll \frac{1}{p\log \mathrm{rd}_L} = \frac{1}{p\log p}(1+o_{p\to\infty}(1)).$$

As for the variance, Theorem 1.4 gives

$$\left|\frac{\nu(K_{a,p}/\mathbb{Q}, t; \eta)}{\alpha(|\hat{\eta}|^2)\lambda_{1,2}(t)\log \mathrm{rd}_L} - 1\right| \le S_t + O\left(\frac{1}{\log_2(p+2)}\right).$$

Next we use the value of S_t computed in Proposition 2.4: $S_t = o_{p\to\infty}(1)$. Plugging these bounds into (9), we conclude the proof. □

6.4. ***Real parts of characters as class functions.*** In this section we prove Proposition 2.6. We will need the following group theoretic preparatory result.

Lemma 6.1. *Let G be a finite group and let $\rho\colon G \to \mathrm{GL}(V)$ be an irreducible finite dimensional complex representation of G. Let χ be the character of ρ and let $a \in G$. We denote by $[a]$ the class of a in $G/\ker\rho$. Then we have the following equivalences*:

(1) $|\chi(a)| = \chi(1)$ *if and only if* $[a]$ *lies in the center* $Z(G/\ker\rho)$ *of* $G/\ker\rho$.

(2) $|\chi(a)+\overline{\chi(a)}| = 2\chi(1)$ *if and only if* $[a]$ *is an element of order* 1 *or* 2 *in* $Z(G/\ker\rho)$.

Proof. (1) First assume $|\chi(a)| = \chi(1)$. Since $\chi(a)$ is a sum of $\chi(1)$ roots of unity and by the triangle inequality, we obtain that $\rho(a)$ has a unique root of unity as eigenvalue. Being diagonalizable (since the separable polynomial $X^{|G|}-1$ vanishes at $\rho(a)$) we deduce that $\rho(a)$ is a scalar matrix, thus commutes with every element of $\mathrm{End}(V)$. Since ρ induces a faithful representation of $G/\ker\rho$ with representation space V, we conclude that the class of a in $G/\ker\rho$ lies in its center. Conversely, assume $[a]$ commutes with every element of $G/\ker\rho$. Then $\rho(a)$ commutes with every element of $\mathrm{End}(V)$. Since ρ is irreducible, Schur's lemma implies that $\rho(a)$ is a scalar matrix and thus $|\chi(a)| = \chi(1)$.

(2) Since $|\chi(a)| \le \chi(1)$, the equality $|\chi(a)+\overline{\chi(a)}| = 2\chi(1)$ is equivalent to $\chi(a) = \pm\chi(1)$. By (1), this condition on a implies that $[a]$ lies in the center of $G/\ker\rho$ with $\rho(a)$ a scalar matrix of trace $\pm\chi(1)$. In other words $\rho(a) = \pm\,\mathrm{Id}$, i.e., $\rho(a^2) = \mathrm{Id}$. Since ρ induces a faithful representation of $G/\ker\rho$ this is in turn equivalent to $[a]$ having order at most 2 in $Z(G^+/\ker\rho)$. The converse holds since if $[a]$ is an element of order at most 2 in $Z(G/\ker\rho)$, then $\rho(a) = \pm\,\mathrm{Id}$ and therefore $\chi(a) = \pm\chi(1)$. □

Proof of Proposition 2.6. Since $t^+ = (\chi + \overline{\chi}/2)$, then $\widehat{t^+}(\psi) = \frac{1}{2}$ if $\psi \in \{\chi, \overline{\chi}\}$, and $\widehat{t^+}(\psi) = 0$ for every other irreducible character of G^+. We deduce that $S_{t^+} = \max_{a\neq 1}|\chi(a) + \overline{\chi}(a)|/(2\chi(1))$. By

Lemma 6.1(2), we deduce that $S_{t^+} = 1$ if and only if $Z(G/\ker\rho)$ has an element of order 1 or 2. This is in turn equivalent to $\ker\rho = \{e\}$ and $|Z(G^+)|$ odd. □

We see that the particular case where $\mathbb{Q} = F = K$ and $G^+ = \mathrm{Gal}(L/\mathbb{Q})$ admits a faithful irreducible character χ and where $Z(G^+)$ has odd order is precisely that of Section 2.3.

6.5. *S_n-extensions.*

In the section, we prove Proposition 2.7.

Proof of Proposition 2.7. We begin by noting that following [Fiorilli and Jouve 2024, Proof of Lemma 7.4], one can show that Roichman's bound [1996] combined with the hook-length formula imply that for any $\chi \in \mathrm{Irr}(S_n)$,

$$\max_{\mathrm{id}\neq\pi\in S_n} \frac{\chi(\pi)}{\chi(1)} \leq \left(\max\left(q,\, \frac{\log(kn!/\chi(1)) + 2n/\mathrm{e}}{\log n!}\right)\right)^b, \tag{50}$$

where $0 < q < 1$, $k \geq 1$ and $b > 0$ are absolute constants. For simplicity, let us denote $t = t_{C_1,C_2}$. We will apply the bound (50) on characters for which $\chi(1) \geq \|t\|_2(4p(n)^{1/2}\|t\|_1)^{-1}$. Note that

$$\|t\|_2^2 = \frac{n!}{|C_1|} + \frac{n!}{|C_2|}, \quad \|t\|_1 = 2.$$

We may now apply Theorem 1.4, in the generalized form given in Remark 1.7. Setting

$$\Xi_{n;C_1,C_2} := \{\chi \in \mathrm{Irr}(S_n) : \chi(1) \geq \|t\|_2(8p(n)^{1/2})^{-1}\},$$

it follows that for all large enough n,

$$\begin{aligned} S_t(\Xi_{n;C_1,C_2}) &\leq \left(\max\left(q,\, \frac{\log(kn!^{1/2}\min(|C_1|,|C_2|)^{1/2}) + 2n/\mathrm{e}}{\log n!}\right)\right)^b \\ &\leq \max\left(\theta_1,\, \left(1 - \frac{\log(n!/\min(|C_1|,|C_2|))}{2\log n!} + \frac{2 + o_{n\to\infty}(1)}{\mathrm{e}\log n}\right)^b\right) \\ &\leq 1 - \theta_2\frac{\log(n!/\min(|C_1|,|C_2|))}{2\log n!}, \end{aligned}$$

where $0 < \theta_1 < 1$ and $\theta_2 > 0$ are absolute. We now claim that $\lambda_{1,2}(t,\Xi) \gg \lambda_{1,2}(t)$. To see this, we argue as in [Fiorilli and Jouve 2024, Proposition 4.7]. We have the bound

$$\lambda_{1,2}(t, \mathrm{Irr}(G)\setminus\Xi) \leq \frac{\|t\|_2}{8p(n)^{1/2}}\lambda_{0,2}(t) = \frac{\|t\|_2^3}{8p(n)^{1/2}},$$

by Parseval's identity in the form $\lambda_{0,2}(t) = \|t\|_2^2$. Moreover, [Fiorilli and Jouve 2024, (111)] implies that

$$\lambda_{1,2}(t) \geq \frac{\|t\|_2^3}{2\sqrt{2}p(n)^{1/2}\|t\|_1},$$

and as a result we deduce that

$$\lambda_{1,2}(t;\, \Xi_{n;C_1,C_2}) \gg \frac{\|t\|_2^3}{p(n)^{1/2}}.$$

We can now apply Theorem 1.1 to deduce the claimed bound. For the case $t = t_{C_1}$, the proof is identical. □

Acknowledgements

The work of Jouve was partly funded by the ANR through project FLAIR (ANR-17-CE40-0012). The authors would like to thank *Villa La Stella* in Florence for their hospitality and excellent working conditions during a stay in March 2022 where substantial parts of this work were accomplished. Finally we would like to thank the referee for the careful reading of our manuscript and for providing numerous helpful suggestions.

References

[Artin 1931] E. Artin, "Zur Theorie der L-reihen mit allgemeinen Gruppencharakteren", *Abh. Math. Sem. Univ. Hamburg* **8**:1 (1931), 292–306. MR Zbl

[Bellaïche 2016] J. Bellaïche, "Théorème de Chebotarev et complexité de Littlewood", *Ann. Sci. École Norm. Sup.* (4) **49**:3 (2016), 579–632. MR Zbl

[de la Bretèche and Fiorilli 2021] R. de la Bretèche and D. Fiorilli, "On a conjecture of Montgomery and Soundararajan", *Math. Ann.* **381**:1-2 (2021), 575–591. MR Zbl

[de la Bretèche and Fiorilli 2023] R. de la Bretèche and D. Fiorilli, "Moments of moments of primes in arithmetic progressions", *Proc. Lond. Math. Soc.* (3) **127**:1 (2023), 165–220. MR Zbl

[de la Bretèche et al. 2023] R. de la Bretèche, D. Fiorilli, and F. Jouve, "Moments in the Chebotarev density theorem: non-Gaussian families", preprint, 2023. arXiv 2301.12826

[Carneiro et al. 2015] E. Carneiro, V. Chandee, and M. B. Milinovich, "A note on the zeros of zeta and L-functions", *Math. Z.* **281**:1-2 (2015), 315–332. MR Zbl

[Cohen et al. 1998] H. Cohen, F. Diaz y Diaz, and M. Olivier, "Computing ray class groups, conductors and discriminants", *Math. Comp.* **67**:222 (1998), 773–795. MR Zbl

[Fiorilli and Jouve 2024] D. Fiorilli and F. Jouve, "Distribution of Frobenius elements in families of Galois extensions", *J. Inst. Math. Jussieu* **23**:3 (2024), 1169–1258. MR Zbl

[Fiorilli and Martin 2013] D. Fiorilli and G. Martin, "Inequities in the Shanks–Rényi prime number race: an asymptotic formula for the densities", *J. Reine Angew. Math.* **676** (2013), 121–212. MR Zbl

[Hooley 1977] C. Hooley, "On the Barban–Davenport–Halberstam theorem, VII", *J. Lond. Math. Soc.* (2) **16**:1 (1977), 1–8. MR Zbl

[Huppert 1998] B. Huppert, *Character theory of finite groups*, de Gruyter Expo. Math. **25**, de Gruyter, Berlin, 1998. MR Zbl

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc. Colloq. Publ. **53**, Amer. Math. Soc., Providence, RI, 2004. MR Zbl

[Kolmogorov and Fomin 1989] A. N. Kolmogorov and S. V. Fomin, Елементы теории функции и функционалного анализа, 6th ed., "Nauka", Moscow, 1989. MR Zbl

[Komatsu 1976] K. Komatsu, "An integral basis of the algebraic number field $Q(\sqrt{t}a, \sqrt{t}1)$", *J. Reine Angew. Math.* **288** (1976), 152–153. MR Zbl

[Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", pp. 409–464 in *Algebraic number fields: L-functions and Galois properties* (Durham, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR Zbl

[Martinet 1977] J. Martinet, "Character theory and Artin L-functions", pp. 1–87 in *Algebraic number fields: L-functions and Galois properties* (Durham, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR Zbl

[Montgomery and Vaughan 2007] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory, I: Classical theory*, Cambridge Stud. Adv. Math. **97**, Cambridge Univ. Press, 2007. MR Zbl

[Pizarro-Madariaga 2011] A. Pizarro-Madariaga, "Lower bounds for the Artin conductor", *Math. Comp.* **80**:273 (2011), 539–561. MR Zbl

[Roichman 1996] Y. Roichman, “Upper bound on the characters of the symmetric groups”, *Invent. Math.* **125**:3 (1996), 451–485. MR Zbl

[Rubinstein and Sarnak 1994] M. Rubinstein and P. Sarnak, “Chebyshev’s bias”, *Exp. Math.* **3**:3 (1994), 173–197. MR Zbl

[Serre 1977] J.-P. Serre, *Linear representations of finite groups*, Grad. Texts in Math. **42**, Springer, 1977. MR Zbl

[Viviani 2004] F. Viviani, “Ramification groups and Artin conductors of radical extensions of $\mathbb{Q}$”, *J. Théor. Nombres Bordeaux* **16**:3 (2004), 779–816. MR Zbl

[Westlund 1910] J. Westlund, “On the fundamental number of the algebraic number-field $k(\sqrt[p]{m})$”, *Trans. Amer. Math. Soc.* **11**:4 (1910), 388–392. MR Zbl

[Wintner 1941] A. Wintner, “On the distribution function of the remainder term of the prime number theorem”, *Amer. J. Math.* **63** (1941), 233–248. MR Zbl

Communicated by Philippe Michel
Received 2023-02-06 Revised 2023-12-19 Accepted 2024-05-23

regis.de-la-breteche@imj-prg.fr *Institut de Mathématiques de Jussieu-Paris Rive Gauche, Université Paris Cité, Sorbonne Université, CNRS UMR 7586, Paris, France*

daniel.fiorilli@universite-paris-saclay.fr *Institut de mathématiques d’Orsay, Université Paris Saclay, Orsay, France*

florent.jouve@math.u-bordeaux.fr *Université de Bordeaux, CNRS UMR 5251, Bordeaux INP, Talence, France*

ALGEBRA AND NUMBER THEORY 19:3 (2025)
https://doi.org/10.2140/ant.2025.19.521

Abelian varieties over finite fields and their groups of rational points

Stefano Marseglia and Caleb Springer

Over a finite field $\mathbb{F}_q$, abelian varieties with commutative endomorphism rings can be described by using modules over orders in étale algebras. By exploiting this connection, we produce four theorems regarding groups of rational points and self-duality, along with explicit examples. First, when $\operatorname{End}(A)$ is locally Gorenstein, we show that the group structure of $A(\mathbb{F}_q)$ is determined by $\operatorname{End}(A)$. In fact, the same conclusion is attained if $\operatorname{End}(A)$ has local Cohen–Macaulay type at most 2, under the additional assumption that A is ordinary or q is prime, although the conclusion is not true in general. Second, the description in the Gorenstein case is used to characterize cyclic isogeny classes in terms of conductor ideals. Third, going in the opposite direction, we characterize squarefree isogeny classes of abelian varieties with N rational points in which every abelian group of order N is realized as a group of rational points. Finally, we study when an abelian variety A over $\mathbb{F}_q$ and its dual $A^\vee$ satisfy or fail to satisfy several interrelated properties, namely $A \cong A^\vee$, $A(\mathbb{F}_q) \cong A^\vee(\mathbb{F}_q)$, and $\operatorname{End}(A) = \operatorname{End}(A^\vee)$. In the process, we exhibit a sufficient condition for $A \ncong A^\vee$ involving the local Cohen–Macaulay type of $\operatorname{End}(A)$. In particular, such an abelian variety A is not a Jacobian, or even principally polarizable.

1. Introduction

The groups of rational points of abelian varieties defined over a finite field $\mathbb{F}_q$ have recently received a considerable amount of attention. For example, [Howe and Kedlaya 2021] showed that every positive integer occurs as the order of the group of rational points of an abelian variety over $\mathbb{F}_2$. Van Bommel, Costa, Li, Poonen and Smith [van Bommel et al. 2021] proved, among other results, a version of this statement over arbitrary finite fields $\mathbb{F}_q$, although only sufficiently large orders are realizable if $q \geq 7$.

These statement are, in fact, results about isogeny classes. Indeed, two abelian varieties A and B are isogenous over $\mathbb{F}_q$ if and only if $\#A(\mathbb{F}_{q^n}) = \#B(\mathbb{F}_{q^n})$ for all $n \geq 1$, or equivalently if $h_A(x) = h_B(x)$, where $h_A, h_B \in \mathbb{Z}[x]$ are the characteristic polynomials of the Frobenius endomorphisms of A and B, respectively; see [Tate 1966, Theorem 1 (c)]. Moreover, one has $\#A(\mathbb{F}_q) = h_A(1)$.

The results mentioned above concerning cardinalities were upgraded to statements about finite abelian groups in [Marseglia and Springer 2023]: for each q in $\{2, 3, 4, 5\}$, we showed that every finite abelian group is isomorphic to the group of rational points of some abelian variety over $\mathbb{F}_q$. This upgrade, however,

MSC2020: primary 14K15; secondary 11G10, 14G15.
Keywords: abelian variety, finite fields, group of rational points.

does not work on the level of isogeny classes. Indeed, the group structure of $A(\mathbb{F}_q)$ is not uniquely determined by its isogeny class. This phenomenon is observed even for elliptic curves. In this paper, we seek to understand and describe this extra level of structure.

Notation and conventions. Before presenting our main results, we set some notation and conventions. Throughout the paper, all isogenies and morphisms between abelian varieties over $\mathbb{F}_q$ are defined over the base field $\mathbb{F}_q$. In particular, given an abelian variety A over $\mathbb{F}_q$ with characteristic polynomial h, we denote its ($\mathbb{F}_q$-rational) endomorphism ring by $\operatorname{End}(A)$ and its ($\mathbb{F}_q$-)isogeny class by $\mathscr{I}_h$. We say that A and $\mathscr{I}_h$ are *squarefree* if h is a squarefree polynomial. An equivalent definition of squarefree is given by requiring the endomorphism algebra $\operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ to be commutative; see [Tate 1966, Theorem 2 (c)]. See also [Marseglia and Springer 2023, Lemma 2.3] for a comparison with other notions of squarefree.

Given a squarefree isogeny class $\mathscr{I}_h$ over $\mathbb{F}_q$, set $K = \mathbb{Q}[x]/(h)$ and let π be the class of x in K. We will denote by $\mathscr{O}_K$ the maximal order of K. For every A in the isogeny class, as in [Waterhouse 1969, §3.1], we fix an isomorphism $\operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$ which sends the Frobenius endomorphism of A to π. From now on, we will identify $\operatorname{End}(A)$ with its image inside K, which is an order. Under this identification, the Rosati involution of A acts as the complex conjugation $x \mapsto \bar{x}$ in K. Note that $\bar{\pi} = q/\pi$. In particular, if $\operatorname{End}(A) = S \subset K$ then $\operatorname{End}(A^\vee) = \bar{S}$, where $A^\vee$ denotes the dual abelian variety of A.

1.1. ***Groups of rational points and endomorphism rings.*** As noted above, given an abelian variety A over a finite field $\mathbb{F}_q$, the sequence $(\#A(\mathbb{F}_{q^n}))_{n \geq 1}$ of point counts is an isogeny invariant, but the group structure of $A(\mathbb{F}_q)$ is not. One well-known refinement of the isogeny classification is given by classifying the abelian varieties in a given isogeny class according to their endomorphism rings, which are orders in the endomorphism algebra. When E is an elliptic curve over $\mathbb{F}_q$, the group structure of $E(\mathbb{F}_{q^n})$ is uniquely determined for all $n \geq 1$ by the endomorphism ring $\operatorname{End}(E)$; see [Lenstra 1996, Theorem 1].

In Main Theorem 1, we exhibit a similar result for abelian varieties of arbitrary dimension under certain hypotheses on the endomorphism ring which are automatically satisfied in the case of elliptic curves. In particular, we use the notion of the (Cohen–Macaulay) type of an order S at a prime $\mathfrak{p}$. This type, denoted $\operatorname{type}_{\mathfrak{p}}(S)$, is defined as the minimal number of generators of $(S^t)_{\mathfrak{p}} = S^t \otimes_S S_{\mathfrak{p}}$, where $S_{\mathfrak{p}}$ is the localization of S at $\mathfrak{p}$ and S^t is the trace dual ideal of S. The order S is Gorenstein at $\mathfrak{p}$ if $\operatorname{type}_{\mathfrak{p}}(S) = 1$. We say that S is Gorenstein if it is so at every prime. See Section 2 for definitions and details. Recall that an abelian variety A over $\mathbb{F}_q$ is called *ordinary* if the coefficient of $x^{\dim A}$ in the characteristic polynomial $h(x)$ of A is coprime to q.

Main Theorem 1. *Let A be an abelian variety in a squarefree isogeny class $\mathscr{I}_h$ over $\mathbb{F}_q$. Write $S = \operatorname{End}(A)$ and fix $n \geq 1$.*

(a) *If S is Gorenstein at all prime ideals containing $(1 - \pi^n)$, then*

$$A(\mathbb{F}_{q^n}) \cong \frac{S}{(1-\pi^n)S}$$

are isomorphic as S-modules.

(b) *Assume* $\mathscr{I}_h$ *is ordinary* (Ord) *or* $q = p$ *is prime* (CS). *If* $\operatorname{type}_{\mathfrak{p}}(S) \leq 2$ *for every prime* $\mathfrak{p}$ *of* S *above* $(1-\pi^n)$, *then*

$$A(\mathbb{F}_{q^n}) \cong \frac{S}{(1-\pi^n)S}$$

are isomorphic as $\mathbb{Z}$*-modules.*

In contrast, in Example 6.7, we show that it is possible to have $A(\mathbb{F}_q) \not\cong B(\mathbb{F}_q)$ for isogenous abelian varieties A and B over $\mathbb{F}_q$, even if $\operatorname{End}(A) = \operatorname{End}(B)$. This example, like all the others in this paper, has been computed with the help of Magma [Bosma et al. 1997].

Part (a), appearing in the text as Corollary 3.3, is proven by generalizing the methods of [Lenstra 1996; Springer 2021]. Specifically, we view the group of rational points $A(\mathbb{F}_q)$ of an abelian variety A over $\mathbb{F}_q$ as a module over the endomorphism ring $\operatorname{End}(A)$ and use the Gorenstein property to describe the module, as desired.

For Part (b), we use the additional assumptions to consider the abelian variety A itself to “be” a module over $\operatorname{End}(A)$, as we now explain. Deligne [1969] constructed an equivalence between the category of ordinary abelian varieties over a finite field $\mathbb{F}_q$ and the category of free $\mathbb{Z}$-modules with a “Frobenius”-like endomorphism. Centeleghe and Stix [2015] extended Deligne’s result, using a different functor, to the category of abelian varieties over a prime field $\mathbb{F}_p$ whose characteristic polynomial does not have real roots.

Given a squarefree isogeny class $\mathscr{I}_h$ over $\mathbb{F}_q$, we write Ord for the condition that $\mathscr{I}_h$ is ordinary, and CS for the condition that $q = p$ is prime. Note that, if $\mathscr{I}_h$ is squarefree, then the characteristic polynomial h does not have real roots. If we restrict the functor of Deligne (resp. Centeleghe–Stix) to a particular squarefree isogeny class $\mathscr{I}_h$ satisfying Ord (resp. CS), then the modules in the image of the functor are precisely the fractional $\mathbb{Z}[\pi, \bar{\pi}]$-ideals in the endomorphism algebra $K = \mathbb{Q}[x]/(h)$. See Section 6 below or [Marseglia 2021] for a detailed account. In particular, this lends itself to another route for describing groups of rational points in terms of orders and fractional ideals in the endomorphism algebra; see Theorem 6.2. This description allows us to deduce Main Theorem 1 (b), written as Proposition 6.5.

Beyond Main Theorem 1, the techniques and perspectives introduced in this section continue to be used extensively throughout the paper. In Section 2, we recall the necessary background and prove some foundational results regarding orders in étale algebras, which we then use in the remainder of the paper.

1.2. ***Cyclicity.*** In Section 4, we study isogeny classes which are *cyclic*, meaning that every abelian variety in the isogeny class has a cyclic group of points. A criterion for cyclicity which only involves the characteristic polynomial was given in [Giangreco-Maidana 2019, Theorem 2.2]. Although this criterion applies a priori to all isogeny classes, we prove in Theorem 4.3 that an isogeny class over $\mathbb{F}_q$ is cyclic if and only if it contains a variety of the form $A_{\mathrm{sf}} \times A_1$, where A_{sf} is squarefree and A_1 has only one rational point. Moreover, A_1 must be 0-dimensional if $q \geq 5$ by the Weil bounds.

We provide a new criterion for cyclicity, written below as Theorem 4.5.

Main Theorem 2. *Consider a squarefree isogeny class* $\mathscr{I}_h$ *of abelian varieties over* $\mathbb{F}_q$. *Let* π *be the class of* x *in the endomorphism algebra* $K = \mathbb{Q}[x]/(h)$. *The isogeny class* $\mathscr{I}_h$ *is cyclic if and only if* $(1-\pi)\mathbb{Z}[\pi, \bar{\pi}]$ *is coprime to the conductor* $\mathfrak{f} = (\mathbb{Z}[\pi, \bar{\pi}] : \mathscr{O}_K)$.

Rather than relating the property of cyclicity to the coefficients of the characteristic polynomial as in [Giangreco-Maidana 2019], Main Theorem 2 relates cyclicity to the algebraic properties of orders in the endomorphism algebra. In particular, it shows that the property of cyclicity is equivalent to the local maximality of the order $\mathbb{Z}[\pi, \bar{\pi}]$ generated by Frobenius and Verschiebung at all primes over $(1-\pi)$. A key ingredient in our proof is Main Theorem 1 (a), applied to abelian varieties A with maximal endomorphism ring.

1.3. ***Richness and noncyclic groups.*** In contrast to cyclic isogeny classes, we inspect the opposite extreme in Section 5. We say that a squarefree isogeny class $\mathscr{I}_h$ is *rich* if every abelian group of order $h(1)$ occurs as the group of rational points of some abelian variety in $\mathscr{I}_h$. In previous work by the authors, it was shown that, for each $N \geq 1$, there are infinitely many rich squarefree isogeny classes $\mathscr{I}_h$ over $\mathbb{F}_2$ with $N = h(1)$; see [Marseglia and Springer 2023, Theorem 5.3]. These isogeny classes are built from Kedlaya's infinite sets of simple isogeny classes of abelian varieties over $\mathbb{F}_2$ with prescribed numbers of points; see [Kedlaya 2024, Theorem 1.1]. We must use a different technique to find rich isogeny classes in general because there are at most finitely many simple abelian varieties over $\mathbb{F}_q$ with a prescribed number of points N when $q > 2$ [Kadets 2021].

We present a criterion for richness in Main Theorem 3 which is easy to compute using only the characteristic polynomial. An expanded statement is proved as Theorem 5.7, and we compare the conditions of cyclicity and richness for abelian varieties of small dimension over small finite fields in Example 5.9.

Main Theorem 3. *Consider a squarefree isogeny class $\mathscr{I}_h$ of abelian varieties over $\mathbb{F}_q$ of dimension g. Let $K = \mathbb{Q}[x]/(h)$ be the endomorphism algebra, and let π be the class of x. Write*

$$N = h(1) = \prod_{j=1}^{s} \ell_j^{e_j}$$

for the number of rational points on each abelian variety in $\mathscr{I}_h$. The following are equivalent:

(a) *$\mathscr{I}_h$ is rich, that is, every abelian group of order N arises as $A(\mathbb{F}_q)$ for some $A \in \mathscr{I}_h$.*

(b) *For all $1 \leq i \leq 2g$, we have*

$$\frac{h^{(i)}(1)}{i!} \cdot \ell_1^{i-e_1} \cdots \ell_s^{i-e_s} \in \mathbb{Z}.$$

To obtain this theorem, we first prove Lemma 5.4, generalizing [Giangreco-Maidana 2019, Lemma 2.1] which was originally used to study cyclicity. We then deduce Main Theorem 3 by applying [Rybakov 2010, Theorem 1.1]. As a consequence, we also prove that a squarefree isogeny class is rich if and only if its simple factors are rich; see Corollary 5.8.

We conclude Section 5 by proving the existence of certain abelian varieties whose groups of rational points are noncyclic. In particular, we show in Corollary 5.11 that a squarefree isogeny class $\mathscr{I}_h$ over $\mathbb{F}_q$ is noncyclic if q is odd and $h(1)$ is divisible by 4. Finally, we prove the existence of ordinary abelian varieties over $\mathbb{F}_4$ with certain prescribed noncyclic groups of rational points in Theorem 5.13, thereby improving [Marseglia and Springer 2023, Theorem 3.3].

1.4. *Duality.* In Section 7, we turn our attention to the dual $A^\vee$ of an abelian variety A. At the June 2019 AMS Mathematical Research Communities meeting *Explicit Methods in Arithmetic Geometry in Characteristic p*, Bjorn Poonen suggested the problem of finding an abelian variety A defined over a finite field $\mathbb{F}_q$ such that $A(\mathbb{F}_q) \not\cong A^\vee(\mathbb{F}_q)$. In Example 7.2, we find such a variety by using Main Theorem 1 (a). In this example, we observe that A is geometrically simple and $\mathrm{End}(A)$ is a Gorenstein order satisfying $\mathrm{End}(A) \neq \mathrm{End}(A^\vee)$. In Example 7.3, we show that squarefree examples are not rare. We remark that a nonsimple squarefree example was produced in [Rybakov 2014, Example 4.2] using a different method.

Section 7 concludes with a further investigation of the relationships between these properties, along with the properties of being a Jacobian, principally polarizable, or self-dual. More precisely, when A is squarefree, consider the following well-known implications, which are recalled below in Theorem 7.4:

$$\begin{tikzcd}
 & & & A(\mathbb{F}_q) \cong A^\vee(\mathbb{F}_q) \\
A \cong \mathrm{Jac}(C) \arrow[r, Rightarrow] & A \text{ has a principal polarization} \arrow[r, Rightarrow] & A \cong A^\vee \arrow[ur, Rightarrow] \arrow[dr, Rightarrow] & \\
 & & & \mathrm{End}(A) = \mathrm{End}(A^\vee)
\end{tikzcd}$$

Examples 7.5, 7.6 and 7.8, which are likely unsurprising to experts, illustrate that none of the reverse implications are true. Additionally, Example 7.9 exhibits an abelian variety A over $\mathbb{F}_3$ such that $A(\mathbb{F}_3) \cong A^\vee(\mathbb{F}_3)$, but $\mathrm{End}(A) \neq \mathrm{End}(A^\vee)$; hence there is no downward implication on the right side of the diagram. In each case, there are many suitable examples. On the other hand, it is unknown whether there are examples where $A(\mathbb{F}_q) \not\cong A^\vee(\mathbb{F}_q)$ and $\mathrm{End}(A) = \mathrm{End}(A^\vee)$. Observe that, under the hypotheses of either part of Main Theorem 1, $\mathrm{End}(A) = \mathrm{End}(A^\vee)$ implies that $A(\mathbb{F}_q) \cong A^\vee(\mathbb{F}_q)$; see also Proposition 7.1.

Main Theorem 4 provides a sufficient condition for $A \not\cong A^\vee$ which only depends on the properties of the orders in the endomorphism algebra. It is a key ingredient for producing Example 7.8 and may be of independent interest. It is proved in the text as Proposition 7.7.

Main Theorem 4. *Let A be an abelian variety in a squarefree isogeny class $\mathscr{I}_h$ over $\mathbb{F}_q$, let S be an order in $K = \mathbb{Q}[x]/(h)$ such that $S = \bar{S}$, and let $\mathfrak{p}$ be a prime of S satisfying*

$$\mathfrak{p} = \bar{\mathfrak{p}} \quad \textit{and} \quad \mathrm{type}_{\mathfrak{p}}(S) = 2.$$

Assume that A is ordinary (Ord) *or that q is prime* (CS). *If $S \subseteq \mathrm{End}(A)$ and $S_{\mathfrak{p}} = \mathrm{End}(A)_{\mathfrak{p}}$, then $A \not\cong A^\vee$. In particular, such an A is not principally polarizable and cannot be a Jacobian.*

1.5. *Related literature.* We conclude the introduction by mentioning some additional related results. There are several papers on the classification of the groups of rational points of elliptic curves; see for example [Rück 1987; Tsfasman 1985; Tsfasman et al. 2007; Voloch 1988]. The cases of abelian surfaces and threefolds were studied in [David et al. 2014; Kotelnikova 2019; Rybakov 2015; 2012; Xing 1994; 1996]. Additional results about cyclic isogeny classes can be found in [Berardini and Giangreco-Maidana 2022; Giangreco-Maidana 2020].

2. Fractional ideals in orders

In this section we recall definitions and properties of orders and their fractional ideals. These concepts are well known in the context of number fields, but we will work in a more general setting. Additional details and proofs can be found in [Marseglia 2024, Section 2].

Let Z be a Dedekind domain with field of fractions Q. In practice, for the purpose of this paper, it will be enough to consider $Z=\mathbb{Z}$ and $Z=\mathbb{Z}_p$. Let K be a finite *étale algebra* over Q, that is, a finite product of finite separable extensions of Q. A *Z-lattice* L in K is a finitely generated free sub-Z-module of K such that $L\otimes_Z Q=K$. Given two lattices L_1 and L_2 in K, we define the *colon* as

$$(L_1:L_2)=\{x\in K : xL_2\subseteq L_1\}.$$

A *Z-order* S in K is a subring of K which is also a Z-lattice. Observe that K is the total ring of quotients of any Z-order S in K. When no confusion can arise, we will drop the base ring Z from the terminology and simply write lattice and order. When $S\subseteq S'$ are orders in K, the colon $(S:S')$ is called the *conductor* of S in S'.

A *fractional S-ideal* I is a finitely generated S-submodule of K which is also a lattice. Given a lattice L in K, we define its *multiplicator ring* as $(L:L)$. Observe that $(L:L)$ is an order in K, and hence L is a fractional $(L:L)$-ideal.

Given two lattices I and J in K (resp. fractional S-ideals) then the sum $I+J$, the intersection $I\cap J$, the product IJ, and the colon $(I:J)$ are lattices in K (resp. fractional S-ideals).

Let S be an order in K. A *prime* of S is a maximal ideal of S. We denote by $S_{\mathfrak{p}}$ the localization of S at $\mathfrak{p}$, and by $\widehat{S}_{\mathfrak{p}}$ the completion of S at $\mathfrak{p}$. For an S-module M, we put $M_{\mathfrak{p}}=M\otimes_S S_{\mathfrak{p}}$ and $\widehat{M}_{\mathfrak{p}}=M\otimes_S \widehat{S}_{\mathfrak{p}}$. Observe that $\widehat{S}_{\mathfrak{p}}$ is a $\widehat{Z}_p$-order, where p is the contraction of $\mathfrak{p}$ in Z. Also, if I is a fractional S-ideal, then $\widehat{I}_{\mathfrak{p}}$ is a fractional $\widehat{S}_{\mathfrak{p}}$-ideal. We will say that I is *principal at* $\mathfrak{p}$ if $I_{\mathfrak{p}}$ is a principal $S_{\mathfrak{p}}$-module, or, equivalently, $\widehat{I}_{\mathfrak{p}}$ is a principal fractional $\widehat{S}_{\mathfrak{p}}$-ideal. A fractional S-ideal I is called *invertible* if $I(S:I)=S$, or equivalently if it is principal at $\mathfrak{p}$ for every prime $\mathfrak{p}$ of S. See for example [Marseglia 2024, Lemmas 2.12 and 2.17]. Given orders $S\subseteq S'$ in K, we can consider S' as a fractional S-ideal. Lemma 2.1 below tells us when S' is principal at a prime $\mathfrak{p}$ of S.

Lemma 2.1. *Let $S\subseteq S'$ be orders. Given a prime $\mathfrak{p}$ of S, the following statements are equivalent*:

(a) $(S:S')\subseteq\mathfrak{p}$.

(b) ${S'}_{\mathfrak{p}}$ *is not a principal $S_{\mathfrak{p}}$-module.*

(c) $S_{\mathfrak{p}}\neq {S'}_{\mathfrak{p}}$.

Proof. We first prove that ${S'}_{\mathfrak{p}}$ is a principal $S_{\mathfrak{p}}$-module if and only if $S_{\mathfrak{p}}={S'}_{\mathfrak{p}}$. One implication is trivial. For the other, assume that ${S'}_{\mathfrak{p}}=\alpha S_{\mathfrak{p}}$. Hence $\alpha\in {S'}_{\mathfrak{p}}^{\times}$, which shows that

$$S_{\mathfrak{p}}=\frac{1}{\alpha}{S'}_{\mathfrak{p}}={S'}_{\mathfrak{p}}.$$

To conclude, observe that $S_{\mathfrak{p}}\subsetneq {S'}_{\mathfrak{p}}$ if and only if $(S_{\mathfrak{p}}:{S'}_{\mathfrak{p}})\subsetneq S_{\mathfrak{p}}$, which occurs if and only if $(S:S')\subseteq\mathfrak{p}$. □

Later in the paper we will study groups of rational points of abelian varieties over finite fields by describing them in terms of quotients of fractional ideals. In turn, we describe such quotients locally.

Lemma 2.2. *Let $J \subseteq I$ be fractional ideals over an order S. Then we have an isomorphism of S-modules*

$$\frac{I}{J} \simeq \bigoplus_{\mathfrak{p}} \Big(\frac{I}{J}\Big)_{\mathfrak{p}},$$

where the direct sum is over the finitely many primes for which $I_{\mathfrak{p}} \neq J_{\mathfrak{p}}$.

Proof. The quotient I/J is a finitely generated torsion Z-module; see for example [Cohen 2000, Section 1.7]. Hence I/J is an Artinian and Noetherian S-module, so the result follows from [Eisenbud 1995, Theorem 2.13 (b)]. □

Proposition 2.3. *Let $S \subsetneq S'$ be orders. If $r \in S$ is not a zero-divisor and rS is not coprime to the conductor $\mathfrak{f} = (S : S')$, then the quotient $M = S'/rS'$ is not a cyclic S-module.*

Proof. By assumption there exists a maximal ideal $\mathfrak{p}$ of S such that

$$rS + \mathfrak{f} \subseteq \mathfrak{p},$$

which implies

$$rS' + \mathfrak{f} \subseteq \mathfrak{p}S'.$$

Since $\mathfrak{p}$ is above the conductor $\mathfrak{f}$, by Lemma 2.1, we have that $S'_{\mathfrak{p}}$ is not a principal $S_{\mathfrak{p}}$-module, or equivalently the $S/\mathfrak{p}$-vector space $S'/\mathfrak{p}S'$ has dimension strictly bigger than 1. Observe that

$$\frac{M}{\mathfrak{p}M} \cong \frac{S'/rS'}{\mathfrak{p}S'/rS'} \cong \frac{S'}{\mathfrak{p}S'}.$$

Hence the $S_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ is not cyclic. By Lemma 2.2, we conclude that M is not a cyclic S-module. □

The isomorphism class of a quotient of fractional ideals can be deduced from local information at finitely many primes, as explained in the following lemma.

Lemma 2.4. *Let I and J be fractional ideals over an order S, and let $r \in S$ be a nonzero divisor. Let $\mathscr{S}$ be the set of primes of S containing r. Assume that we have an $S_{\mathfrak{p}}$-linear isomorphism $\varphi_{\mathfrak{p}} : I_{\mathfrak{p}} \xrightarrow{\sim} J_{\mathfrak{p}}$ for every $\mathfrak{p} \in \mathscr{S}$. Then there is an S-linear isomorphism*

$$\psi : \frac{I}{rI} \xrightarrow{\sim} \frac{J}{rJ}$$

such that $\psi \otimes S_{\mathfrak{p}} = \varphi_{\mathfrak{p}} \otimes (S/rS)$ for every prime $\mathfrak{p} \in \mathscr{S}$.

Proof. Set $M = I/rI$ and $N = J/rJ$. By assumption, we have isomorphisms

$$\varphi_{\mathfrak{p}} \otimes \Big(\frac{S}{rS}\Big) : M_{\mathfrak{p}} \xrightarrow{\sim} N_{\mathfrak{p}}$$

for each $\mathfrak{p} \in \mathscr{S}$. We now claim that, given a prime $\mathfrak{p}$ of S, we have $M_{\mathfrak{p}} \neq 0$ if and only if $r \in \mathfrak{p}$. If $r \notin \mathfrak{p}$ then $(S/rS)_{\mathfrak{p}} = 0$, and hence $M_{\mathfrak{p}} = (I \otimes_S (S/rS)) = 0$ as well. Conversely, if $r \in \mathfrak{p}$ then $rI \subseteq \mathfrak{p}I$, and hence we obtain a surjective map $M_{\mathfrak{p}} \to I/\mathfrak{p}I$, which shows that $M_{\mathfrak{p}} \neq 0$, completing the proof of the claim. The same is true for the S-module N.

By Lemma 2.2, we have

$$M \cong \bigoplus_{\mathfrak{p}\in\mathscr{S}} M_{\mathfrak{p}} \quad \text{and} \quad N \cong \bigoplus_{\mathfrak{p}\in\mathscr{S}} N_{\mathfrak{p}}.$$

We conclude by setting

$$\psi = \bigoplus_{\mathfrak{p}\in\mathscr{S}} \varphi_{\mathfrak{p}} \otimes \left(\frac{S}{rS}\right). \qquad \square$$

The étale algebra K comes equipped with a *trace* map

$$\mathrm{Tr}_{K/Q} : K \to Q$$

that associates to every element $x \in K$ the trace of the matrix representing the multiplication-by-x map with respect to any Q-basis of K. The existence of such a nondegenerate trace implies that the integral closure $\mathscr{O}_K$ of Z in K is an order, called the *maximal order*, since every other order is contained in $\mathscr{O}_K$. Recall that $\mathscr{O}_K$ is characterized by the fact that every localization is a principal ideal ring.

The following proposition refines Lemma 2.4, in the sense that we only need local information above the conductor to understand the isomorphism class.

Proposition 2.5. *Let S be an order in K, and let r be a nonzero divisor of K. Assume that rS is coprime to the conductor $\mathfrak{f} = (S : \mathscr{O}_K)$. Then, for every fractional S-ideal I, we have an S-linear isomorphism*

$$\frac{I}{rI} \cong \frac{S}{rS}.$$

Proof. Because rS is coprime to the conductor, by Lemma 2.1 we have $S_{\mathfrak{p}} = \mathscr{O}_{K,\mathfrak{p}}$ for any prime $\mathfrak{p}$ containing r. This implies that $I_{\mathfrak{p}} \cong S_{\mathfrak{p}}$ for every such prime $\mathfrak{p}$. We conclude by Lemma 2.4. □

Given a lattice L in K, we define its *trace dual* as

$$L^t = \{x \in K : \mathrm{Tr}_{K/Q}(xL) \subseteq Z\}.$$

In the following lemma, we record some well-known properties of trace duals.

Lemma 2.6. *Let L, L_1, and L_2 be lattices, and let S be an order in K. Then*

(a) $(L^t)^t = L$,

(b) $(L_1 : L_2) = (L_1^t L_2)^t$,

(c) $(L_1 : L_2) = (L_2^t : L_1^t)$,

(d) $(L : L) = S$ *if and only if* $LL^t = S^t$.

Proof. See for example [Voight 2021, Section 15.6]. □

Let S be an order, $\mathfrak{p}$ be a prime of S, and p its contraction in Z. Denote by $\widehat{Q}_p$ the fraction field of $\widehat{Z}_p$ and by $\widehat{K}_{\mathfrak{p}}$ the total ring of quotients of $\widehat{S}_{\mathfrak{p}}$. The trace $\mathrm{Tr}_{K/Q}$ naturally induces a trace $\mathrm{Tr}_{\widehat{K}_{\mathfrak{p}}/\widehat{Q}_p}$. It follows that taking trace duals commutes with completion. So, given a fractional S-ideal I, the notation $\widehat{I^t_{\mathfrak{p}}}$ is not ambiguous.

Lemma 2.7. *Let S be an order and $\mathfrak{p}$ be a prime of S. For fractional S-ideals I and J, we have $I_{\mathfrak{p}} \cong J_{\mathfrak{p}}$ as $S_{\mathfrak{p}}$-modules if and only if $(I^t)_{\mathfrak{p}} \cong (J^t)_{\mathfrak{p}}$.*

Proof. By [Eisenbud 1995, Exercise 7.5, p. 203], it is enough to prove the equivalent statement with completion instead of localization. Assume that $\widehat{I_{\mathfrak{p}}} \cong \widehat{J_{\mathfrak{p}}}$, that is, $\widehat{I_{\mathfrak{p}}} = \alpha \widehat{J_{\mathfrak{p}}}$ for some $\alpha \in \widehat{K_{\mathfrak{p}}}^{\times}$. Then $\widehat{I^t_{\mathfrak{p}}} = \alpha^{-1}\widehat{J^t_{\mathfrak{p}}}$. Hence $\widehat{I^t_{\mathfrak{p}}} \cong \widehat{J^t_{\mathfrak{p}}}$, as required. We used here that completions and trace duals commute, as noted above. The converse direction follows from Lemma 2.6 (a). □

Recall that Lemma 2.4 provides an S-linear isomorphism of quotients of fractional ideals, under certain local conditions. However, when comparing a fractional ideal and its dual, we can obtain a Z-linear isomorphism between quotients, regardless of the local behavior.

Lemma 2.8. *Let S be an order with fractional ideals I and J, and let $r \in S$ be a nonzero divisor. Then we have a Z-linear isomorphism*

$$\frac{I}{rI} \cong \frac{I^t}{rI^t}.$$

Proof. This is a special case of [Marseglia 2024, Lemma 2.4 (iv)], which is an application of Matlis duality; see for example [Ooishi 1976, Theorem 1.7]. □

We now recall some properties of orders that were studied in [Marseglia 2024, Section 3]. The *Cohen–Macaulay type* of an order S at a prime $\mathfrak{p}$, denoted by $\operatorname{type}_{\mathfrak{p}}(S)$, is the minimal number of generators of $(S^t)_{\mathfrak{p}}$ as an $S_{\mathfrak{p}}$-module. This definition is equivalent to the usual one; see [Marseglia 2024, Section 3]. We say that an order S is *Gorenstein* at a prime $\mathfrak{p}$ if its Cohen–Macaulay $\operatorname{type}_{\mathfrak{p}}(S)$ is equal to 1, that is, if $(S^t)_{\mathfrak{p}}$ is a principal $S_{\mathfrak{p}}$-module. We say that S is Gorenstein if it is so at every prime. This definition of Gorenstein is equivalent to the ones typically used in the literature. For example, a ring with finite (Krull) dimension is called Gorenstein if it has finite injective dimension. See [Bass 1963, Section 1] for another equivalent definition, and see [Bass 1963, Theorem 6.3] and [Buchmann and Lenstra 1994, Proposition 2.7] for the proof of the equivalence with the one used in this paper. In fact, using the latter reference, one can deduce the following lemma. We give a complete proof for convenience.

Proposition 2.9. *Let S be an order and $\mathfrak{p}$ be prime of S. Then S is Gorenstein at $\mathfrak{p}$ if and only if every fractional S-ideal I with $(I : I)_{\mathfrak{p}} = S_{\mathfrak{p}}$ is principal at $\mathfrak{p}$.*

Proof. Observe that S is Gorenstein at $\mathfrak{p}$ if and only if $\widehat{S^t_{\mathfrak{p}}} = \alpha\widehat{S_{\mathfrak{p}}}$ for some $\alpha \in \widehat{K_{\mathfrak{p}}}^{\times}$. Assume now that S is Gorenstein at $\mathfrak{p}$. Pick a fractional S-ideal I with $(I : I)_{\mathfrak{p}} = S_{\mathfrak{p}}$. By taking the completion we get that $\widehat{(I : I)_{\mathfrak{p}}} = \widehat{S_{\mathfrak{p}}}$. By Lemma 2.6 (d), we obtain $\widehat{I_{\mathfrak{p}}}\widehat{I^t_{\mathfrak{p}}} = \widehat{S^t_{\mathfrak{p}}} = \alpha\widehat{S_{\mathfrak{p}}}$. Hence, $\widehat{I_{\mathfrak{p}}}$ is invertible. Because invertible fractional $\widehat{S_{\mathfrak{p}}}$-ideals are principal, we get that $I_{\mathfrak{p}}$ is a principal $S_{\mathfrak{p}}$-module, as required. For the converse, it is enough to observe that S^t has multiplicator ring S. □

Similarly to the Gorenstein case, locally, we have a classification of fractional ideals with multiplicator ring of type 2.

Proposition 2.10 [Marseglia 2024, Theorem 6.2]. *Let S be an order and $\mathfrak{p}$ a prime of S such that* $\operatorname{type}_{\mathfrak{p}}(S) = 2$. *Then, for every fractional S-ideal I such that $(I : I)_{\mathfrak{p}} = S_{\mathfrak{p}}$, either $I_{\mathfrak{p}} \cong S_{\mathfrak{p}}$ or $I_{\mathfrak{p}} \cong (S^t)_{\mathfrak{p}}$.*

We exploit the classifications of Propositions 2.9 and 2.10 to understand quotients of fractional ideals, as we show in the next proposition. We invite the reader to compare the statement with Proposition 2.5, where the isomorphism is S-linear, while here we only get a Z-linear isomorphism.

Proposition 2.11. *Let $r \in S$ be a nonzero divisor. If* $\operatorname{type}_{\mathfrak{p}}(S) \leq 2$ *for all primes $\mathfrak{p}$ of S containing r then, for any fractional S-ideal I with $(I : I)_{\mathfrak{p}} = S_{\mathfrak{p}}$, we have a Z-linear isomorphism*

$$\frac{I}{rI} \cong \frac{S}{rS}.$$

Proof. Fix $\mathfrak{p}$ containing r. If S is Gorenstein at $\mathfrak{p}$ then $I_{\mathfrak{p}} \cong S_{\mathfrak{p}}$ by Proposition 2.9. If $\operatorname{type}_{\mathfrak{p}}(S) = 2$ then $I_{\mathfrak{p}} \cong S_{\mathfrak{p}}$ or $I_{\mathfrak{p}} \cong (S^t)_{\mathfrak{p}}$ by Proposition 2.10. Set $M = I/rI$ and $N = S/rS$. If $I_{\mathfrak{p}} \cong S_{\mathfrak{p}}$ then we have an induced $S_{\mathfrak{p}}$-linear isomorphism

$$M_{\mathfrak{p}} \cong N_{\mathfrak{p}}.$$

If $I_{\mathfrak{p}} \cong (S^t)_{\mathfrak{p}}$ then first we observe that $\widehat{I_{\mathfrak{p}}} \cong \widehat{S^t_{\mathfrak{p}}}$. So we have an induced $\widehat{S_{\mathfrak{p}}}$-linear isomorphism

$$\widehat{M_{\mathfrak{p}}} \cong \frac{\widehat{S^t_{\mathfrak{p}}}}{r\widehat{S^t_{\mathfrak{p}}}},$$

which combined with Lemma 2.8 gives a $\widehat{Z_p}$-linear isomorphism

$$\widehat{M_{\mathfrak{p}}} \cong \widehat{N_{\mathfrak{p}}}.$$

Since $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$ are finitely generated Z_p-modules, we obtain a Z_p-linear isomorphism

$$M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$$

by [Eisenbud 1995, Exercise 7.5, p. 203].

By Lemma 2.2, we have

$$M \cong \bigoplus_{\mathfrak{p}} M_{\mathfrak{p}} \quad \text{and} \quad N \cong \bigoplus_{\mathfrak{p}} N_{\mathfrak{p}},$$

where the direct sums run over the primes $\mathfrak{p}$ containing r, since $M_{\mathfrak{p}} = N_{\mathfrak{p}} = 0$ for all other primes. We conclude that $M \cong N$ as Z-modules. □

As previously anticipated, we will apply the results contained in this section to orders in commutative endomorphism algebras of abelian varieties over finite fields. Such algebras have an automorphism that corresponds to the Rosati involution and acts as complex conjugation. Putting together previously stated results with this extra structure, we obtain the following proposition, which will be used to prove that certain abelian varieties are not self-dual in Proposition 7.7.

Proposition 2.12. *Assume that K has an involution $x \mapsto \bar{x}$ which fixes Q pointwise. Let S be an order in K satisfying $S = \bar{S}$. Let $\mathfrak{p}$ be a prime of S such that* $\operatorname{type}_{\mathfrak{p}}(S) = 2$. *Then $\mathfrak{p} = \bar{\mathfrak{p}}$ if and only if all fractional S-ideals I with $(I : I)_{\mathfrak{p}} = S_{\mathfrak{p}}$ satisfy $I_{\mathfrak{p}} \ncong (\bar{I}^t)_{\mathfrak{p}}$.*

Proof. Assume that $\mathfrak{p} = \bar{\mathfrak{p}}$. By Proposition 2.10, we have that $I_\mathfrak{p} \cong S_\mathfrak{p}$ or $I_\mathfrak{p} \cong (S^t)_\mathfrak{p}$. Assume the former. By Lemma 2.7, we obtain

$$(\bar{I}^t)_\mathfrak{p} = (\bar{I}^t)_{\bar{\mathfrak{p}}} \cong (\bar{S}^t)_{\bar{\mathfrak{p}}} = (S^t)_\mathfrak{p}.$$

Similarly, if $I_\mathfrak{p} \cong (S^t)_\mathfrak{p}$ then

$$(\bar{I}^t)_\mathfrak{p} = (\bar{I}^t)_{\bar{\mathfrak{p}}} \cong \bar{S}_{\bar{\mathfrak{p}}} = S_\mathfrak{p}.$$

In both cases, if $I_\mathfrak{p} \cong (\bar{I}^t)_\mathfrak{p}$ then S^t is principal at $\mathfrak{p}$, that is, S is Gorenstein at $\mathfrak{p}$, which is a contradiction.

Now assume that $\mathfrak{p} \neq \bar{\mathfrak{p}}$. Let $d \in K^\times$ such that $dS^t \subseteq S$ and $m > 0$ such that $\bar{\mathfrak{p}}^m S_{\bar{\mathfrak{p}}} \subseteq (dS^t)_{\bar{\mathfrak{p}}}$. Consider the fractional S-ideal I defined as

$$I = dS^t + \bar{\mathfrak{p}}^m.$$

For every $\mathfrak{l} \neq \bar{\mathfrak{p}}$, we have

$$I_\mathfrak{l} = (dS^t)_\mathfrak{l} + S_\mathfrak{l} = S_\mathfrak{l}$$

and

$$I_{\bar{\mathfrak{p}}} = (dS^t)_{\bar{\mathfrak{p}}} + \bar{\mathfrak{p}}^m S_{\bar{\mathfrak{p}}} = (dS^t)_{\bar{\mathfrak{p}}}.$$

It follows by Lemma 2.7 that $(\bar{I}^t)_\mathfrak{p} \cong \bar{S}_\mathfrak{p} = S_\mathfrak{p}$, which gives us $I_\mathfrak{p} \cong (\bar{I}^t)_\mathfrak{p}$. Moreover, we see that $(I : I) = S$ by checking the equality locally at every prime. □

Remark 2.13. Note that in the proof of Proposition 2.12 we showed that if $\mathfrak{p} \neq \bar{\mathfrak{p}}$ then there exists a fractional ideal I such that $I_\mathfrak{p} \cong (\bar{I}^t)_\mathfrak{p}$ with multiplicator ring $S = (I : I)$ globally not only locally at $\mathfrak{p}$.

3. Groups of rational points and Gorenstein orders

Our goal is to understand groups of rational points $A(\mathbb{F}_q)$ for abelian varieties A defined over $\mathbb{F}_q$. To accomplish this goal in practice, it is productive to view $A(\mathbb{F}_q)$ as not merely a group, but as a module over its endomorphism ring $\mathrm{End}_{\mathbb{F}_q}(A)$. Although requesting a description of the additional structure may appear to make the problem harder a priori, the module structure can be exploited and cleanly described in many cases, which allows one to deduce the group structure immediately.

Given a separable endomorphism $s \colon A \to A$ of an abelian variety A over $\mathbb{F}_q$, we denote by $A[s]$ the $\overline{\mathbb{F}}_q$-points of the kernel of s.

Proposition 3.1. *If A is a squarefree abelian variety over $\mathbb{F}_q$ and s is a separable endomorphism of A, then $\#A[s] = \deg(s) = N_{K/\mathbb{Q}}(s)$, where $K = \mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q}$.*

Proof. Write $A \sim B_1 \times \cdots \times B_r$ as the product of simple pairwise nonisogenous varieties. Then

$$K = \mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q} \cong \prod_{i=1}^{r} K_i$$

is the product of the number fields $K_i = \mathrm{End}(B_i) \otimes_\mathbb{Z} \mathbb{Q}$. Without loss of generality, by [Waterhouse 1969, Theorem 3.13], we can choose each B_i so that $\mathrm{End}(B_i)$ is the maximal order $\mathscr{O}_{K_i}$ in K_i. Since $\mathrm{End}(A) \subseteq \prod_{i=1}^{r} \mathscr{O}_{K_i}$, we can write $s = (s_1, \dots, s_r)$ for $s_i \in \mathscr{O}_{K_i}$. It is therefore enough to consider the case where $A = B_1 \times \cdots \times B_r$. When A is simple, i.e., when $r = 1$, the statement follows from [Milne 1986, Proposition 12.12]. Therefore, by definition,

$$N_{K/\mathbb{Q}}(s) = \prod_{i=1}^{r} N_{K_i/\mathbb{Q}}(s_i) = \prod_{i=1}^{r} \deg(s_i) = \deg(s),$$

where the final equality follows from the fact that $\deg(s) = \#A[s]$ and $\deg(s_i) = \#B_i[s_i]$ by separability. □

Theorem 3.2 and Corollary 3.3 below were proven in the case where A is an elliptic curve in [Lenstra 1996] and generalized to the case of simple abelian varieties in [Springer 2021]. To obtain the same result for squarefree varieties, we follow the proof method used in the simple case.

Theorem 3.2. *Let A be a squarefree abelian variety over $\mathbb{F}_q$, and let s be a separable endomorphism of A. If* $\operatorname{End}(A)$ *is Gorenstein at the primes containing s, then*

$$A[s] \cong \frac{\operatorname{End}(A)}{s \cdot \operatorname{End}(A)}$$

is an isomorphism of $\operatorname{End}(A)$*-modules.*

Proof. Write $S = \operatorname{End}(A)$, $S_0 = S/Ss$, and $M = A[s]$. By the universal property of quotients, if $rA[s] = 0$, then $r = ts$ for some $t \in S$. This implies that M is a faithful S_0-module.

Moreover, because S is Gorenstein at every prime ideal containing s and s is a nonzero-divisor, we deduce that S_0 is a finite Gorenstein ring by [Matsumura 1986, Example 18.1]. Therefore, M contains a free S_0-submodule N of rank 1 by [Springer 2021, Lemma 2.3]. By Proposition 3.1, and the fact that the modules are finite, we have

$$\#M = \deg s = N_{K/\mathbb{Q}}(s) = \#(S/Ss) = \#S_0.$$

We deduce that $M = N \cong S/Ss$, as desired. □

Corollary 3.3. *Let A be a squarefree abelian variety over $\mathbb{F}_q$, and let π be the Frobenius endomorphism of A. If $n \geq 1$ and* $\operatorname{End}(A)$ *is Gorenstein at the prime ideals containing $1 - \pi^n$, then there is an isomorphism of* $\operatorname{End}(A)$*-modules*

$$A(\mathbb{F}_{q^n}) \cong \frac{\operatorname{End}(A)}{(1-\pi^n)\operatorname{End}(A)}.$$

In particular, $B(\mathbb{F}_{q^n}) \cong A(\mathbb{F}_{q^n})$ are isomorphic groups for all abelian varieties B which are isogenous to A with $\operatorname{End}(B) = \operatorname{End}(A)$.

Proof. We may apply Theorem 3.2 because $A(\mathbb{F}_{q^n}) = A[1-\pi^n]$ and $1-\pi^n$ is a separable isogeny. □

However, note that these results are not true in general when we remove the assumption that $\operatorname{End}(A)$ is Gorenstein; see Example 6.7.

4. Cyclic isogeny classes

In this section, we study isogeny classes containing only abelian varieties with cyclic groups of rational points.

Definition 4.1. We say that an isogeny class is *cyclic* if every variety A in the isogeny class has a cyclic group $A(\mathbb{F}_q)$ of rational $\mathbb{F}_q$-points.

Any isogeny class of abelian varieties with a single point is trivially cyclic. In Section 4.1, we show that, except for such trivial factors, every cyclic isogeny class is squarefree. Then, in Section 4.2, we provide a characterization of precisely which squarefree isogeny classes are cyclic in terms of conductor ideals.

4.1. ***Reducing to the squarefree case.*** In this subsection, we consider abelian varieties whose endomorphism algebras are not necessarily commutative. In general, if B is an abelian variety over $\mathbb{F}_q$, then $\operatorname{End}(B)$ is an order in the endomorphism algebra $K = \operatorname{End}(B) \otimes_{\mathbb{Z}} \mathbb{Q}$, that is a subring which is a finitely generated free module over $\mathbb{Z}$ and whose $\mathbb{Q}$-span is the whole algebra K. Observe that this notion of order specializes to the one introduced in Section 2 in the commutative case.

Proposition 4.2. *If B is a simple abelian variety over $\mathbb{F}_q$ such that $B(\mathbb{F}_q)$ is a nontrivial cyclic group and* $\operatorname{End}(B)$ *is a maximal order in* $\operatorname{End}(B) \otimes_{\mathbb{Z}} \mathbb{Q}$, *then* $\operatorname{End}(B)$ *is commutative, that is, B is squarefree.*

Proof. Let L be the center of the endomorphism algebra $\operatorname{End}(B) \otimes_{\mathbb{Z}} \mathbb{Q}$. Because B is simple, $L = \mathbb{Q}(\pi)$, where π is a root in L of the polynomial $h_B(x)$; see [Waterhouse and Milne 1971, Theorem 8]. The center of $\operatorname{End}(B)$ is $\mathcal{O}_L$ by the maximality of $\operatorname{End}(B)$. By [Springer 2021, Theorem 1.3 (b)], there is an isomorphism of $\mathcal{O}_L$-modules

$$B(\mathbb{F}_q) \cong \left(\frac{\mathcal{O}_L}{(1-\pi)\mathcal{O}_L} \right)^d,$$

where $d = 2\dim(B)/[L : \mathbb{Q}]$. In particular, because the group of points is nontrivial and cyclic by hypothesis, we must have $d = 1$, which is equivalent to $\mathcal{O}_L = \operatorname{End}(B)$ by [Waterhouse and Milne 1971, Theorem 8]. □

Theorem 4.3. *If A is an abelian variety over $\mathbb{F}_q$ whose isogeny class is cyclic, then $A \sim A_1 \times A_{\mathrm{sf}}$ for abelian varieties A_1 and A_{sf} over $\mathbb{F}_q$, possibly of dimension* 0, *such that A_{sf} is squarefree and* $\#A_1(\mathbb{F}_q) = 1$. *If $q \geq 5$, then A itself is squarefree.*

Proof. Decompose the isogeny class $A \sim B_1^{e_1} \times \cdots \times B_r^{e_r}$ into distinct simple factors. By [Waterhouse 1969, Theorem 3.13], we may assume that each $\operatorname{End}(B_j)$ is a maximal order in its endomorphism algebra.

After possibly reordering, let r_1 be such that $\#B_j(\mathbb{F}_q) = 1$ for all $1 \leq j \leq r_1$ and $\#B_j(\mathbb{F}_q) > 1$ for all $r_1 < j \leq r$. Define

$$A_1 = \prod_{1 \leq j \leq r_1} B_j^{e_j} \quad \text{and} \quad A_{\mathrm{sf}} = \prod_{r_1 < j \leq r} B_j^{e_j}.$$

It suffices to show A_{sf} is squarefree. In this case, $e_j = 1$ for all $r_1 < j \leq r$ because the isogeny class is cyclic, and Proposition 4.2 shows that

$$\mathrm{End}(A_{\mathrm{sf}}) \cong \prod_{r_1 < j \leq r} \mathrm{End}(B_j)$$

is commutative, that is, A_{sf} is squarefree. The theorem then follows because the Weil bound states that $\#B(\mathbb{F}_q) \geq (\sqrt{q}-1)^{2\dim(B)}$ for any abelian variety B over $\mathbb{F}_q$; see [Weil 1948]. Thus $\#B(\mathbb{F}_q) = 1$ implies $q \leq 4$. □

Remark 4.4. There are infinitely many simple abelian varieties over $\mathbb{F}_2$ with a single rational point by [Madan and Pal 1977]; see also [Kedlaya 2024]. However, there is only one simple isogeny class over each of $\mathbb{F}_3$ and $\mathbb{F}_4$ with a single rational point; see [Kadets 2021, Theorem 3.2] and isogeny classes 1.3.ad and 1.4.ae [LMFDB 2022].

4.2. *The cyclicity of squarefree abelian varieties.*

We will use the same notation as in the previous sections. Let $\mathscr{I}_h$ be a squarefree isogeny class of abelian varieties over $\mathbb{F}_q$. Put $K = \mathbb{Q}[x]/(h) = \mathbb{Q}[\pi]$ and $R = \mathbb{Z}[\pi, \bar{\pi}]$.

Theorem 4.5. *The isogeny class $\mathscr{I}_h$ is cyclic if and only if $(1-\pi)R$ is coprime to the conductor $\mathfrak{f} = (R : \mathscr{O}_K)$; that is, $(1-\pi)R + \mathfrak{f} = R$.*

This theorem is a straightforward combination of Proposition 4.7 and Corollary 4.9. We remark that the following is a simple application of Theorem 4.5.

Corollary 4.6. *If $h(1)$ is a squarefree integer, where $h(t)$ is the characteristic polynomial of π, then $(1-\pi)R$ is coprime with $\mathfrak{f} = (R : \mathscr{O}_K)$.*

Proof. Because $h(1)$ is squarefree, any finite abelian group of order $h(1)$ is cyclic. Thus, the isogeny class is cyclic, and we conclude via Theorem 4.5. □

The next proposition proves one direction in Theorem 4.5.

Proposition 4.7. *If $(1-\pi)R$ is coprime to the conductor $\mathfrak{f} = (R : \mathscr{O}_K)$, then, for every A in $\mathscr{I}_h$, we have an R-linear isomorphism*

$$A(\mathbb{F}_q) \cong \frac{R}{(1-\pi)R}.$$

In particular, the isogeny class $\mathscr{I}_h$ is cyclic.

Proof. Let A be an abelian variety in $\mathscr{I}_h$. Put $S = \mathrm{End}(A)$, and note that $R \subseteq S$. Hence $(1-\pi)S$ is coprime to the conductor $(S : \mathscr{O}_K)$ of S in $\mathscr{O}_K$. For every prime $\mathfrak{p}$ of S containing $(1-\pi)$, we have $S_{\mathfrak{p}} = \mathscr{O}_{K,\mathfrak{p}}$ by Lemma 2.1. Therefore S is Gorenstein at $\mathfrak{p}$ for every $\mathfrak{p}$ containing $(1-\pi)$. By Theorem 3.2, we have that

$$A(\mathbb{F}_q) \cong \frac{S}{(1-\pi)S}.$$

Since S is a fractional R-ideal, Proposition 2.5 gives us an R-linear isomorphism $S/(1-\pi)S \cong R/(1-\pi)R$. We conclude by observing that

$$\frac{R}{(1-\pi)R} \cong \frac{\mathbb{Z}[x, y]}{(h(1), x-1, y-q)} \cong \frac{\mathbb{Z}}{(h(1))},$$

which is immediate from the method of the proof of [Marseglia and Springer 2023, Proposition 2.7]. □

We now prove a strong converse to Proposition 4.7.

Proposition 4.8. *Let A be a squarefree abelian variety over $\mathbb{F}_q$ with Gorenstein endomorphism ring $S = \mathrm{End}(A)$ and Frobenius endomorphism π. If $(1-\pi)R$ is not coprime to the conductor $\mathfrak{f} = (R : S)$, then $A(\mathbb{F}_{q^n})$ is a noncyclic R-module for all $n \geq 1$. In particular, every abelian variety in the isogeny class with endomorphism ring S has a noncyclic group of points.*

Proof. We have $A(\mathbb{F}_{q^n}) \cong S/(1-\pi^n)S$ as S-modules by Corollary 3.3. Observe that $(1-\pi^n)R$ is not coprime to $\mathfrak{f}$ because $(1-\pi^n) = (1-\pi)(1+\pi+\cdots+\pi^{n-1})$ implies

$$R \supsetneq (1-\pi)R + \mathfrak{f} \supseteq (1-\pi^n)R + \mathfrak{f} \quad \text{for all } n \geq 1.$$

Therefore, $A(\mathbb{F}_{q^n})$ is a noncyclic R-module by Proposition 2.3. □

Corollary 4.9. *If $(1-\pi)R$ is not coprime to the conductor $\mathfrak{f} = (R : \mathcal{O}_K)$, then $A(\mathbb{F}_{q^n})$ is a noncyclic R-module for all $n \geq 1$ for every A in $\mathscr{I}_h$ with maximal endomorphism ring. In particular, the isogeny class $\mathscr{I}_h$ is noncyclic.*

Proof. Observe that $\mathcal{O}_K$ is the endomorphism ring of an abelian variety in $\mathscr{I}_h$ by [Waterhouse 1969, Theorem 3.13]. Now, apply Proposition 4.8 with $S = \mathcal{O}_K$, which is Gorenstein. □

5. Noncyclic groups of rational points

In Section 4, we gave a characterization of isogeny classes in which every abelian variety has a cyclic group of points. In this section, we go in the opposite direction. In Theorem 5.7, we characterize isogeny classes $\mathscr{I}_h$ in which every abelian group of order $h(1)$ occurs as the group of rational points, and we call such isogeny classes *rich*; see Definition 5.3.

There are two main tools which we require to study rich isogeny classes. The first is Lemma 5.4. It generalizes [Giangreco-Maidana 2019, Lemma 2.1] which was originally used to study cyclic isogeny classes. We also use a theorem of Rybakov, recalled below as Theorem 5.6, which provides a criterion for the existence of abelian varieties in a given squarefree isogeny class with a prescribed group of rational points.

To conclude the section, we use Rybakov's theorem again to prove in Proposition 5.10 the existence of ordinary abelian varieties over $\mathbb{F}_q$ whose ℓ-primary part has two generators whenever $q \equiv 1 \bmod \ell$. This allows us to deduce an improved version of [Marseglia and Springer 2023, Theorem 3.3], which we present below as Theorem 5.13.

5.1. ***Lemmas about characteristic polynomials.*** We provide some basic lemmas concerning minimal polynomials which we will apply to the polynomial h for a squarefree isogeny class $\mathscr{I}_h$. For an element α in an étale algebra K over $\mathbb{Q}$, we write $h_\alpha(x)$ and $m_\alpha(x)$ for the characteristic and minimal polynomials, respectively, of the $\mathbb{Q}$-linear map on K defined by multiplication by α. Note that if $K = \prod_{j=1}^t K_j$ for number fields $K_1, \dots, K_t$ and $\alpha = (\alpha_1, \dots, \alpha_t)$, then we have $h_\alpha(x) = \prod_{j=1}^t h_{\alpha_i}(x)$. Observe that α is in the maximal order $\mathscr{O}_K$ of K if and only if $m_\alpha(x)$ has integer coefficients.

For a squarefree isogeny class $\mathscr{I}_h$, the previous notation applied to the étale algebra $K = \mathbb{Q}[x]/(h)$ leads to $h(x) = h_\pi(x) = m_\pi(x)$, where $\pi \in K$ corresponds to the Frobenius endomorphism on any abelian variety in $\mathscr{I}_h$.

Lemma 5.1. *Let K be an étale algebra, let $\alpha \in K^\times$, and let $b, c \in \mathbb{Q}$, with $b \neq 0$. Define $r = \deg h_\alpha$. Then*

$$h_{b\alpha+c}(x) = b^r \cdot h_\alpha\Big(\frac{x}{b} - \frac{c}{b}\Big)$$

and

$$h_{1/\alpha}(x) = \frac{x^r}{h_\alpha(0)} \cdot h_\alpha\Big(\frac{1}{x}\Big).$$

In other words, we recognize $h_{1/\alpha}(x)$ as the reverse of the polynomial $h_\alpha(x)/h_\alpha(0)$.

Proof. First, we prove the statements when $K = \mathbb{Q}(\alpha)$ is a number field. Both

$$b^r \cdot m_\alpha\Big(\frac{x}{b} - \frac{c}{b}\Big) \quad \text{and} \quad \frac{x^r}{m_\alpha(0)} \cdot m_\alpha\Big(\frac{1}{x}\Big)$$

are monic, with coefficients in $\mathbb{Q}$, of degree r, and are 0 when evaluated at $b\alpha + c$ and $1/\alpha$, respectively. They are irreducible since we have isomorphisms $\mathbb{Q}(\alpha) \cong \mathbb{Q}(b\alpha + c) \cong \mathbb{Q}(1/\alpha)$.

In general, we write $K = \prod_{j=1}^t K_j$ for number fields $K_1, \dots, K_t$, and $\alpha = (\alpha_1, \dots, \alpha_t)$. Setting $d_j = [K_j : \mathbb{Q}(\alpha_j)]$, we observe that $h_\alpha(x) = \prod_{j=1}^t m_{\alpha_j}(x)^{d_j}$. The claims follow from the previous case:

$$h_{b\alpha+c}(x) = \prod_{j=1}^t m_{b\alpha_j+c}(x)^{d_j} = \prod_{j=1}^t b^{d_j \deg m_{\alpha_j}} \cdot m_{\alpha_j}\Big(\frac{x}{b} - \frac{c}{b}\Big)^{d_j} = b^r \cdot h_\alpha\Big(\frac{x}{b} - \frac{c}{b}\Big),$$

$$h_{1/\alpha}(x) = \prod_{j=1}^t m_{1/\alpha_j}(x)^{d_j} = \prod_{j=1}^t \frac{x^{d_j \deg m_{\alpha_j}}}{m_{\alpha_j}(0)} \cdot m_{\alpha_j}\Big(\frac{1}{x}\Big)^{d_j} = \frac{x^r}{h_\alpha(0)} \cdot h_\alpha\Big(\frac{1}{x}\Big). \qquad \square$$

We apply the previous lemma to obtain a formula for the coefficients of the minimal polynomials of two related algebraic numbers.

Lemma 5.2. *Let α be an element of an étale algebra K over $\mathbb{Q}$ satisfying $1 - \alpha \in K^\times$, and let $d \in \mathbb{Q}$. The coefficients of $h_{d/(1-\alpha)}(x) = \sum_{i=0}^r a_i x^i$ are given by the formula*

$$a_i = \frac{(-1)^{r+i} d^{r-i} h_\alpha^{(r-i)}(1)}{(r-i)!\, h_\alpha(1)},$$

where $h_\alpha^{(i)}(x)$ is the i-th derivative of the polynomial $h_\alpha(x)$.

Proof. We will use Lemma 5.1 several times. Let $\beta = (1-\alpha)/d$. We have

$$h_{d/(1-\alpha)}(x) = h_{1/\beta}(x) = \frac{x^r}{h_\beta(0)} h_\beta\Big(\frac{1}{x}\Big), \tag{1}$$

$$h_\beta(x) = \Big(\frac{1}{d}\Big)^r h_{1-\alpha}(dx), \tag{2}$$

$$h_{1-\alpha}(x) = (-1)^r h_\alpha(1-x). \tag{3}$$

Using (2) with (3), we get

$$h_\beta(0) = \Big(\frac{1}{d}\Big)^r h_{1-\alpha}(0) = (-1)^r \Big(\frac{1}{d}\Big)^r h_\alpha(1). \tag{4}$$

Combining (4) and (2) with (1), we obtain

$$h_{d/(1-\alpha)}(x) = \frac{(-x)^r}{h_\alpha(1)} h_{1-\alpha}\Big(\frac{d}{x}\Big). \tag{5}$$

Define $h_{1-\alpha}(x) = x^r + b_{r-1}x^{r-1} + \cdots + b_1 x + b_0$ and set $b_r = 1$. By (3), for every $i = 1, \dots, r$, we get

$$b_i = \frac{1}{i!} h_{1-\alpha}^{(i)}(x)\Big|_{x=0} = \frac{1}{i!}(-1)^{r+i} h_\alpha^{(i)}(1-x)\Big|_{x=0} = \frac{1}{i!}(-1)^{r+i} h_\alpha^{(i)}(1). \tag{6}$$

Combining (5) and (6), we obtain

$$\begin{aligned} h_{d/(1-\alpha)}(x) &= \frac{(-x)^r}{h_\alpha(1)}\bigg(\Big(\frac{d}{x}\Big)^r + b_{r-1}\Big(\frac{d}{x}\Big)^{r-1} + \cdots + b_1\Big(\frac{d}{x}\Big) + b_0\bigg) = \sum_{i=0}^{r} \frac{(-x)^r}{h_\alpha(1)} \Big(\frac{d}{x}\Big)^{r-i} b_{r-i} \\ &= \sum_{i=0}^{r} \frac{(-x)^r}{h_\alpha(1)} \Big(\frac{d}{x}\Big)^{r-i} \cdot \frac{1}{(r-i)!}(-1)^i h_\alpha^{(r-i)}(1) = \sum_{i=0}^{r} \frac{(-1)^{r+i} d^{r-i} h_\alpha^{(r-i)}(1)}{(r-i)!\, h_\alpha(1)} x^i. \end{aligned}$$

□

5.2. *Rich isogeny classes.* In Section 4, we studied cyclic isogeny classes. Now we study the opposite extreme.

Definition 5.3. We call an isogeny class $\mathscr{I}_h$ *rich* if every abelian group of order $h(1)$ occurs as the group of rational points for some abelian variety in $\mathscr{I}_h$.

The following lemma detects the annihilator of the group of rational points in terms of the existence of certain endomorphisms. It generalizes [Giangreco-Maidana 2019, Lemma 2.1], which was originally presented for the sake of studying cyclic isogeny classes. We use our generalization to study rich isogeny classes instead.

Lemma 5.4. *Let A be an abelian variety over $\mathbb{F}_q$ with N rational points. Denote by π the Frobenius of A. Let d be a divisor of N. Then the following are equivalent*:

(a) $dA(\mathbb{F}_q) = 0$.

(b) $A(\mathbb{F}_q) \subseteq \ker([d])(\bar{\mathbb{F}}_q)$.

(c) *There exists $\varphi \in \mathrm{End}_{\mathbb{F}_q}(A)$ such that $[d] = \varphi \circ (1-\pi)$. Moreover, such a φ lives in the center of* $\mathrm{End}_{\mathbb{F}_q}(A)$.

Proof. The first two statements are clearly equivalent. To show that the second and the third are equivalent, we first observe that $A(\mathbb{F}_q) = \ker(1-\pi)(\overline{\mathbb{F}}_q)$. In particular, it is clear that the third statement implies the second. Now, assume that the second statement holds; that is, $\ker(1-\pi)(\overline{\mathbb{F}}_q) \subseteq \ker([d])(\overline{\mathbb{F}}_q)$. Then by the separability of $1-\pi$, we have also $\ker(1-\pi) \subseteq \ker([d])$. Consider the commutative diagram

$$\begin{tikzcd}
 & A \\
A \arrow[ur, "{[d]}"] \arrow[r, two heads] \arrow[dr, "1-\pi"'] & \dfrac{A}{\ker(1-\pi)} \arrow[u, "\tilde{\varphi}"'] \arrow[d, "\iota"] \\
 & A
\end{tikzcd}$$

where the middle arrow is the canonical projection, ι is the isomorphism induced by $1-\pi$, and $\tilde{\varphi}$ is the (unique) map induced by the inclusion $\ker(1-\pi) \subseteq \ker([d])$ via the universal property of the quotient. Put $\varphi = \tilde{\varphi} \circ \iota^{-1}$. Therefore

$$\varphi \circ (1-\pi) = [d].$$

Since both $1-\pi$ and $[d]$ are in the center and defined over $\mathbb{F}_q$, the same holds for φ, as required. □

Given two isogenous abelian varieties A and B over $\mathbb{F}_q$, we will identify the endomorphism algebras $\operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \operatorname{End}(B) \otimes_{\mathbb{Z}} \mathbb{Q}$ with an isomorphism which maps the Frobenius endomorphism of A to the Frobenius endomorphism of B. We denote this element by π.

Proposition 5.5. *Let A be an abelian variety over $\mathbb{F}_q$ whose group of rational points $A(\mathbb{F}_q)$ is annihilated by an integer d. For every maximal order $\mathcal{O}$ in the endomorphism algebra* $\operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, *there is an abelian variety B which is isogenous to A such that* $\operatorname{End}(B) \cong \mathcal{O}$. *Furthermore, $B(\mathbb{F}_q)$ is also annihilated by d for all B with endomorphism ring* $\operatorname{End}(B) \cong \mathcal{O}$.

Proof. The existence statement is [Waterhouse 1969, Theorem 13]. Because d kills $A(\mathbb{F}_q)$, we see that $d/(1-\pi)$ is an endomorphism of A which lies in the center of its endomorphism algebra by Lemma 5.4. Because B has maximal endomorphism ring, $\operatorname{End}(B)$ contains the maximal order of the center of its endomorphism algebra. In particular, $d/(1-\pi)$ is an element of $\operatorname{End}(B)$, which implies that d kills $B(\mathbb{F}_q)$ by another application of Lemma 5.4. □

We emphasize the fact that Lemma 5.4 and Proposition 5.5 apply to any abelian variety defined over a finite field. In the rest of the section, we restrict our attention to the squarefree case.

For a positive integer N, we write $\operatorname{rad}(N)$ for its radical; that is, if $N = \prod_{j=1}^{s} \ell_j^{e_j}$, then we define $\operatorname{rad}(N) = \prod_{j=1}^{s} \ell_j$. We say that N is the *exponent* of an abelian group G if N is the smallest positive integer which annihilates G. The minimal possible exponent for a finite abelian group of order N is $\operatorname{rad}(N)$, which is achieved by the "least cyclic" group of order N. This notion is made precise by the following definition.

Let $g \geq 1$ be an integer, and let ℓ be prime. Consider a group H with ℓ-primary part $H_\ell = \prod_{j=1}^{2g} (\mathbb{Z}/\ell^{e_j}\mathbb{Z})$, where $0 \leq e_1 \leq \cdots \leq e_{2g}$. The *$\ell$-Hodge polygon* of H is the polygon with vertices $\bigl(i, \sum_{j=1}^{2g-i} e_j\bigr)$;

see [Rybakov 2010, Definition 1.1] for details and examples. We will use this notion when H is the group of rational points of an abelian variety A, in which case $g = \dim(A)$. Note that the group $(\mathbb{Z}/\ell\mathbb{Z})^f$ has the highest ℓ-Hodge polygon among abelian groups of order ℓ^f, while $(\mathbb{Z}/\ell^f\mathbb{Z})$ has the lowest.

Given a polynomial $h(x) = \sum_{i=1}^{2g} a_i x^i \in \mathbb{Z}[x]$ with $a_0 \neq 0$, the *ℓ-Newton polygon* of h is the boundary of the lower convex hull of the points $(i, \operatorname{ord}_\ell(a_i))$ for $0 \leq i \leq 2g$. The following theorem of Rybakov describes the groups of rational points occurring in squarefree isogeny classes by comparing Hodge polygons and Newton polygons.

Theorem 5.6 [Rybakov 2010, Theorem 1.1]. *Given a squarefree isogeny class $\mathscr{I}_h$ of abelian varieties over $\mathbb{F}_q$, a finite abelian group G of order $h(1)$ occurs as the group of rational points of some abelian variety A in $\mathscr{I}_h$ if and only if the ℓ-Hodge polygon of G lies on or below the ℓ-Newton polygon of $h(1-t)$ for all primes ℓ.*

We exploit this theorem to characterize which squarefree isogeny classes are rich.

Theorem 5.7. *Consider a squarefree isogeny class $\mathscr{I}_h$ of abelian varieties over $\mathbb{F}_q$ of dimension g. Let $K = \mathbb{Q}[x]/(h)$ be the endomorphism algebra, and let π be the class of x. Write $N = h(1) = \prod_{j=1}^{s} \ell_j^{e_j}$ for the number of rational points on each abelian variety in $\mathscr{I}_h$. The following are equivalent*:

(a) *$\mathscr{I}_h$ is rich*; *that is*, *every abelian group of order N arises as $A(\mathbb{F}_q)$ for some $A \in \mathscr{I}_h$.*

(b) *There is an abelian variety $A \in \mathscr{I}_h$ whose group of rational points has exponent* $\operatorname{rad}(N)$; *that is,*

$$A(\mathbb{F}_q) \cong \prod_{j=1}^{s} \left(\frac{\mathbb{Z}}{\ell_j\mathbb{Z}}\right)^{e_j}.$$

(c) *The coefficients of the characteristic polynomial $h_{\operatorname{rad}(N)/(1-\pi)}(x)$ are integers.*

(d) *For all $1 \leq i \leq 2g$, we have*

$$\frac{h^{(i)}(1)}{i!} \cdot \ell_1^{i-e_1} \cdots \ell_s^{i-e_s} \in \mathbb{Z}.$$

If one of the equivalent conditions holds, then $A(\mathbb{F}_q)$ has exponent $\operatorname{rad}(N)$ *for every A in $\mathscr{I}_h$ with maximal endomorphism ring.*

Proof. Trivially, (a) implies (b). The reverse direction is a consequence of Theorem 5.6 because, among abelian groups of order N, the group of exponent $\operatorname{rad}(N)$ has the highest ℓ-Hodge polygon for every prime ℓ. If $A(\mathbb{F}_q)$ has exponent $\operatorname{rad}(N)$ for some $A \in \mathscr{I}_h$, then $\operatorname{rad}(N)/(1-\pi)$ is an element of $\operatorname{End}(A)$ by Lemma 5.4. In particular, $\operatorname{rad}(N)/(1-\pi)$ is an integral element, so its minimal polynomial has integer coefficients. Since $K = \mathbb{Q}[\pi]$, the characteristic and minimal polynomials $h_{\operatorname{rad}(N)/(1-\pi)}(x) = m_{\operatorname{rad}(N)/(1-\pi)}(x)$ coincide. It follows that (b) implies (c).

Conversely, assume that the minimal polynomial of $\operatorname{rad}(N)/(1-\pi)$ has integer coefficients. Then $\operatorname{rad}(N)/(1-\pi)$ is contained in the maximal order $\mathscr{O}_K$ of the endomorphism algebra $K = \mathbb{Q}[x]/(h)$. By [Waterhouse 1969, Theorem 3.13], there is always at least one abelian variety $A \in \mathscr{I}_h$ whose endomorphism ring $\mathrm{End}(A)$ is the maximal order $\mathscr{O}_K$ in $K = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\pi)$. Therefore, by Lemma 5.4, $A(\mathbb{F}_q)$ is killed by $\mathrm{rad}(N)$, so (c) implies (b).

Recall that $h(x) = h_\pi(x)$. Applying Lemma 5.2 with $d = \mathrm{rad}(N)$, we see that the polynomial $h_{\mathrm{rad}(N)/(1-\pi)}(x)$ is in $\mathbb{Z}[x]$ if and only if

$$\frac{h^{(i)}(1)}{i!}\frac{\mathrm{rad}(N)^i}{N} = \frac{h^{(i)}(1)}{i!} \cdot \ell_1^{i-e_1} \cdots \ell_s^{i-e_s} \in \mathbb{Z}$$

for $i = 1, \dots, 2g$. Hence parts (c) and (d) are also equivalent.

The final claim about varieties with maximal endomorphism ring follows after combining Proposition 5.5 and part (b). □

As an application of Theorem 5.7, we show the following.

Corollary 5.8. *A squarefree isogeny class is rich if and only if its simple factors are rich.*

Proof. Consider a squarefree isogeny class $\mathscr{I}_h$ over $\mathbb{F}_q$ whose abelian varieties have N rational points. Let A be an abelian variety in $\mathscr{I}_h$ with maximal endomorphism ring. By Theorem 5.7, the isogeny class $\mathscr{I}_h$ is rich if and only if the exponent of $A(\mathbb{F}_q)$ is a squarefree integer, namely $\mathrm{rad}(N)$.

Because $\mathrm{End}(A)$ is maximal, $\mathrm{End}(A) \cong \prod_{j=1}^{r} \mathscr{O}_{K_j}$, where $K_j = \mathbb{Q}[x]/(h_j)$ according to the factorization $h = h_1 \cdots h_r$ into irreducible polynomials. Moreover, $A \cong A_1 \times \cdots \times A_r$, where each A_j is simple and has maximal endomorphism ring $\mathrm{End}(A_j) \cong \mathscr{O}_{K_j}$. Observe that the exponent of $A(\mathbb{F}_q) \cong \prod_{j=1}^{r} A_j(\mathbb{F}_q)$ is the least common multiple of the exponents of $A_j(\mathbb{F}_q)$ for $1 \le j \le r$. Therefore, the exponent of $A(\mathbb{F}_q)$ is a squarefree integer if and only if the exponent of $A_j(\mathbb{F}_q)$ is a squarefree integer for all $1 \le j \le r$. □

It is now straightforward to determine when a squarefree isogeny class is rich because Theorem 5.7 (d) provides a criterion which only involves computing the derivatives of the characteristic polynomial. Although Theorem 4.5 provides a criterion for cyclicity in terms of conductor ideals, it is faster to use [Giangreco-Maidana 2019, Theorem 2.2], which only requires computing one derivative of the characteristic polynomial. We exhibit some statistics over small finite fields in the following example.

Example 5.9. Let $\mathscr{I}^{\mathrm{sf}}(g, q)$ be the set of squarefree isogeny classes of dimension g over $\mathbb{F}_q$, and let $\mathscr{R}(g, q)$ and $\mathscr{C}(g, q)$ be the subsets containing the rich and cyclic isogeny classes, respectively. In Table 1, we collect statistics concerning the cardinalities of these sets for small values of g and q.

An isogeny class is simultaneously rich and cyclic precisely when the properties are trivially satisfied, namely when the number of rational points $N = \mathrm{rad}(N)$ is squarefree. As a result, the intersection $\mathscr{R}(g, q) \cap \mathscr{C}(g, q)$ can be considered the set of trivial examples. Asymptotically, the proportion of integers which are squarefree is $6/\pi^2 \approx 60\%$.

5.3. *Groups with two generators.*

To conclude this section, we consider the existence of abelian varieties whose groups of rational points are not cyclic, but are, locally, the product of only two cyclic factors. As an application, we improve [Marseglia and Springer 2023, Theorem 3.3] in the case of ordinary abelian varieties over $\mathbb{F}_4$.

$\mathbb{F}_q$	g	$\mathscr{R}\setminus\mathscr{C}$ only rich	$\mathscr{C}\setminus\mathscr{R}$ only cyclic	$\mathscr{R}\cap\mathscr{C}$ both	$\mathscr{I}^{\mathrm{sf}}\setminus(\mathscr{R}\cup\mathscr{C})$ neither
$\mathbb{F}_2$	1	0%	20.0%	80.0%	0%
	2	3.45%	17.2%	75.9%	3.45%
	3	8.66%	18.4%	66.0%	7.02%
	4	10.5%	19.8%	61.0%	8.67%
	5	10.7%	20.5%	58.6%	10.2%
	6	10.0%	21.3%	58.5%	10.2%
$\mathbb{F}_3$	1	14.3%	0%	85.8%	0%
	2	23.6%	5.45%	67.2%	3.64%
	3	21.6%	8.38%	60.9%	9.17%
	4	19.4%	9.31%	59.8%	11.5%
	5	18.1%	9.83%	60.0%	12.1%
$\mathbb{F}_4$	1	0%	28.6%	71.4%	0%
	2	11.9%	16.4%	61.2%	10.5%
	3	13.1%	14.8%	60.1%	12.0%
	4	12.9%	15.8%	60.3%	11.0%
$\mathbb{F}_5$	1	11.1%	11.1%	66.6%	11.1%
	2	16.8%	9.25%	61.4%	12.6%
	3	17.0%	10.4%	59.5%	13.1%
	4	16.7%	10.4%	60.0%	12.9%

Table 1. For $2 \leq q \leq 5$, we count the number of cyclic and rich squarefree isogeny classes of small dimension g over $\mathbb{F}_q$ by applying [Giangreco-Maidana 2019, Theorem 2.2] and Theorem 5.7 to data in [LMFDB 2022]. See also [Dupuy et al. 2021].

Proposition 5.10. *Let ℓ be a prime and $1 \leq s_1 \leq s_2$. If $q \equiv 1 \bmod \ell^{s_1}$ is a prime power, then every squarefree isogeny class $\mathscr{I}_h$ over $\mathbb{F}_q$ with $\mathrm{ord}_\ell(h(1)) = s_1 + s_2$ contains an abelian variety A such that the ℓ-primary part of the group of rational points is*

$$A(\mathbb{F}_q)_\ell \cong (\mathbb{Z}/\ell^{s_1}\mathbb{Z}) \times (\mathbb{Z}/\ell^{s_2}\mathbb{Z}).$$

Proof. The group $(\mathbb{Z}/\ell^{s_1}\mathbb{Z}) \times (\mathbb{Z}/\ell^{s_2}\mathbb{Z})$ has ℓ-Hodge polygon defined by the points $(0, s_1+s_2)$, $(1, s_1)$, and $(2, 0)$. Therefore, using the notation $h(1-x) = \sum_{j=0}^{2g} b_j x^j$, it is enough show that $\mathrm{ord}_\ell(b_0) \geq s_1 + s_2$ and $\mathrm{ord}_\ell(b_1) \geq s_1$ by Theorem 5.6. The first holds by hypothesis because $b_0 = h(1)$.

By the q-symmetry of $h(x)$, we write

$$h(x) = \left(\sum_{j=1}^{g-1} a_{2g-j}(x^{2g-j} + q^{g-j}x^j)\right) + a_g x^g.$$

Because $q \equiv 1 \bmod \ell^{s_1}$, we deduce that

$$2g - j + jq^{g-j} \equiv g(1 + q^{g-j}) \bmod \ell^{s_1} \quad \text{for all } 0 \leq j \leq g-1.$$

Combined with the fact that the polynomial $(1-x)^j$ has linear coefficient $-j$ for any $j \geq 0$, we observe

$$-b_1 = \left(\sum_{j=1}^{g-1} a_{2g-j}(2g-j+jq^{g-j})\right) + ga_g \equiv \left(\sum_{j=1}^{g-1} ga_{2g-j}(1+q^{g-j})\right) + ga_g \equiv gh(1) \bmod \ell^{s_1}.$$

Thus, $\operatorname{ord}_\ell(b_1) \geq s_1$ because $\operatorname{ord}_\ell(h(1)) = s_1 + s_2$, and we are done. □

Corollary 5.11. *Let q be an odd prime power. If $\mathscr{I}$ is a squarefree cyclic isogeny class over $\mathbb{F}_q$, then its point count is not divisible by* 4.

Proof. If the point count is divisible by 4, then we apply Proposition 5.10 with $\ell = 2$ and $s_1 = 1$ to find a noncyclic variety. □

Corollary 5.12. *For every $s \geq 1$, the group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^s\mathbb{Z}$ arises as the group of rational points of a squarefree ordinary abelian variety over $\mathbb{F}_4$.*

Proof. Apply Proposition 5.10 with $\ell = 3,\ q = 4,\ s_1 = 1$, and $s_2 = s$. The existence of ordinary isogeny classes with the desired number of points follows from Theorem 1.13 and Remark 1.16 in [van Bommel et al. 2021]. □

For every $N \geq 1$, there is an abelian variety A over $\mathbb{F}_4$ with $A(\mathbb{F}_4) \cong (\mathbb{Z}/N\mathbb{Z})$, and A can be taken to be ordinary if and only if $N \neq 3$. In particular, by taking products, this shows that every finite abelian group arises as the group of rational points of an abelian variety over $\mathbb{F}_4$ which is not necessarily ordinary; see [Marseglia and Springer 2023, Theorem 3.3]. Corollary 5.12 extends that result by proving that the abelian variety can be taken to be ordinary in additional noncyclic cases. We record the improved theorem here.

Theorem 5.13. *Every finite abelian group G arises as the group of rational points $G \cong A(\mathbb{F}_q)$ for an abelian variety A over $\mathbb{F}_4$. Moreover, A can be taken to be ordinary, except possibly if $G = (\mathbb{Z}/3\mathbb{Z})^n$ for an odd integer n.*

Proof. It is already established by [Marseglia and Springer 2023, Theorem 3.3] that every finite abelian group occurs as the group of rational points of an abelian variety over $\mathbb{F}_4$, and that the abelian variety can be taken to be ordinary except possibly when G takes the form $(\mathbb{Z}/3\mathbb{Z})^{n_1} \times \prod_{j>1}(\mathbb{Z}/3^j\mathbb{Z})^{n_j}$, where n_1 is odd. Now consider one of the exceptional groups G where additionally $n_s \geq 1$ for some $s > 1$. There are ordinary abelian varieties A_1 and A_2 over $\mathbb{F}_4$ whose groups of rational points are

$$A_1(\mathbb{F}_4) \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3^s)$$

and

$$A_2(\mathbb{F}_4) \cong (\mathbb{Z}/3\mathbb{Z})^{n_1-1} \times (\mathbb{Z}/3^s/\mathbb{Z})^{n_s-1} \times \prod_{j\notin\{1,s\}} (\mathbb{Z}/3^j\mathbb{Z})^{n_j}$$

by Corollary 5.12 and [Marseglia and Springer 2023, Theorem 3.3], respectively. Therefore, $G \cong (A_1 \times A_2)(\mathbb{F}_4)$, as desired. □

6. Groups of rational points and categorical equivalences

In this section, we first present Theorem 6.2, which describes groups of rational points by deploying a categorical equivalence between abelian varieties in certain squarefree isogeny classes and fractional ideals in étale algebras. In such an isogeny class, we deduce in Proposition 6.5 that every abelian variety A with endomorphism ring $\operatorname{End}(A) = S$ has the same group of rational points if S satisfies a certain local condition. In Remark 6.6, we compare this result to Corollary 3.3.

Throughout this section we use the usual notation. We denote by $\mathscr{I}_h$ a squarefree isogeny class over $\mathbb{F}_q$. We set $K = \mathbb{Q}[x]/(h)$ and $R = \mathbb{Z}[\pi, \bar{\pi}]$, where π is the class of x in K.

Definition 6.1. We say that $\mathscr{I}_h$ satisfies

- Ord if $\mathscr{I}_h$ is ordinary,
- CS if q is prime.

Theorem 6.2. *If $\mathscr{I}_h$ satisfies* Ord (*resp.* CS) *then there exists a covariant* (*resp. contravariant*) *equivalence between $\mathscr{I}_h$ and the category of fractional R-ideals* (*with R-linear morphisms*)*. Denote by $\mathscr{F}$ the functor inducing the equivalence. Let A be an abelian variety in $\mathscr{I}_h$, with dual variety $A^\vee$. Put $\mathscr{F}(A) = I$, where I is a fractional R-ideal.*

(a) *We have $\mathscr{F}(A^\vee) = \bar{I}^t$ and* $\operatorname{End}(A^\vee) = \overline{\operatorname{End}(A)}$.

(b) *There is a $\mathbb{Z}$-linear isomorphism*

$$A(\mathbb{F}_{q^n}) \cong \frac{I}{(1-\pi^n)I}$$

for all $n \geq 1$.

(c) *There are $\mathbb{Z}$-linear isomorphisms*

$$A^\vee(\mathbb{F}_{q^n}) \cong \frac{\bar{I}^t}{(1-\pi^n)\bar{I}^t} \cong \frac{I^t}{(1-\bar{\pi}^n)I^t} \cong \frac{I}{(1-\bar{\pi}^n)I} \cong \frac{\bar{I}}{(1-\pi^n)\bar{I}}$$

for all $n \geq 1$.

Proof. The existence of the equivalence is given by [Deligne 1969] in the Ord case, and by [Centeleghe and Stix 2015] in the CS case. Part (a) is [Marseglia 2021, Theorem 5.2] in the Ord case, and [Bergström et al. 2023, Corollary 3.26] in the CS case. Part (b), for $n = 1$, is [Marseglia 2021, Corollary 4.7] for both cases, but the proof is identical for $n > 1$. In the Ord case, the key ingredients are [Howe 1995, Lemma 4.13 and Proposition 4.14], while the proof in the CS case uses a local argument.

For Part (c), observe that the first $\mathbb{Z}$-linear isomorphism is the combination of Parts (a) and (b), while the second and fourth are the application of complex conjugation. For the third isomorphism, we use Lemma 2.8 to deduce

$$\frac{I^t}{(1-\bar{\pi}^n)I^t} \cong \frac{(1-\bar{\pi}^n)^{-1}I}{I} \cong \frac{I}{(1-\bar{\pi}^n)I}. \qquad \square$$

Remark 6.3. We emphasize that the hypotheses for Theorem 6.2 only impose conditions on the isogeny class over the base field $\mathbb{F}_q$. Observe that the property of being squarefree is not stable under base extension, and the functor we invoke in the CS case requires the base field to be prime. Nevertheless, we describe $A(\mathbb{F}_{q^n})$ for all $n \geq 1$ because $A(\mathbb{F}_{q^n}) = \ker(1-\pi^n)$ is the kernel of an isogeny defined over the base field $\mathbb{F}_q$.

Remark 6.4. For $n = 1$, the $\mathbb{Z}$-linear isomorphisms in Theorem 6.2 are trivially R-linear. Indeed, for part (b), since R is generated over $\mathbb{Z}$ by π and $\overline{\pi} = q/\pi$, and $I/(1-\pi)I$ is annihilated by $(1-\pi)$, R-linearity trivially follows from $\mathbb{Z}$-linearity. The same applies for part (c).

Now we show that, in the Ord and CS cases, the group of rational points is uniquely determined by the endomorphism ring under certain conditions.

Proposition 6.5. *Let A be an abelian variety in a squarefree isogeny class $\mathscr{I}_h$ over $\mathbb{F}_q$ satisfying* Ord *or* CS. *Write $S = \operatorname{End}(A)$. For each $n \geq 1$, if $\operatorname{type}_{\mathfrak{p}}(S) \leq 2$ for every prime $\mathfrak{p}$ of S above $(1-\pi^n)$, then the group of $\mathbb{F}_{q^n}$-rational points of A is uniquely determined by S. Specifically,*

$$A(\mathbb{F}_{q^n}) \cong \frac{S}{(1-\pi^n)S}$$

are isomorphic as $\mathbb{Z}$-modules.

Proof. The statement follows from Proposition 2.11 with Theorem 6.2. □

Remark 6.6. As noted in Section 2, an order S is Gorenstein at a prime $\mathfrak{p}$ if and only if $\operatorname{type}_{\mathfrak{p}}(S) = 1$. Hence Proposition 6.5 is a generalization of Corollary 3.3. As a trade-off, the isomorphism is $\mathbb{Z}$-linear rather than S-linear, and we need further hypotheses on the isogeny class.

In Proposition 6.5, it is important that the local type of the endomorphism ring is at most 2 at primes above $1-\pi^n$. Indeed, in Example 6.7, we produce abelian varieties with the same endomorphism ring of (local) type 3 but nonisomorphic groups of points.

Example 6.7. The polynomial

$$h = x^4 + 6x^2 + 25 = (x^2 - 2x + 5)(x^2 + 2x + 5)$$

defines an isogeny class $\mathscr{I}_h$ of ordinary abelian surfaces over $\mathbb{F}_5$, which has LMFDB label 2.5.a_g. Consider the order $S = \mathbb{Z} + 2\mathscr{O}_K$. This is the unique overorder of R with $[\mathscr{O}_K : S] = [S : R] = 8$. Moreover, S is the unique overorder of R with a prime $\mathfrak{p}$ with $\operatorname{type}_{\mathfrak{p}}(S) = 3$. This prime is $\mathfrak{p} = 2\mathscr{O}_K$, which is also the conductor of S in $\mathscr{O}_K$.

Using Theorem 6.2 and algorithms from [Marseglia 2020], we compute that there are 5 isomorphism classes of abelian varieties with endomorphism ring S, represented by fractional ideals S, I, I^t, J, and S^t. One has $J \cong J^t$. Let A_S, A_I, A_{I^t}, A_J, and A_{S^t} be the corresponding abelian varieties, respectively; see Theorem 6.2. We have

$$A_S(\mathbb{F}_5) \cong A_{S^t}(\mathbb{F}_5) \cong A_J(\mathbb{F}_5) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{8\mathbb{Z}} \quad \text{and} \quad A_I(\mathbb{F}_5) \cong A_{I^t}(\mathbb{F}_5) \cong \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{8\mathbb{Z}}.$$

7. The dual abelian variety

In this section, we study the relationship between an abelian variety and its dual. We use the categorical equivalences presented in Theorem 6.2 which builds a bridge between abelian varieties and fractional ideals. In the first part, we will prove that we have an isomorphism $A(\mathbb{F}_q) \cong A^\vee(\mathbb{F}_q)$ under certain conditions on the endomorphism ring $\operatorname{End}(A)$ and the fractional ideal associated to A. Clearly, $A(\mathbb{F}_q) \cong A^\vee(\mathbb{F}_q)$ whenever A is the Jacobian of a curve or, more generally, a principally polarizable abelian variety. In fact, the implication only uses that A is a self-dual abelian variety, that is, $A \cong A^\vee$.

In the second part of the section, we investigate when an abelian variety fails to be self-dual. In particular, we prove that A is not self-dual if its endomorphism ring $\operatorname{End}(A)$ satisfies a certain local condition. To conclude, we provide a sequence of examples comparing various properties implying and implied by self-duality.

In this section, we use the same notation as Section 6. Specifically, we denote by $\mathscr{I}_h$ a squarefree isogeny class over $\mathbb{F}_q$. We set $K = \mathbb{Q}[x]/(h)$ and $R = \mathbb{Z}[\pi, \bar{\pi}]$, where π is the class of x in K.

7.1. ***The group of points of the dual abelian variety.*** In Proposition 7.1, building on results proven previously, we give a list of conditions that guarantee the existence of an isomorphism $A(\mathbb{F}_{q^n}) \cong A^\vee(\mathbb{F}_{q^n})$. In Example 7.2, we exhibit a geometrically simple ordinary abelian variety A with $A(\mathbb{F}_q) \not\cong A^\vee(\mathbb{F}_q)$. In Example 7.3, we show that squarefree ordinary examples over $\mathbb{F}_q$ always exist in small dimensions for small finite fields $\mathbb{F}_q$. In [Rybakov 2014, Example 4.2], a nonsimple abelian surface A with $A(\mathbb{F}_q) \not\cong A^\vee(\mathbb{F}_q)$ is produced using a different method.

Proposition 7.1. *Let A be in $\mathscr{I}_h$, and put $S = \operatorname{End}(A)$. Fix $n \geq 1$. If one of the following assumptions holds, then $A(\mathbb{F}_{q^n}) \cong A^\vee(\mathbb{F}_{q^n})$:*

(a) *$S = \bar{S}$ and S is Gorenstein at $\mathfrak{p}$ for every prime $\mathfrak{p}$ of S above $(1-\pi^n)$.*

(b) *$\mathscr{I}_h$ satisfies* Ord *or* CS, *$S = \bar{S}$, and $\operatorname{type}_{\mathfrak{p}}(S) \leq 2$ for every prime $\mathfrak{p}$ of S above $(1-\pi^n)$.*

(c) *$\mathscr{I}_h$ satisfies* Ord *or* CS, *and one of the following holds, where $\mathscr{F}(A) = I$:*

- *For every prime $\mathfrak{p}$ of R above $(1-\pi^n)$, we have an R-linear isomorphism $I_{\mathfrak{p}} \cong (\bar{I})_{\mathfrak{p}}$.*
- *For every prime $\mathfrak{p}$ of R above $(1-\pi^n)$, we have an R-linear isomorphism $I_{\mathfrak{p}} \cong (\bar{I}^t)_{\mathfrak{p}}$.*

Proof. Part (a) follows from Corollary 3.3 because $\operatorname{End}(A^\vee) = \bar{S} = S$. Part (b) follows similarly from Proposition 6.5. By Theorem 6.2, we have $\mathbb{Z}$-linear isomorphisms

$$A(\mathbb{F}_{q^n}) \cong I \otimes_R \frac{R}{(1-\pi^n)R} \quad \text{and} \quad A^\vee(\mathbb{F}_{q^n}) \cong \bar{I} \otimes_R \frac{R}{(1-\pi^n)R} \cong \bar{I}^t \otimes_R \frac{R}{(1-\pi^n)R}.$$

Combined with Lemma 2.4, this proves Part (c). □

Example 7.2. Consider the isogeny class $\mathscr{I}_h$ of ordinary abelian surfaces over $\mathbb{F}_4$ determined by the polynomial $h = x^4 + 2x^3 + x^2 + 8x + 16$. According to [LMFDB 2022], this isogeny class, which has label 2.4.c_b, is geometrically simple and contains a Jacobian. Let $\mathscr{O}_K$ be the maximal order of K. We have $2\mathscr{O}_K = \mathfrak{p}^2\bar{\mathfrak{p}}^2$, where $\mathfrak{p}$ is a prime of $\mathscr{O}_K$. Consider the order $S = R + \mathfrak{p}^2$. It turns out that R has three overorders, namely, S, $\overline{S}$, and $\mathcal{O}_K$, and all of these orders are Gorenstein. Using Theorem 6.2, there is an abelian variety A with $\mathrm{End}(A) = S$; hence $\mathrm{End}(A^\vee) = \overline{S}$. Using Corollary 3.3, one computes that $A(\mathbb{F}_4)$ and $A^\vee(\mathbb{F}_4)$ are not isomorphic. Indeed, they are

$$\frac{\mathbb{Z}}{28\mathbb{Z}} \quad \text{and} \quad \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{14\mathbb{Z}}.$$

Example 7.3. Consider the following set of pairs of positive integers (g, q):

$$\{(2, q) : 2 \leq q \leq 128 \text{ is a prime power}\} \cup \{(3, q) : 2 \leq q \leq 9 \text{ is a prime power}\}$$
$$\cup \{(3, 16), (3, 25)\} \cup \{(4, q) : q \in \{2, 3, 4\}\} \cup \{(5, 2)\}.$$

For each pair (g, q) in the set above, there is a squarefree ordinary abelian variety A of dimension g over $\mathbb{F}_q$ satisfying

$$A(\mathbb{F}_q) \not\cong A^\vee(\mathbb{F}_q).$$

7.2. ***Self-duality.*** Recall the following well-known theorem.

Theorem 7.4. *If A is an abelian variety over $\mathbb{F}_q$, then each statement below implies the next*:

(a) *A is a Jacobian variety.*

(b) *A is a principally polarizable abelian variety.*

(c) *$A \cong A^\vee$ is self-dual.*

(d) *$A(\mathbb{F}_q) \cong A^\vee(\mathbb{F}_q)$ are isomorphic groups.*

When A is squarefree, *the following item* (d$'$) *is also implied by self-duality* (c):

(d$'$) $\mathrm{End}(A) = \overline{\mathrm{End}(A)}$ *is stable under complex conjugation.*

We already observed in Example 7.2 that properties (d) and (d$'$) do not always hold. Now we show that there are counterexamples to all of the reverse implications in Theorem 7.4. For (b) $\not\Rightarrow$ (a), see Example 7.5, and for (c) $\not\Rightarrow$ (b), see Example 7.6. In Example 7.8, we show that (d) and (d$'$) combined do not imply (c). Moreover, in Example 7.9, we show that (d) $\not\Rightarrow$ (d$'$), which is another exhibition that (d$'$) $\not\Rightarrow$ (c). Note that we have the implication (d$'$) $\Rightarrow$ (d) under certain hypotheses; see Proposition 7.1.

The following example is well known, but we record it for completeness.

Example 7.5 (principally polarizable but not Jacobian). It is easy to find principally polarizable varieties which are not Jacobians. For example, there are currently 30,079 geometrically simple ordinary isogeny classes in the LMFDB which contain a principally polarizable abelian variety but no Jacobian varieties [LMFDB 2022].

Example 7.6 (self-dual but not principally polarizable). If $\mathscr{I}_h$ is a simple ordinary isogeny class, then the class number of the field $K = \mathbb{Q}[x]/(h)$ is equal to the number of abelian varieties in $\mathscr{I}_h$ whose endomorphism ring is maximal; see [Waterhouse 1969, Theorem 6.2]. In particular, if K has class number 1, then any abelian variety A in $\mathscr{I}_h$ whose endomorphism ring is $\mathrm{End}(A) = \mathcal{O}_K$ must be self-dual.

It is easy to find isogeny classes satisfying this property which do not contain any principally polarizable abelian varieties by using [Howe 1995, Theorem 1.3], for example. See the LMFDB isogeny class 2.2.ab_ab for a concrete ordinary example, or 4.2.ad_c_f_an for one which is also geometrically simple.

One way to find examples of abelian varieties which are not self-dual is to first use the categorical equivalence in Theorem 6.2 to compute all isomorphism classes, and then use Theorem 6.2 (a) to determine which classes are self-dual. Alternatively, one may use the following proposition which only requires inspecting the local properties of orders in the endomorphism algebra. The latter technique easily finds Example 7.8.

Proposition 7.7. *Let A be any abelian variety in $\mathscr{I}_h$ satisfying* Ord *or* CS, *let S be an order in K such that $S = \bar{S}$, and let $\mathfrak{p}$ be a prime of S such that* $\operatorname{type}_{\mathfrak{p}}(S) = 2$ *and* $\mathfrak{p} = \bar{\mathfrak{p}}$. *If* $S \subseteq \operatorname{End}(A)$ *and* $S_{\mathfrak{p}} = \operatorname{End}(A)_{\mathfrak{p}}$, *then A is not self-dual. In particular, such an A is not principally polarizable and cannot be a Jacobian.*

Proof. This follows from Proposition 2.12 and Theorem 6.2 (a). □

Example 7.8 (same endomorphism ring but not self-dual). We go back to the isogeny class $\mathscr{I}_h$ from Example 6.7. One computes that R has a unique minimal overorder T and $[T : R] = 2$. Such an order is then necessarily stable under complex conjugation; that is, $T = \overline{T}$. Also, T has a unique prime $\mathfrak{q}$ above 2 which also then satisfies $\mathfrak{q} = \bar{\mathfrak{q}}$. This prime is the unique noninvertible prime of T, and we have $\operatorname{type}_{\mathfrak{q}}(T) = 2$. Recall that abelian varieties in $\mathscr{I}_h$ with endomorphism ring T exist by Theorem 6.2. By Proposition 6.5, every abelian variety with endomorphism ring T has group of rational points isomorphic to $T/(1-\pi)T$. On the other hand, by Proposition 7.7, we see that $A \ncong A^\vee$ for every abelian variety A with endomorphism ring T.

We observe that the non-self-dual abelian variety A found in Example 7.8 also satisfies $A(\mathbb{F}_5) \cong A^\vee(\mathbb{F}_5)$, thereby exhibiting (d) $\not\Leftarrow$ (c) in Theorem 7.4. This is also exhibited in the following example, which additionally proves (d) $\not\Leftarrow$ (d′) in the same theorem.

Example 7.9 (isomorphic groups but different endomorphism ring). Consider the ordinary isogeny class $\mathscr{I}_h$ of abelian surfaces defined over $\mathbb{F}_3$ determined by the polynomial

$$h = x^4 - x^3 + 4x^2 - 3x + 9 = (x^2 - 2x + 3)(x^2 + x + 3).$$

The order $R = \mathbb{Z}[\pi, \bar{\pi}]$ has index $[\mathscr{O}_K : R] = 9$ in the maximal order $\mathscr{O}_K$ of K. Since $h(1) = 10$ is coprime with the conductor $(R : \mathscr{O}_K)$, we deduce that $\mathscr{I}_h$ is cyclic by Theorem 4.5. Moreover, since 10 is a squarefree integer, we get that $\mathscr{I}_h$ is also trivially rich; see Theorem 5.7.

We observe that R has exactly two primes above the singular rational prime 3. These two primes are complex conjugates to each other, and we denote them by $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. There are only two orders between R and $\mathscr{O}_K$, both with index 3. These can be realized as the multiplicator rings $S = (\mathfrak{p} : \mathfrak{p})$ and $\bar{S} = (\bar{\mathfrak{p}} : \bar{\mathfrak{p}})$. By Theorem 6.2, we conclude that there is an abelian variety A in $\mathscr{I}_h$ such that $\operatorname{End}(A) = S$ and $\operatorname{End}(A^\vee) = \bar{S}$ are not equal, but $A(\mathbb{F}_3) \cong A^\vee(\mathbb{F}_3) \cong \mathbb{Z}/10\mathbb{Z}$.

Acknowledgements

We thank Jonas Bergström, Valentijn Karemaker, and Bjorn Poonen for providing comments on a draft version of this paper. We thank the referee for pointing us to the reference [Rybakov 2014].

Marseglia is supported by NWO grant VI.Veni.202.107. Springer is partially supported by National Science Foundation award CNS-2001470 and by the Additional Funding Programme for Mathematical Sciences, delivered by EPSRC (EP/V521917/1) and the Heilbronn Institute for Mathematical Research.

References

[Bass 1963] H. Bass, "On the ubiquity of Gorenstein rings", *Math. Z.* **82** (1963), 8–28. MR Zbl

[Berardini and Giangreco-Maidana 2022] E. Berardini and A. J. Giangreco-Maidana, "Weil polynomials of abelian varieties over finite fields with many rational points", *Int. J. Number Theory* **18**:7 (2022), 1591–1603. MR Zbl

[Bergström et al. 2023] J. Bergström, V. Karemaker, and S. Marseglia, "Polarizations of abelian varieties over finite fields via canonical liftings", *Int. Math. Res. Not.* **2023**:4 (2023), 3194–3248. MR Zbl

[van Bommel et al. 2021] R. van Bommel, E. Costa, W. Li, B. Poonen, and A. Smith, "Abelian varieties of prescribed order over finite fields", preprint, 2021. arXiv 2106.13651

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Buchmann and Lenstra 1994] J. A. Buchmann and H. W. Lenstra, Jr., "Approximating rings of integers in number fields", *J. Théor. Nombres Bordeaux* **6**:2 (1994), 221–260. MR Zbl

[Centeleghe and Stix 2015] T. G. Centeleghe and J. Stix, "Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$", *Algebra Number Theory* **9**:1 (2015), 225–265. MR Zbl

[Cohen 2000] H. Cohen, *Advanced topics in computational number theory*, Grad. Texts in Math. **193**, Springer, 2000. MR Zbl

[David et al. 2014] C. David, D. Garton, Z. Scherr, A. Shankar, E. Smith, and L. Thompson, "Abelian surfaces over finite fields with prescribed groups", *Bull. Lond. Math. Soc.* **46**:4 (2014), 779–792. MR Zbl

[Deligne 1969] P. Deligne, "Variétés abéliennes ordinaires sur un corps fini", *Invent. Math.* **8** (1969), 238–243. MR

[Dupuy et al. 2021] T. Dupuy, K. Kedlaya, D. Roe, and C. Vincent, "Isogeny classes of abelian varieties over finite fields in the LMFDB", pp. 375–448 in *Arithmetic geometry, number theory, and computation*, Springer, 2021. MR Zbl

[Eisenbud 1995] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Grad. Texts in Math. **150**, Springer, 1995. MR Zbl

[Giangreco-Maidana 2019] A. J. Giangreco-Maidana, "On the cyclicity of the rational points group of abelian varieties over finite fields", *Finite Fields Appl.* **57** (2019), 139–155. MR Zbl

[Giangreco-Maidana 2020] A. J. Giangreco-Maidana, "Local cyclicity of isogeny classes of abelian varieties defined over finite fields", *Finite Fields Appl.* **62** (2020), art. id. 101628. Correction in **69**:2 (2021), art. id. 101703. MR Zbl

[Howe 1995] E. W. Howe, "Principally polarized ordinary abelian varieties over finite fields", *Trans. Amer. Math. Soc.* **347**:7 (1995), 2361–2401. MR Zbl

[Howe and Kedlaya 2021] E. W. Howe and K. S. Kedlaya, "Every positive integer is the order of an ordinary abelian variety over $\mathbb{F}_2$", *Res. Number Theory* **7**:4 (2021), art. id. 59. MR Zbl

[Kadets 2021] B. Kadets, "Estimates for the number of rational points on simple abelian varieties over finite fields", *Math. Z.* **297**:1-2 (2021), 465–473. MR Zbl

[Kedlaya 2024] K. S. Kedlaya, "Abelian varieties over $\mathbb{F}_2$ of prescribed order", pp. 43–58 in *Publ. Math. Besançon* (Août, French Polynesia, 2021), Algèbre et théorie des nombres **2024**, Presses Univ. Franche-Comté, 2024. MR Zbl

[Kotelnikova 2019] Y. Kotelnikova, "Groups of points on abelian threefolds over finite fields", *Finite Fields Appl.* **58** (2019), 177–199. MR Zbl

[Lenstra 1996] H. W. Lenstra, Jr., "Complex multiplication structure of elliptic curves", *J. Number Theory* **56**:2 (1996), 227–241. MR Zbl

[LMFDB 2022] "The L-functions and modular forms database", electronic reference, 2022, available at http://www.lmfdb.org. Accessed 18 November 2022.

[Madan and Pal 1977] M. L. Madan and S. Pal, "Abelian varieties and a conjecture of R. M. Robinson", *J. Reine Angew. Math.* **291** (1977), 78–91. MR Zbl

[Marseglia 2020] S. Marseglia, "Computing the ideal class monoid of an order", *J. Lond. Math. Soc.* (2) **101**:3 (2020), 984–1007. MR Zbl

[Marseglia 2021] S. Marseglia, "Computing square-free polarized abelian varieties over finite fields", *Math. Comp.* **90**:328 (2021), 953–971. MR Zbl

[Marseglia 2024] S. Marseglia, "Cohen–Macaulay type of orders, generators and ideal classes", *J. Algebra* **658** (2024), 247–276. MR Zbl

[Marseglia and Springer 2023] S. Marseglia and C. Springer, "Every finite abelian group is the group of rational points of an ordinary abelian variety over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_5$", *Proc. Amer. Math. Soc.* **151**:2 (2023), 501–510. MR Zbl

[Matsumura 1986] H. Matsumura, *Commutative ring theory*, Cambridge Stud. Adv. Math. **8**, Cambridge Univ. Press, 1986. MR Zbl

[Milne 1986] J. S. Milne, "Abelian varieties", pp. 103–150 in *Arithmetic geometry* (Storrs, CT, 1984), Springer, 1986. MR Zbl

[Ooishi 1976] A. Ooishi, "Matlis duality and the width of a module", *Hiroshima Math. J.* **6**:3 (1976), 573–587. MR Zbl

[Rück 1987] H.-G. Rück, "A note on elliptic curves over finite fields", *Math. Comp.* **49**:179 (1987), 301–304. MR Zbl

[Rybakov 2010] S. Rybakov, "The groups of points on abelian varieties over finite fields", *Cent. Eur. J. Math.* **8**:2 (2010), 282–288. MR Zbl

[Rybakov 2012] S. Rybakov, "The groups of points on abelian surfaces over finite fields", pp. 151–158 in *Arithmetic*, *geometry*, *cryptography and coding theory* (Marseille/Bastia, France, 2011), Contemp. Math. **574**, Amer. Math. Soc., Providence, RI, 2012. MR Zbl

[Rybakov 2014] S. Rybakov, "Finite group subschemes of abelian varieties over finite fields", *Finite Fields Appl.* **29** (2014), 132–150. MR Zbl

[Rybakov 2015] S. Rybakov, "On classification of groups of points on abelian varieties over finite fields", *Mosc. Math. J.* **15**:4 (2015), 805–815. MR Zbl

[Springer 2021] C. Springer, "The structure of the group of rational points of an abelian variety over a finite field", *Eur. J. Math.* **7**:3 (2021), 1124–1136. MR Zbl

[Tate 1966] J. Tate, "Endomorphisms of abelian varieties over finite fields", *Invent. Math.* **2** (1966), 134–144. MR Zbl

[Tsfasman 1985] M. A. Tsfasman, "Group of points of an elliptic curve over a finite field", pp. 286–287 in *Theory of numbers and its applications* (Tbilisi, Georgia, 1985), Univ. Georgia, 1985. In Russian. Zbl

[Tsfasman et al. 2007] M. Tsfasman, S. Vlăduţ, and D. Nogin, *Algebraic geometric codes*: *basic notions*, Math. Surv. Monogr. **139**, Amer. Math. Soc., Providence, RI, 2007. MR Zbl

[Voight 2021] J. Voight, *Quaternion algebras*, Grad. Texts in Math. **288**, Springer, 2021. MR Zbl

[Voloch 1988] J. F. Voloch, "A note on elliptic curves over finite fields", *Bull. Soc. Math. France* **116**:4 (1988), 455–458. MR Zbl

[Waterhouse 1969] W. C. Waterhouse, "Abelian varieties over finite fields", *Ann. Sci. École Norm. Sup.* (4) **2** (1969), 521–560. MR Zbl

[Waterhouse and Milne 1971] W. C. Waterhouse and J. S. Milne, "Abelian varieties over finite fields", pp. 53–64 in 1969 *Number Theory Institute* (Stony Brook, NY, 1969), Proc. Sympos. Pure Math. **20**, Amer. Math. Soc., Providence, RI, 1971. MR Zbl

[Weil 1948] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publ. Inst. Math. Univ. Strasbourg **7**, Hermann & Cie, Paris, 1948. MR Zbl

[Xing 1994] C. P. Xing, "The structure of the rational point groups of simple abelian varieties of dimension two over finite fields", *Arch. Math.* (*Basel*) **63**:5 (1994), 427–430. MR Zbl

[Xing 1996] C. Xing, "On supersingular abelian varieties of dimension two over finite fields", *Finite Fields Appl.* **2**:4 (1996), 407–421. MR Zbl

Communicated by Bjorn Poonen
Received 2023-04-21 Revised 2024-03-13 Accepted 2024-04-29

s.marseglia@uu.nl *Mathematical Institute, Utrecht University, Utrecht, Netherlands*

c.springer@ucl.ac.uk *Department of Mathematics, University College London, London, United Kingdom*

The Heilbronn Institute for Mathematical Research, Bristol, United Kingdom

mathematical sciences publishers msp

ALGEBRA AND NUMBER THEORY 19:3 (2025)
https://doi.org/10.2140/ant.2025.19.551

Algebraic cycles and functorial lifts from G_2 to PGSp_6

Antonio Cauchi, Francesco Lemma and Joaquín Rodrigues Jacinto

We study instances of Beilinson–Tate conjectures for automorphic representations of PGSp_6 whose spin L-function has a pole at $s = 1$. We construct algebraic cycles of codimension 3 in the Siegel–Shimura variety of dimension 6 and we relate its regulator to the residue at $s = 1$ of the L-function of certain cuspidal forms of PGSp_6. Using the exceptional theta correspondence between the split group of type G_2 and PGSp_6 and assuming the nonvanishing of a certain archimedean integral, this allows us to confirm a conjecture of Gross and Savin on rank-7 motives of type G_2.

1. Introduction

We establish a connection between algebraic cycles in Siegel sixfolds and the residue at $s = 1$ of spin L-functions of automorphic representations of GSp_6, as predicted by conjectures of Beilinson and Tate. Moreover, we exploit an exceptional theta correspondence between the split group of type G_2 and PGSp_6 to answer a question of Gross and Savin.

Cauchi was supported by the European Research Council under the European Union's Horizon 2020 research and innovation programme (grant 682152) as well as by the NSERC grant RGPIN-2018-04392 and Concordia Horizon postdoc fellowship n.8009. Lemma was supported by the ANR Ferplay and the ANR ClapClap. Rodrigues Jacinto was financially supported by the ERC-2018-COG-818856-HiCoShiVa and by the project ANR-19-CE40-0015 COLOSS.

MSC2020: 11F46, 11F67, 14G10, 14G35.

Keywords: theta correspondence, algebraic cycles, Beilinson conjecture, Tate conjecture.

1.1. ***Motivation.*** Let $\pi = \pi_\infty \otimes \pi_f$ be a cohomological cuspidal automorphic representation of $\mathrm{PGSp}_6(\mathbb{A})$, let $M(\pi_f)$ denote the spin Chow motive with coefficients in a number field L conjecturally attached to π and let $L(s, M(\pi_f)(3))$ be its Hasse–Weil L-function. Let

$$r_{\mathcal{H}} : H^1_{\mathcal{M}}(M(\pi_f)(4)) \oplus N(M(\pi_f)(3)) \to H^1_{\mathcal{H}}(M(\pi_f)(4))$$

denote Beilinson–Deligne regulator. Here $H^1_{\mathcal{M}}(M(\pi_f)(4))$ denotes the first motivic cohomology group of $M(\pi_f)(4)$, the group $N(M(\pi_f)(3))$ denotes algebraic cycles in $M(\pi_f)(3)$ up to homological equivalence and $H^1_{\mathcal{H}}(M(\pi_f)(4))$ denotes the first absolute Hodge cohomology group of $M(\pi_f)(4)$.

Conjecture 1.1 (Beilinson–Tate). (1) The map $r_{\mathcal{H}}$ induces an isomorphism

$$(H^1_{\mathcal{M}}(M(\pi_f)(4)) \oplus N(M(\pi_f)(3))) \otimes_{\mathbb{Q}} \mathbb{R} \to H^1_{\mathcal{H}}(M(\pi_f)(4)).$$

(2) $\mathrm{ord}_{s=0} L(s, M(\pi_f)(3)) = \dim_L H^1_{\mathcal{M}}(M(\pi_f)(4))$.

(3) $-\mathrm{ord}_{s=1} L(s, M(\pi_f)(3)) = \dim_L N(M(\pi_f)(3))$.

(4) $\det(\mathrm{Im}\, r_{\mathcal{H}}) = L^*(1, M(\pi_f)(3))\mathcal{D}(M(\pi_f)(4))$, where $\mathcal{D}(M(\pi_f)(4))$ denotes the Deligne L-structure of $\det(H^1_{\mathcal{H}}(M(\pi_f)(4))$.

In [Burgos Gil et al. 2024], we studied the contribution of the motivic cohomology to this conjecture. This corresponds to the case where $L(s, M(\pi_f)(3))$ does not have a pole at $s = 1$. In this article, we focus on the contribution of algebraic cycles, which corresponds to the case where $L(s, M(\pi_f)(3))$ has a simple pole at $s = 1$.

The ℓ-adic étale realization $M_\ell(\pi_f)$ of $M(\pi_f)$ is expected to be a $\mathrm{GL}_8(\overline{\mathbb{Q}}_\ell)$-valued Galois representation factoring through the spin representation $\mathrm{Spin} : \mathrm{Spin}_7(\overline{\mathbb{Q}}_\ell) \to \mathrm{GL}_8(\overline{\mathbb{Q}}_\ell)$. If $L(s, M(\pi_f)(3))$ has a pole at $s = 1$, Conjecture 1.1(3) implies the existence of an invariant vector in this eight-dimensional Galois representation. As the stabilizer in $\mathrm{Spin}_7(\overline{\mathbb{Q}}_\ell)$ of a generic vector in the spin representation is the exceptional group $G_2(\overline{\mathbb{Q}}_\ell)$, by Langlands reciprocity principle, π should be a functorial lift from a group G of type G_2. In fact, we have $\mathrm{Spin}_{|_{G_2}} = \mathrm{Std} \oplus \mathbf{1}$, where Std denotes the standard representation of G_2 and $\mathbf{1}$ denotes the trivial representation. Then, if σ is a cuspidal automorphic representation of $G(\mathbb{A})$ lifting to π, Gross and Savin [1998] conjectured that the motive $M(\pi_f)$ decomposes as the direct sum of the rank-7 motive $M(\sigma_f)$ attached to σ and the rank-1 trivial motive generated by the class given in Conjecture 1.1. Moreover, inspired by local calculations, they conjectured that this class should arise from a Hilbert modular threefold.

1.2. ***Main results.*** Let F denote a real étale quadratic $\mathbb{Q}$-algebra, i.e., F is either a quadratic extension of $\mathbb{Q}$ or $\mathbb{Q} \times \mathbb{Q}$. Associated to the totally real étale cubic algebra $E = \mathbb{Q} \times F$ of $\mathbb{Q}$ there is a Hilbert modular threefold $\mathrm{Sh}_{\boldsymbol{H}} / \mathbb{Q}$, with underlying reductive group $\boldsymbol{H} = \{g \in \mathrm{Res}_{E/\mathbb{Q}} \mathrm{GL}_{2,E} \mid \det(g) \in \boldsymbol{G}_m\}$. The group $\boldsymbol{H}$ embeds naturally into $\boldsymbol{G} = \mathrm{GSp}_6$ and one has a closed embedding $\iota : \mathrm{Sh}_{\boldsymbol{H}} \hookrightarrow \mathrm{Sh}_{\boldsymbol{G}}$ of codimension 3 in the Shimura variety attached to $\boldsymbol{G}$, which is the Siegel variety of dimension 6. Let V^λ be the irreducible algebraic representation of $\boldsymbol{G}$ of highest weight $\lambda = (\lambda_1, \lambda_2, \lambda_3, c)$ (see Section 2 for notation on algebraic representations). The representation V^λ contains the trivial $\boldsymbol{H}$-representation if and only if $c=0$ and $\lambda_1=\lambda_2+\lambda_3$. When this holds ι^*V^λ contains $\lambda_2-\lambda_3+1$ copies of the trivial representation of $\boldsymbol{H}$, which we index by the values $\lambda_2\geq\mu\geq\lambda_3$. Then, for any such μ, the cycle $\mathrm{Sh}_{\boldsymbol{H}}$ of $\mathrm{Sh}_{\boldsymbol{G}}$ induces a class

$$\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{M}}\in H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}},\mathscr{V}^\lambda_{\mathcal{M}}(3)),$$

where $\mathscr{V}^\lambda_{\mathcal{M}}$ is the Chow local system associated to V^λ and $H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}},\mathscr{V}^\lambda_{\mathcal{M}}(3))$ is the motivic cohomology group of $\mathrm{Sh}_{\boldsymbol{G}}$ with coefficients in $\mathscr{V}^\lambda_{\mathcal{M}}(3)$. We denote by $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}\in H^7_{\mathcal{H}}(\mathrm{Sh}_{\boldsymbol{G}},\mathscr{V}^\lambda_{\mathcal{H}}(4))$ (resp. $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B}\in H^6_B(\mathrm{Sh}_{\boldsymbol{G}},\mathscr{V}^\lambda_B(3))$) the image of $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{M}}$ in absolute Hodge cohomology, (resp. Betti cohomology) (see Definition 3.11 for the precise definition of $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}$). Let π be a cuspidal automorphic representation of $\mathrm{PGSp}_6(\mathbb{A})$ whose archimedean component belongs to the discrete series L-packet of V^λ and has Hodge type $(3,3)$. For a cusp form $\Psi=\Psi_\infty\otimes\Psi_f$ in the space of π, whose archimedean component Ψ_∞ is a highest weight vector in the minimal K-type of π_∞, we have a vector valued harmonic differential form ω_Ψ whose cohomology class $[\omega_\Psi]$ is an element of $H^6_{\mathrm{dR},c}(\mathrm{Sh}_{\boldsymbol{G}},\mathscr{V}^\lambda_{\mathrm{dR}})$. Poincaré duality induces maps

$$\langle\,\cdot\,,[\omega_\Psi]\rangle_B : H^6_B(\mathrm{Sh}_{\boldsymbol{G}},\mathscr{V}^\lambda_B(3))\to\mathbb{C},$$
$$\langle\,\cdot\,,[\omega_\Psi]\rangle_{\mathcal{H}} : H^7_{\mathcal{H}}(\mathrm{Sh}_{\boldsymbol{G}},\mathscr{V}^\lambda_{\mathcal{H}}(4))\to\mathbb{C}.$$

The pairings $\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B},[\omega_\Psi]\rangle_B$ and $\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}},[\omega_\Psi]\rangle_{\mathcal{H}}$ are computed in terms of the residue of a certain adelic integral of Rankin–Selberg type considered in [Pollack and Shah 2018]. Therein it is shown that, if π supports certain Fourier coefficients associated to F, then the local factors at unramified places v of this integral represent the degree 8 local spin L-function $L(s,\pi_v,\mathrm{Spin})$ of π_v. The following result gives evidence for Conjecture 1.1 for the motive associated to π.

Theorem 1.2 (Theorem 5.11). *Let $\pi=\pi_\infty\otimes\pi_f$ be a cuspidal automorphic representation of $\mathrm{PGSp}_6(\mathbb{A})$ such that π_∞ is a discrete series of Hodge type $(3,3)$ in the discrete series L-packet of V^λ. Then*

$$\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B},[\omega_\Psi]\rangle_B=\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}},[\omega_\Psi]\rangle_{\mathcal{H}}=C\cdot\mathrm{Res}_{s=1}(\mathcal{I}_S(\Phi,\Psi^{[\lambda,\mu]},s)L^S(s,\pi,\mathrm{Spin})),$$

where C is an explicit nonzero constant independent of π, S is a sufficiently large set of places containing the ramified and archimedean places, $\Psi^{[\lambda,\mu]}=A^{[\lambda,\mu]}\cdot\Psi$ for some weight lowering operator $A^{[\lambda,\mu]}$ defined in Proposition 4.8, Φ is a Schwartz–Bruhat function and $\mathcal{I}_S(\Phi,\Psi^{[\lambda,\mu]},s)$ is the integral defined in Theorem 5.8.

Remark 1.3. We point out that, according to [Gan and Gurevich 2009, Proposition 12.1] there exist a Schwartz–Bruhat function Φ and a vector $\Psi\in\pi$ such that $\mathcal{I}_S(\Phi,\Psi,1)$ is nonzero. However we do not know if this holds for Ψ_∞ in the minimal K-type of π_∞. Moreover, one can show that there exists a cusp form $\widetilde{\Psi}\in\pi$, which coincides with Ψ at the archimedean place and away from S, such that

$$\mathcal{I}_S(\Phi,\widetilde{\Psi}^{[\lambda,\mu]},s)=\mathcal{I}_\infty(\Phi_\infty,\Psi^{[\lambda,\mu]}_\infty,s).$$

Although we have not been able to calculate it, we expect that for a natural choice of Φ_∞ the archimedean integral $\mathcal{I}_\infty(\Phi_\infty, \Psi_\infty^{[\lambda,\mu]}, s)$ is the Gamma factor of the spin motive attached to π by the rule of Serre, and hence holomorphic and nonzero at $s = 1$.

As a corollary of this theorem, one can deduce, under the additional assumption that π is the Steinberg representation at a finite place, a weak version of Conjecture 1.1(1) (Corollary 5.15) and Conjecture 1.1(3) (Corollary 5.14).

When $\mathrm{Res}_{s=1} L^S(s, \pi, \mathrm{Spin})$ is nonzero then (see [Gan and Savin 2020, Theorem 1.1]) π is a weak functorial lift of a cuspidal automorphic representation σ of an exceptional group of type G_2. Moreover (see Proposition 8.1), we have

$$\mathrm{Res}_{s=1} L^S(s, \pi, \mathrm{Spin}) = L^S(1, \sigma, \mathrm{Std}) \mathrm{Res}_{s=1} \zeta^S(s).$$

Hence, up to controlling the value of the archimedean integral at $s = 1$, Theorem 1.2 above gives a cohomological formula for the critical value $L^S(1, \sigma, \mathrm{Std})$.

Our second main result concerns the program of Gross and Savin on rank-7 motives of Galois type G_2. The first step towards the conjecture of Gross and Savin was made in [Kret and Shin 2023], where the authors constructed GSpin-valued Galois representations associated to cohomological cuspidal automorphic forms of symplectic groups. Moreover, based on the calculations of [Gross and Savin 1998], Kret and Shin [2023, Theorem 11.1] verified that, for suitable automorphic representations of $\mathrm{PGSp}_6(\mathbb{A})$ in the image of the exceptional theta correspondence from the compact form G_2^c of type G_2, the image of their Galois representation lies actually in $G_2(\overline{\mathbb{Q}}_\ell)$. More precisely, let ρ_π be the $\mathrm{Spin}_7(\overline{\mathbb{Q}}_\ell)$-valued Galois representation attached to π. Assuming that π is a nontrivial small theta lift of σ, we have

$$\mathrm{Spin} \circ \rho_\pi = \mathrm{Std} \circ \rho_\sigma \oplus \mathbf{1}, \tag{1}$$

where $\mathrm{Std} \circ \rho_\sigma$ is the standard Galois representation attached to σ and $\mathbf{1}$ denotes the one-dimensional trivial representation.

Remark 1.4. Technically speaking, only the dual pair (G_2^c, PGSp_6) is considered in [Gross and Savin 1998], but their conjecture also applies to the dual pair (G_2, PGSp_6). Using the results of [Kret and Shin 2023] and the study of the exceptional theta correspondence for (G_2, PGSp_6) (see Theorem 1.8 below), we construct (Theorem 8.3), under some assumptions, Galois representations associated to cohomological cuspidal automorphic representations σ of $G_2(\mathbb{A})$, which sit in a decomposition as that of (1).

Theorem 1.5 (Theorem 8.6). *Let σ be an irreducible cuspidal automorphic representation of $G_2^c(\mathbb{A})$ or $G_2(\mathbb{A})$ such that the big theta lift $\Theta(\sigma)$ to* $\mathrm{PGSp}_6(\mathbb{A})$ *has an irreducible subquotient $\pi = \bigotimes_v' \pi_v$, which is a cuspidal automorphic representation such that π_∞ is cohomological for V as above and π_p is the Steinberg representation for some prime number p. Assume that the integral* $\mathcal{I}_S(\Phi, \Psi^{[\lambda,\mu]}, 1)$ *is nonzero for some Φ and $\Psi^{[\lambda,\mu]}$ as above. Then, the trivial representation* $\mathbf{1}$ *in* (1) *is generated by the étale realization of $\mathcal{Z}_{\boldsymbol{H},\mathcal{M}}^{[\lambda,\mu]}$.*

Remark 1.6. Note that the archimedean part π_∞ of π is not necessarily of Hodge type $(3, 3)$. However, it is one of the main results of [Kret and Shin 2023] that the L-packet of π is stable at infinity. In particular, there exists a cuspidal automorphic representation $\pi^{3,3} = \pi_\infty^{3,3} \otimes \pi_f$ whose archimedean part is cohomological and of Hodge type $(3, 3)$ and whose nonarchimedean part is equivalent to π_f. In the integral appearing in the statement of Theorem 1.2, the archimedean part of the cusp form $\Psi^{[\lambda,\mu]}$ is a suitable vector in the minimal K-type of $\pi_\infty^{3,3}$.

Remark 1.7. In Proposition 8.4 we give a list of cases where σ is known to have a small theta lift $\pi = \bigotimes_v' \pi_v$ of σ to $\mathrm{PGSp}_6(\mathbb{A})$ which is a cuspidal automorphic representation such that π_∞ is cohomological for V as above and π_p is the Steinberg representation for some prime number p, as in the previous theorem.

We conclude this introduction explaining a result which provides cases where Theorem 1.5 can be applied and which has its own interest. Indeed, note that a necessary condition for the integral $\mathcal{I}_S(\Phi, \Psi^{[\lambda,\mu]}, 1)$ to be nonzero, is that π supports a rank-2 Fourier coefficient associated to F. By a result of Gan [2005, Theorem 3.1], every cuspidal automorphic representation σ of $G_2(\mathbb{A})$ supports a Fourier coefficient associated to an étale cubic algebra E.

Theorem 1.8 (Theorem 7.2, Proposition 7.13). *Let σ be a cuspidal automorphic representation of $G_2(\mathbb{A})$. Assume that*

- *σ is not globally generic*;
- *σ_p is generic at some finite place p.*

Then the big theta lift $\Theta(\sigma)$ is cuspidal. Moreover $\Theta(\sigma)$ supports a rank-2 Fourier coefficient associated to F (and is in particular nonzero) if and only if σ supports a Fourier coefficient associated to $\mathbb{Q} \times F$.

1.3. ***Overview of the proofs.*** The main difficulty for calculating the pairing of Theorem 1.2 between the motivic class and the cohomology class $[\omega_\Psi]$ resides on the fact that the first class is constructed from the decomposition into irreducible components of the restriction of V to the subgroup $\boldsymbol{H}$, while the test vector is constructed from its restriction to the maximal compact subgroup $\mathrm{U}(3)$ of $\boldsymbol{G}(\mathbb{R})$. One needs to carefully study the relationship between these two different decompositions (Theorem 4.2). As a consequence we get a formula for the pairing in terms of a period integral (Propositions 4.8 and 4.10). These adelic integrals are in turn related to the residue of the partial spin L-function of π by means of the work of Pollack and Shah (Proposition 5.10), which allows to conclude the proof. Theorem 1.5 follows basically from Theorem 1.2 and 1.8. The proof of Theorem 1.8 goes as follows. We first prove (Theorem 7.2 and Corollary 7.3) that σ lifts to a cuspidal representation using the tower of exceptional correspondences for G_2 studied in [Ginzburg et al. 1997b], which reduces the problem to the vanishing of certain automorphic period integrals. Finally, we establish (Proposition 7.13) a correspondence between Fourier coefficients of σ and its theta lift, which in particular implies the nonvanishing of the latter.

1.4. ***Structure of the manuscript.*** In Section 2 we fix notation, conventions, and basic results that will be useful in the body of the article. In particular, we prove that, under some mild assumptions, the localization at a maximal ideal of the Hecke algebra of the cohomology of the Siegel sixfold is cuspidal and concentrated in the middle degree. We also introduce Absolute Hodge cohomology and compute the dimension of its π_f-isotypical component. In Section 3 we explain the construction of the motivic class $\mathscr{Z}_{\mathcal{M}}^{[\lambda,\mu]}$ and its realizations. In Section 4 we construct the harmonic differential form ω_Ψ associated to a suitable cuspidal form Ψ in the space of π and we prove our first main result concerning the calculation of the pairing between the motivic class and the cohomology class $[\omega_\Psi]$. In Section 5, we use the results of Pollack and Shah to relate the pairing to the residue of the spin L-function. Sections 6 and 7 are devoted to the study of the exceptional theta correspondence between G_2 and PGSp_6 and contain the proof of Theorem 1.8. Finally, in Section 8 we relate the pairing to a critical value of the standard L-function of G_2. We also deduce from the work of Kret and Shin the existence of Galois representations attached to certain cuspidal representations of G_2 and we conclude with a proof of Theorem 1.5.

2. Preliminaries

2.1. ***Algebraic groups and algebraic representations.*** Let ψ denote an antisymmetric nondegenerate bilinear form on a finite-dimensional $\mathbb{Q}$-vector space V. The symplectic group $\mathrm{GSp}(V,\psi)$ is the $\mathbb{Q}$-group scheme defined by

$$\mathrm{GSp}(V,\psi)=\{g\in\mathrm{GL}(V)\mid\forall v,w\in V,\ \psi(gv,gw)=\nu(g)\psi(v,w),\ \nu(g)\in\boldsymbol{G}_m\}.$$

Then $\nu:\mathrm{GSp}(V,\psi)\to\boldsymbol{G}_m$ is a character. Let I_n denote the identity matrix of size n. When V is the $\mathbb{Q}$-vector space $\mathbb{Q}^{2n}$ endowed with the bilinear form whose matrix is $J=\left(\begin{smallmatrix}0 & I_n\\ -I_n & 0\end{smallmatrix}\right)$, we let GSp_{2n} denote $\mathrm{GSp}(\mathbb{Q}^{2n},J)$ and we let Sp_{2n} denote $\ker\nu$. In this paper, we are mainly interested in the case $n=3$. Hence we will denote by $\boldsymbol{G}$ the group GSp_6 and by $\boldsymbol{G}_0$ the group Sp_6. Let $\boldsymbol{T}\subset\boldsymbol{G}$ denote the maximal diagonal torus and $\boldsymbol{B}\subset\boldsymbol{G}$ denote the standard Borel. We have

$$\boldsymbol{T}=\{\mathrm{diag}(\alpha_1,\alpha_2,\alpha_3,\alpha_1^{-1}\nu,\alpha_2^{-1}\nu,\alpha_3^{-1}\nu),\alpha_1,\alpha_2,\alpha_3,\nu\in\boldsymbol{G}_m\}.$$

We associate to any 4-tuple $(\lambda_1,\lambda_2,\lambda_3,c)\in\mathbb{Z}^4$ such that $c\equiv\lambda_1+\lambda_2+\lambda_3 \pmod 2$ the algebraic character $\lambda(\lambda_1,\lambda_2,\lambda_3,c)$ of $\boldsymbol{T}$ defined by

$$\lambda(\lambda_1,\lambda_2,\lambda_3,c):\mathrm{diag}(\alpha_1,\alpha_2,\alpha_3,\alpha_1^{-1}\nu,\alpha_2^{-1}\nu,\alpha_3^{-1}\nu)\mapsto\alpha_1^{\lambda_1}\alpha_2^{\lambda_2}\alpha_3^{\lambda_3}\nu^{\frac{1}{2}(c-\lambda_1-\lambda_2-\lambda_3)}.$$

This defines an isomorphism between the group of 4-tuples

$$(\lambda_1,\lambda_2,\lambda_3,c)\in\mathbb{Z}^4\quad\text{such that}\quad c\equiv\lambda_1+\lambda_2+\lambda_3 \pmod 2$$

and the group of algebraic characters of $\boldsymbol{T}$. Let $\rho_1=\lambda(1,-1,0,0)$ and $\rho_2=\lambda(0,1,-1,0)$ denote the short simple roots and let $\rho_3=\lambda(0,0,2,0)$ denote the long simple root. The set of roots of $\boldsymbol{T}$ in $\boldsymbol{G}$ is $R=R^+\cup R^-$, where

$$R^+=\{\rho_1,\rho_2,\rho_1+\rho_2,\rho_2+\rho_3,\rho_1+\rho_2+\rho_3,\rho_1+2\rho_2+\rho_3,2\rho_1+2\rho_2+\rho_3,2\rho_2+\rho_3,\rho_3\}$$

is the set of positive roots with respect to $\boldsymbol{B}$ and $R^-=-R^+$. A weight $\lambda=\lambda(\lambda_1,\lambda_2,\lambda_3,c)$ is dominant for $\boldsymbol{B}$ if $\lambda_1\geq\lambda_2\geq\lambda_3\geq 0$. For any such λ, there exists a unique (up to isomorphism) irreducible algebraic representation V^λ of $\boldsymbol{G}$ of highest weight λ and every irreducible algebraic representation of $\boldsymbol{G}$ is obtained in this way (up to isomorphism). Similarly, irreducible algebraic representations of GSp_4 are classified by their highest weight which is a character of the shape $\lambda(\lambda_1, \lambda_2, c)$ with $\lambda_1 \geq \lambda_2 \geq 0$ and $\lambda_1 + \lambda_2 \equiv c \pmod 2$ (see for example [Lemma 2017, §2.3] for more details). We will also use the classification of irreducible algebraic representations of the groups $\boldsymbol{G}_0 = \mathrm{Sp}_6$ and Sp_4. To this end let us recall that the diagonal maximal torus $\boldsymbol{T}_0 = \boldsymbol{T} \cap \boldsymbol{G}_0$ of $\boldsymbol{G}_0$ is

$$\boldsymbol{T}_0 = \{\mathrm{diag}(\alpha_1, \alpha_2, \alpha_3, \alpha_1^{-1}, \alpha_2^{-1}, \alpha_3^{-1}), \alpha_1, \alpha_2, \alpha_3 \in \boldsymbol{G}_m\}$$

and that its group of algebraic characters is isomorphic to $\mathbb{Z}^3$ via $(\lambda_1, \lambda_2, \lambda_3) \mapsto \lambda(\lambda_1, \lambda_2, \lambda_3)$, where

$$\lambda(\lambda_1, \lambda_2, \lambda_3) : \mathrm{diag}(\alpha_1, \alpha_2, \alpha_3, \alpha_1^{-1}, \alpha_2^{-1}, \alpha_3^{-1}) \mapsto \alpha_1^{\lambda_1}\alpha_2^{\lambda_2}\alpha_3^{\lambda_3}. \tag{2}$$

A weight $\lambda = \lambda(\lambda_1, \lambda_2, \lambda_3)$ is dominant with respect to the standard Borel $\boldsymbol{B}_0 = \boldsymbol{B} \cap \boldsymbol{G}_0$ if $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq 0$ and for any such λ there exists a unique (up to isomorphism) irreducible algebraic representation V^λ of $\boldsymbol{G}_0$ of highest weight λ and every irreducible algebraic representation of $\boldsymbol{G}_0$ is obtained in this way (up to isomorphism). Similarly, irreducible algebraic representations of Sp_4 are classified by characters $\lambda(\lambda_1, \lambda_2)$ with $\lambda_1 \geq \lambda_2$, with obvious notation.

2.2. ***Compact Lie groups and representations.*** Let $\mathrm{U}(n) = \{g \in \mathrm{GL}_n(\mathbb{C}) \mid {}^t\,\bar{g}g = I_n\}$ denote the unitary group and let $K_\infty \subset \boldsymbol{G}_0(\mathbb{R})$ be the subgroup defined as

$$K_\infty = \left\{\left(\begin{smallmatrix} A & B \\ -B & A \end{smallmatrix}\right) \,\middle|\, AA^t + BB^t = 1,\, AB^t = BA^t\right\}.$$

We have an isomorphism $\kappa : \mathrm{U}(3) \simeq K_\infty$ defined by $A + iB \mapsto \left(\begin{smallmatrix} A & B \\ -B & A \end{smallmatrix}\right)$. In fact K_∞ is a maximal compact subgroup of $\boldsymbol{G}_0(\mathbb{R})$. Let $T_\infty \subset K_\infty$ denote $\{\kappa(\mathrm{diag}(z_1, z_2, z_3)), z_1, z_2, z_3 \in \mathrm{U}(1)\}$. Then T_∞ is Cartan subgroup of K_∞. Its group of algebraic characters is isomorphic to $\mathbb{Z}^3$ via $(\lambda_1, \lambda_2, \lambda_3) \mapsto \lambda'(\lambda_1, \lambda_2, \lambda_3)$, where

$$\lambda'(\lambda_1, \lambda_2, \lambda_3) : \kappa(\mathrm{diag}(z_1, z_2, z_3)) \mapsto z_1^{\lambda_1} z_2^{\lambda_2} z_3^{\lambda_3}.$$

An algebraic character is dominant if $\lambda_1 \geq \lambda_2 \geq \lambda_3$. For any dominant integral weight λ', there exists a unique (up to isomorphism) irreducible representation $\tau_{\lambda'}$ of K_∞ in a finite-dimensional $\mathbb{C}$-vector space and every irreducible representation of K_∞ is obtained in this way (up to isomorphism). In what follows, we will simply denote the irreducible representation of highest weight $\lambda'(\lambda_1, \lambda_2, \lambda_3)$ by $\tau_{(\lambda_1, \lambda_2, \lambda_3)}$. Let us explain the connection between the weights λ of $\boldsymbol{T}_0$ defined by (2) in the previous section and the weights λ' defined above. Let $J \in \boldsymbol{G}_0(\mathbb{C})$ denote the matrix $J = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} I_3 & iI_3 \\ iI_3 & I_3 \end{smallmatrix}\right)$. Then we have

$$J^{-1}\kappa(\mathrm{diag}(z_1, z_2, z_3))J = \mathrm{diag}(z_1, z_2, z_3)$$

and so, for any $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{Z}^3$, we have

$$\lambda(\lambda_1, \lambda_2, \lambda_3)(J^{-1}\kappa(z_1, z_2, z_3)J) = \lambda'(\lambda_1, \lambda_2, \lambda_3)(\mathrm{diag}(z_1, z_2, z_3)).$$

In brief, the character $\lambda'(\lambda_1, \lambda_2, \lambda_3)$ of T_∞ is conjugated to the restriction of $\lambda(\lambda_1, \lambda_2, \lambda_3)$ to $\mathrm{U}(1)^3 \subset \mathbb{C}^\times \times \mathbb{C}^\times \times \mathbb{C}^\times = \boldsymbol{T}_0(\mathbb{C})$.

2.3. ***Lie algebras.*** Let $\mathfrak{g}_0$ (resp. $\mathfrak{k}$) denote the Lie algebra of $\boldsymbol{G}_0(\mathbb{R})$ (resp. K_∞) and let $\mathfrak{g}_{0,\mathbb{C}}$ (resp. $\mathfrak{k}_\mathbb{C}$) denote its complexification. Then

$$\mathfrak{g}_0 = \left\{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in M_6(\mathbb{R}) \mid B = B^t, C = C^t, A = -D^t\right\},$$
$$\mathfrak{k} = \left\{\left(\begin{smallmatrix} A & B \\ -B & A \end{smallmatrix}\right) \in M_6(\mathbb{R}) \mid A = -A^t, B = B^t\right\}.$$

The Lie algebra $\mathfrak{k}$ is the 1-eigenspace for the Cartan involution $\theta(X) = -X^t$. The (-1)-eigenspace is $\mathfrak{p} = \left\{\left(\begin{smallmatrix} A & B \\ B & -A \end{smallmatrix}\right) \in M_6(\mathbb{R}) \mid A = A^t, B = B^t\right\}$. Letting

$$\mathfrak{p}_\mathbb{C}^\pm = \left\{\left(\begin{smallmatrix} A & \pm iA \\ \pm iA & -A \end{smallmatrix}\right) \in M_6(\mathbb{C}) \mid A = A^t\right\},$$

we have $\mathfrak{p}_\mathbb{C} = \mathfrak{p}_\mathbb{C}^+ \oplus \mathfrak{p}_\mathbb{C}^-$ and one has the Cartan decomposition

$$\mathfrak{g}_{0,\mathbb{C}} = \mathfrak{k}_\mathbb{C} \oplus \mathfrak{p}_\mathbb{C}^+ \oplus \mathfrak{p}_\mathbb{C}^-.$$

For $1 \le j \le 3$, let $D_j \in M_3(\mathbb{C})$ be the matrix with entry 1 at position (j, j) and 0 elsewhere. Define $T_j = \left(\begin{smallmatrix} 0 & D_j \\ -D_j & 0 \end{smallmatrix}\right)$. Then the Lie algebra $\mathfrak{h}$ of T_∞ is $\mathfrak{h} = \mathbb{R} \cdot T_1 \oplus \mathbb{R} \cdot T_2 \oplus \mathbb{R} \cdot T_3$. This is a compact Cartan subalgebra of $\mathfrak{g}_0$. Let (e_1, e_2, e_3) denote the basis of $\mathfrak{h}_\mathbb{C}^*$ dual to $(-iT_1, -iT_2, -iT_3)$. A system of positive roots for $(\mathfrak{g}_{0,\mathbb{C}}, \mathfrak{h}_\mathbb{C})$ is then given by

$$\{e_1 \pm e_2, e_1 \pm e_3, e_2 \pm e_3, 2e_1, 2e_2, 2e_3\}.$$

The simple roots are $e_1 - e_2$, $e_2 - e_3$ and $2e_3$. We note that $\mathfrak{p}_\mathbb{C}^+$ is spanned by the root spaces corresponding to the positive roots of type $2e_j$ and $e_j + e_k$. We denote by $\Delta = \{\pm 2e_j, \pm(e_j \pm e_k)\}$ the set of all roots, $\Delta_\mathrm{c} = \{\pm(e_j - e_k)\}$ the set of compact roots and $\Delta_\mathrm{nc} = \Delta - \Delta_\mathrm{c}$ the noncompact roots. Finally, we denote by Δ^+, Δ_c^+ and Δ_nc^+ the set of positive, positive compact and positive noncompact roots, respectively.

2.4. ***Weyl groups.*** Recall that the Weyl group of $\boldsymbol{G}_0$ is given by $\mathfrak{W}_{\boldsymbol{G}_0} = \{\pm 1\}^3 \rtimes \mathfrak{S}_3$. The reflection σ_j in the hyperplane orthogonal to $2e_j$ simply reverses the sign of e_j while leaving the other e_k fixed. The reflection σ_{jk} in the hyperplane orthogonal to $e_j - e_k$ exchanges e_j and e_k and leaves the remaining e_ℓ fixed. The Weyl group $\mathfrak{W}_{K_\infty}$ of $K_\infty \cong U(3)$ is isomorphic to $\mathfrak{S}_3$ and, via the embedding into $\boldsymbol{G}$, identifies with the subgroup of $\mathfrak{W}_{\boldsymbol{G}_0}$ generated by the σ_{jk}. With the identification $\mathfrak{W}_{\boldsymbol{G}_0} = N(\boldsymbol{T}_0)/Z(\boldsymbol{T}_0)$, an explicit description of $\mathfrak{W}_{\boldsymbol{G}_0}$ and $\mathfrak{W}_{K_\infty}$ is given as follows. The matrices corresponding to the reflections σ_{jk} are $\left(\begin{smallmatrix} S_{jk} & 0 \\ 0 & -S_{jk} \end{smallmatrix}\right)$, where S_{jk} is the matrix with entry 1 at places (ℓ, ℓ), $\ell \neq j, k$, (k, j) and (j, k) and zeroes elsewhere. The matrices corresponding to the reflection σ_j in the hyperplane orthogonal to $2e_j$ are of the form $\left(\begin{smallmatrix} 0 & U_j \\ -U_j & 0 \end{smallmatrix}\right)$, where U_j denotes the diagonal matrix with -1 at the place (j, j) and ones at the other entries of the diagonal. This gives an explicit description of the elements of $\mathfrak{W}_{K_\infty}$ and their length:

$$\mathfrak{W}_{K_\infty} = \{1, \sigma_{12}, \sigma_{13}, \sigma_{23}, \sigma_{12}\sigma_{13}, \sigma_{12}\sigma_{23}\} \xrightarrow{\ell(\bullet)} \{0, 1, 1, 1, 2, 2\}.$$

2.5. ***Discrete series.*** We recall standard facts on discrete series for $\boldsymbol{G}_0(\mathbb{R}) = \mathrm{Sp}_6(\mathbb{R})$ and for $\mathrm{PGSp}_6(\mathbb{R})$. For any nonsingular weight Λ define

$$\Delta^+(\Lambda) := \{\alpha \in \Delta \mid \langle \alpha, \Lambda \rangle > 0\}, \quad \Delta_c^+(\Lambda) = \Delta^+(\Lambda) \cap \Delta_c,$$

where $\langle\ ,\ \rangle$ is the standard scalar product on $\mathbb{R}^3$. Let $\lambda = (\lambda_1, \lambda_2, \lambda_3)$ be a weight of T_∞ such that $\lambda_1 \ge \lambda_2 \ge \lambda_3 \ge 0$ and let $\rho = \frac{1}{2}\sum_{\alpha\in\Delta^+}\alpha = (3, 2, 1)$. As $|\mathfrak{W}_{\boldsymbol{G}_0}/\mathfrak{W}_{K_\infty}| = 8$, by [Knapp 1986, Theorem 9.20], the set of equivalence classes of irreducible discrete series representations of $\boldsymbol{G}_0(\mathbb{R})$ with Harish-Chandra parameter $\lambda+\rho$ contains 8 elements. More precisely, choose representatives $\{w_1, \dots, w_8\}$ of $\mathfrak{W}_{\boldsymbol{G}_0}/\mathfrak{W}_{K_\infty}$ of increasing length and such that for any $1 \le i \le 8$. Then the weight $w_i(\lambda+\rho)$ is dominant for K_∞. The representatives, defined by their action on ρ, are $w_1(3, 2, 1) = (3, 2, 1)$, $w_2(3, 2, 1) = (3, 2, -1)$, $w_3(3, 2, 1) = (3, 1, -2)$, $w_4(3, 2, 1) = (2, 1, -3)$, $w_5(3, 2, 1) = (3, -1, -2)$, $w_6(3, 2, 1) = (2, -1, -3)$, $w_7(3, 2, 1) = (1, -2, -3)$, $w_8(3, 2, 1) = (-1, -2, -3)$. Then, for any $1 \le i \le 8$, there exists an irreducible discrete series π_∞^Λ, where $\Lambda = w_i(\lambda+\rho)$, of Harish-Chandra parameter Λ and containing with multiplicity 1 the minimal K_∞-type with highest weight $\Lambda + \delta_{\boldsymbol{G}_0} - 2\delta_{K_\infty}$, where $\delta_{\boldsymbol{G}_0}$ (resp. δ_{K_∞}) is the half-sum of roots (resp. of compact roots) which are positive with respect to the Weyl chamber in which Λ lies, i.e., $2\delta_{\boldsymbol{G}_0} := \sum_{\alpha\in\Delta^+(\Lambda)}\alpha$ (resp. $2\delta_{K_\infty} := \sum_{\alpha\in\Delta_c^+(\Lambda)}\alpha$). Moreover, for $i \neq j$, $\Lambda = w_i(\lambda+\rho)$, $\Lambda = w_j(\lambda+\rho)$, the representations π_∞^Λ and π_∞^Λ are not equivalent and any discrete series of $\boldsymbol{G}_0$ is obtained in this way. Let V^λ be the irreducible algebraic representation of $\boldsymbol{G}_0$ of highest weight $\lambda = (\lambda_1, \lambda_2, \lambda_3)$ (for $\boldsymbol{T}_0$).

Definition 2.1. The discrete series L-packet $P(V^\lambda)$ associated to λ is the set of isomorphism classes of discrete series of $\boldsymbol{G}_0(\mathbb{R})$ whose Harish-Chandra parameter is of the form $\Lambda = w_i(\lambda+\rho)$ as i varies.

By [Borel and Wallach 1980, Theorem II.5.3], for each $\pi_\infty^\Lambda \in P(V^\lambda)$, the space

$$\operatorname{Hom}_{K_\infty}\big(\textstyle\bigwedge^6 \mathfrak{g}_{0,\mathbb{C}}/\mathfrak{k}_\mathbb{C} \otimes V^\lambda, \pi_\infty^\Lambda\big)$$

has dimension 1. This is a consequence of the fact (see the proof of [Borel and Wallach 1980, Theorem II.5.3]) that the minimal K_∞-type of π_∞^Λ appears uniquely in $\bigwedge^6 \mathfrak{g}_{0,\mathbb{C}}/\mathfrak{k}_\mathbb{C} \otimes V^\lambda$. Using the Cartan decomposition, we get

$$\textstyle\bigwedge^6 \mathfrak{g}_{0,\mathbb{C}}/\mathfrak{k}_\mathbb{C} = \bigoplus\limits_{p+q=6} \bigwedge^p \mathfrak{p}_\mathbb{C}^+ \otimes_\mathbb{C} \bigwedge^q \mathfrak{p}_\mathbb{C}^-.$$

Hence, there exists a unique pair (p, q) such that $\operatorname{Hom}_{K_\infty}\big(\bigwedge^p \mathfrak{p}_\mathbb{C}^+ \otimes \bigwedge^q \mathfrak{p}_\mathbb{C}^- \otimes V^\lambda, \pi_\infty^\Lambda\big)$ is nonzero and hence of dimension 1. We call such a pair (p, q) the Hodge type of π_∞^Λ.

Lemma 2.2. *There exist two elements $\pi_{\infty,1}^{3,3}$ and $\bar{\pi}_{\infty,1}^{3,3}$ in $P(V^\lambda)$ of Hodge type $(3, 3)$. They are characterized by having Harish-Chandra parameters $(\lambda_2+2, \lambda_3+1, -\lambda_1-3)$ and $(\lambda_1+3, -\lambda_3-1, -\lambda_2-2)$ and minimal K_∞-types $\tau_{(\lambda_2+2,\lambda_3+2,-\lambda_1-4)}$ and $\tau_{(\lambda_1+4,-\lambda_3-2,-\lambda_2-2)}$ respectively.*

Proof. The discrete series $\pi_{\infty,1}^{3,3}$ and $\bar{\pi}_{\infty,1}^{3,3}$ correspond to the Weyl representatives w_4 and w_5. Since $w_4\lambda = (\lambda_2, \lambda_3, -\lambda_1)$ and $w_5\lambda = (\lambda_1, -\lambda_3, -\lambda_2)$, the Harish-Chandra parameters of $\pi_{\infty,1}^{3,3}$ and $\bar{\pi}_{\infty,1}^{3,3}$ are as desired. When $\Lambda = w_4(\lambda+\rho)$ (resp. $\Lambda = w_5(\lambda+\rho)$), observe that $\delta_{\boldsymbol{G}_0}$ is equal to $(2, 1, -3)$ (resp. $(3, -1, -2)$), while $\delta_{K_\infty} = (1, 0, -1)$ in both cases. Hence, using the formula above, the minimal K_∞-types of $\pi_{\infty,1}^{3,3}$ and $\bar{\pi}_{\infty,1}^{3,3}$ are $\tau_{(\lambda_2+2,\lambda_3+2,-\lambda_1-4)}$ and $\tau_{(\lambda_1+4,-\lambda_3-2,-\lambda_2-2)}$ respectively.

Recall that, after [Vogan and Zuckerman 1984, Proposition 6.19], the Hodge type of a discrete series representation of Harish-Chandra parameter Λ is (p, q), where p (resp. q) is the number of positive noncompact roots in $\Delta^+(\Lambda)$ (resp. $\Delta^-(\Lambda)$). Using this, one easily checks that the Hodge type of $\pi^{3,3}_{\infty,1}$ and $\bar{\pi}^{3,3}_{\infty,1}$ is $(3, 3)$. □

The picture for $\mathrm{PGSp}_6(\mathbb{R})$ is similar, but the set of its Harish-Chandra parameters changes slightly. This is due to the fact that, since its maximal compact subgroup has two connected components, the set of parameters has to be considered up to the action of $\mathfrak{W}_{K_\infty}$ and of w_8, as the latter, which is the antidiagonal matrix with all entries -1, now belongs to the connected component away from the identity of the maximal compact subgroup. Concretely, any parameter $\mu = (\mu_1, \mu_2, \mu_3)$ has to be identified with $w_8\mu = (-\mu_3, -\mu_2, -\mu_1)$. If $\lambda = (\lambda_1, \lambda_2, \lambda_3)$ is such that $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq 0$ and $\sum_i \lambda_i \equiv 0 \pmod 2$, then the irreducible algebraic $\boldsymbol{G}$-representation $V^{(\lambda,0)}$ of highest weight $\lambda(\lambda_1, \lambda_2, \lambda_3, 0)$ defines a representation of PGSp_6. The corresponding discrete series L-packet $P(V^{(\lambda,0)})$ for $\mathrm{PGSp}_6(\mathbb{R})$ has thus four elements. Any element $\pi_\infty \in P(V^{(\lambda,0)})$ of Harish-Chandra parameter μ, viewed as a $\boldsymbol{G}(\mathbb{R})$-representation, decomposes when restricted to $\boldsymbol{G}_0(\mathbb{R})$ as the direct sum of two discrete series in $P(V^\lambda)$ of Harish-Chandra parameters μ and $w_8\mu$. As a consequence, for any such π_∞, the space

$$H^6(\mathfrak{g}, K_{\boldsymbol{G}}; \pi_\infty \otimes V^{(\lambda,0)}) = \mathrm{Hom}_{K_{\boldsymbol{G}}}\big(\textstyle\bigwedge^6 \mathfrak{g}_{\mathbb{C}}/\mathrm{Lie}(K_{\boldsymbol{G}})_{\mathbb{C}}, \pi_\infty \otimes V^{(\lambda,0)}\big),$$

where $\mathfrak{g} = \mathrm{Lie}(\boldsymbol{G})$, $\mathfrak{g}_{\mathbb{C}}$ is its complexification and $K_{\boldsymbol{G}} = \mathbb{R}_+^\times K_\infty$, is two-dimensional. The discussion above implies the following.

Lemma 2.3. *Let* $\lambda = (\lambda_1, \lambda_2, \lambda_3)$ *be a dominant weight for* $\boldsymbol{G}_0$ *such that* $\sum_i \lambda_i \equiv 0 \pmod 2$. *Then there exists a unique discrete series* $\pi^{3,3}_\infty \in P(V^{(\lambda,0)})$ *of* $\mathrm{PGSp}_6(\mathbb{R})$, *with Harish-Chandra parameter* $(\lambda_2 + 2, \lambda_3 + 1, -\lambda_1 - 3)$, *such that*

$$\pi^{3,3}_{\infty}{}_{|\boldsymbol{G}_0(\mathbb{R})} = \pi^{3,3}_{\infty,1} \oplus \bar{\pi}^{3,3}_{\infty,1}.$$

We will refer to $\pi^{3,3}_\infty$ as the discrete series of $\mathrm{PGSp}_6(\mathbb{R})$ in $P(V^{(\lambda,0)})$ of Hodge type $(3, 3)$.

2.6. *Shimura varieties.* Let F denote a real étale quadratic $\mathbb{Q}$-algebra, i.e., F is either a totally real quadratic extension of $\mathbb{Q}$ or $\mathbb{Q} \times \mathbb{Q}$. Denote by $\mathrm{GL}^*_{2,F}/\mathbb{Q}$ the subgroup scheme of $\mathrm{Res}_{F/\mathbb{Q}}\,\mathrm{GL}_{2,F}$ sitting in the Cartesian diagram

$$\begin{tikzcd}
\mathrm{GL}^*_{2,F} \arrow[r, hook] \arrow[d] & \mathrm{Res}_{F/\mathbb{Q}}\,\mathrm{GL}_{2,F} \arrow[d, "\det"] \\
\boldsymbol{G}_m \arrow[r, hook] & \mathrm{Res}_{F/\mathbb{Q}}\,\boldsymbol{G}_{m,F}
\end{tikzcd}$$

For instance, when $F = \mathbb{Q} \times \mathbb{Q}$, we have

$$\mathrm{GL}^*_{2,F} = \{(g_1, g_2) \in \mathrm{GL}_2 \times \mathrm{GL}_2 \mid \det(g_1) = \det(g_2)\}.$$

Let $\boldsymbol{H}$ denote the group

$$\boldsymbol{H} = \mathrm{GL}_2 \boxtimes \mathrm{GL}^*_{2,F} = \{(g_1, g_2) \in \mathrm{GL}_2 \times \mathrm{GL}^*_{2,F} \mid \det(g_1) = \det(g_2)\}. \tag{3}$$

We embed $\boldsymbol{H}$ into $\boldsymbol{G}$ as follows. Let us consider the $\mathbb{Q} \times F$-module

$$V := \mathbb{Q}e_1 \oplus Fe_2 \oplus \mathbb{Q}f_1 \oplus Ff_2,$$

where $V_1 := \mathbb{Q}e_1 \oplus \mathbb{Q}f_1$ and $V_2 := Fe_2 \oplus Ff_2$ are respectively the standard representations of GL_2 and $\mathrm{GL}^*_{2,F}$. We equip V with the $\mathbb{Q} \times F$-valued alternating form $\psi' : V \times V \to \mathbb{Q} \times F$, such that $\psi'(e_1, f_1) = (1, 0)$, $\psi'(e_2, f_2) = \left(0, \frac{1}{2}\right)$ and V_1 is orthogonal to V_2. The group $\boldsymbol{H}$ acts naturally on V and preserves ψ' up to a scalar. We can regard V as a six-dimensional $\mathbb{Q}$-vector space with $\mathbb{Q}$-valued symplectic form $\psi := \mathrm{tr}_{(\mathbb{Q}\times F)/\mathbb{Q}} \circ \psi'$. Explicitly, we have

$$\psi(ae_1 + \alpha e_2, bf_1 + \beta f_2) = ab + \tfrac{1}{2}\mathrm{tr}_{F/\mathbb{Q}}(\alpha\beta).$$

This identification defines an embedding $\boldsymbol{H} \hookrightarrow \mathrm{GSp}(V, \psi)$. We now identify $\mathrm{GSp}(V, \psi)$ with $\boldsymbol{G}$ by choosing a suitable $\mathbb{Q}$-basis of V. Recall that the set of real quadratic $\mathbb{Q}$-algebras is parametrized by $D \in \mathbb{Q}^\times_{>0}/(\mathbb{Q}^\times_{>0})^2$, via $D \mapsto F = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$. Using the decomposition $F = \mathbb{Q} \oplus \mathbb{Q}\sqrt{D}$, we consider the $\mathbb{Q}$-basis of V given by

$$\{e_1, e_2, e_3, f_1, f_2, f_3\} := \left\{e_1, e_2, \sqrt{D}e_2, f_1, f_2, \tfrac{1}{\sqrt{D}}f_2\right\}.$$

In this basis, ψ is represented by the matrix $J = \left(\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\right)$; thus we obtain an isomorphism $\mathrm{GSp}(V, \psi) \simeq \boldsymbol{G}$ and the embedding

$$\iota : \boldsymbol{H} \hookrightarrow \boldsymbol{G}.$$

Note that the group

$$\boldsymbol{H}' := \mathrm{GL}_2 \boxtimes \mathrm{GSp}_4 := \{(g_1, g_2) \in \mathrm{GL}_2 \times \mathrm{GSp}_4 \mid \det(g_1) = \nu(g_2)\}$$

is also naturally embedded in $\boldsymbol{G}$ and ι factors through $\boldsymbol{H}'$.

Recall from [Burgos Gil et al. 2024, §2.2] that there is a three-dimensional Shimura variety $\mathrm{Sh}_{\boldsymbol{H}}$ associated to the $\boldsymbol{H}(\mathbb{R})$-conjugacy class of

$$h : \boldsymbol{S} \to \boldsymbol{H}_{/\mathbb{R}}, \quad x + iy \mapsto \left(\left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right), \left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right), \left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)\right),$$

where $\boldsymbol{S} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\, \boldsymbol{G}_{m/\mathbb{C}}$ is the Deligne torus. The associated Shimura datum has reflex field is $\mathbb{Q}$ and the Shimura variety $\mathrm{Sh}_{\boldsymbol{H}}$ can be described as follows. If $V \subseteq \boldsymbol{H}(\mathbb{A}_f)$ is a fiber product (over the similitude characters) $V_1 \times_{\mathbb{A}_f^\times} V_2$ of sufficiently small subgroups, we have

$$\mathrm{Sh}_{\boldsymbol{H}}(V) = \mathrm{Sh}_{\mathrm{GL}_2}(V_1) \times_{\boldsymbol{G}_m} \mathrm{Sh}_{\mathrm{GL}^*_{2,F}}(V_2),$$

where $\times_{\boldsymbol{G}_m}$ denotes the fiber product over the zero-dimensional Shimura variety of level $W = \det(V_1) = \det(V_2)$. The connected components are given by

$$\pi_0(\mathrm{Sh}_{\boldsymbol{H}}(V)(\mathbb{C})) = \widehat{\mathbb{Z}}^\times / W.$$

Hence, $\mathrm{Sh}_{\boldsymbol{H}}$ can be thought as the fiber product of a modular curve and a Hilbert–Blumenthal modular surface. We also recall that the complex points of $\mathrm{Sh}_{\boldsymbol{H}}(V)$ are given by

$$\mathrm{Sh}_{\boldsymbol{H}}(V)(\mathbb{C}) = \boldsymbol{H}(\mathbb{Q})\backslash \boldsymbol{H}(\mathbb{A})/\mathbb{Z}_{\boldsymbol{H}}(\mathbb{R})K_{\boldsymbol{H},\infty}V,$$

where $\mathbb{Z}_{\boldsymbol{H}}$ denotes the center of $\boldsymbol{H}$ and $K_{\boldsymbol{H},\infty} \subseteq \boldsymbol{H}(\mathbb{R})$ is the maximal compact defined as the product $\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$.

The embedding $\iota : \boldsymbol{H} \hookrightarrow \boldsymbol{G}$ induces a Shimura datum for $\boldsymbol{G}$ whose reflex field is $\mathbb{Q}$. For any sufficiently small compact open subgroup U of $\boldsymbol{G}(\mathbb{A}_f)$, denote by $\mathrm{Sh}_{\boldsymbol{G}}(U)$ the associated Shimura variety of dimension 6. We also write $\iota : \mathrm{Sh}_{\boldsymbol{H}}(U \cap \boldsymbol{H}) \hookrightarrow \mathrm{Sh}_{\boldsymbol{G}}(U)$ the closed embedding of codimension 3 induced by the group homomorphism $\iota : \boldsymbol{H} \hookrightarrow \boldsymbol{G}$.

Remark 2.4. If $E/\mathbb{Q}$ is a totally real cubic field extension of $\mathbb{Q}$ then one can analogously define $\boldsymbol{H} = \{g \in \mathrm{Res}_{E/\mathbb{Q}} \mathrm{GL}_{2,E} \mid \det(g) \in \boldsymbol{G}_m\}$ and there is a natural embedding $\iota : \boldsymbol{H} \hookrightarrow \boldsymbol{G}$ (see [Piatetski-Shapiro and Rallis 1987, §1] for details) inducing closed embeddings $\iota : \mathrm{Sh}_{\boldsymbol{H}}(U \cap \boldsymbol{H}) \hookrightarrow \mathrm{Sh}_{\boldsymbol{G}}(U)$ for sufficiently small open compact U. All our results up to Section 5 will hold for any real étale cubic algebra E over $\mathbb{Q}$. Our main interest in the case $E = \mathbb{Q} \times F$ for F a real étale quadratic algebra over $\mathbb{Q}$ is motivated by the integral representation of the spin L-function of $\boldsymbol{G}$ of [Pollack and Shah 2018].

2.7. *Cohomology of Siegel sixfolds.*

Let π be a cuspidal automorphic representation of $\boldsymbol{G}(\mathbb{A})$ having nonzero fixed vectors by a neat compact open group $U \subseteq \boldsymbol{G}(\mathbb{A}_f)$. We assume that π has trivial central character and hence we regard it as a cuspidal automorphic representation of $\mathrm{PGSp}_6(\mathbb{A})$. Our purpose is to establish that, under mild assumptions, suitable localizations at π of cuspidal, L^2, inner Betti and Betti cohomologies coincide and are concentrated in the middle degree. The assumptions are the following:

(DS) The archimedean component π_∞ is a discrete series representation of $\mathrm{PGSp}_6(\mathbb{R})$.

(St) At a finite place p the component π_p is the Steinberg representation of $\mathrm{PGSp}_6(\mathbb{Q}_p)$.

Let us fix for the rest of this section $\lambda = (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{Z}^3$ satisfying $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq 0$ and $\sum \lambda_i \equiv 0 \pmod 2$. We will denote by V, without mentioning λ anymore, the irreducible algebraic representation of $\boldsymbol{G}$ of highest weight $(\lambda, 0)$. As V has trivial central character, it will be considered as an irreducible representation of PGSp_6. Then π_∞ belongs to the discrete series L-packet $P(V)$. As a consequence,

$$H^6(\mathfrak{g}, K_{\boldsymbol{G}}; \pi_\infty \otimes V) = \mathrm{Hom}_{K_{\boldsymbol{G}}}\big(\textstyle\bigwedge^6 \mathfrak{g}_{\mathbb{C}}/\mathrm{Lie}(K_{\boldsymbol{G}})_{\mathbb{C}}; \pi_\infty \otimes V\big) \neq 0,$$

where $K_{\boldsymbol{G}} = \mathbb{R}_+^\times K_\infty$.

There are natural inclusions of spaces of $\mathbb{C}$-valued functions

$$\mathcal{C}^\infty_{\mathrm{cusp}}(\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A})) \subseteq \mathcal{C}^\infty_{\mathrm{rd}}(\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A})) \subseteq \mathcal{C}^\infty_{(2)}(\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A})) \subseteq \mathcal{C}^\infty(\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A})),$$

where these spaces denote, respectively, the space of cuspidal square-integrable functions, rapidly decreasing functions, square-integrable functions and smooth functions, and

$$\mathcal{C}^\infty_{\mathrm{c/center}}(\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A})) \subseteq \mathcal{C}^\infty_{\mathrm{rd}}(\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A})),$$

where the first space is the space of compactly supported modulo the center functions (for the precise definition of these spaces, we refer to [Borel 1981]). Tensoring by V the inclusions above and applying the $(\mathfrak{g}, K_{\boldsymbol{G}})$-cohomology functor, we obtain the natural maps

$$\begin{tikzcd}
H^{\bullet}_{\mathrm{cusp}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}) \arrow[r] & H^{\bullet}_{\mathrm{rd}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}) \arrow[r] & H^{\bullet}_{(2)}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}) \arrow[r] & H^{\bullet}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}) \\
& H^{\bullet}_{\mathrm{c}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}) \arrow[u] & &
\end{tikzcd}$$

where $\mathcal{V}_{\mathbb{C}}$ is the $\mathbb{C}$-local system associated to V. Let $H^{\bullet}_{!}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})$ denote the image of $H^{\bullet}_{c}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})$ in $H^{\bullet}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})$. Let N denote the positive integer defined as the product of prime numbers ℓ such that π_ℓ is ramified. The fact that π_∞ is cohomological implies that there exists a number field L whose ring of integers $\mathcal{O}_L$ contains the eigenvalues of the spherical Hecke algebra $\mathcal{H}^{\mathrm{sph},N}$ away from N and with coefficients in $\mathbb{Z}$ acting on $\bigotimes'_{\ell \nmid N} \pi_\ell^{\boldsymbol{G}(\mathbb{Z}_\ell)}$. Let $\mathcal{H}_L^{\mathrm{sph},N}$ denote the spherical Hecke algebra away from N with coefficients in L, let $\theta_\pi : \mathcal{H}_L^{\mathrm{sph},N} \to L$ denote the Hecke character of π and let $\mathfrak{m}_\pi := \ker(\theta_\pi)$. Considering the localization at $\mathfrak{m}_\pi$ of the above cohomology groups, we have the following result.

Proposition 2.5. *Let π satisfy the hypotheses* (DS) *and* (St) *above. Then*

$$H^{\bullet}_{\mathrm{cusp}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} = H^{\bullet}_{(2)}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} = H^{\bullet}_{!}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} = H^{\bullet}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi}.$$

Proof. By [Borel 1981, Theorem 5.3 & Corollary 5.5], the compositions of the horizontal maps

$$H^{\bullet}_{\mathrm{cusp}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}) \hookrightarrow H^{\bullet}_{*}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}),$$

for $* \in \{\mathrm{rd}, (2), \varnothing\}$, are injections. By [Borel 1981, Theorem 5.2], one has an isomorphism

$$H^{\bullet}_{\mathrm{c}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}) \cong H^{\bullet}_{\mathrm{rd}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}).$$

Hence, if the equality $H^{\bullet}_{\mathrm{cusp}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} = H^{\bullet}_{(2)}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi}$ holds, we have

$$H^{\bullet}_{\mathrm{cusp}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} = H^{\bullet}_{(2)}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} = H^{\bullet}_{!}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi}.$$

We show the former equality as follows. By [Borel 1980, §4],

$$H^{\bullet}_{(2)}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}) = \bigoplus_{\sigma \subset L^2_d} \sigma_f^U \otimes H^{\bullet}(\mathfrak{g}, K_{\boldsymbol{G}}; \sigma_\infty \otimes V)^{m(\sigma)}, \tag{4}$$

where σ runs over the set of isomorphism classes of automorphic representations appearing in the discrete spectrum L^2_d of $L^2(Z(\mathbb{A})\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A}))$. Similarly,

$$H^{\bullet}_{\mathrm{cusp}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}) = \bigoplus_{\sigma \subset L^2_0} \sigma_f^U \otimes H^{\bullet}(\mathfrak{g}, K_{\boldsymbol{G}}; \sigma_\infty \otimes V)^{m_0(\sigma)},$$

where σ runs over the set of isomorphism classes of automorphic representations in the cuspidal spectrum $L^2_0 \subset L^2_d$. From (4), we can write

$$H^{\bullet}_{(2)}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} = \bigoplus_{\sigma = \sigma_\infty \otimes \sigma_f} \sigma_f^U \otimes H^{\bullet}(\mathfrak{g}, K_{\boldsymbol{G}}; \sigma_\infty \otimes V)^{m(\sigma)},$$

where $\sigma \in L^2_d$ is such that $\sigma_\ell^{\boldsymbol{G}(\mathbb{Z}_\ell)} \simeq \pi_\ell^{\boldsymbol{G}(\mathbb{Z}_\ell)} \neq 0$ at all $\ell \nmid N$. Notice that the latter implies that $\sigma_f^N \simeq \pi_f^N$, where for any automorphic representation τ we have denoted $\tau_f^N = \otimes_{\ell \nmid N} \tau_\ell$. By [Kret and Shin 2023, Lemma 8.1(2)], the Steinberg condition implies that the representation π_ℓ is tempered and unitary at each $\ell \nmid N$ (as π has trivial central character). Thus, if σ contributes nontrivially to the above sum, its local component at a finite place $\ell \nmid N$ is tempered. This implies that σ is necessarily cuspidal and thus appears in $H^\bullet_{\mathrm{cusp}}(\mathrm{Sh}_{\boldsymbol{G}}, \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi}$ with multiplicity $m_0(\sigma) = m(\sigma)$. This last statement follows from the fact that any noncuspidal automorphic representation appearing in L^2_d is obtained as a residue of an Eisenstein series and in particular it is nontempered at every place (see [Labesse 1999, Proposition 4.5.4]). We are left to show that

$$H^\bullet_{(2)}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} = H^\bullet(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi}.$$

Recall that Franke's decreasing filtration on the space of automorphic forms for $\boldsymbol{G}(\mathbb{A})$ (see [Waldspurger 1997, §4.7]) yields a spectral sequence $E_1^{p,q} \Rightarrow H^{p+q}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})$, where

$$E_1^{p,q} = \bigoplus_{\substack{(w,P)\in B(p)\\ \ell(w)\le p+q}} \bigoplus_{\sigma=\sigma_\infty\otimes\sigma_f} (\mathrm{Ind}_{P(\mathbb{A}_f)}^{\boldsymbol{G}(\mathbb{A}_f)} \sigma_f)^U \otimes H^{p+q-\ell(w)}(\mathfrak{m}, K_M; \sigma_\infty \otimes W^{w(\lambda+\rho)-\rho}),$$

where, for all $p \in \mathbb{Z}_{\geq 0}$, $B(p)$ denotes a certain subset depending on p of elements (w, P) (see [Waldspurger 1997, §4.8]), with $w \in \mathfrak{W}_{\boldsymbol{G}}$ and $P = M \cdot U_P$ a standard parabolic subgroup of $\boldsymbol{G}$, $W^{w(\lambda+\rho)-\rho}$ denotes the irreducible algebraic representation of M of highest weight $w(\lambda+\rho)-\rho$, and σ runs over the set of isomorphism classes of automorphic representations appearing in the discrete spectrum of $L^2(Z_M(\mathbb{A})M(\mathbb{Q})\backslash M(\mathbb{A}))$. By the proof of [Kret and Shin 2023, Lemma 8.1(1)], we have that $E_{1,\mathfrak{m}_\pi}^{p,q}$ are zero unless when $(w, P) = (1, \boldsymbol{G})$, in which case there exists a unique $p_0 \in \mathbb{Z}_{\geq 0}$, for which

$$E_{1,\mathfrak{m}_\pi}^{p,q} = \begin{cases} H_{(2)}^{p+q}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} & \text{if } p = p_0, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, the spectral sequence for the localization degenerates at the first page and gives

$$H_{(2)}^{p_0+\bullet}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} = E_{1,\mathfrak{m}_\pi}^{p_0,\bullet} = H^{p_0+\bullet}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi}. \qquad \square$$

Proposition 2.6. *Let π satisfy the hypotheses* (DS) *and* (St) *above. Then*

$$H^\bullet(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} = H^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi} \neq 0.$$

Proof. Suppose that τ_f contributes to $H^i(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})_{\mathfrak{m}_\pi}$. As we noted in the proof of Proposition 2.5, this implies that, for every $\ell \nmid N$, $\tau_\ell \simeq \pi_\ell$ is tempered and unitary (see [Kret and Shin 2023, Lemma 8.1(2)]). Let us fix $\ell \nmid N$; the action of the Frobenius correspondence on intersection cohomology Frob_ℓ on $IH^i(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})[\tau_f]$ and thus on $H^i(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})[\tau_f]$ is pure of weight i, i.e., its eigenvalues all have absolute value $\ell^{i/2}$ (see [Morel 2010, Remark 7.2.5]). On the other hand, by the congruence relation conjectured in [Blasius and Rogawski 1994, §6] and verified in [Wedhorn 2000], Frob_ℓ is a root of the Hecke polynomial

$$H_\ell(T) := \det(T - \ell^3 \mathrm{spin}(\mathrm{Fr}_\ell \ltimes \hat{g})),$$

which is a polynomial in T whose coefficients are elements in the coordinate ring of the set of Fr_ℓ-conjugacy classes of semisimple elements of $\widehat{\boldsymbol{G}}(\mathbb{C}) = \mathbf{GSpin}_7(\mathbb{C})$, for Fr_ℓ a Frobenius element in the Weil group of $\mathbb{Q}_\ell$. By the untwisted Satake isomorphism, we can see $H_\ell(T)$ as a polynomial with coefficients in the spherical Hecke algebra $\mathcal{H}(\boldsymbol{G}(\mathbb{Q}_\ell)//\boldsymbol{G}(\mathbb{Z}_\ell), \mathbb{Q})$ (see [Wedhorn 2000, (2.2.1) & Corollary (2.8)]) and thus we can denote by $H_\ell(T; \tau_\ell)$ the specialization of $H_\ell(T)$ to τ_ℓ, i.e.,

$$H_\ell(T; \tau_\ell) = \det(T - \ell^3 \mathrm{spin}(\phi_{\tau_\ell}(\mathrm{Fr}_\ell))),$$

where ϕ_{τ_ℓ} is the unramified Langlands parameter of τ_ℓ. The congruence relation gives that $H_\ell(\mathrm{Frob}_\ell; \tau_\ell) = 0$ on $IH^\bullet(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_\mathbb{C})[\tau_f]$, which implies that the eigenvalues of Frob_ℓ on $IH^\bullet(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_\mathbb{C})[\tau_f]$ are a subset of the ones of $\ell^3 \mathrm{spin}(\phi_{\tau_\ell}(\mathrm{Frob}_\ell))$. As τ_ℓ is tempered, all the eigenvalues of $\mathrm{spin}(\phi_{\tau_\ell}(\mathrm{Fr}_\ell))$ have absolute value equal to 1 (see [Gross 1998, §6]). Hence the eigenvalues of $\ell^3 \mathrm{spin}(\phi_{\tau_\ell}(\mathrm{Fr}_\ell))$, and thus of Frob_ℓ, have all absolute value equal to ℓ^3. In particular, $H^i(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_\mathbb{C})[\tau_f]$ is zero unless $i = 6$. Finally, notice that $H^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_\mathbb{C})_{\mathfrak{m}_\pi} \neq 0$ as the assumption (DS) implies $H^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_\mathbb{C})[\pi_f] \neq 0$. □

Remark 2.7. The proof of Proposition 2.6 is similar to that of [Kret and Shin 2023, Proposition 8.2], where the proof is carried out with a trace formula argument.

2.8. *Hodge theory.*

We keep the same notation as Section 2.7. In particular, $\pi = \pi_\infty \otimes \pi_f$ is a cuspidal automorphic representation of $\boldsymbol{G}$ with trivial central character which satisfies (DS) and (St), with $\pi_\infty \in P(V)$ for some irreducible algebraic representation V of $\boldsymbol{G}$ as above.

Let $\mathcal{V}$ denote the $\mathbb{Q}$-local system on $\mathrm{Sh}_{\boldsymbol{G}}(U)$ attached to V. We can take the π_f-isotypic component $H^6_{B,*}[\pi_f]$ of $H^6_*(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_\mathbb{C})$, where $* \in \{\varnothing, !\}$ and where $\mathcal{V}_\mathbb{C}$ denotes $\mathcal{V} \otimes_\mathbb{Q} \mathbb{C}$. Propositions 2.5 and 2.6 imply

$$H^\bullet_B[\pi_f] = H^\bullet_{B,!}[\pi_f] = H^6_{B,!}[\pi_f] \neq 0. \tag{5}$$

By [Blasius and Rogawski 1994, (2.3.1)] (see also [Shin and Templier 2014, Proposition 2.15]), if L is a sufficiently large number field, $H^6_B[\pi_f]$ appears as a subquotient of $H^6_!(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_L)$, where $\mathcal{V}_L$ denotes $\mathcal{V} \otimes_\mathbb{Q} L$. In particular, we have a projection

$$\mathrm{pr}_\pi : H^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_L)_{\mathfrak{m}_\pi}(n) \twoheadrightarrow H^6_B[\pi_f](n).$$

Since $H^6_!(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_L)$ is a pure L-Hodge structure of weight 6, we have

$$H^6_B[\pi_f] = \pi_f^U(L) \otimes M_B(\pi_f),$$

with $\pi_f^U(L)$ a realization of π_f^U over L and $M_B(\pi_f)$ a pure L-Hodge structure of weight 6. Thus we have a decomposition

$$M_B(\pi_f) \otimes \mathbb{C} = \bigoplus_{p+q=6} H^{p,q}(\pi_f).$$

Lemma 2.8. *Under the hypotheses* (DS) *and* (St),

$$\dim_\mathbb{C} H^{p,q}(\pi_f) = \begin{cases} 1 & \text{if } p \neq 3, \\ 2 & \text{if } p = 3. \end{cases}$$

In particular, $\dim_L M_B(\pi_f) = 8$.

Proof. Thanks to (5), we have that

$$H^6_B[\pi_f]\otimes\mathbb{C}=H^6_{B,!}[\pi_f]\otimes\mathbb{C}=H^6_{B,\mathrm{cusp}}[\pi_f]\otimes\mathbb{C};$$

hence

$$H^6_B[\pi_f]\otimes\mathbb{C}=\pi_f^U\otimes\bigoplus_{\sigma_\infty}H^6(\mathfrak{g},K_G;\sigma_\infty\otimes V)^{m(\sigma)},$$

where σ_∞ runs over the elements of the discrete series L-packet $P(V)$ of $\mathrm{PGSp}_6(\mathbb{R})$ and $m(\sigma)$ denotes the multiplicity of $\sigma=\sigma_\infty\otimes\pi_f$. Notice that $H^6(\mathfrak{g},K_G;\sigma_\infty\otimes V)$ equals

$$\mathrm{Hom}_{K_\infty}\big(\textstyle\bigwedge^6\mathfrak{g}_0/\mathfrak{k},\sigma^1_\infty\otimes V\big)\oplus\mathrm{Hom}_{K_\infty}\big(\textstyle\bigwedge^6\mathfrak{g}_0/\mathfrak{k},\bar\sigma^1_\infty\otimes V\big),\tag{6}$$

where we have denoted $\sigma_{\infty|_{G_0(\mathbb{R})}}=\sigma^1_\infty\oplus\bar\sigma^1_\infty$. According to [Borel and Wallach 1980, Theorem II.5.3(b)], each space in the decomposition above is one-dimensional. Moreover there exists a unique pair of integers $(r_{\sigma_\infty},s_{\sigma_\infty})$ satisfying $r_{\sigma_\infty}+s_{\sigma_\infty}=6$ such that (6) equals

$$\mathrm{Hom}_{K_\infty}\big(\textstyle\bigwedge^{r_{\sigma_\infty}}\mathfrak{p}^+_{\mathbb{C}}\otimes\bigwedge^{s_{\sigma_\infty}}\mathfrak{p}^-_{\mathbb{C}},\sigma^1_\infty\otimes V\big)\oplus\mathrm{Hom}_{K_\infty}\big(\textstyle\bigwedge^{s_{\sigma_\infty}}\mathfrak{p}^+_{\mathbb{C}}\otimes\bigwedge^{r_{\sigma_\infty}}\mathfrak{p}^-_{\mathbb{C}},\bar\sigma^1_\infty\otimes V\big).$$

As we remarked in Section 2.5, the set $P(V)$ has four elements and is in bijection with the set of Hodge types up to conjugation. Since the Hodge structure in $H^6_{B,\mathrm{cusp}}[\pi_f]$ is induced by this splitting, we deduce that

$$\dim_{\mathbb{C}}H^{r_{\sigma_\infty},s_{\sigma_\infty}}(\pi_f)=\begin{cases}m(\sigma)&\text{if }r_{\sigma_\infty}\neq3,\\2m(\sigma)&\text{if }r_{\sigma_\infty}=3.\end{cases}$$

By [Kret and Shin 2023, Theorem 12.1], the multiplicity of σ is either 0 or 1, while thanks to [Kret and Shin 2023, Corollaries 8.4 & 12.4] the dimension of $M_B(\pi_f)$ equals 8. Hence $m(\sigma)=1$ for all $\sigma_\infty\in P(V)$, which concludes the proof. □

2.9. ***Absolute Hodge cohomology.*** Let us first recall some definitions from [Beĭlinson 1986]. A mixed $\mathbb{R}$-Hodge structure consists of a finite-dimensional $\mathbb{R}$-vector space $M_{\mathbb{R}}$ equipped with an increasing finite filtration W_* called the weight filtration and a decreasing finite filtration F^* on $M_{\mathbb{C}}=M_{\mathbb{R}}\otimes_{\mathbb{R}}\mathbb{C}$ called the Hodge filtration, such that each pair $(\mathrm{Gr}^W_nM_{\mathbb{R}},(\mathrm{Gr}^W_nM_{\mathbb{C}},F^*))$ is a pure $\mathbb{R}$-Hodge structure of weight n [Deligne 1971, Définition 2.1.10]. The category of mixed $\mathbb{R}$-Hodge structures is an abelian category [Deligne 1971, Théorème (2.3.5)] and we denote it by $\mathrm{MHS}_{\mathbb{R}}$.

Definition 2.9. A real mixed $\mathbb{R}$-Hodge structure is given by a mixed $\mathbb{R}$-Hodge structure such that $M_{\mathbb{R}}$ is equipped with an involution F^*_∞ stabilizing the weight filtration and whose $\mathbb{C}$-antilinear complexification $\overline{F^*_\infty}=F^*_\infty\otimes c$, where c denotes the complex conjugation, defines an involution on $M_{\mathbb{C}}$ stabilizing the Hodge filtration.

We will refer to F^*_∞ as the real Frobenius and to $\overline{F^*_\infty}$ as the de Rham involution. We denote by $\mathrm{MHS}^+_{\mathbb{R}}$ the abelian category of real mixed Hodge $\mathbb{R}$-structures. For any pair of objects $M,N\in D(\mathrm{MHS}^+_{\mathbb{R}})$, one has $R\,\mathrm{Hom}_{\mathrm{MHS}^+_{\mathbb{R}}}(M,N)=R\,\mathrm{Hom}_{\mathrm{MHS}_{\mathbb{R}}}(M,N)^{\overline{F^*_\infty}}$, since taking invariants by $\overline{F^*_\infty}$ is an exact functor.

Definition 2.10. If $M = (M_{\mathbb{R}}, F_\infty^*) \in C(\mathrm{MHS}_{\mathbb{R}}^+)$ is a complex of real mixed $\mathbb{R}$-Hodge structure, its absolute Hodge cohomology is defined as

$$R\Gamma_{\mathcal{H}}(M) = R\,\mathrm{Hom}_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), M_{\mathbb{R}}).$$

Its real absolute Hodge cohomology is defined as

$$R\Gamma_{\mathcal{H}/\mathbb{R}}(M) := R\,\mathrm{Hom}_{\mathrm{MHS}_{\mathbb{R}}^+}(\mathbb{R}(0), M)) = R\Gamma_{\mathcal{H}}(M_{\mathbb{R}})^{\overline{F_\infty^*}}.$$

The cohomology groups $H_B^i(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}})$, where $\mathcal{V}_{\mathbb{R}} = \mathcal{V} \otimes_{\mathbb{Q}} \mathbb{R}$, are equipped with a real Frobenius F_∞^* acting as the complex conjugation on (the complex points) $\mathrm{Sh}_{\boldsymbol{G}}(U)$ and on $\mathcal{V}_{\mathbb{R}}$, define real mixed $\mathbb{R}$-Hodge structures. This can be deduced directly from [Deligne 1971] since the cohomology with coefficients is a direct factor of the cohomology of a fiber product of the universal abelian variety of $\mathrm{Sh}_{\boldsymbol{G}}(U)$, or from the theory of mixed Hodge modules of [Saito 1990]. We let $M \in C(\mathrm{MHS}_{\mathbb{R}}^+)$ be the complex of real mixed $\mathbb{R}$-Hodge structures given by $\big(\bigoplus_{i\in\mathbb{N}} H_B^i(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}})[-i], F_\infty^*\big)$ and we define the absolute real Hodge cohomology $H_{\mathcal{H}}^7(\mathrm{Sh}_{\boldsymbol{G}}(U)/\mathbb{R}, \mathcal{V}_{\mathbb{R}}(4))$ of $\mathrm{Sh}_{\boldsymbol{G}}(U)$ and coefficients in $\mathcal{V}_{\mathbb{R}}(4)$ to be $H^1(R\Gamma_{\mathcal{H}/\mathbb{R}}(M(4)))$. Then we have the short exact sequence

$$\begin{aligned} 0 \to \mathrm{Ext}^1_{\mathrm{MHS}_{\mathbb{R}}^+}(\mathbb{R}(0), H_B^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))) \to H_{\mathcal{H}}^7(\mathrm{Sh}_{\boldsymbol{G}}(U)/\mathbb{R}, \mathcal{V}_{\mathbb{R}}(4)) \\ \to \mathrm{Hom}_{\mathrm{MHS}_{\mathbb{R}}^+}(\mathbb{R}(0), H_B^7(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))) \to 0. \end{aligned}$$

If $\pi = \pi_\infty \otimes \pi_f$ is as above, we denote by

$$H_{\mathcal{H}}^1(M(\pi_f)_{\mathbb{R}}(4)) := \big(H_{\mathcal{H}}^7(\mathrm{Sh}_{\boldsymbol{G}}(U)/\mathbb{R}, \mathcal{V}_{\mathbb{R}}(4)) \otimes L\big)[\pi_f]$$

the π_f-isotypical component.

Lemma 2.11. *Under the hypotheses* (DS) *and* (St), *we have a canonical short exact sequence of finite rank-free* $\mathbb{R} \otimes_{\mathbb{Q}} L$*-modules*

$$0 \to F^4 H^6_{\mathrm{dR}}[\pi_f] \to H^6_{\mathrm{B}}[\pi_f]^{F_\infty^\star = -1}(3) \to H^1_{\mathcal{H}}(M(\pi_f)_{\mathbb{R}}(4)) \to 0.$$

Moreover, we have

$$\dim_{\mathbb{R}\otimes_{\mathbb{Q}} L} H^1_{\mathcal{H}}(M(\pi_f)_{\mathbb{R}}(4)) = \dim_{\mathbb{C}} \pi_f^U.$$

Proof. It follows from the existence of the short exact sequence above and from Proposition 2.6 that we have a canonical isomorphism

$$H^1_{\mathcal{H}}(M(\pi_f)_{\mathbb{R}}(4)) \simeq \mathrm{Ext}^1_{\mathrm{MHS}_{\mathbb{R}}^+}(\mathbb{R}(0), H_B^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))[\pi_f]).$$

Hence, the first statement of the lemma follows as in [Lemma 2017, Lemma 4.11]. In particular, the map $F^4 H^6_{\mathrm{dR}}[\pi_f] \to H^6_{\mathrm{B}}[\pi_f]^{F_\infty^\star = -1}(3)$ is defined by the composition of

$$F^4 H^6_{\mathrm{dR}}[\pi_f] \to H^6_{\mathrm{dR}}[\pi_f] \otimes \mathbb{C} \simeq H_B^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}})[\pi_f],$$

of the projection to $H^6_B(\mathrm{Sh}_{\boldsymbol{G}}(U),\mathcal{V}_{\mathbb{C}})[\pi_f]^{\overline{F^*_\infty}=1}$, where $\overline{F^*_\infty}$ is the complexification $F^*_\infty\otimes c$, with c denoting the complex conjugation, and of the projection

$$H^6_B(\mathrm{Sh}_{\boldsymbol{G}}(U),\mathcal{V}_{\mathbb{C}})[\pi_f]^{\overline{F^*_\infty}=1}=H^6_{\mathrm{B}}[\pi_f]^{F^\star_\infty=-1}(3)\oplus H^6_{\mathrm{B}}[\pi_f]^{F^\star_\infty=1}(4)\to H^6_{\mathrm{B}}[\pi_f]^{F^\star_\infty=-1}(3).$$

Finally, by Lemma 2.8, we have that

$$\dim_{\mathbb{R}\otimes_{\mathbb{Q}}L} F^4H^6_{\mathrm{dR}}[\pi_f]=3\dim_L\pi_f^U(L)=3\dim_{\mathbb{C}}\pi_f^U.$$

On the other hand,

$$\dim_{\mathbb{R}\otimes_{\mathbb{Q}}L} H^6_{\mathrm{B}}[\pi_f]^{F^\star_\infty=-1}(3)=(3+h^{3,+})\dim_{\mathbb{C}}\pi_f^U,$$

where $h^{3,+}$ is the dimension of the $\mathbb{C}$-vector space $\{x\in H^{3,3}(\pi_f):F^*_\infty(x)=-x\}$ (see [Burgos Gil et al. 2024, §3.4.2]). By the proof of Lemma 2.8, we have $h^{3,+}=1$, which implies the result. □

3. Construction of the motivic class

3.1. ***Cartan product.*** Before starting, we briefly recall some properties of the Cartan product of irreducible representations that will be needed (see [Sun 2017, §2.5] for more details). Let A denote either a connected compact Lie group or a semisimple algebraic group. Fix a Cartan subgroup of A and an orientation of the roots. Irreducible algebraic representations of A are parametrized by dominant weights. If λ and σ are two dominant weights with corresponding representations V^λ and V^σ, then the representation $V^{\lambda+\sigma}$ appears in $V^\lambda\otimes V^\sigma$ with multiplicity one. We denote it by $V^\lambda\cdot V^\sigma$ and we call it the Cartan component of $V^\lambda\otimes V^\sigma$. Clearly, the tensor product of two highest weight vectors maps to a corresponding highest weight vector. We denote by $v\otimes w\mapsto v\cdot w$ the projection from $V^\lambda\otimes V^\sigma$ to its Cartan component $V^\lambda\cdot V^\sigma$.

Lemma 3.1 [Sun 2017, Lemma 2.12]. *Every nonzero pure tensor in $V^\lambda\otimes V^\sigma$ projects nontrivially to the Cartan component.*

3.2. ***Branching laws.*** In what follows, we fix a totally real field F over which $\boldsymbol{H}$ splits. Since $\boldsymbol{H}$ is split over F, its finite-dimensional irreducible representations are determined by the highest weight theory and we can thus use the branching laws for algebraic representations from $\boldsymbol{G}$ to $\boldsymbol{H}$ established in [Cauchi and Rodrigues Jacinto 2020].

Lemma 3.2. *The $\boldsymbol{G}$-representation V^λ over F of highest weight $\lambda=(\lambda_1,\lambda_2,\lambda_3,c)$ contains the trivial $\boldsymbol{H}$-representation if and only if $c=0$ and $\lambda_1=\lambda_2+\lambda_3$. When this holds the trivial representation of $\boldsymbol{H}$ appears in $(V^\lambda)_{|\boldsymbol{H}}$ with multiplicity $\lambda_2-\lambda_3+1$.*

Proof. From [Cauchi and Rodrigues Jacinto 2020, Lemma 2.10], the sum of all irreducible sub-$\boldsymbol{H}$-representations of V^λ isomorphic (up to a twist) to $\mathrm{Sym}^{(k,0,0)}$ for some $k\geq 0$ is given by

$$\bigoplus_{\substack{k=|\lambda_1-\lambda_2-\lambda_3|\\ k\equiv|\lambda|\ (\mathrm{mod}\ 2)}}^{\lambda_1-\lambda_2+\lambda_3} r\cdot\mathrm{Sym}^{(k,0,0)}\otimes\det^{\frac{1}{2}(|\lambda|-k)}$$

for $r = \lambda_2 - \lambda_3 + 1$. From this we deduce that V^λ contains the trivial $\boldsymbol{H}$-representation with multiplicity $r = \lambda_2 - \lambda_3 + 1$ if and only if $\lambda_1 - \lambda_2 - \lambda_3 = 0$. □

It will be useful to construct explicitly generators of the trivial $\boldsymbol{H}$-representations inside V^λ given by the branching laws. We achieve this by constructing some vectors in the representations $V^{(1,1,0,0)}$ and $V^{(2,1,1,0)}$ and then by taking their Cartan product. From now on, all the representations are defined over F. Moreover, since the branching laws are determined by the restriction to the derived subgroups, in the following we work with the groups

$$\boldsymbol{H}_0 := \mathrm{SL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2 \hookrightarrow \boldsymbol{H}_0' := \mathrm{SL}_2 \times \mathrm{Sp}_4 \hookrightarrow \boldsymbol{G}_0 = \mathrm{Sp}_6.$$

Recall that we associate to any $\lambda = (\lambda_1, \lambda_2) \in \mathbb{Z}^2$ such that $\lambda_1 \geq \lambda_2 \geq 0$, the irreducible Sp_4-representation with highest weight λ. Applying the branching laws [Cauchi and Rodrigues Jacinto 2020, Proposition 2.8], we get the following decompositions of representations of $\boldsymbol{H}_0'$:

$$\begin{aligned} V^{(1,1,0)} &= (\mathrm{Sym}^0 \boxtimes V^{(0,0)}) \oplus (\mathrm{Sym}^0 \boxtimes V^{(1,1)}) \oplus (\mathrm{Sym}^1 \boxtimes V^{(1,0)}), \\ V^{(2,1,1)} &= (\mathrm{Sym}^0 \boxtimes V^{(1,1)}) \oplus (\mathrm{Sym}^0 \boxtimes V^{(2,0)}) \oplus (\mathrm{Sym}^1 \boxtimes V^{(1,0)}) \oplus (\mathrm{Sym}^1 \boxtimes V^{(2,1)}) \oplus (\mathrm{Sym}^2 \boxtimes V^{(1,1)}). \end{aligned}$$

By Lemma 3.2, $V^{(1,1,0)}$ contains two copies of the trivial $\boldsymbol{H}_0$-representation, each of which lies respectively in $\mathrm{Sym}^0 \boxtimes V^{(0,0)}$ and $\mathrm{Sym}^0 \boxtimes V^{(1,1)}$, while $V^{(2,1,1)}$ contains a unique trivial $\boldsymbol{H}_0$-representation appearing in $\mathrm{Sym}^0 \boxtimes V^{(1,1)}$. Using these facts, we can explicitly define generators of these three trivial representations of $\boldsymbol{H}_0$.

Let V be the standard representation of $\boldsymbol{G}_0$ with its symplectic basis $\langle e_1, e_2, e_3, f_1, f_2, f_3\rangle$ given in Section 2.6. According to our choice of embedding $\boldsymbol{H}_0' \hookrightarrow \boldsymbol{G}_0$, $\langle e_1, f_1\rangle$ (resp. $\langle e_2, e_3, f_2, f_3\rangle$) defines a basis of the standard representation of SL_2 (resp. Sp_4). We first recall how one can realize the representations $V^{(1,1,0)}$ and $V^{(1,1,1)}$. As explained in [Fulton and Harris 1991, §17.1], $V^{(1,1,0)}$ is realized inside $\bigwedge^2 V$ as the complement of the $\boldsymbol{G}_0$-invariant subspace generated by the vector $e_1 \wedge f_1 + e_2 \wedge f_2 + e_3 \wedge f_3$ corresponding to the symplectic form or, in other words, as the kernel of the map $\bigwedge^2 V \to V$ sending $v_1 \wedge v_2$ to $\psi(v_1, v_2)$. By [Fulton and Harris 1991, Theorem 17.5], the irreducible representation $V^{(1,1,1)}$ is identified with the kernel of the map $\varphi : \bigwedge^3 V \to V,\ v_1 \wedge v_2 \wedge v_3 \mapsto \sum_{i<j,k\neq i,j} \psi(v_i, v_j)(-1)^{i-j+1} v_k$.

Lemma 3.3. *Let $F(0)$ denote the trivial $\boldsymbol{H}_0$-representation. We have*

$$\begin{aligned} v &:= e_2 \wedge f_2 - e_3 \wedge f_3 \in F(0) \subseteq \mathrm{Sym}^0 \boxtimes V^{(1,1)} \subseteq V^{(1,1,0)}, \\ w &:= e_2 \wedge f_2 + e_3 \wedge f_3 - 2e_1 \wedge f_1 \in F(0) \subseteq \mathrm{Sym}^0 \boxtimes V^{(0,0)} \subseteq V^{(1,1,0)}, \\ z &:= z_1 - z_2 \in F(0) \subseteq \mathrm{Sym}^0 \boxtimes V^{(1,1)} \subseteq V^{(2,1,1)}, \end{aligned}$$

where

$$\begin{aligned} z_1 &:= e_1 \cdot (f_1 \wedge e_2 \wedge f_2 - f_1 \wedge e_3 \wedge f_3), \\ z_2 &:= f_1 \cdot (e_1 \wedge e_2 \wedge f_2 - e_1 \wedge e_3 \wedge f_3), \end{aligned}$$

and $\cdot$ denotes the Cartan product.

Proof. The vector v is obtained from the highest weight vector $e_1 \wedge e_2$ in $V^{(1,1,0)}$ by applying the composition $X_{(0,1,-1)} \circ X_{(0,-2,0)} \circ X_{(-1,0,1)}$, where $X_{(-1,0,1)}, X_{(0,-2,0)}, X_{(0,1,-1)} \in \mathfrak{sp}_6$ denote the weight vectors for $\lambda(-1,0,1)$, $\lambda(0,-2,0)$, and $\lambda(0,1,-1)$ respectively (see [Fulton and Harris 1991, §16.1] for the precise description). Moreover, the vector $X_{(-1,0,1)}(e_1 \wedge e_2) = -e_2 \wedge e_3$ is of weight $(0,1,1)$, which appears only in the component $\mathrm{Sym}^0 \boxtimes V^{(1,1)}$, and $X_{(0,1,-1)}, X_{(0,-2,0)} \in \mathfrak{sp}_4 \subseteq \mathfrak{sp}_6$ so v still lies inside $\mathrm{Sym}^0 \boxtimes V^{(1,1)}$. The vector w is $\boldsymbol{H}_0'$-invariant and therefore it generates the only trivial $\boldsymbol{H}_0'$-representation in $V^{(1,1,0)}$. We now explain the definition of z. Note that $e_1 \in V^{(1,0,0)}$ and $f_1 \wedge e_2 \wedge f_2 - f_1 \wedge e_3 \wedge f_3 \in V^{(1,1,1)}$. Thus, by the properties of the Cartan product

$$V^{(1,0,0)} \otimes V^{(1,1,1)} = V^{(1,1,0)} \oplus V^{(2,1,1)} \to V^{(2,1,1)}, \quad v_1 \otimes v_2 \mapsto v_1 \cdot v_2,$$

z_1 is a nonzero vector in $V^{(2,1,1)}$ by Lemma 3.1. The vector z_1 is fixed by $\{I_2\} \times \mathrm{SL}_2^2$, but not by $\mathrm{SL}_2 \times \{I_2\} \times \{I_2\}$, however, as it is easy to verify, we have that

$$z = z_1 + h \cdot z_1 = z_1 - z_2 \in F(0) \subset V^{(2,1,1)}, \quad \text{with } h = \left(\left(\begin{smallmatrix} & 1 \\ -1 & \end{smallmatrix}\right), I_2, I_2\right),$$

generates the unique trivial $\boldsymbol{H}_0$-representation of $V^{(2,1,1)}$. □

Lemma 3.4. *Let $\lambda = (\lambda_2 + \lambda_3, \lambda_2, \lambda_3, 0)$ with $\lambda_2 \geq \lambda_3 \geq 0$. For each $\lambda_2 \geq \mu \geq \lambda_3$, the vector*

$$v^{[\lambda,\mu]} := v^{\lambda_2 - \mu} \cdot w^{\mu - \lambda_3} \cdot z^{\lambda_3} \in F(0) \subseteq (V^\lambda)_{|\boldsymbol{H}}$$

realizes a distinct copy of the trivial representation $F(0)$ of $\boldsymbol{H}$ inside $(V^\lambda)_{|\boldsymbol{H}}$.

Proof. For $p, q, r \in \mathbb{N}$, we have

$$v^p \cdot w^q \cdot z^r \in F(0) \subseteq \mathrm{Sym}^0 \boxtimes V^{(p+r,p+r)} \subseteq V^{(p+q+2r,p+q+r,r)}.$$

The vectors v, w, z are $\boldsymbol{H}$-highest weight vectors, and thus $v^{[\lambda,\mu]}$ is too. We are left to show that each of the vectors is different. This follows from the fact that each $v^{[\lambda,\mu]}$ lies in $\mathrm{Sym}^0 \boxtimes V^{(\lambda_2+\lambda_3-\mu,\lambda_2+\lambda_3-\mu)} \otimes \nu^{\mu-\lambda_2-\lambda_3}$ and these representations are all different as μ varies. □

3.3. ***The motivic class.*** As in the section above, we fix a totally real field F such that $\boldsymbol{H}$ splits over F. For a smooth quasiprojective scheme S over a field of characteristic zero, let $\mathrm{CHM}_L(S)$ denote the tensor category of relative Chow motives over S with coefficients in a number field L and denote by $M : \mathrm{Var}/S \to \mathrm{CHM}_L(S)$ the contravariant functor from the category of smooth projective schemes over S to the category of relative Chow motives over S (see [Ancona 2015, §2.1]). By [Deninger and Murre 1991, Corollary 3.2], if A/S is an abelian scheme of relative dimension g, there is a decomposition $M(A) = \bigoplus_{i=1}^{2g} h^i(A)$ in $\mathrm{CHM}_L(S)$. Let G temporarily denote one of the groups $\boldsymbol{H}$ or $\boldsymbol{G}$, and denote by $\mathrm{Rep}_F(G)$ the category of finite-dimensional algebraic representations of G defined over F. Ancona [2015] constructed an additive functor

$$\mu_U^G : \mathrm{Rep}_F(G) \to \mathrm{CHM}_F(\mathrm{Sh}_G(U)),$$

where U is a sufficiently small open compact subgroup of $G(\mathbb{A}_f)$. We recall some of its properties.

Proposition 3.5 [Ancona 2015, Théorème 8.6]. *The functor μ_U^G respects duals, tensor products and satisfies the following properties.*

(1) *If V is the standard representation of G, then $\mu_U^G(V) = h^1(\mathscr{A}_G)$, where $\mathscr{A}_G$ is the universal abelian scheme over* $\mathrm{Sh}_G(U)$.

(2) *If $\nu : G \to \boldsymbol{G}_m$ is the multiplier, then $\mu_U^G(\nu)$ is the Lefschetz motive $F(-1)$.*

(3) *For a G-representation V defined over F, the Betti realization of $\mu_U^G(V)$ is the local system $\mathcal{V}_F$ associated to the vector bundle*

$$G(\mathbb{Q})\backslash(X_G \times V \times (G(\mathbb{A}_f)/U)) \to \mathrm{Sh}_G(U)(\mathbb{C}).$$

(4) *For any prime v of F above ℓ and G-representation V, the v-adic étale realization $\mathcal{V}_v$ of $\mu_U^G(V)$ is the étale sheaf associated to $V \otimes_F F_v$, with U acting on the left via $U \hookrightarrow G(\mathbb{A}_f) \to G(\mathbb{Q}_\ell)$.*

Definition 3.6. Let V^λ be the finite-dimensional irreducible algebraic representation over $\mathbb{Q}$ of $\boldsymbol{G}$ of highest weight λ. We denote by $\mathscr{V}_F^\lambda$ the relative Chow motive associated to $V^\lambda \otimes F$.

Let $U \subset \boldsymbol{G}(\mathbb{A}_f)$ be a sufficiently small compact open subgroup and let $U' = U \cap \boldsymbol{H}(\mathbb{A}_f)$. Recall that we have a closed embedding $\iota : \mathrm{Sh}_{\boldsymbol{H}}(U') \hookrightarrow \mathrm{Sh}_{\boldsymbol{G}}(U)$ which is of codimension 3. Let V^λ the algebraic representation of $\boldsymbol{G}$ (over F) of highest weight $\lambda = (\lambda_1, \lambda_2, \lambda_3, c)$ such that $\lambda_1 = \lambda_2 + \lambda_3$ and $c = 0$. Using the branching laws of Lemma 3.2 and [Torzewski 2020, Theorem 1.2], we get the following (see [Cauchi and Rodrigues Jacinto 2020, Proposition 2.17]).

Proposition 3.7. *For any $\lambda_2 \geq \mu \geq \lambda_3$, we have a Gysin morphism*

$$\iota_*^{[\lambda,\mu]} : H^0_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{H}}(U'), F(0)) \to H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}_F^\lambda(3)),$$

corresponding to the embedding of $F(0) \subset \iota^* V^\lambda$ given by the $\boldsymbol{H}$-trivial vector $v^{[\lambda,\mu]}$ of Lemma 3.4.

Definition 3.8. We let $\mathscr{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{M}} \in H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}_F^\lambda(3))$ be the image by $\iota_*^{[\lambda,\mu]}$ of

$$\mathbf{1}_{\mathrm{Sh}_{\boldsymbol{H}}(U')} \in \mathrm{CH}^0(\mathrm{Sh}_{\boldsymbol{H}}(U'))_F = H^0_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{H}}(U'), F(0)).$$

3.4. *Realizations.*

3.4.1. *Étale realization.* Let $\mathfrak{l}$ be a prime of F above ℓ. We have an étale cycle class map

$$\mathrm{cl}_{\text{ét}} : \mathrm{H}^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(\mathrm{U}), \mathscr{V}^\lambda_{\mathrm{F}}(3)) \to \mathrm{H}^6_{\text{ét}}(\mathrm{Sh}_{\boldsymbol{G}}(\mathrm{U}), \mathcal{V}^\lambda_{\mathfrak{l}}(3)) \to \mathrm{H}^6_{\text{ét}}(\mathrm{Sh}_{\boldsymbol{G}}(\mathrm{U})_{\overline{\mathbb{Q}}}, \mathcal{V}^\lambda_{\mathfrak{l}}(3))^{\mathrm{G}_{\mathbb{Q}}},$$

where the last arrow is the natural map obtained from the Hochschild–Serre spectral sequence. We define the following.

Definition 3.9. We let $\mathscr{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\text{ét}} := \mathrm{cl}_{\text{ét}}(\mathscr{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{M}}) \in \mathrm{H}^6_{\text{ét}}(\mathrm{Sh}_{\boldsymbol{G}}(\mathrm{U})_{\overline{\mathbb{Q}}}, \mathcal{V}^\lambda_{\mathfrak{l}}(3))^{\mathrm{G}_{\mathbb{Q}}}$.

Remark 3.10. • Notice that $\mathscr{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\text{ét}}$ equals to the image of $\mathbf{1} \in H^0_{\text{ét}}(\mathrm{Sh}_{\boldsymbol{H}}(U')_{\overline{\mathbb{Q}}}, F_{\mathfrak{l}}(0))$ via the étale Gysin map

$$\iota^{[\lambda,\mu]}_{\text{ét},*} : H^0_{\text{ét}}(\mathrm{Sh}_{\boldsymbol{H}}(U')_{\overline{\mathbb{Q}}}, F_{\mathfrak{l}}(0)) \to H^0_{\text{ét}}(\mathrm{Sh}_{\boldsymbol{H}}(U')_{\overline{\mathbb{Q}}}, \iota^*\mathcal{V}^\lambda_{\mathfrak{l}}) \to H^6_{\text{ét}}(\mathrm{Sh}_{\boldsymbol{G}}(U)_{\overline{\mathbb{Q}}}, \mathcal{V}^\lambda_{\mathfrak{l}}(3)).$$

- As the representation V^λ is self dual, we have a Galois equivariant perfect pairing

$$H^6_{\text{ét},c}(\mathrm{Sh}_{\boldsymbol{G}}(U)_{\overline{\mathbb{Q}}}, \mathcal{V}^\lambda_{\mathfrak{l}}(3)) \times H^6_{\text{ét}}(\mathrm{Sh}_{\boldsymbol{G}}(U)_{\overline{\mathbb{Q}}}, \mathcal{V}^\lambda_{\mathfrak{l}}(3)) \to F_{\mathfrak{l}}(0).$$

Hence, by duality, $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\text{ét}}$ determines a map

$$H^6_{\text{ét},c}(\mathrm{Sh}_{\boldsymbol{G}}(U)_{\overline{\mathbb{Q}}}, \mathcal{V}^\lambda_{\mathfrak{l}}(3)) \to F_{\mathfrak{l}}(0).$$

3.4.2. *Betti realizations.* As in the previous subsection, we define the class

$$\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B} \in H^6_B(\mathrm{Sh}_{\boldsymbol{G}}(U)(\mathbb{C}), \mathcal{V}^\lambda_F(3))$$

as the image of $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{M}}$ via the Betti cycle class map

$$\mathrm{cl_B} : \mathrm{H}^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(\mathrm{U}), \mathscr{V}^\lambda_{\mathrm{F}}(3)) \to \mathrm{H}^6_{\mathrm{B}}(\mathrm{Sh}_{\boldsymbol{G}}(\mathrm{U})(\mathbb{C}), \mathcal{V}^\lambda_{\mathrm{F}}(3)).$$

Note that, as F is totally real, the image satisfies

$$\mathrm{Im}(\mathrm{cl_B}) \subset \mathrm{H}^6_{\mathrm{B}}(\mathrm{Sh}_{\boldsymbol{G}}(\mathrm{U})(\mathbb{C}), \mathcal{V}^\lambda_{\mathbb{R}}(3))^{\mathrm{F}^*_\infty=1},$$

where F^*_∞ denotes the composition of the map induced by complex conjugation on the $\mathbb{C}$-points of $\mathrm{Sh}_{\boldsymbol{G}}(U)$ with complex conjugation on the coefficients.

3.4.3. *Absolute Hodge realizations.* Let $H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))^0 = \ker(\mathrm{cl}_B)$ denote the subgroup of homologically trivial classes and let $H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))_{\text{hom}}$ denote the quotient

$$H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))/H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))^0.$$

Note that when $\lambda_2 = \lambda_3 = 0$, i.e., the representation V^λ is the trivial representation, then

$$H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3)) = H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), F(3)) = \mathrm{CH}^3(\mathrm{Sh}_{\boldsymbol{G}}(U))_F$$

is the usual Chow group of 3-codimensional cycles modulo rational equivalence and the space

$$H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))_{\text{hom}} = \mathrm{N}^3(\mathrm{Sh}_{\boldsymbol{G}}(U))_F$$

is the space of 3-codimensional cycles modulo homological equivalence, with coefficients in F. In this section, we define a natural injective map

$$H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))_{\text{hom}} \to H^7_{\mathcal{H}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^\lambda_{\mathbb{R}}(4)). \tag{7}$$

The definition is similar to the one for smooth projective varieties (see [Schneider 1988, §5]) and we recall it for the convenience of the reader. The cycle class map is an injection

$$\mathrm{cl}_B : H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))_{\text{hom}} \to H^6_B(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_F(3))^{F^*_\infty=1} \cap H^6_B(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^\lambda_{\mathbb{C}}(3))^{0,0},$$

where $H^6_B(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^\lambda_{\mathbb{C}}(3))^{0,0}$ denotes the subspace of

$$W_0 H^6_B(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^\lambda_{\mathbb{C}}(3)) = \mathrm{Gr}^W_0 H^6_B(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^\lambda_{\mathbb{C}}(3))$$

of vectors which have Hodge type $(0, 0)$. The composite of the inclusions

$$\begin{aligned}&H_B^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_F(3))^{F_\infty^*=1} \cap H_B^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{C}}^{\lambda}(3))^{0,0}\\ &\qquad\hookrightarrow W_0H^6_{\mathrm{dR}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(3)) \hookrightarrow W_2H^6_{\mathrm{dR}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(3)) = W_0H^6_{\mathrm{dR}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))\end{aligned}$$

and of the projection

$$\begin{aligned}&W_0H^6_{\mathrm{dR}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))\\ &\qquad\to W_0H^6_B(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))^+\backslash W_0H^6_{\mathrm{dR}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))/F^0W_0H^6_{\mathrm{dR}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))\end{aligned}$$

is injective. As the last space above is canonically isomorphic to

$$\mathrm{Ext}^1_{\mathrm{MHS}^+_{\mathbb{R}}}(\mathbb{R}(0), H_B^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))),$$

we obtain a natural injective map

$$H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^{\lambda}_F(3))_{\mathrm{hom}} \to \mathrm{Ext}^1_{\mathrm{MHS}^+_{\mathbb{R}}}(\mathbb{R}(0), H_B^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))).$$

Composing this map with the canonical injection

$$\mathrm{Ext}^1_{\mathrm{MHS}^+_{\mathbb{R}}}(\mathbb{R}(0), H_B^6(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))) \to H^7_{\mathcal{H}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^{\lambda}_{\mathbb{R}}(4))$$

we obtain the map (7). We denote by $\overline{\mathrm{cl}}_{\mathcal{H}} : H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^{\lambda}_F(3)) \to H^7_{\mathcal{H}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^{\lambda}_{\mathbb{R}}(4))$ the composition of the map (7) with the projection $H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^{\lambda}_F(3)) \to H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^{\lambda}_F(3))_{\mathrm{hom}}$.

Definition 3.11. We define

$$\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}} := \overline{\mathrm{cl}}_{\mathcal{H}}(\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{M}}) \in H^7_{\mathcal{H}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^{\lambda}_{\mathbb{R}}(4)).$$

Remark 3.12. Let π be a cuspidal automorphic representation of $\mathrm{PGSp}_6(\mathbb{A})$ which satisfies the hypotheses of Lemma 2.11 and let S be a finite set of places containing the ramified places of π_f and ∞. By the conjectures of Beilinson and Tate and the local calculations of Gross and Savin [1998], there should exist a cubic étale algebra $E/\mathbb{Q}$ such that the cycle $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}$, with $\boldsymbol{H}$ defined by $E/\mathbb{Q}$, and their Hecke translates are expected to generate $H^1_{\mathcal{H}}(M(\pi_f)_{\mathbb{R}}(4))$ when $\mathrm{ord}_{s=1}L^S(s, \pi, \mathrm{Spin}) = -1$. Assuming the nonvanishing of the archimedean integral, Corollary 5.15 confirms this expectation.

4. Construction of the differential form and pairing with the motivic class

The purpose of this section is to study the Betti and Hodge realizations of the cycle constructed in Section 3.3 by relating their pairing with a suitable cuspidal harmonic differential form to an automorphic period.

4.1. ***Test vectors.*** Recall that the discrete series L-packets for $\mathrm{PGSp}_6(\mathbb{R})$ have four elements, each indexed by a Hodge type (and its conjugate). Let π denote a cuspidal automorphic representation of $\mathrm{PGSp}_6(\mathbb{A})$ for which π_∞ is the discrete series of Hodge type (3,3) in the L-packet of V^λ, where $\lambda = (\lambda_1, \lambda_2, \lambda_3, 0)$

and $\lambda_1 = \lambda_2 + \lambda_3$. This translates into saying that π is a cuspidal automorphic representation of $\boldsymbol{G}(\mathbb{A})$ with trivial central character for which

$$H^6(\mathfrak{g}, K_{\boldsymbol{G}}; \pi_\infty \otimes V^\lambda) \neq 0,$$

and such that $\pi_\infty|_{\boldsymbol{G}_0(\mathbb{R})} = \pi^{3,3}_{\infty,1} \oplus \bar{\pi}^{3,3}_{\infty,1}$ is the direct sum of the discrete series representations of respective Harish-Chandra parameters $(\lambda_2+2, \lambda_3+1, -\lambda_1-3)$ and $(\lambda_1+3, -\lambda_3-1, -\lambda_2-2)$. Recall that these discrete series contain with multiplicity one their minimal K_∞-types $\tau_{(\lambda_2+2,\lambda_3+2,-\lambda_1-4)}$ and $\tau_{(\lambda_1+4,-\lambda_3-2,-\lambda_2-2)}$ respectively. On the other hand, as K_∞-representations we have

$$\textstyle\bigwedge^6 \mathfrak{p}_{\mathbb{C}} \supseteq \bigwedge^3 \mathfrak{p}^+_{\mathbb{C}} \otimes \bigwedge^3 \mathfrak{p}^-_{\mathbb{C}} = \displaystyle\bigoplus_i \tau_i \supseteq \tau_{(2,2,-4)} \oplus \tau_{(4,-2,-2)},$$

where the equality expresses the decomposition of the tensor product into irreducible K_∞-representations. This fact will be useful to construct an element in

$$H^6(\mathfrak{g}, K_{\boldsymbol{G}}; \pi_\infty \otimes V^\lambda) = \mathrm{Hom}_{K_\infty}\big(\textstyle\bigwedge^6 \mathfrak{p}_{\mathbb{C}}, \pi_\infty \otimes V^\lambda\big) \simeq \mathrm{Hom}_{K_\infty}\big(\textstyle\bigwedge^6 \mathfrak{p}_{\mathbb{C}} \otimes V^\lambda, \pi_\infty\big),$$

where the last equality follows from the fact that V^λ is self-dual. Before stating the next result, let us fix the following data:

- A highest weight vector Ψ_∞ of the minimal K_∞-type $\tau_{(\lambda_2+2,\lambda_3+2,-\lambda_1-4)}$ of $\pi^{3,3}_{\infty,1}$.
- A highest weight vector $\overline{\Psi}_\infty$ of the minimal K_∞-type $\tau_{(\lambda_1+4,-\lambda_3-2,-\lambda_2-2)}$ of $\bar{\pi}^{3,3}_{\infty,1}$.
- A highest weight vector $X_{(2,2,-4)}$ of $\tau_{(2,2,-4)}$.
- A highest weight vector $X_{(4,-2,-2)}$ of $\tau_{(4,-2,-2)}$.
- A highest weight vector $v^{\lambda'}$ of $\tau_{\lambda'} \subseteq V^\lambda$, where $\tau_{\lambda'}$ denotes the irreducible algebraic K_∞-representations of highest weight $\lambda' = (\lambda_2, \lambda_3, -\lambda_1)$.
- A highest weight vector $v^{\bar{\lambda}'}$ of $\tau_{\bar{\lambda}'} \subseteq V^\lambda$, where $\tau_{\bar{\lambda}'}$ denotes the irreducible algebraic K_∞-representations of highest weight $\bar{\lambda}' = (\lambda_1, -\lambda_3, -\lambda_2)$.

Lemma 4.1. *The spaces* $\mathrm{Hom}_{K_\infty}\big(\bigwedge^6 \mathfrak{p}_{\mathbb{C}} \otimes V^\lambda, \pi^{3,3}_{\infty,1}\big)$ *and* $\mathrm{Hom}_{K_\infty}\big(\bigwedge^6 \mathfrak{p}_{\mathbb{C}} \otimes V^\lambda, \bar{\pi}^{3,3}_{\infty,1}\big)$ *are of dimension 1 and the elements*

$$\omega_{\Psi_\infty} \in \mathrm{Hom}_{K_\infty}\big(\textstyle\bigwedge^6 \mathfrak{p}_{\mathbb{C}} \otimes V^\lambda, \pi^{3,3}_{\infty,1}\big), \quad \omega_{\overline{\Psi}_\infty} \in \mathrm{Hom}_{K_\infty}\big(\textstyle\bigwedge^6 \mathfrak{p}_{\mathbb{C}} \otimes V^\lambda, \bar{\pi}^{3,3}_{\infty,1}\big)$$

defined by

$$\omega_{\Psi_\infty}(X_{(2,2,-4)} \otimes v^{\lambda'}) = \Psi_\infty, \quad \omega_{\overline{\Psi}_\infty}(X_{(4,-2,-2)} \otimes v^{\bar{\lambda}'}) = \overline{\Psi}_\infty$$

are generators of these spaces.

Proof. This is a consequence of [Borel and Wallach 1980, Theorem II.5.3 b)] and its proof. □

4.2. ***Restriction to H.*** Let $\lambda = (\lambda_1, \lambda_2, \lambda_3, 0)$, with $\lambda_1 = \lambda_2 + \lambda_3$ and let V^λ be as above. Let $\mathfrak{h}$ denote the Lie algebra of $\boldsymbol{H}(\mathbb{R})$ and $\mathfrak{k}_{\boldsymbol{H}}$ the maximal compact modulo the center $K_{\boldsymbol{H}}$. Observe that via the embedding $\iota : \boldsymbol{H}(\mathbb{R}) \hookrightarrow \boldsymbol{G}(\mathbb{R})$, the group $K_{\boldsymbol{H}}$ is isomorphic to T_∞. One has a Cartan decomposition $\mathfrak{h}_{\mathbb{C}} = \mathfrak{k}_{\boldsymbol{H},\mathbb{C}} \oplus \mathfrak{p}_{\boldsymbol{H},\mathbb{C}}$, where $\mathfrak{p}_{\boldsymbol{H},\mathbb{C}}$ is six-dimensional and is spanned by the noncompact root spaces. We fix once and for all a generator X_0 of the one-dimensional $\mathbb{C}$-vector space $\bigwedge^6 \mathfrak{p}_{\boldsymbol{H},\mathbb{C}} \subseteq \bigwedge^6 \mathfrak{p}_{\mathbb{C}}$ as in [Burgos Gil et al. 2024, §5.2]. The main result of this section is the following.

Theorem 4.2. *Let ω_{Ψ_∞} and $\omega_{\overline{\Psi}_\infty}$ be the elements of $\mathrm{Hom}_{K_\infty}\big(\bigwedge^6 \mathfrak{p}_{\mathbb{C}} \otimes V^\lambda, \pi_\infty\big)$ defined in Lemma 4.1. Let X_0 be as above and let v be any $\boldsymbol{H}$-invariant vector in V^λ. Then*

$$\omega_{\Psi_\infty}(X_0 \otimes v) \neq 0, \quad \omega_{\overline{\Psi}_\infty}(X_0 \otimes v) \neq 0.$$

The proof of Theorem 4.2 will be constructive and occupies the rest of this section. We start by recalling the following result.

Lemma 4.3 [Burgos Gil et al. 2024, Lemma 5.4]. *Let X_0 be as above. Then the image of X_0 by*

$$\textstyle\bigwedge^6 \mathfrak{p}_{\boldsymbol{H},\mathbb{C}} \to \bigwedge^6 \mathfrak{p}_{\mathbb{C}} \to \bigwedge^3 \mathfrak{p}^+_{\mathbb{C}} \otimes \bigwedge^3 \mathfrak{p}^-_{\mathbb{C}} \to \tau_{(2,2,-4)},$$

where the first map is induced by the embedding $\boldsymbol{H} \to \boldsymbol{G}$ and the second and the third maps are the natural projections, is nonzero.

We next study the interaction between the branching laws of V^λ to the subgroup $\boldsymbol{H}$ of $\boldsymbol{G}$ and to its maximal compact subgroup. More precisely, we show that the $\boldsymbol{H}$-invariant vectors constructed in Lemma 3.4 project nontrivially to $\tau_{\lambda'}$ and $\tau_{\overline{\lambda}'}$ and moreover that their projections form a basis of the corresponding $(0, 0, 0)$-weight spaces for the action of T_∞.

Lemma 4.4. *Let $\tau_{\lambda'}$ and $\tau_{\overline{\lambda}'}$ be the irreducible algebraic sub-K_∞-representations of V^λ of highest weight $\lambda' = (\lambda_2, \lambda_3, -\lambda_1)$ and $\overline{\lambda}' = (\lambda_1, -\lambda_3, -\lambda_2)$. Then the weight $(0, 0, 0)$ appears in both $\tau_{\lambda'}$ and $\tau_{\overline{\lambda}'}$ with multiplicity $\lambda_2 - \lambda_3 + 1$.*

Proof. Let $n_0(\lambda')$ denote the multiplicity of the weight $(0, 0, 0)$ in $\tau_{\lambda'}$. The Kostant multiplicity formula reads as

$$n_0(\lambda') = \sum_{w \in \mathfrak{W}_{K_\infty}} (-1)^{\ell(w)} P(w(\lambda' + \rho_{K_\infty}) - \rho_{K_\infty}),$$

where $\rho_{K_\infty} = \frac{1}{2}\sum_{\alpha \in \Delta_c^+} \alpha = (1, 0, -1)$ and the function $\mu \mapsto P(\mu)$ calculates the number of ways for which the weight μ can be expressed as a linear combination

$$\alpha(e_1 - e_2) + \beta(e_1 - e_3) + \gamma(e_2 - e_3),$$

with $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}$ (see [Fulton and Harris 1991]). Using this formula, it is a tedious but straightforward calculation to verify that $n_0(\lambda') = \lambda_2 - \lambda_3 + 1$ and the same for $\overline{\lambda}' = w_8 \lambda'$. □

According to Lemma 4.4, there are $\lambda_2 - \lambda_3 + 1$ linearly independent vectors of weight $(0, 0, 0)$ in $\tau_{\lambda'}$. We now show that these weight vectors correspond one to one to the $\boldsymbol{H}$-invariant vectors of Lemma 3.2.

Lemma 4.5. *Let v, w be the vectors of $V^{(1,1,0)}$ and let z be the vector of $V^{(2,1,1)}$ defined in Lemma 3.3. The irreducible algebraic representation $\tau_{(1,0,-1)}$ (resp. $\tau_{(1,1,-2)}$ and $\tau_{(2,-1,-1)}$) appear in the restriction* *of $V^{(1,1,0)}$ (resp. of $V^{(1,1,1)}$) to K_∞ with multiplicity* 1. *Moreover, we have $v, w \in \tau_{(1,0,-1)} \subseteq V^{(1,1,0)}$, and $z \in \tau_{(1,1,-2)} \oplus \tau_{(2,-1,-1)} \subseteq V^{(1,1,1)}$, with z projecting nontrivially to each factor of this decomposition.*

Proof. First observe that $v, w \in V^{(1,1,0)}$ and $z \in V^{(2,1,1)}$ are vectors of weight $(0,0,0)$ both for the split and the compact tori of $\boldsymbol{G}_0(\mathbb{R})$. Indeed these vectors are fixed (up to a constant) by the matrix J sending the noncompact torus $\boldsymbol{T}_0$ to the compact torus T_∞ defined in Section 2.2. Using branching laws from $\boldsymbol{G}_0(\mathbb{R})$ to K_∞, we have a decomposition of K_∞-representations

$$V^{(1,1,0)} = \tau_{(1,1,0)} \oplus \tau_{(1,0,-1)} \oplus \tau_{(0,-1,-1)}.$$

The weight $(0,0,0)$ appears only in $\tau_{(1,0,-1)}$ and with multiplicity 2. Since it has also multiplicity 2 in $V^{(1,1,0)}$, we deduce that $\{v, w\}$ forms a basis for the $(0,0,0)$-eigenspace of $\tau_{(1,0,-1)}$. On the other hand, we have

$$V^{(2,1,1)} = \tau_{(-1,-1,-2)} \oplus \tau_{(1,-1,-2)} \oplus \tau_{(1,1,0)} \oplus \tau_{(1,1,-2)} \oplus \tau_{(1,0,-1)} \oplus \tau_{(2,-1,-1)} \oplus \tau_{(2,1,-1)} \oplus \tau_{(2,1,1)} \oplus \tau_{(0,-1,-1)}.$$

The weight $(0,0,0)$ only appears in $\tau_{(1,1,-2)} \oplus \tau_{(1,0,-1)} \oplus \tau_{(2,-1,-1)}$, which implies that

$$z \in \tau_{(1,1,-2)} \oplus \tau_{(1,0,-1)} \oplus \tau_{(2,-1,-1)}.$$

Notice that the decomposition of the standard representation of $\boldsymbol{G}_0$

$$V = \tau_{(1,0,0)} \oplus \tau_{(0,0,-1)}$$

of K_∞-representations can be realized by picking the basis $\{v_1, v_2, v_3, w_1, w_2, w_3\}$, where $v_r := e_r + i f_r$ and $w_r := i e_r + f_r$. The set $\{v_r\}_{1 \le r \le 3}$ (resp. $\{w_r\}_{1 \le r \le 3}$) defines a basis for $\tau_{(1,0,0)}$ (resp. $\tau_{(0,0,-1)}$). We now write z in terms of this basis. By using the relations

$$e_r = \tfrac{1}{2} v_r - \tfrac{i}{2} w_r, \quad f_r = \tfrac{1}{2} w_r - \tfrac{i}{2} v_r,$$

we have that

$$e_1 \otimes f_1 \wedge (e_2 \wedge f_2 - e_3 \wedge f_3) - f_1 \otimes e_1 \wedge (e_2 \wedge f_2 - e_3 \wedge f_3)$$

is equal to

$$\tfrac{1}{4}\big(v_1 \otimes w_1 \wedge (v_2 \wedge w_2 - v_3 \wedge w_3) - w_1 \otimes v_1 \wedge (v_2 \wedge w_2 - v_3 \wedge w_3)\big).$$

Thus,

$$z = z_1 - z_2 = \tfrac{1}{4}\big(v_1 \cdot w_1 \wedge (v_2 \wedge w_2 - v_3 \wedge w_3) - w_1 \cdot v_1 \wedge (v_2 \wedge w_2 - v_3 \wedge w_3)\big).$$

Notice that the vector $w_1 \wedge (v_2 \wedge w_2 - v_3 \wedge w_3) \in V^{(1,1,1)}$ is of weight $(-1,0,0)$ for T_∞, while $v_1 \wedge (v_2 \wedge w_2 - v_3 \wedge w_3) \in V^{(1,1,1)}$ is of weight $(1,0,0)$ for T_∞. As

$$V^{(1,1,1)} = \tau_{(1,1,1)} \oplus \tau_{(1,-1,-1)} \oplus \tau_{(1,1,-1)} \oplus \tau_{(-1,-1,-1)},$$

and as the weight $(-1,0,0)$ appears only in $\tau_{(1,-1,-1)}$ and $(1,0,0)$ only in $\tau_{(1,1,-1)}$, we have that

$$w_1 \wedge (v_2 \wedge w_2 - v_3 \wedge w_3) \in \tau_{(1,-1,-1)}, \quad v_1 \wedge (v_2 \wedge w_2 - v_3 \wedge w_3) \in \tau_{(1,1,-1)}.$$

By the properties of the Cartan product, the vector $s_1 := v_1 \cdot w_1 \wedge (v_2 \wedge w_2 - v_3 \wedge w_3)$ is nonzero in $\tau_{(2,-1,-1)}$, while $s_2 := w_1 \cdot v_1 \wedge (v_2 \wedge w_2 - v_3 \wedge w_3)$ is nonzero in $\tau_{(1,1,-2)}$. This shows that the vector $z \in V^{(2,1,1)}$ lives in $\tau_{(2,-1,-1)} \oplus \tau_{(1,1,-2)}$, thus finishing the proof. □

Proposition 4.6. *The set* $\{\mathrm{pr}_{\tau_{\lambda'}}(v^{[\lambda,\mu]})\}_\mu$ *(resp.* $\{\mathrm{pr}_{\tau_{\bar{\lambda}'}}(v^{[\lambda,\mu]})\}_\mu$*) forms a basis of the weight* $(0,0,0)$*-eigenspace of* $\tau_{\lambda'} \subset V^\lambda$ *(resp.* $\tau_{\bar{\lambda}'} \subset V^\lambda$*).*

Proof. Recall that we have defined

$$v^{[\lambda,\mu]} := v^{\lambda_2-\mu} \cdot w^{\mu-\lambda_3} \cdot z^{\lambda_3} \in F(0) \subseteq (V^\lambda)_{|\boldsymbol{H}}.$$

By Lemma 4.5, we have that $v, w \in \tau_{(1,0,-1)} \subseteq V^{(1,1,0)}$ so that, for any $\lambda_3 \le \mu \le \lambda_2$, we have $v^{\lambda_2-\mu} \otimes w^{\mu-\lambda_3} \in \tau_{(1,0,-1)}^{\otimes\lambda_2-\lambda_3}$ and we deduce that the projection of $v^{\lambda_2-\mu} \cdot w^{\mu-\lambda_3} \in V^{(\lambda_2-\lambda_3,\lambda_2-\lambda_3,0)}$ to $\tau_{(\lambda_2-\lambda_3,0,\lambda_3-\lambda_2)}$ coincides with their Cartan product with respect to K_∞. Moreover, each of these projections is nonzero because of Lemma 3.1. Since the vectors

$$v^{\lambda_2-\mu} \cdot w^{\mu-\lambda_3} \in \tau_{(\lambda_2-\lambda_3,0,\lambda_3-\lambda_2)}$$

are all different as they live in different $\boldsymbol{H}_0'$ subrepresentations (see the proof of Lemma 3.4), we conclude that they span the $\lambda_2 - \lambda_3 + 1$-dimensional weight $(0,0,0)$-eigenspace of $\tau_{(\lambda_2-\lambda_3,0,\lambda_3-\lambda_2)}$. We now show that z^{λ_3} projects nontrivially to both $\tau_{(2\lambda_3,-\lambda_3,-\lambda_3)}$ and $\tau_{(\lambda_3,\lambda_3,-2\lambda_3)}$. Notice that, as the weights $(2\lambda_3,-\lambda_3,-\lambda_3)$ and $(\lambda_3,\lambda_3,-2\lambda_3)$ are extremal in $V^{(2\lambda_3,\lambda_3,\lambda_3)}$ and appear uniquely, we have a commutative diagram

$$\begin{tikzcd}
(V^{(2,1,1)})^{\otimes\lambda_3} \arrow[r, two heads, "\cdot"] \arrow[d, two heads, "{(\mathrm{pr}_1,\mathrm{pr}_1')}"'] & V^{(2\lambda_3,\lambda_3,\lambda_3)} \arrow[d, two heads, "\mathrm{pr}_2"] \\
(\tau_{(2,-1,-1)})^{\otimes\lambda_3} \oplus (\tau_{(1,1,-2)})^{\otimes\lambda_3} \arrow[r, two heads, "\cdot"] & \tau_{(2\lambda_3,-\lambda_3,-\lambda_3)} \oplus \tau_{(\lambda_3,\lambda_3,-2\lambda_3)}
\end{tikzcd}$$

where the horizontal arrows are the Cartan projections and the vertical arrows are the natural projections given by the decomposition of $V^{(2r,r,r)}$ as K_∞-representations. Thanks to the commutativity of the diagram, we know that the vector $z^{\otimes\lambda_3} \in (V^{(2,1,1)})^{\otimes\lambda_3}$ maps to

$$\mathrm{pr}_2(z^{\lambda_3}) = \mathrm{pr}_1(z)^{\lambda_3} + \mathrm{pr}_1'(z)^{\lambda_3} = s_1^{\lambda_3} + s_2^{\lambda_3},$$

where s_1, s_2 are as in Lemma 4.5. This shows, again by Lemma 3.1, that each $v^{[\lambda,\mu]}$ projects nontrivially to both $\tau_{\lambda'}$ and $\tau_{\bar{\lambda}'}$ and that each of these projections are different by Lemma 3.4. Indeed,

$$\mathrm{pr}_{\tau_{\lambda'}}(v^{[\lambda,\mu]}) = v^{\lambda_2-\mu} \cdot w^{\mu-\lambda_3} \cdot s_1^{\lambda_3}, \quad \mathrm{pr}_{\tau_{\bar{\lambda}'}}(v^{[\lambda,\mu]}) = v^{\lambda_2-\mu} \cdot w^{\mu-\lambda_3} \cdot s_2^{\lambda_3}.$$

By Lemma 4.4, this means that $\{\mathrm{pr}_{\tau_{\lambda'}}(v^{[\lambda,\mu]})\}_\mu$ (resp. $\{\mathrm{pr}_{\tau_{\bar{\lambda}'}}(v^{[\lambda,\mu]})\}_\mu$) defines a basis of the weight $(0,0,0)$-eigenspace of $\tau_{\lambda'}$ (resp. $\tau_{\bar{\lambda}'}$). This finishes the proof. □

We can now conclude the proof of Theorem 4.2

Proof of Theorem 4.2. By construction, the map ω_{Ψ_∞} factors through $\tau_{\lambda'+(2,2,-4)} \subseteq \tau_{(2,2,-4)} \otimes \tau_{\lambda'}$. Lemma 4.3 shows that the projection of X_0 to $\tau_{(2,2,-4)}$ is nonzero, while Proposition 4.6 shows that $\mathrm{pr}_{\tau_{\lambda'}}(v^{[\lambda,\mu]})$ is nonzero. Since $\tau_{\lambda'+(2,2,-4)}$ is the Cartan product of $\tau_{(2,2,-4)}$ and $\tau_{\lambda'}$, we deduce from Lemma 3.1 that the image of the pure tensor $\mathrm{pr}_{\tau_{(2,2,-4)}}(X_0) \otimes \mathrm{pr}_{\tau_{\lambda'}}(v^{[\lambda,\mu]})$ is nonzero. □

4.3. ***The pairing.*** Let π denote a cuspidal automorphic representation of $\mathrm{PGSp}_6(\mathbb{A})$ for which π_∞ is the discrete series of Hodge type (3,3) in the L-packet of V^λ with $\lambda = (\lambda_2+\lambda_3, \lambda_2, \lambda_3, 0)$. Let $\Psi = \Psi_\infty \otimes \Psi_f$ denote a cusp form in $\pi = \pi_\infty \otimes \pi_f$. We assume that Ψ_∞ is a highest weight vector of the minimal K_∞-type $\tau_{(\lambda_2+2,\lambda_3+2,-\lambda_1-4)}$ of $\pi_\infty|_{\boldsymbol{G}_0(\mathbb{R})}$. We let $[\omega_{\Psi_\infty}] \in H^6(\mathfrak{g}, K_{\boldsymbol{G}}; \pi_\infty \otimes V^\lambda)$ be the cohomology class of the harmonic differential form ω_{Ψ_∞} defined in Lemma 4.1. We also assume that $\Psi_f \in V_{\pi_f}$ is U-invariant. Then we have $[\omega_\Psi] := [\omega_{\Psi_\infty} \otimes \Psi_f] \in H^6(\mathfrak{g}, K_{\boldsymbol{G}}; \pi^U \otimes V^\lambda)$.

Lemma 4.7. *There is a Hecke-equivariant inclusion*

$$H^6(\mathfrak{g}, K_{\boldsymbol{G}}; \pi^U \otimes V^\lambda) \subset H^6_{\mathrm{dR},c}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^\lambda_{\mathbb{C}}).$$

Moreover, if π_w is the Steinberg representation for some finite place w, such an inclusion is unique.

Proof. Let $\mathcal{C}^\infty_{\mathrm{rd}}(\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A})/U, V^\lambda)$ denote the space of V^λ-valued $\mathcal{C}^\infty$-functions on the double quotient $\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A})/U$ which, together with all their right $\mathfrak{U}(\mathfrak{g}_{\mathbb{C}})$-derivatives, are rapidly decreasing in the sense of [Harris 1990]. As π is cuspidal and cusp forms are rapidly decreasing, we have $H^6(\mathfrak{g}, K_{\boldsymbol{G}}; \pi_\infty \otimes V^\lambda_{\mathbb{C}})^{m(\pi)} \otimes \pi_f^U \subset H^6(\mathfrak{g}, K_{\boldsymbol{G}}; \mathcal{C}^\infty_{\mathrm{rd}}(\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A})/U, V^\lambda))$. Thus the result follows from the fact that, according to [Borel 1981, Theorem 5.2] (see also [Harris 1990, Theorem 1.4.1]), there exists a canonical Hecke equivariant isomorphism $H^6_{\mathrm{dR},c}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^\lambda) \simeq H^6(\mathfrak{g}, K_{\boldsymbol{G}}; \mathcal{C}^\infty_{\mathrm{rd}}(\boldsymbol{G}(\mathbb{Q})\backslash\boldsymbol{G}(\mathbb{A})/U, V^\lambda))$. Finally, if π_w is Steinberg at a finite place w, we have, as in Lemma 2.8, that $m(\pi) = 1$. □

4.3.1. *The pairing in Betti cohomology.* Poincaré duality is a perfect pairing

$$\langle\ ,\ \rangle : H^6_B(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^\lambda_F(3)) \times H^6_{B,c}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^\lambda_F) \to F(-3),$$

which is a morphism of mixed F-Hodge structures. Fix the choice of a measure dh on $\boldsymbol{H}(\mathbb{A})$ as follows. For each finite place p, we take the Haar measure dh_p on $\boldsymbol{H}(\mathbb{Q}_p)$ that assigns volume 1 to $\boldsymbol{H}(\mathbb{Z}_p)$. For the archimedean place, we let $X_0 \in \bigwedge^6 \mathfrak{p}_{\boldsymbol{H},\mathbb{C}}$ be the generator fixed at the beginning of Section 4.2. The choice of X_0 induces an equivalence between top differential forms on $X_{\boldsymbol{H}} = \boldsymbol{H}(\mathbb{R})/K_{\boldsymbol{H},\infty}$ and invariant measures dh_∞ on $\boldsymbol{H}(\mathbb{R})$ assigning measure one to $K_{\boldsymbol{H},\infty}$ (see [Harris 1997, p. 83] for details). We let dh_∞ denote the measure associated in this way to the pullback of $\iota^{[\lambda,\mu]*}\omega_\Psi$ to $X_{\boldsymbol{H}}$ and we then define $dh = dh_\infty \prod_p dh_p$.

Proposition 4.8. *We have*

$$\langle \mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B}, [\omega_\Psi]\rangle = \frac{h_{U'}}{(2\pi i)^3 \cdot \mathrm{vol}(U')} \int_{\boldsymbol{H}(\mathbb{Q})\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A})\backslash\boldsymbol{H}(\mathbb{A})} A^{[\lambda,\mu]} \cdot \Psi(h)\, dh,$$

where $h_{U'} = 4^{-1}|\mathbb{Z}_{\boldsymbol{G}}(\mathbb{Q})\backslash\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A}_f)/(\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A}_f) \cap U')|$ and $A^{[\lambda,\mu]} \in U(\mathfrak{k}_{\mathbb{C}})$ is an element for which $A^{[\lambda,\mu]} \cdot \Psi_\infty = \omega_{\Psi_\infty}(X_0 \otimes v^{[\lambda,\mu]})$.

Proof. By [Borel 1981, Corollary 5.5], there exists a $\mathcal{V}^\lambda$-valued rapidly decreasing differential form η of degree five on $\mathrm{Sh}_{\boldsymbol{G}}(U)$ such that $\omega_c := \omega_\Psi + d\eta$ is compactly supported. We have

$$\begin{aligned}\langle \mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B}, [\omega_\Psi]\rangle &= \langle \mathrm{cl}_B(\iota^{[\lambda,\mu]}_* \mathbf{1}_{\mathrm{Sh}_{\boldsymbol{H}}(U')}), [\omega_c]\rangle \\ &= \langle \iota^{[\lambda,\mu]}_* \mathrm{cl}_B(\mathbf{1}_{\mathrm{Sh}_{\boldsymbol{H}}(U')}), [\omega_c]\rangle \\ &= \langle \mathrm{cl}_B(\mathbf{1}_{\mathrm{Sh}_{\boldsymbol{H}}(U')}), \iota^{[\lambda,\mu]*}[\omega_c]\rangle \\ &= \frac{1}{(2\pi i)^3}\int_{\mathrm{Sh}_{\boldsymbol{H}}(U')} \iota^{[\lambda,\mu]*}\omega_c,\end{aligned}$$

where $\iota^{[\lambda,\mu]*} : \iota^* V^\lambda \to F(0)$ is the $\boldsymbol{H}$-equivariant projection dual to the inclusion $\iota^{[\lambda,\mu]} : F(0) \to \iota^* V^\lambda$ defined by $1 \mapsto v^{[\lambda,\mu]} \in V^\lambda$, where $v^{[\lambda,\mu]}$ is the vector defined in Lemma 3.4. According to [Borel 1981, §5.6], we have

$$\int_{\mathrm{Sh}_{\boldsymbol{H}}(U')} \iota^{[\lambda,\mu]*}\, d\eta = 0.$$

Hence, using Theorem 4.2 we have

$$\begin{aligned}\langle \mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B}, [\omega_\Psi]\rangle &= \frac{1}{(2\pi i)^3}\int_{\mathrm{Sh}_{\boldsymbol{H}}(U')} \iota^{[\lambda,\mu]*}\omega_\Psi \\ &= \frac{1}{(2\pi i)^3}\int_{\mathrm{Sh}_{\boldsymbol{H}}(U')} \omega_\Psi(X_0 \otimes v^{[\lambda,\mu]})(h)\, dh \\ &= \frac{1}{(2\pi i)^3}\int_{\boldsymbol{H}(\mathbb{Q})\backslash \boldsymbol{H}(\mathbb{A})/\mathbb{Z}_{\boldsymbol{H}}(\mathbb{R})K_{\boldsymbol{H},\infty}U'} A^{[\lambda,\mu]} \cdot \Psi(h)\, dh \\ &= \frac{h_{U'}}{(2\pi i)^3}\int_{\boldsymbol{H}(\mathbb{Q})\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A})\backslash \boldsymbol{H}(\mathbb{A})/U'} A^{[\lambda,\mu]} \cdot \Psi(h)\, dh \\ &= \frac{h_{U'}}{(2\pi i)^3 \cdot \mathrm{vol}(U')}\int_{\boldsymbol{H}(\mathbb{Q})\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A})\backslash \boldsymbol{H}(\mathbb{A})} A^{[\lambda,\mu]} \cdot \Psi(h)\, dh,\end{aligned}$$

where the third equality follows from Theorem 4.2 as $\omega_{\Psi_\infty}(X_0 \otimes v^{[\lambda,\mu]})$ is nonzero and thus it is of the form $A^{[\lambda,\mu]} \cdot \Psi_\infty$, for some $A^{[\lambda,\mu]} \in U(\mathfrak{k}_\mathbb{C})$, because Ψ_∞ is the highest weight vector of the minimal K_∞-type $\tau_{(\lambda_2+2,\lambda_3+2,-\lambda_1-4)}$. Moreover, the fourth equality follows from the fact that Ψ is fixed by the center of $\boldsymbol{G}$, whence, using that $|\mathbb{Z}_{\boldsymbol{H}}(\mathbb{R})/(\mathbb{Z}_{\boldsymbol{G}} \cap \boldsymbol{H})(\mathbb{R})| = 4$, the constant $h_{U'}$ is equal to $4^{-1}|\mathbb{Z}_{\boldsymbol{G}}(\mathbb{Q})\backslash\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A}_f)/(\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A}_f) \cap U')|$. □

Remark 4.9. In view of Proposition 4.8, we immediately notice that if π is not $\boldsymbol{H}$-distinguished, namely

$$\int_{\boldsymbol{H}(\mathbb{Q})\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A})\backslash \boldsymbol{H}(\mathbb{A})} \varphi_\pi(h)\, dh = 0$$

for any cusp form φ_π in the space of π, we have that $\mathrm{pr}_{\pi^\vee}\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B} = 0$. As we discuss later in Section 8, the $\boldsymbol{H}$-distinguishability is related to the property of π being a (functorial) lift from G_2, which is (conjecturally) equivalent to the fact that the spin L-function of π has a pole at $s = 1$.

4.3.2. *The pairing in absolute Hodge cohomology.* Let

$$\langle\ ,\ \rangle_{\mathcal{H}} : H^7_{\mathcal{H}}(\mathrm{Sh}_{\boldsymbol{G}}(U)/\mathbb{R}, \mathcal{V}_{\mathbb{R}}(4)) \times H^6_{\mathcal{H},c}(\mathrm{Sh}_{\boldsymbol{G}}(U)/\mathbb{R}, \mathcal{V}_{\mathbb{R}}(3)) \to \mathbb{R}$$

be the natural pairing between absolute Hodge cohomology and compactly supported cohomology as constructed in [Beĭlinson 1986, §4.2]. In order to ease notation, we will denote by $H^*_{B,c}(i)$ and $H^*_B(i)$ the cohomology groups $H^*_{B,c}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_F(i))$ and $H^*_B(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_F(i))$, respectively. Recall from Section 2.9 that absolute Hodge cohomology and compactly supported cohomology live in exact sequences

$$0 \to \mathrm{Ext}^1_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^6_B(4)) \to H^7_{\mathcal{H}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4)) \to \mathrm{Hom}_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^7_B(4)) \to 0, \tag{8}$$

$$0 \to \mathrm{Ext}^1_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^5_{B,c}(3)) \to H^6_{\mathcal{H},c}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(3)) \to \mathrm{Hom}_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^6_{B,c}(3)) \to 0, \tag{9}$$

which are deduced from the description of absolute Hodge cohomology as a cone of a diagram of complexes of Hodge structures. Let $[\omega_\Psi] \in H^6_{B,c}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}^\lambda_{\mathbb{R}}(3))$ be the compactly supported cohomology class of the harmonic differential form ω_Ψ. This class is of Hodge type (3, 3) and hence, since $W_0 H^6_{B,c}(3) = H^6_{B,c}(3)$, it naturally lives in the space $\mathrm{Hom}_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^6_{B,c}(3)) = W_0 H_{B,c}(3) \cap F^0 H_{B,c}(3)_{\mathbb{C}}$. Denote by $\widetilde{[\omega_\Psi]}$ any lift of $[\omega_\Psi]$ in $H^6_{\mathcal{H},c}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(3))$ via the surjection of the exact sequence (9).

Proposition 4.10. *The pairing $\langle \mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}, \widetilde{[\omega_\Psi]}\rangle_{\mathcal{H}}$ depends only on $[\omega_\Psi]$ and not on the choice of lift. We denote this value by $\langle \mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}, [\omega_\Psi]\rangle_{\mathcal{H}}$. Moreover, the pairing is given by the natural Poincaré duality pairing. In particular, we have*

$$\langle \mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}, [\omega_\Psi]\rangle_{\mathcal{H}} = \frac{h_{U'}}{(2\pi i)^3 \cdot \mathrm{vol}(U')} \int_{\boldsymbol{H}(\mathbb{Q})\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A})\backslash \boldsymbol{H}(\mathbb{A})} A^{[\lambda,\mu]} \cdot \Psi(h)\, dh.$$

Proof. We give a sketch of the proof and we refer to [Beĭlinson 1986] or to [Burgos Gil et al. 2007, §5.1] for the facts used here. It follows from the description of the pairing between absolute Hodge cohomology and compactly supported cohomology given in [Beĭlinson 1986, §4.2] that, since our cycle class $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}$ lives in the subspace $\mathrm{Ext}^1_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^6_B(4))$ of $H^7_{\mathcal{H}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(4))$, the map

$$\langle [\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}], -\rangle : H^6_{\mathcal{H},c}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathcal{V}_{\mathbb{R}}(3)) \to \mathbb{R}$$

factors through $\mathrm{Hom}_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^6_{B,c}(3))$ and coincides with the natural Poincaré duality pairing

$$\begin{aligned}\mathrm{Ext}^1_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^6_B(4)) \otimes \mathrm{Hom}_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^6_{B,c}(3)) &\longrightarrow \mathrm{Ext}^1_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^6_B(4) \otimes H^6_{B,c}(3))\\ &\xrightarrow{\cup} \mathrm{Ext}^1_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), H^{12}_{B,c}(7))\\ &\xrightarrow{\mathrm{Tr}} \mathrm{Ext}^1_{\mathrm{MHS}_{\mathbb{R}}}(\mathbb{R}(0), \mathbb{R}(1)) = \mathbb{R}.\end{aligned}$$

This shows the first two assertions. The last formula follows from Proposition 4.8. □

5. Integral representation and residue of the spin L-function

In this section, using the result of [Pollack and Shah 2018], we explain the precise connection between the period integral appearing in the statement of Proposition 4.8 and the residue of the spin L-function of π in the case where the cubic totally real étale algebra E over $\mathbb{Q}$ defining $\boldsymbol{H}$ is of the form $\mathbb{Q}\times F$, with F a quadratic real étale algebra over $\mathbb{Q}$. We start by recalling well-known analytic properties of some Eisenstein series for GL_2.

5.1. ***Eisenstein series for*** $\mathbf{GL_2}$**.** Let $\boldsymbol{T}_2$ denote the maximal diagonal torus of GL_2 and let $\boldsymbol{B}_2=\boldsymbol{T}_2\boldsymbol{U}_2$ denote the standard Borel. We denote by δ the character of $\boldsymbol{T}_2$ defined by $\mathrm{diag}(t_1,t_2)\mapsto t_1/t_2$ and we regard δ as a character of $\boldsymbol{B}_2$ by extending it trivially to the unipotent radical. Let $\Phi\in\mathcal{S}(\mathbb{A}^2)$ be a Schwartz–Bruhat function. Following Jacquet, for any $s\in\mathbb{C}$, we attach to Φ the function $f_\Phi\in\mathrm{Ind}_{\boldsymbol{B}_2(\mathbb{A})}^{\mathrm{GL}_2(\mathbb{A})}\delta^s$ defined by

$$f_\Phi(h,s)=|\det(h)|^s\int_{\mathbb{A}^\times}\Phi((0,t)h)|t|^{2s}\,d^\times t$$

and the Eisenstein series

$$E_\Phi(h,s)=\sum_{\gamma\in\boldsymbol{B}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{Q})}f_\Phi(\gamma h,s).$$

In the statement of the following lemma, we denote by $\widehat{\Phi}(0)=\int_{\mathbb{A}^2}\Phi(x,y)\,dx\,dy$ the value at 0 of the Fourier transform of Φ.

Lemma 5.1. (1) *The Eisenstein series $E_\Phi(h,s)$ is absolutely convergent for* $\mathrm{Re}(s)$ *big enough and has a meromorphic continuation to* $\mathbb{C}$.

(2) *We have*

$$E_\Phi(h,s)=\frac{|\det(h)|^{s-1}\widehat{\Phi}(0)}{2(s-1)}+R(h,s),$$

where $R(h,s)$ is an entire function in s for any $h\in\mathrm{GL}_2(\mathbb{A})$.

Proof. Statement (1) is [Jacquet 1972, Proposition 19.2]. According to [Jacquet and Shalika 1981, Lemma (4.2)] and its proof, we have

$$E_\Phi(h,s)=\frac{c|\det(h)|^{s-1}\widehat{\Phi}(0)}{s-1}+R(h,s),$$

where $R(h,s)$ is holomorphic for $\mathrm{Re}(s)>0$ and $c=(s-1)\int_{|t|\le 1}|t|^{2(s-1)}\,d^\times t$, the integral being over the set $\{t\in\mathbb{A}^\times/\mathbb{Q}^\times:|t|\le 1\}$. By Iwasawa–Tate we have $c=\frac{1}{2}$. □

5.2. ***Fourier coefficients.*** Here we discuss the definition and basic properties of some Fourier coefficients for cusp forms for $\boldsymbol{G}$, which appear in the integral representation of the spin L-function of [Pollack and Shah 2018].

5.2.1. *The Siegel parabolic.* We let $Q=L_3U_3$ denote the standard Siegel parabolic subgroup of $\boldsymbol{G}$, with Levi $L_3\simeq\mathrm{GL}_3\times\mathrm{GL}_1$. Explicitly,

$$L_3=\left\{m(g,\mu)=\begin{pmatrix} g & \\ & \mu\,{}^tg^{-1}\end{pmatrix}\mid g\in\mathrm{GL}_3,\ \mu\in\mathrm{GL}_1\right\},$$
$$U_3=\left\{n(u)=\begin{pmatrix} I_3 & u\\ & I_3\end{pmatrix},\ u\in M_3\mid u^t=u\right\}.$$

Denote $\mathrm{Sym}(3) = \{\alpha \in M_3 \mid \alpha^t = \alpha\}$. To each $\alpha \in \mathrm{Sym}(3)(\mathbb{Q})$, we associate the unitary character $\psi_\alpha : U_3(\mathbb{Q})\backslash U_3(\mathbb{A}) \to \mathbb{C}^\times$ by $n(u) \in U_3(\mathbb{A}) \mapsto e(\mathrm{Tr}(\alpha u))$, where $e : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$ is the additive character with $e_\infty(x) := e^{2\pi i x}$ for $x \in \mathbb{R}$, and conductor 1 at the finite places. For each $\alpha \in \mathrm{Sym}(3)(\mathbb{Q})$, we define a Fourier coefficient along U_3 for a cuspidal automorphic representation π of $\boldsymbol{G}(\mathbb{A})$ as follows.

Definition 5.2. Let Ψ be a cusp form in the space of π. Define

$$\Psi_{U_3,\psi_\alpha}(g) := \int_{U_3(\mathbb{Q})\backslash U_3(\mathbb{A})} \psi_\alpha^{-1}(u)\Psi(ug)\,du.$$

We let $L_3(\mathbb{Q})$ acts on $\mathrm{Sym}(3)(\mathbb{Q})$ via the right action $\alpha \cdot m(g,\mu) = \mu^{-1} g^t \alpha g$.

Lemma 5.3. *Let $\alpha, \beta \in \mathrm{Sym}(3)(\mathbb{Q})$. If there exists $m \in L_3(\mathbb{Q})$ such that $\beta = \alpha \cdot m$, then*

$$\Psi_{U_3,\psi_\beta}(g) = \Psi_{U_3,\psi_\alpha}(mg).$$

Proof. Suppose that $\beta = \alpha \cdot m$ with $m = m(g,\mu)$. The result follows from the equality

$$\psi_\beta(n(u)) = e(\mathrm{Tr}(\mu^{-1} g^t \alpha g u)) = e(\mathrm{Tr}(\alpha g u \mu^{-1} g^t)) = \psi_\alpha(m n(u) m^{-1}). \qquad \square$$

In this manuscript, we are interested in Fourier coefficients associated to the set of rank-2 elements of $\mathrm{Sym}(3)(\mathbb{Q})$, which we denote by $\mathrm{Sym}^{\mathrm{rk2}}(3)(\mathbb{Q})$. Let $D \in \mathbb{Q}^\times$ and let F denote the étale quadratic extension $\mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$. If D is not a square then F is a field, else $F = \mathbb{Q} \times \mathbb{Q}$.

Definition 5.4. We let $\psi_D : U_3(\mathbb{Q})\backslash U_3(\mathbb{A}) \to \mathbb{C}^\times$ be the unitary character

$$\psi_D : n(u) \mapsto e(\mathrm{Tr}(\alpha_D u)) = e(u_{33} - D u_{22})$$

associated to $\alpha_D = \begin{pmatrix} 0 & & \\ & -D & \\ & & 1 \end{pmatrix} \in \mathrm{Sym}^{\mathrm{rk2}}(3)(\mathbb{Q})$.

Lemma 5.5. *A set of representatives of* $\mathrm{Sym}^{\mathrm{rk2}}(3)(\mathbb{Q})/_{\sim M_3(\mathbb{Q})}$ *is given by*

$$\{\alpha_D : D \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2\}.$$

In view of Lemmas 5.3 and 5.5, the set of Fourier coefficients associated to the Siegel parabolic and a rank-2 symmetric matrix is parametrized by the set of étale quadratic algebras of $\mathbb{Q}$.

5.2.2. *Fourier coefficients of type* (4 2). We now turn our attention to Fourier coefficients associated to the unipotent orbit of $\boldsymbol{G}$ associated to the partition (4 2). The corresponding unipotent subgroup is the unipotent radical subgroup of the nonmaximal standard parabolic $P = L_P \cdot U_P$, which arises as the intersection of the Siegel parabolic Q with the Klingen parabolic. Notice that P has Levi $L_P = \mathrm{GL}_2 \times \mathrm{GL}_1^2$, given by

$$\left\{ \begin{pmatrix} a & & & \\ & g & & \\ & & \mu a^{-1} & \\ & & & \mu\, {}^t g^{-1} \end{pmatrix} : a, \mu \in \mathrm{GL}_1,\ g \in \mathrm{GL}_2 \right\}.$$

Following [Pollack and Shah 2018, §2.1], we define a unitary character which we still denote

$$\psi_D : U_P(\mathbb{Q})\backslash U_P(\mathbb{A}) \to \mathbb{C}^\times$$

as follows. Every element of $U_P/[U_P, U_P]$ can be expressed as the product of $n(v)\tilde{n}(u)$, where

$$n(v) = \begin{pmatrix} 1 & v_1 & v_2 & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & -v_1 & 1 & \\ & & & -v_2 & & 1 \end{pmatrix} \in \boldsymbol{G}, \quad \tilde{n}(u) = \begin{pmatrix} 1 & & & & & \\ & 1 & & & u_{22} & u_{23} \\ & & 1 & & u_{23} & u_{33} \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix} \in U_3.$$

We will denote by N_v (resp. N_u) the set of the $n(v)$'s (resp. $\tilde{n}(u)$'s). If $n \equiv n(v)\tilde{n}(u)$ modulo $[U_P, U_P]$, define

$$\psi_D(n) := e(v_1 + u_{33} - Du_{22}) = e(v_1)\psi_D(n(u)).$$

Let π be a cuspidal automorphic representation of $\boldsymbol{G}(\mathbb{A})$. We define the following Fourier coefficients.

Definition 5.6. Let Ψ be a cusp form in the space of π. Define

$$\Psi_{U_P,\psi_D}(g) := \int_{U_P(\mathbb{Q})\backslash U_P(\mathbb{A})} \psi_D^{-1}(u)\Psi(ug)\,du.$$

In the following proposition, we relate these Fourier coefficients to the ones for the Siegel parabolic associated to rank-2 symmetric matrices.

Proposition 5.7. *For a cusp form Ψ in the space of π, the following two conditions are equivalent.*

(1) $\Psi_{U_P,\psi_D}(g) \not\equiv 0$.

(2) *There exists $\alpha \in \mathrm{Sym}^{\mathrm{rk}2}(3)(\mathbb{Q})$ with $\alpha \sim_{L(\mathbb{Q})} \alpha_D$ such that $\Psi_{U_3,\alpha}(g) \not\equiv 0$.*

Proof. Fourier expand $\Psi_{U_3,\psi_D}(g)$ over N_v to get

$$\Psi_{U_3,\psi_D}(g) = \int_{(\mathbb{Q}\backslash\mathbb{A})^2} \Psi_{U_3,\psi_D}(n(v)g)\,dv + \sum_{\gamma\in\mathrm{Stab}_L(\psi_D)(\mathbb{Q})\backslash L(\mathbb{Q})} \Psi_{U_P,\psi_D}(\gamma g).$$

The term

$$\int_{(\mathbb{Q}\backslash\mathbb{A})^2} \Psi_{U_3,\psi_D}(n(v)g)\,dv = \int_{N_u(\mathbb{Q})\backslash N_u(\mathbb{A})} \psi_D^{-1}(\tilde{n}(u)) \int_{U_K(\mathbb{Q})\backslash U_K(\mathbb{A})} \Psi(n_k\tilde{n}(u)g)\,dn_k\,d\tilde{n}(u)$$

and the inner integral vanishes because of cuspidality of Ψ along the unipotent radical U_K of the Klingen parabolic. Thus

$$\Psi_{U_3,\psi_D}(g) = \sum_{\gamma} \Psi_{U_P,\psi_D}(\gamma g).$$

This relation implies the result as follows. If $\Psi_{U_3,\psi_D}(g) \not\equiv 0$, the Fourier coefficient $\Psi_{U_P,\psi_D}(g)$ does not vanish identically. Vice versa, if $\Psi_{U_P,\psi_D}(g) \not\equiv 0$ then there is a character ψ' in the $L(\mathbb{Q})$-orbit of ψ_D such that $\Psi_{U_3,\psi'}(g) \not\equiv 0$. □

5.3. ***The spin L-function and its residue at s = 1.*** Let π denote any cuspidal automorphic representation of $\boldsymbol{G}(\mathbb{A})$ with trivial central character. Let S denote a finite set of places of $\mathbb{Q}$ containing the ones where π

is ramified and the archimedean place. If Spin : $\mathrm{Spin}_7(\mathbb{C}) \to \mathrm{GL}(V_8)$ denotes the eight-dimensional spin representation, the partial spin L-function of π is defined to be

$$L^S(s, \pi, \mathrm{Spin}) := \prod_{\ell \notin S} \frac{1}{\det(1 - \ell^{-s}\,\mathrm{Spin}(s_{\pi_\ell}))},$$

where s_{π_ℓ} denotes the Satake parameter of the unramified local component π_ℓ. Let $\boldsymbol{H}$ be the group (3) associated to the étale cubic algebra $\mathbb{Q} \times F$, where $F = \mathbb{Q}(\sqrt{D})$ with either $D \not\equiv 1 \in \mathbb{Q}^\times_{>0}/(\mathbb{Q}^\times)^2$, in which case F is a real quadratic field, or $D \equiv 1 \bmod (\mathbb{Q}^\times)^2$, in which case $F = \mathbb{Q} \times \mathbb{Q}$. For any cusp form $\Psi \in V_\pi$, Pollack and Shah [2018] gave an integral representation

$$\mathcal{I}(\Phi, \Psi, s) = \int_{\mathbb{Z}(\mathbb{A})\boldsymbol{H}(\mathbb{Q})\backslash \boldsymbol{H}(\mathbb{A})} E_\Phi(h_1, s)\Psi(h)\,dh$$

of $L^S(s, \pi, \mathrm{Spin})$. For any Φ and Ψ, the integral $\mathcal{I}(\Phi, \Psi, s)$ is absolutely convergent for $\mathrm{Re}(s)$ big enough and has a meromorphic continuation to $\mathbb{C}$. According to [Gan and Gurevich 2009, Proposition 7.1], for $\mathrm{Re}(s)$ big enough we have the unfolding

$$\mathcal{I}(\Phi, \Psi, s) = \int_{U_{B_{\boldsymbol{H}}}(\mathbb{A})Z(\mathbb{A})\backslash \boldsymbol{H}(\mathbb{A})} f_\Phi(h_1, s)\Psi_{U_P,\psi_D}(h)\,dh,$$

where $U_{B_{\boldsymbol{H}}}$ is the unipotent radical of the upper triangular Borel subgroup $B_{\boldsymbol{H}}$ of $\boldsymbol{H}$ and Ψ_{U_P,ψ_D} is the Fourier coefficient of Definition 5.6.

Theorem 5.8 [Pollack and Shah 2018]. *For a set Σ of places of $\mathbb{Q}$, denote*

$$\mathcal{I}_\Sigma(\Phi, \Psi, s) = \int_{U_{B_{\boldsymbol{H}}(\mathbb{Q}_\Sigma)}Z_{\boldsymbol{G}}(\mathbb{Q}_\Sigma)\backslash \boldsymbol{H}(\mathbb{Q}_\Sigma)} f(h_1, \Phi_\Sigma, s)\Psi_{U_P,\psi_D}(h)\,dh.$$

Let Ψ be a cusp form in the space of π. Then, for any factorizable Schwartz–Bruhat function Φ on $\mathbb{A}^2$ and up to enlarging S, we have

$$\mathcal{I}(\Phi, \Psi, s) = \mathcal{I}_S(\Phi, \Psi, s)L^S(s, \pi, \mathrm{Spin}).$$

Moreover, there exists a cusp form $\widetilde{\Psi}$ in the space of π and a factorizable Schwartz–Bruhat function Φ on $\mathbb{A}^2$ such that

$$\mathcal{I}(\Phi, \widetilde{\Psi}, s) = \mathcal{I}_\infty(\Phi, \Psi, s)L^S(s, \pi, \mathrm{Spin}).$$

Note that if π does not support a rank-2 Fourier coefficient (for the Siegel parabolic Q) and thus, by Proposition 5.7, a Fourier coefficient for P, the integral $\mathcal{I}(\Phi, \Psi, s)$ is identically zero.

Corollary 5.9 [Pollack and Shah 2018]. *Suppose that π supports a rank-2 Fourier coefficient. Then the partial spin L-function $L^S(s, \pi, \mathrm{Spin})$ has meromorphic continuation in s, is holomorphic outside $s = 1$, and has at worst a simple pole at $s = 1$.*

As we explain in later sections, using results of Gan and Gurevich, Pollack and Shah further proved that when $L^S(s, \pi, \mathrm{Spin})$ has a simple pole at $s = 1$, π lifts to the split G_2 under the exceptional theta correspondence. This observation is based on the following key relation between the residue at $s=1$ of $L^S(s,\pi,\mathrm{Spin})$ and the automorphic period we have introduced in Section 4.3.

Proposition 5.10. *For any factorizable Schwartz–Bruhat function Φ on $\mathbb{A}^2$, we have*

$$\frac{\widehat{\Phi}(0)}{2}\cdot\int_{\mathbb{Z}(\mathbb{A})\boldsymbol{H}(\mathbb{Q})\backslash\boldsymbol{H}(\mathbb{A})}\Psi(h)\,dh=\mathrm{Res}_{s=1}\big(\mathcal{I}_S(\Phi,\Psi,s)L^S(s,\pi,\mathrm{Spin})\big).$$

Proof. Thanks to Lemma 5.1, the residue at $s=1$ of $\mathcal{I}(\Phi,\Psi,s)$ equals

$$\frac{\widehat{\Phi}(0)}{2}\cdot\int_{\mathbb{Z}(\mathbb{A})\boldsymbol{H}(\mathbb{Q})\backslash\boldsymbol{H}(\mathbb{A})}\Psi(h)\,dh.$$

The result then follows from Theorem 5.8. □

We now state our first main result. Let π denote a cuspidal automorphic representation of $\mathrm{PGSp}_6(\mathbb{A})$ for which π_∞ is the discrete series of Hodge type (3,3) in the L-packet of V^λ with $\lambda=(\lambda_2+\lambda_3,\lambda_2,\lambda_3,0)$. Let $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B}$, $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}$, and ω_Ψ be as in Sections 3.4 and 4.3. Let $\Psi^{[\lambda,\mu]}$ denote $A^{[\lambda,\mu]}\cdot\Psi$, where $A^{[\lambda,\mu]}\in U(\mathfrak{k}_\mathbb{C})$ is the operator defined in Proposition 4.8.

Theorem 5.11. *We have*

$$\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}},[\omega_\Psi]\rangle_{\mathcal{H}}=\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B},[\omega_\Psi]\rangle=C\cdot\mathrm{Res}_{s=1}\big(\mathcal{I}_S(\Phi,\Psi^{[\lambda,\mu]},s)L^S(s,\pi,\mathrm{Spin})\big),$$

where

$$C=\frac{\widehat{\Phi}(0)h_{U'}}{2(2\pi i)^3\cdot\mathrm{vol}(U')}.$$

Proof. By Propositions 4.8 and 4.10, we have that

$$\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}},[\omega_\Psi]\rangle_{\mathcal{H}}=\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B},[\omega_\Psi]\rangle=\frac{h_{U'}}{(2\pi i)^3\cdot\mathrm{vol}(U')}\int_{\boldsymbol{H}(\mathbb{Q})\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A})\backslash\boldsymbol{H}(\mathbb{A})}\Psi^{[\lambda,\mu]}(h)\,dh,$$

where $U'=U\cap\boldsymbol{H}(\mathbb{A}_f)$ and $h_{U'}=4^{-1}|\mathbb{Z}_{\boldsymbol{G}}(\mathbb{Q})\backslash\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A}_f)/(\mathbb{Z}_{\boldsymbol{G}}(\mathbb{A}_f)\cap U')|$. By Proposition 5.10, we have

$$\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B},[\omega_\Psi]\rangle=C\cdot\mathrm{Res}_{s=1}\big(\mathcal{I}_S(\Phi,\Psi^{[\lambda,\mu]},s)L^S(s,\pi,\mathrm{Spin})\big),$$

where

$$C=\frac{\widehat{\Phi}(0)h_{U'}}{2(2\pi i)^3\cdot\mathrm{vol}(U')}.$$

This finishes the proof. □

Let us fix a Schwartz–Bruhat function Φ such that $\widehat{\Phi}(0)\neq 0$.

Corollary 5.12. *Suppose that π satisfies the following hypotheses*:

- $\mathcal{I}_S(\Phi,\Psi^{[\lambda,\mu]},1)\neq 0$ *for some μ.*
- *The partial L-function $L^S(s,\pi,\mathrm{Spin})$ has a pole at $s=1$.*

Then

$$\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B},[\omega_\Psi]\rangle=\langle\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}},[\omega_\Psi]\rangle_{\mathcal{H}}\neq 0.$$

Proof. By [Pollack and Shah 2018, Theorem 1.3] the function $L^S(s, \pi, \mathrm{Spin}) = 1$ has at most a simple pole. As a consequence $\mathrm{Res}_{s=1} L^S(s, \pi, \mathrm{Spin}) \neq 0$. By Theorem 5.11, under the assumption that $\mathcal{I}_S(\Phi, \Psi^{[\lambda,\mu]}, 1) \neq 0$, this implies that $\langle \mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B}, [\omega_\Psi] \rangle \neq 0$. □

Remark 5.13. If the automorphic representation π supports a rank-2 Fourier coefficient and its partial spin L-function has a (necessarily simple) pole at $s = 1$, by the results of [Pollack and Shah 2018] it is $\boldsymbol{H}$-distinguished, namely the map $\mathcal{P}_{\boldsymbol{H}} \in \mathrm{Hom}_{\boldsymbol{H}(\mathbb{A})}(\pi, \mathbf{1})$ defined by

$$\Psi \mapsto \mathcal{P}_{\boldsymbol{H}}(\Psi) := \int_{Z(\mathbb{A})\boldsymbol{H}(\mathbb{Q})\backslash \boldsymbol{H}(\mathbb{A})} \Psi(h)\, dh$$

is not identically zero. Then, asking $\mathcal{I}_S(\Phi, \Psi^{[\lambda,\mu]}, 1) \neq 0$ for some μ is equivalent to asking that the map obtained as the composition of $\mathcal{P}_{\boldsymbol{H}}$ with an $\boldsymbol{H}(\mathbb{R})$-equivariant embedding $\pi_\infty \to \pi$ restricts nontrivially to the minimal K_∞-type of π_∞.

Denote by $H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))_{\mathrm{hom}}$ the F-vector space defined in Section 3.4.3 and denote by $H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))_{\mathrm{hom}}[\pi_f^\vee]$ its $\pi_f^\vee$-isotypical component. This is a finite-dimensional L-vector space, where L is the number field introduced in Section 2.8. The Tate conjecture for the motive attached to π (see Conjecture 1.1(3)) predicts the equality

$$-\mathrm{ord}_{s=1} L(s, \pi, \mathrm{Spin}) = \dim_L H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))_{\mathrm{hom}}[\pi_f^\vee].$$

Corollary 5.14. *If* $\mathcal{I}_S(\Phi, \Psi^{[\lambda,\mu]}, 1) \neq 0$, *then*

$$-\mathrm{ord}_{s=1} L^S(s, \pi, \mathrm{Spin}) \leq \dim_L H^6_{\mathcal{M}}(\mathrm{Sh}_{\boldsymbol{G}}(U), \mathscr{V}^\lambda_F(3))_{\mathrm{hom}}[\pi_f^\vee].$$

Proof. If $L^S(s, \pi, \mathrm{Spin})$ does not have a pole at $s = 1$, there is nothing to prove. If not, Corollary 5.12 implies that the projection of $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},B}$ to the $\pi_f^\vee$-isotypical component is nonzero, showing the result. □

The following result verifies a weaker form of Conjecture 1.1(3) for the motive $M(\pi_f^\vee)(3)$ at the cost of supposing that $\mathcal{I}_S(\Phi, \Psi^{[\lambda,\mu]}, 1)$ is nonzero for some μ.

Corollary 5.15. *Suppose that π satisfies the hypotheses of Corollary 5.12 and that* (St) *holds. Then* $\mathrm{pr}_{\pi^\vee} \mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}$ *and its Hecke translates generate* $H^1_{\mathcal{H}}(M(\pi_f^\vee)_{\mathbb{R}}(4))$.

Proof. If π_p is the Steinberg representation, it follows from the second statement of Lemma 2.11 and its proof that $H^1_{\mathcal{H}}(M(\pi_f^\vee)_{\mathbb{R}}(4))$ is a rank-1 module over the full Hecke algebra of level U. Hence the result follows by Corollary 5.12. □

6. Exceptional theta lifts from G_2 to PGSp_6

In this section, we discuss the exceptional theta correspondence for the dual reductive pair (G_2, PGSp_6) and describe the set of Fourier coefficients associated to the Heisenberg parabolic for cuspidal automorphic forms of $G_2(\mathbb{A})$. Its sole purpose is to fix notation and to recall some well-known results that will be used later, so the knowledgeable reader might skip it.

	s_1	s_2	s_3	t_1	t_2	t_3	s_4	t_4
s_1	0	$-t_3$	t_2	s_4	0	0	0	s_1
s_2	t_3	0	$-t_1$	0	s_4	0	0	s_2
s_3	$-t_2$	t_1	0	0	0	s_4	0	s_3
t_1	t_4	0	0	0	s_3	$-s_2$	t_1	0
t_2	0	t_4	0	$-s_3$	0	s_1	t_2	0
t_3	0	0	t_4	s_2	$-s_1$	0	t_3	0
s_4	s_1	s_2	s_3	0	0	0	s_4	0
t_4	0	0	0	t_1	t_2	t_3	0	t_4

Table 1. Multiplication table for the basis $\{s_1, s_2, s_3, s_4, t_1, t_2, t_3, t_4\}$.

6.1. ***Split G_2 and E_7.*** In this section we will follow the exposition of the Appendix of [Harris et al. 2023] by Savin.

6.1.1. *The group G_2.* Let $\mathbb{H}$ be the algebra of Hamilton quaternions over $\mathbb{Q}$ with the usual basis $\{1, i, j, k\}$. The conjugate $\bar{a}$ of an element $a = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in \mathbb{H}$ is $\bar{a} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$. The split octonion algebra over $\mathbb{Q}$ is $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}$ with multiplication

$$(a, b) \cdot (c, d) = (ac + d\bar{b}, \bar{a}d + cb).$$

Then $\mathbb{O}$ is a noncommutative, nonassociative $\mathbb{Q}$-algebra. However it is alternative, which means that for any $x, y \in \mathbb{O}$ we have $x \cdot (x \cdot y) = (x \cdot x) \cdot y$ and $(x \cdot y) \cdot y = x \cdot (y \cdot y)$ (see [Jacobson 1958]). If $x = (a, b)$, let $\bar{x} = (\bar{a}, -b)$. Then $x \mapsto \bar{x}$ is a $\mathbb{Q}$-linear involution on $\mathbb{O}$ satisfying $\overline{x \cdot y} = \bar{y} \cdot \bar{x}$. The norm $\mathrm{N} : \mathbb{O} \to \mathbb{Q}$ is the quadratic form defined by $x \mapsto x \cdot \bar{x} = \bar{x} \cdot x$. The trace $\mathrm{Tr} : \mathbb{O} \to \mathbb{Q}$ is defined by $x \mapsto x + \bar{x}$. For any $x, y, z \in \mathbb{O}$, the properties

$$\mathrm{N}(x \cdot y) = \mathrm{N}(x)\mathrm{N}(y),$$
$$\mathrm{Tr}(x \cdot y) = \mathrm{Tr}(y \cdot x),$$
$$\mathrm{Tr}(x \cdot (y \cdot z)) = \mathrm{Tr}((x \cdot y) \cdot z)$$

are satisfied. For $x, y \in \mathbb{O}$, we write $y \in x^{\perp}$ if y is orthogonal to x with respect to the bilinear form $(x, y) \mapsto \mathrm{Tr}(x \cdot \bar{y})$, which means that $x \cdot \bar{y} + y \cdot \bar{x} = 0$.

Let $l = (0, 1) \in \mathbb{O}$ so that $\{1, i, j, k, l, li, lj, lk\}$ is a basis of $\mathbb{O}$. From this, one constructs another useful basis $\{s_1, s_2, s_3, s_4, t_1, t_2, t_3, t_4\}$, where

$$s_1 = \tfrac{1}{2}(i + li), \quad s_2 = \tfrac{1}{2}(j + lj), \quad s_3 = \tfrac{1}{2}(k + lk), \quad s_4 = \tfrac{1}{2}(1 + l),$$
$$t_1 = \tfrac{1}{2}(i - li), \quad t_2 = \tfrac{1}{2}(j - lj), \quad t_3 = \tfrac{1}{2}(k - lk), \quad t_4 = \tfrac{1}{2}(1 - l).$$

See Table 1 for the multiplication table, as given in Table 1 of the Appendix of [Harris et al. 2023].

We define

$$G_2 := \{g \in \mathrm{GL}(\mathbb{O}) \mid g(x \cdot y) = (gx) \cdot (gy), \forall x, y \in \mathbb{O}\}.$$

to be the group of automorphisms of $\mathbb{O}$. We note that G_2 acts transitively on nonzero elements of trace zero and norm zero. We will denote the set of trace zero octonions by either $\mathbb{O}^0$ or V_7, where the latter notation emphasizes that this set defines the standard irreducible seven-dimensional representation of G_2 and induces an embedding

$$G_2 \hookrightarrow \mathrm{SO}_7.$$

6.1.2. *The dual reductive pair.* We consider the Albert algebra J over $\mathbb{Q}$, which is the set of matrices

$$A = \begin{pmatrix} d & \bar{z} & y \\ z & e & \bar{x} \\ \bar{y} & x & f \end{pmatrix},$$

where $d, e, f \in \mathbb{Q}$ and $x, y, z \in \mathbb{O}$. The algebra J is equipped with a cubic form, called the determinant, which is given by

$$\det(A) = def - dN(x) - eN(y) - fN(z) + \mathrm{Tr}(zyx).$$

The group of isogenies of this form is a group of type E_6 and its orbits on J are classified by the rank. We will need to consider the set Ω of rank-1 elements $A \in J$, i.e., those $A \neq 0$ such that $A^2 = \mathrm{Tr}(A) \cdot A$. This condition means that the entries of A satisfy the equalities

$$\begin{gathered} \mathrm{N}(x) = ef, \qquad \mathrm{N}(y) = df, \qquad \mathrm{N}(z) = de, \\ dx = \bar{y} \cdot \bar{z}, \qquad ey = \bar{z} \cdot \bar{x}, \qquad fz = \bar{x} \cdot \bar{y}. \end{gathered} \tag{10}$$

Let G denote the split adjoint group of type E_7, which is constructed from J by the Koecher–Tits construction (see Section 3 of [Kobayashi and Savin 2015]). The group G has a maximal parabolic $P = MN$ and its opposite $\bar{P} = M\bar{N}$, with $N \simeq J$ and such that the action under conjugation of the Levi M on N gives an isomorphism of M and the group of similitudes of the cubic form on J

$$M \cong \{g \in \mathrm{GL}(J) \mid \det(gA) = \lambda \det(A) \text{ for some } \lambda \in \boldsymbol{G}_m \text{ and all } A \in J\}.$$

The group G_2 can be realized as a subgroup of M via its action on J by the rule

$$g \cdot \begin{pmatrix} d & \bar{z} & y \\ z & e & \bar{x} \\ \bar{y} & x & f \end{pmatrix} = \begin{pmatrix} d & g\bar{z} & gy \\ gz & e & g\bar{x} \\ g\bar{y} & gx & f \end{pmatrix}.$$

This action has fixed points J_3, the Jordan algebra of symmetric 3×3 matrices with entries in $\mathbb{Q}$. Note that the left action of GL_3 on $J_3 \cong N$ given by

$$g \cdot A = \det(g)^{-1} g A g^t \tag{11}$$

extends to an action on J preserving the determinant form up to scalar, thus defining an embedding of GL_3 into M. Then GL_3 is the centralizer of G_2 in M and $Q = \mathrm{GL}_3 U_3$ (which is the Siegel parabolic of PGSp_6) is the centralizer of G_2 in P. Similarly, the opposite $\bar{Q}$ is the centralizer of G_2 in $\bar{P}$. This gives the dual reductive pair (G_2, PGSp_6) in G.

6.2. *Fourier coefficients for G_2.*

6.2.1. *Root system and parabolic subgroups.* Let T be a (rank-2) maximal split torus over $\mathbb{Q}$ in G_2 and let Δ (resp. $\Delta^+ \subset \Delta$) be the set of roots (resp. a subset of positive roots) for G_2. Let a (resp. b) denote the long (resp. short) simple root in Δ^+. Then

$$\Delta^+ = \{a, b, a+b, a+2b, a+3b, 2a+3b\}.$$

We let $B = TU$ denote the Borel subgroup of G_2 associated to Δ^+. Other than B, there are two proper standard parabolic subgroups P_a and P_b of G_2, such that $P_a \cap P_b = B$. They are characterized by the following. For any $\alpha \in \Delta^+$, denote by $x_\alpha : \boldsymbol{G}_a \hookrightarrow U$ the one parameter unipotent subgroup associated to α. Then, for each $r \in \{a, b\}$, the Levi L_r of P_r is isomorphic to GL_2 and contains x_r. We fix an isomorphism $\mathrm{GL}_2 \simeq L_r$ such that $\left(\begin{smallmatrix} 1 & u \\ & 1 \end{smallmatrix}\right) \mapsto x_r(u)$.

Let U_a be the unipotent radical of P_a. It is a 3-step nilpotent group of dimension 5 with filtration

$$U_a \supset U_1 \supset U_2 \supset \{1\},$$

where U_a/U_1 is generated by $\{x_b, x_{a+b}\}$, U_1/U_2 is isomorphic to the one parameter unipotent subgroup x_{a+2b}, and U_2 is generated by $\{x_{a+3b}, x_{2a+3b}\}$. As representations of L_a, U_a/U_1 is the standard representation, while U_1/U_2 is the determinant (see [Gan and Savin 2023, §2.4]).

We denote by $H := P_b$ the so-called Heisenberg parabolic and let $L_H U_H$ denote its Levi decomposition. The unipotent radical U_H is of dimension 5 and admits the filtration

$$U_H \supset [U_H, U_H] \supset \{1\},$$

with $U_H/[U_H, U_H]$ being the four-dimensional abelian unipotent group generated by

$$\{x_a, x_{a+b}, x_{a+2b}, x_{a+3b}\},$$

while $[U_H, U_H]$ is isomorphic to the one parameter unipotent subgroup x_{2a+3b}.

6.2.2. *An embedding of* SL_3 *into* G_2. The group G_2 acts transitively on the set

$$\Gamma_c := \{x \in \mathbb{O}^0 \mid N(x) = -c\}.$$

By [Jacobson 1958, Theorem 4], the stabilizer of an element $y_0 \in \Gamma_1$ is isomorphic to SL_3. Choose y_0 such that the unipotent radical U_{SL_3} of the upper triangular Borel of SL_3 is generated by the one-parameter subgroups

$$\{x_a, x_{a+3b}, x_{2a+3b}\}.$$

In terms of the basis chosen in Section 6.1.1, this is achieved by choosing $y_0 = s_4 - t_4$. In this case, one shows (see [Rallis and Schiffmann 1989, Lemma 2]) that the stabilizer of y_0 leaves invariant the subspace $\langle s_1, s_2, s_3 \rangle$ and is identified with $\mathrm{SL}_3 = \mathrm{SL}(\langle s_1, s_2, s_3 \rangle)$.

6.2.3. *The Lie algebra of* G_2. The multiplication map on $\mathbb{O}$ induces a map $V_7 \otimes V_7 \to V_7$ given by $x \otimes y \mapsto \frac{1}{2}(xy - yx)$. This map is alternating; hence it induces a G_2-equivariant map $\bigwedge^2 V_7 \to V_7$ which is surjective. Then the Lie algebra $\mathfrak{g}_2$ of G_2 can be identified with the kernel of this map. Under this identification, one has an explicit description of the action of $\mathfrak{g}_2$ on V_7, namely

$$(w \wedge x) \cdot v = \langle x, v \rangle w - \langle w, v \rangle x.$$

We will also need (see [Fulton and Harris 1991, §22.2]) the decomposition

$$\mathfrak{g}_2 = \mathfrak{sl}_3 \oplus \mathrm{Std}_3 \oplus \mathrm{Std}_3^*, \tag{12}$$

where Std_3 is the standard representation of SL_3 with basis $\{v_1, v_2, v_3\}$ and Std_3^* is its dual with basis $\{\delta_1, \delta_2, \delta_3\}$ and where we denote by E_{ij}, $1 \leq i < j \leq 3$ the standard basis vectors of $\mathfrak{sl}_3$. The identification between the two descriptions (see [Pollack 2021, §2.2]) of $\mathfrak{g}_2$ is given by $E_{ij} = t_j \wedge s_i$, $1 \leq i < j \leq 3$, $v_i = (s_4 - t_4) \wedge s_i + t_{i+1} \wedge t_{i+2}$ and $\delta_i = (s_4 - t_4) \wedge t_i + s_{i+1} \wedge s_{i+2}$, $1 \leq i \leq 3$, where indices are taken modulo 3. Moreover, the component $\mathfrak{sl}_3$ is the Lie algebra of the copy of SL_3 embedded into G_2 as above. In particular, E_{12}, E_{13} and E_{23} are root vectors for the roots a, $2a+3b$ and $a+3b$ respectively. Moreover, the vectors v_1, v_2 and δ_3 are root vectors for the roots $a+b$, b and $a+2b$, respectively. Via (12), the Lie algebra $\mathfrak{u}_H$ of U_H is

$$\mathfrak{u}_H = \mathfrak{u}_{\mathrm{SL}_3} \oplus \mathbb{Q}v_1 \oplus \mathbb{Q}\delta_3. \tag{13}$$

Under (12) the Lie algebra $\mathfrak{l}_H$ of the Levi L_H is generated by the Cartan subalgebra and the root vectors v_2, δ_2.

6.2.4. *Fourier coefficients.* We now describe the Fourier coefficients for G_2 associated to the Heisenberg parabolic. We closely follow [Pollack 2021] and refer to it for more details. In order to describe the Fourier coefficients associated to H, we need to study the L_H-representation $V_H := U_H/[U_H, U_H]$. As a GL_2-representation, V_H is isomorphic to $\mathrm{Sym}^3(\mathrm{Std}_2) \otimes \det^{-1}(\mathrm{Std}_2)$, where Std_2 denotes the standard representation of GL_2. Under the identification of (13), (a representative of) an element of $V_H(\mathbb{Q})$ can be written as

$$x_a(\lambda_1)x_{a+b}(\lambda_2/3)x_{a+2b}(\lambda_3/3)x_{a+3b}(\lambda_4), \quad \text{with } \lambda_i \in \mathbb{Q},$$

which corresponds to the binary cubic polynomial

$$p(x, y) = \lambda_1 x^3 + \lambda_2 x^2 y + \lambda_3 x y^2 + \lambda_4 y^3,$$

where x, y form a basis of Std_2. Associated to p, there is the cubic $\mathbb{Q}$-algebra R with basis $\{1, i, j\}$ with multiplicative table

$$\begin{aligned} ij &= -ad \\ i^2 &= -ac + bi - aj \\ j^2 &= -bd + di - cj. \end{aligned}$$

Example 6.1. (1) [Gross and Lucianovic 2009, 3.2] If $p(x, y) = x^2y - xy^2$ then the associated $\mathbb{Q}$-algebra R is isomorphic to $\mathbb{Q}^3$.

(2) [Gross and Lucianovic 2009, 3.3] If $p(x, y) = x^3 - Dxy^2$ $\big($or equivalently $p(x, y) = -Dx^2y + y^3$ using the action of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\big)$ then the associated $\mathbb{Q}$-algebra R is isomorphic to $\mathbb{Q} \oplus \mathbb{Q}(\sqrt{D})$.

There is an action of $\mathrm{GL}_2(\mathbb{Q})$ on the set of bases $\{1, i, j\}$ of a given cubic algebra R, which makes the association $p(X, Y) \mapsto (R, \{1, i, j\})$ $\mathrm{GL}_2(\mathbb{Q})$-equivariant. Since any cubic algebra admits a basis of this shape, we have the following.

Proposition 6.2 [Gross and Lucianovic 2009, Proposition 2.1]. *There is a bijection between the* $\mathrm{GL}_2(\mathbb{Q})$*-orbits on* $V_H(\mathbb{Q})$ *and the set of isomorphism classes of cubic* $\mathbb{Q}$*-algebras. Moreover, each orbit has a well-defined discriminant in* $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Let $e : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$ be the additive character introduced in Section 5.2.1. Let $\langle\ ,\ \rangle$ denote the symplectic pairing on V_H defined as follows. If $v, v' \in V_H$ correspond to $p(x, y)$ and $p'(x, y)$ respectively, then

$$\langle v, v'\rangle = \lambda_1\lambda_4' - \tfrac{1}{3}\lambda_2\lambda_3' + \tfrac{1}{3}\lambda_3\lambda_2' - \lambda_4\lambda_1'.$$

Any character $\psi : U_H(\mathbb{Q})\backslash U_H(\mathbb{A}) \to \mathbb{C}^\times$ factors through $V_H(\mathbb{A})$; hence we consider the projection $\bar{n}$ of $n \in U_H(\mathbb{A})$ to $V_H(\mathbb{A})$, which, by (13), can be written as

$$\bar{n} = x_a(\lambda_1')x_{a+b}\tfrac{1}{3}\lambda_2' x_{a+2b}\tfrac{1}{3}\lambda_3' x_{a+3b}(\lambda_4').$$

If $v \in V_H(\mathbb{Q})$ corresponds to $p(x, y)$, we then define $\psi_v : U_H(\mathbb{Q})\backslash U_H(\mathbb{A}) \to \mathbb{C}^\times$ by

$$n \mapsto e(\langle v, \bar{n}\rangle) = e\bigl(\lambda_1\lambda_4' - \tfrac{1}{3}\lambda_2\lambda_3' + \tfrac{1}{3}\lambda_3\lambda_2' - \lambda_4\lambda_1'\bigr).$$

The character ψ_v is nondegenerate if and only if v corresponds to an étale cubic algebra over $\mathbb{Q}$. In this manuscript, we are interested in étale cubic algebras of the form $\mathbb{Q} \times F$, with F of either the form $\mathbb{Q}(\sqrt{D})$ (with $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \ni D \not\equiv 1$) or $\mathbb{Q} \times \mathbb{Q}$ (with $D \equiv 1 \bmod (\mathbb{Q}^\times)^2$).

Definition 6.3. Let $\psi_{H,D} : U_H(\mathbb{Q})\backslash U_H(\mathbb{A}) \to \mathbb{C}^\times$ denote the character associated to $\mathbb{Q} \times F$. Given a cusp form φ for $G_2(\mathbb{A})$, define

$$\varphi_{U_H,\psi_{H,D}}(g) := \int_{U_H(\mathbb{Q})\backslash U_H(\mathbb{A})} \psi_{H,D}^{-1}(n)\varphi(ng)\,dn.$$

6.3. ***The theta lift from G_2 to* PGSp_6.** Let $\Pi = \bigotimes_v' \Pi_v$ denote the restricted tensor product of the minimal representations Π_v of $E_7(\mathbb{Q}_v)$ over all places v of $\mathbb{Q}$. A unitary model of the minimal representation is given by $L^2(\Omega)$, where recall that Ω denotes the subset of rank-1 elements in J. There is a unique up to a nonzero scalar embedding

$$\theta : \Pi \to \mathcal{A}(E_7(\mathbb{Q})\backslash E_7(\mathbb{A}))$$

of Π in the space $\mathcal{A}(E_7(\mathbb{Q})\backslash E_7(\mathbb{A}))$ of automorphic forms of E_7 (see [Ginzburg et al. 1997a; Kobayashi and Savin 2015]). For $f \in \Pi$ and $\varphi \in \mathcal{A}(G_2(\mathbb{Q})\backslash G_2(\mathbb{A}))$, we define a function $\Theta(f, \varphi)$ on $\mathrm{PGSp}_6(\mathbb{A})$ by

$$\Theta(f, \varphi)(g) = \int_{G_2(\mathbb{Q})\backslash G_2(\mathbb{A})} \theta(f)(g'g)\varphi(g')\,dg'.$$

Definition 6.4. Let σ be a cuspidal automorphic representation of $G_2(\mathbb{A})$.

(1) Define $\Theta(\sigma)$ to be the span of the functions $\Theta(f, \varphi)$, where $f \in \Pi$ and φ runs through the cusp forms in the contragredient $\sigma^\vee$ of σ.

(2) We say that a cuspidal automorphic representation π of $\mathrm{PGSp}_6(\mathbb{A})$ is a Θ-lift of σ if it appears as an irreducible subquotient of $\Theta(\sigma)$.

If a Θ-lift of σ exists, then its local constituents are compatible with the local theta correspondence between G_2 and PGSp_6.

Proposition 6.5. *Let π be a Θ-lift of σ. Then π_v is an irreducible subquotient of $\Theta(\sigma_v)$.*

Proof. See [Harris et al. 2023, Theorem 1.7(i)]. □

After imposing certain local conditions on σ, in the next section we use one of the main results of [Ginzburg et al. 1997b] to show that $\Theta(\sigma)$ is nonzero and cuspidal, thus proving the existence of a nontrivial Θ-lift of σ. Before doing so, we first recall the properties of the local theta correspondence needed later.

6.3.1. *Discrete series and a conjecture of Gross.* Let T_c denote a compact torus in $G_2(\mathbb{R})$, which is contained in the maximal compact subgroup $K_{G_2} \simeq (\mathrm{SU}_2 \times \mathrm{SU}_2)/\mu_2$ of $G_2(\mathbb{R})$. We abuse notation denoting again by a, b the simple positive roots for T_c (with the short root b which we assume to be compact) and Δ^+ the resulting set of positive roots. Then, $\rho = \frac{1}{2}\sum_{\alpha\in\Delta^+}\alpha = 3a+5b$. The set of positive compact roots is given by

$$\Delta_c^+ = \{b, 2a+3b\},$$

which, in the notation of [Li 1997], is $\{2\varepsilon_2, 2\varepsilon_1\}$. The Weyl group $\mathfrak{W}_{G_2}$ is isomorphic to the dihedral group D_6 of 12 elements and it is generated by w_a and w_b, where w_α denotes the reflections around the line orthogonal to α. The Weyl group $\mathfrak{W}_{K_{G_2}} \simeq (\mathbb{Z}/2\mathbb{Z})^2$ is generated by w_b and $w_{2a+3b} = w_a w_b w_a w_b w_a$.

Let γ be a dominant weight for G_2 with respect to T_c. The set of equivalence classes of irreducible discrete series of $G_2(\mathbb{R})$ associated to γ has cardinality equal to $|\mathfrak{W}_{G_2}/\mathfrak{W}_{K_{G_2}}| = 3$. Choose representatives $\{w_1, w_2, w_3\}$ of $\mathfrak{W}_{G_2}/\mathfrak{W}_{K_{G_2}}$ such that $w_i\rho$ is dominant for K_{G_2}. Then, for any $1 \le i \le 3$, there exists an irreducible discrete series σ_∞^Γ of Harish-Chandra parameter $\Gamma = w_i(\gamma+\rho)$ and minimal K_{G_2}-type $\Gamma+\delta_{G_2}-2\delta_{K_{G_2}}$, where δ_{G_2} (resp. $\delta_{K_{G_2}}$) is the half-sum of roots (resp. compact roots) which are positive with respect to the Weyl chamber in which Γ lies. Precisely, if we let $w_1 = \mathrm{id}$, $w_2 = w_a$, and $w_3 = w_b w_a$, then

$$\begin{aligned} w_1\rho &= \rho = 3\varepsilon_1 + \varepsilon_2, \\ w_2\rho &= 2a+5b = 2\varepsilon_1 + 4\varepsilon_2, \\ w_3\rho &= a+4b = \varepsilon_1 + 5\varepsilon_2. \end{aligned}$$

We let $\mathcal{D}_{3,1}$, $\mathcal{D}_{2,4}$, and $\mathcal{D}_{1,5}$ denote the sets of discrete series of $G_2(\mathbb{R})$ whose Harish-Chandra parameter lies in the Weyl chamber corresponding to $w_1\rho$, $w_2\rho$, and $w_3\rho$ respectively. Elements of $\mathcal{D}_{3,1}$ are the quaternionic discrete series, while elements of $\mathcal{D}_{2,4}$ are the generic discrete series.

Gross has given a precise conjectural description of the entire discrete spectrum of the dual pair (G_2, PGSp_6) (see [Li 1997, Conjecture 1.2]). Recall that there are four families of discrete series for $\mathrm{PGSp}_6(\mathbb{R})$, indexed by the set of Hodge types up to conjugation. In particular, the discrete series of $\mathrm{PGSp}_6(\mathbb{R})$ of Hodge type (4, 2) (resp. (6, 0)) are the generic (resp. holomorphic) discrete series.

Conjecture 6.6 (Gross). Let Π_∞ be the minimal representation of $E_7(\mathbb{R})$. The discrete spectrum of the restriction of Π_∞ to the dual pair $G_2(\mathbb{R}) \times \mathrm{PGSp}_6(\mathbb{R})$ is the direct sum of all tensor products $\sigma_\infty \otimes \theta(\sigma_\infty)$, where σ_∞ belongs to the discrete series of G_2. If σ_∞ has infinitesimal character $\gamma+\rho=r\varepsilon_1+s\varepsilon_2$ and belongs to either $\mathcal{D}_{3,1}$, $\mathcal{D}_{2,4}$, or $\mathcal{D}_{1,5}$, then $\theta(\sigma_\infty)$ is the discrete series of $\mathrm{PGSp}_6(\mathbb{R})$ with infinitesimal character $\big(r, \frac{1}{2}(r+s), \frac{1}{2}(r-s)\big)$ and Hodge type $(3,3)$, $(4,2)$, or $(5,1)$ respectively.

Partial results towards the conjecture of Gross were shown by Li for discrete series in $\mathcal{D}_{3,1}$ (see Section 6.3.2 below) and for the generic family $\mathcal{D}_{2,4}$ by Harris, Khare and Thorne [Harris et al. 2023, Theorems 1.5 and 1.7(ii)] using the main result of Savin's appendix to [Harris et al. 2023] and the nonvanishing of the global theta lift given by [Ginzburg et al. 1997b, Corollary 4.2]. Li [1997, Theorem 4.3] also gave evidence to the predictions of Gross for a proper subset $\mathcal{D}'_{1,5}$ of $\mathcal{D}_{1,5}$. We also note that the remaining equivalence class of holomorphic discrete series of $\mathrm{PGSp}_6(\mathbb{R})$ (of Hodge type $(6,0)$) is realized in an exceptional theta correspondence studied by Gross and Savin between the compact real form $G_2^c(\mathbb{R})$ of G_2 and $\mathrm{PGSp}_6(\mathbb{R})$ and moreover this is the only Hodge type that appears in that correspondence (see [Gross and Savin 1998, Theorem 3.5]).

6.3.2. *Quaternionic discrete series and their theta lift.* We describe the main result of [Li 1997]. We first notice that a discrete series $\sigma_\infty^{x,y}$ of Harish-Chandra parameter $x\varepsilon_1+y\varepsilon_2$ lies in the set of quaternionic discrete series $\mathcal{D}_{3,1}$ if x, y are two nonnegative integers such that $x-3\geq y-1\geq 0$ and $x-y$ is even. The minimal K_{G_2}-type of $\sigma_\infty^{x,y}\in\mathcal{D}_{3,1}$ is given by

$$\mathrm{Sym}^{x+1}(\mathrm{Std}_{\varepsilon_1})\boxtimes\mathrm{Sym}^{y-1}(\mathrm{Std}_{\varepsilon_2}),$$

where $\mathrm{Std}_{\varepsilon_1}$ (resp. $\mathrm{Std}_{\varepsilon_2}$) is the standard representation of the SU_2 corresponding to the long root ε_1 (resp. the short root ε_2).

Proposition 6.7. *Let Π_∞ denote the minimal representation of $E_7(\mathbb{R})$. We have*

$$\Pi_\infty|_{G_2(\mathbb{R})\times\mathrm{PGSp}_6(\mathbb{R})}\supseteq\bigoplus_{\sigma_\infty^{x,y}\in\mathcal{D}_{3,1}}\sigma_\infty^{x,y}\otimes\theta(\sigma_\infty^{x,y}),$$

where $\theta(\sigma_\infty^{x,y})\in P(V^\lambda)$, with $\lambda=\big(x-3, \frac{1}{2}(x+y)-2, \frac{1}{2}(x-y)-1, 0\big)$, is the discrete series $\pi_\infty^{3,3}$ of Hodge type $(3,3)$ and Harish-Chandra parameter $\big(\frac{1}{2}(x+y), \frac{1}{2}(x-y), -x\big)$.

Proof. See [Li 1997, Theorem 1.1; Huang et al. 1996, Theorem 5.4]. □

The set $\mathcal{D}_{3,1}$ contains an important family of discrete series, which were studied by Gross and Wallach [1994; 1996].

Definition 6.8. For every $n\geq 2$, the quaternionic discrete series σ_n is the element of $\mathcal{D}_{3,1}$ of Harish-Chandra parameter $(2n-1)\varepsilon_1+\varepsilon_2$ and minimal K_{G_2}-type

$$\mathrm{Sym}^{2n}(\mathrm{Std}_{\varepsilon_1})\boxtimes\mathbf{1}.$$

A fundamental property of the members of this family is that they admit (unique) models with respect to the unipotent radical of the Heisenberg parabolic and nondegenerate characters corresponding to totally real étale cubic algebras. Recall, as in Section 6.2.4, that a nondegenerate character $\psi: U_H(\mathbb{R})\to\mathbb{C}^\times$

corresponds to a cubic algebra, whose discriminant is either positive or negative. The first type corresponds to the $\mathrm{GL}_2(\mathbb{R})$-orbit on $V_H(\mathbb{R})$ given by $\mathbb{R}^3$, while the second to the $\mathrm{GL}_2(\mathbb{R})$-orbit of $\mathbb{R}\times\mathbb{C}$. A representative $\psi : U_H(\mathbb{R}) \to \mathbb{C}^\times$ of the totally real orbit is given by $e^{2\pi i f}$, where $f : U_H(\mathbb{R}) \to \mathbb{R}$ is nonzero on the one parameter unipotent subgroups x_{a+b} and x_{a+2b} and trivial on x_a and x_{a+3b} (see [Gan et al. 2002, §6]). A special case of the main result of [Wallach 2003] gives the following.

Proposition 6.9. *Let ψ be a nondegenerate character of $V_H(\mathbb{R})$. There is* (*at most*) *a one-dimensional space of ψ-equivariant linear functionals on σ_n. Moreover*,

$$\dim \mathrm{Hom}_{U_H(\mathbb{R})}(\sigma_n, \psi) = 1,$$

exactly when ψ corresponds to a totally real cubic algebra.

6.3.3. *The nonarchimedean theta correspondence.* We describe the properties of the nonarchimedean theta correspondence which will be later needed to study the global theta correspondence. Let σ be an irreducible admissible representation of $G_2(\mathbb{Q}_p)$. The maximal σ-isotypic quotient of the minimal representation Π_p of $E_7(\mathbb{Q}_p)$ can be expressed as $\sigma \boxtimes \Theta(\sigma)$, with $\Theta(\sigma)$ a smooth representation of $\mathrm{PGSp}_6(\mathbb{Q}_p)$ which is called the big theta lift of σ.

Proposition 6.10. *For an irreducible admissible representation σ of $G_2(\mathbb{Q}_p)$, $\Theta(\sigma)$ has finite length with unique irreducible quotient* (*if nonzero*) *$\theta(\sigma)$. Moreover*, *one has the following.*

(1) *Let σ be an unramified generic representation of $G_2(\mathbb{Q}_p)$ with Satake parameter s. Then $\pi = \theta(\sigma)$ is the unramified representation of* $\mathrm{PGSp}_6(\mathbb{Q}_p)$ *whose Satake parameter is $\varphi \circ s$, where $\varphi : G_2 \hookrightarrow \mathrm{Spin}_7$ is the map of L-groups.*

(2) *Let* St_{G_2} (*resp.* $\mathrm{St}_{\mathrm{PGSp}_6}$) *be the Steinberg representation of $G_2(\mathbb{Q}_p)$* (*resp.* $\mathrm{PGSp}_6(\mathbb{Q}_p)$). *Then* $\theta(\mathrm{St}_{G_2}) = \mathrm{St}_{\mathrm{PGSp}_6}$.

Proof. See [Gan and Savin 2023, Theorems 1.2, 15.3(v); Gross and Savin 1998, Proposition 3.1]. □

7. Cuspidality and Fourier coefficients of the global theta lift

In this section, based on [Ginzburg et al. 1997b; Gross and Savin 1998], and the appendix of Savin in [Harris et al. 2023], we give a criterion on the cuspidality of representations in the image of the exceptional theta lift and on their possession of Fourier coefficients of type $(4\,2)$.

7.1. ***Cuspidality of the global lift.*** Let V denote the unipotent subgroup of SL_3 (embedded into G_2 as in Section 6.2.2) generated by the roots $a+3b$ and $2a+3b$. We further consider the subgroup SL_2 embedded into G_2 via the Levi of the "long root" parabolic P_a and denote, for any cusp form φ for $G_2(\mathbb{A})$,

$$\varphi^{\mathrm{SL}_2 V}(g) := \int_{\mathrm{SL}_2(\mathbb{Q})\backslash \mathrm{SL}_2(\mathbb{A})} \int_{V(\mathbb{Q})\backslash V(\mathbb{A})} \varphi(vmg)\, dv\, dm.$$

We will now show that the above period vanishes whenever φ is not globally generic. We are thankful to David Ginzburg for kindly sharing with us a proof of this fact.

Lemma 7.1. *Let σ be a cuspidal automorphic representation of $G_2(\mathbb{A})$, which is not globally generic. For any cusp form $\varphi \in V_\sigma$ and $g \in G_2(\mathbb{A})$, we have $\varphi^{\mathrm{SL}_2 V}(g) = 0$.*

Proof. Let Z denote the unipotent subgroup of G_2 generated by the roots $a+2b$, $a+3b$, and $2a+3b$. Let $\varphi \in V_\sigma$. If we Fourier expand the period $\varphi^{\mathrm{SL}_2 V}(g)$ along the one-dimensional unipotent subgroup $x_{a+2b}(r)$ of G_2, we get

$$\varphi^{\mathrm{SL}_2 V}(g) = \varphi^{\mathrm{SL}_2 Z}(g) + \sum_{\psi} \varphi^{\mathrm{SL}_2 Z,\psi}(g),$$

where the sum runs over nontrivial additive characters $\psi : Z(\mathbb{Q})\backslash Z(\mathbb{A}) \to \mathbb{C}^\times$ supported on the root $a+2b$, $\varphi^{\mathrm{SL}_2 Z}(g)$ is the period of φ over $[\mathrm{SL}_2 Z]$, and

$$\varphi^{\mathrm{SL}_2 Z,\psi}(g) := \int_{\mathrm{SL}_2(\mathbb{Q})\backslash \mathrm{SL}_2(\mathbb{A})} \int_{Z(\mathbb{Q})\backslash Z(\mathbb{A})} \varphi(umg)\psi(u)\,du\,dm.$$

By [Ginzburg et al. 1997b, Lemma 2.1], $\varphi^{\mathrm{SL}_2 Z}(g) = 0$ for all φ in σ and $g \in G_2(\mathbb{A})$. Hence $\varphi^{\mathrm{SL}_2 V}(g) = 0$ if and only if $\varphi^{\mathrm{SL}_2 Z,\psi}(g) = 0$ for all nontrivial ψ. We now argue by contradiction. Suppose that $\varphi^{\mathrm{SL}_2 Z,\psi}(g) \neq 0$ for a certain ψ. We claim that this implies that σ supports Whittaker Fourier coefficients, thus contradicting our hypothesis.

Let U_a be the unipotent radical of P_a introduced in Section 6.2.1. Since V is normal in U_a, we can consider the quotient $V_0 = U_a/V$, which is isomorphic to the Heisenberg group in three variables and it is generated by the roots b, $a+b$, and $a+2b$. The center of V_0 is generated by the root $a+2b$ and is identified with the quotient $Z_0 := Z/V$. As SL_2 is embedded into G_2 via the Levi L_a of P_a, it acts trivially on the quotient Z_0. Therefore, $D := \mathrm{SL}_2 V_0$ is a Jacobi group in the sense of [Ikeda 1994, Definition on p. 619]. Let

$$\widetilde{D(\mathbb{A})} := \widetilde{\mathrm{SL}_2(\mathbb{A})}\, V_0(\mathbb{A}),$$

with $\widetilde{\mathrm{SL}_2(\mathbb{A})}$ denoting the metaplectic cover of $\mathrm{SL}_2(\mathbb{A})$, and denote by $C^\infty_\psi(D(\mathbb{Q})\backslash\widetilde{D(\mathbb{A})})$ the space of functions f on $D(\mathbb{Q})\backslash\widetilde{D(\mathbb{A})}$ such that $f(zvh) = \psi(z)f(vh)$ for any $z \in Z_0(\mathbb{A})$, $v \in V_0(\mathbb{A})$, $h \in \widetilde{\mathrm{SL}_2(\mathbb{A})}$. For any Schwartz function $\Phi \in \mathcal{S}(\mathbb{A})$, we let $\theta^{\Phi}_{\mathrm{SL}_2} \in C^\infty_\psi(D(\mathbb{Q})\backslash\widetilde{D(\mathbb{A})})$ be the theta function defined in [Ikeda 1994, p. 620]. By [Ikeda 1994, Proposition 1.3], if W is a closed subspace of $C^\infty_{\psi^{-1}}(D(\mathbb{Q})\backslash\widetilde{D(\mathbb{A})})$ which is invariant under right translation of $V_0(\mathbb{A})$, the functions of the form

$$vh \mapsto \overline{\theta^{\Phi_1}_{\mathrm{SL}_2}}(vh) \int_{V_0(\mathbb{Q})\backslash V_0(\mathbb{A})} f(uh)\theta^{\Phi_2}_{\mathrm{SL}_2}(uh)\,du, \tag{14}$$

with $v \in V_0(\mathbb{A})$, $h \in \widetilde{\mathrm{SL}_2(\mathbb{A})}$, $f \in W$, $\Phi_1, \Phi_2 \in \mathcal{S}(\mathbb{A})$, generate a dense subspace of W. We apply this to the space W given by the closure of the subspace generated by the right $V_0(\mathbb{A})$-translations of

$$\varphi^{Z,\psi}(g) := \int_{Z(\mathbb{Q})\backslash Z(\mathbb{A})} \varphi(ug)\psi(u)\,du.$$

Assume that $\varphi^{\mathrm{SL}_2 Z,\psi}$ is not identically zero. By considering right translates of φ we can assume that $\varphi^{\mathrm{SL}_2 Z,\psi}(1)$ is nonzero. This implies that the integral

$$I_1(\varphi, \Phi_1, \Phi_2) := \int_{\mathrm{SL}_2(\mathbb{Q})\backslash \mathrm{SL}_2(\mathbb{A})} \overline{\theta^{\Phi_1}_{\mathrm{SL}_2}}(m) \int_{V_0(\mathbb{Q})\backslash V_0(\mathbb{A})} \varphi^{Z,\psi}(um)\theta^{\Phi_2}_{\mathrm{SL}_2}(um)\,du\,dm$$

is nonzero for some choice of data (Φ_1, Φ_2). Note that the integral $I_1(\varphi, \Phi_1, \Phi_2)$ is well-defined because the functions in (14) are not genuine for our space W. Since $\theta^{\Phi_2}_{\widetilde{\mathrm{SL}}_2}(zg) = \psi(z)\theta^{\Phi_2}_{\widetilde{\mathrm{SL}}_2}(g)$ for all $z \in Z_0(\mathbb{A})$, we can write $I_1(\varphi, \Phi_1, \Phi_2)$ as

$$\int_{\mathrm{SL}_2(\mathbb{Q})\backslash \mathrm{SL}_2(\mathbb{A})} \int_{(\mathbb{Q}\backslash\mathbb{A})^5} \varphi(x_b(v_1)x_{a+b}(v_2)x_{a+2b}(r_1)x_{a+3b}(r_2)x_{2a+3b}(r_3)m) \\ \cdot \theta^{\Phi_2}_{\widetilde{\mathrm{SL}}_2}(x_b(v_1)x_{a+b}(v_2)x_{a+2b}(r_1)m)\overline{\theta^{\Phi_1}_{\widetilde{\mathrm{SL}}_2}(m)}\, dv_i\, dr_i\, dm.$$

The integral $I_1(\varphi, \Phi_1, \Phi_2)$ is the residue of the global zeta integral which calculates the standard L-function for φ when φ admits Whittaker coefficients. Namely, by the Siegel–Weil formula $\overline{\theta^{\Phi_1}_{\widetilde{\mathrm{SL}}_2}(m)}$ is the residue at $s = \frac{3}{4}$ of an Eisenstein series $\mathrm{Eis}_{\widetilde{\mathrm{SL}}_2}(m, s)$ (depending on Φ_1) on the metaplectic cover of SL_2 normalized as in [Ginzburg 1993, §2]. By [Ginzburg 1993, Theorem 4] $I_1(\varphi, \Phi_1, \Phi_2)$ is the residue of

$$I_2(\varphi, \Phi_1, \Phi_2, s) := \int_{\mathrm{SL}_2(\mathbb{Q})\backslash \mathrm{SL}_2(\mathbb{A})} \int_{(\mathbb{Q}\backslash\mathbb{A})^5} \varphi(x_b(v_1)x_{a+b}(v_2)x_{a+2b}(r_1)x_{a+3b}(r_2)x_{2a+3b}(r_3)m) \\ \cdot \overline{\theta^{\Phi_2}_{\widetilde{\mathrm{SL}}_2}}(x_b(v_1)x_{a+b}(v_2)x_{a+2b}(r_1)m)\mathrm{Eis}_{\widetilde{\mathrm{SL}}_2}(m, s)\, dv_i\, dr_i\, dm.$$

We can now prove our claim. Suppose that $\varphi^{\mathrm{SL}_2 Z,\psi}(1) \neq 0$. Then $I_1(\varphi, \Phi_1, \Phi_2)$ is not zero for some choice (Φ_1, Φ_2). This implies that, for $\mathrm{Re}(s)$ large enough, the integral $I_2(\varphi, \Phi_1, \Phi_2, s)$ is not zero. By [Ginzburg 1993, Theorem 1], $I_2(\varphi, \Phi_1, \Phi_2, s)$ unfolds to the Whittaker model and thus contains a Whittaker coefficient of φ as an inner integration. This shows that if $\varphi^{\mathrm{SL}_2 Z,\psi}(1) \neq 0$ for some choice of data, the Whittaker coefficient for φ is nontrivial and thus σ is globally generic. This finishes the proof. □

Theorem 7.2. *Let σ be a cuspidal automorphic representation of $G_2(\mathbb{A})$. Assume that*

(1) *σ is not globally generic*;

(2) *there exists a finite place p such that σ_p is generic.*

Then the big theta lift $\Theta(\sigma)$ of σ to PGSp_6 *is cuspidal.*

Proof. We show the result by using the tower of theta lifts from G_2 and its properties studied in [Ginzburg et al. 1997b]. If σ lifts trivially to PGSp_6 then there is nothing to prove, so suppose that σ has a nonzero theta lift π to PGSp_6. Then, by [Ginzburg et al. 1997b, Theorem A] π is cuspidal if and only if the lifts of σ to PGSp_4 and PGL_3 are both zero. By [Ginzburg et al. 1997b, Theorem 4.1(3)], the lift to PGSp_4 is zero if and only if

$$\varphi^{\mathrm{SL}_3}(g) = \int_{[\mathrm{SL}_3]} \varphi(xg)\, dx = 0 \text{ and } \varphi^{\mathrm{SU}(2,1)}(g) = \int_{[\mathrm{SU}(2,1)]} \varphi(xg)\, dx = 0$$

for any $g \in G_2(\mathbb{A})$, any $\varphi \in V_{\sigma^\vee}$. Here, SL_3 embeds into G_2 as the stabilizer of a norm -1 vector (see Section 6.2.2), while $\mathrm{SU}(2, 1)$ is realized as the stabilizer of a norm $-c$ vector, with c not a square in $\mathbb{Q}$. We argue by contradiction. Suppose that $\sigma^\vee$ has a nontrivial $\mathrm{SU}(2, 1)$-functional. This implies that, at every finite v, σ_v admits one. By Frobenius reciprocity,

$$\mathrm{Hom}_{\mathrm{SU}(2,1)}(\sigma_v^\vee, \mathbb{C}) = \mathrm{Hom}_{G_2}(\text{c-Ind}^{G_2}_{\mathrm{SU}(2,1)}(\mathbb{C}), \sigma_v)$$

and hence, since σ_v is irreducible, one deduces that each local component σ_v of σ is a quotient of $C_c^\infty(G_2(\mathbb{Q}_v)/\mathrm{SU}(2,1)(\mathbb{Q}_v))$. In particular, σ_p is identified with such a quotient. This is a contradiction as, by hypothesis, σ_p is generic but, by [Gross and Savin 1998, Lemma 4.10], $C_c^\infty(G_2(\mathbb{Q}_p)/\mathrm{SU}(2,1)(\mathbb{Q}_p))$ does not admit a Whittaker functional. The same argument also shows the vanishing of φ^{SL_3}. We claim finally that the theta lift of σ to PGL_3 also vanishes. Since σ is not globally generic, Lemma 7.1 shows that, for all $\varphi \in \sigma$, $\varphi^{\mathrm{SL}_2 V}(g) = 0$. We can then apply [Ginzburg et al. 1997b, Theorem 4.1(4)] to deduce that the theta lift of σ to PGL_3 is zero and conclude the proof. □

Corollary 7.3. *Let σ be a cuspidal automorphic representation of $G_2(\mathbb{A})$. Assume that*

(1) *σ_∞ is a discrete series*;

(2) *there exists a finite place p such that σ_p is Steinberg.*

Then $\Theta(\sigma)$ is cuspidal.

Proof. We distinguish two cases. We first suppose that σ is globally generic. Then we apply [Harris et al. 2023, Theorem 1.7(ii)] to deduce that its theta lift is cuspidal. If, instead, σ is not globally generic, the result follows from Theorem 7.2 as the Steinberg representation $\sigma_p = \mathrm{St}_{G_2}$ is generic. □

7.2. *Calculation of orbits.* This preparatory section presents an elementary but crucial calculation needed in the proof of Proposition 7.7.

Let $e : \mathbb{Q}\backslash\mathbb{A} \to \mathbb{C}^\times$ be the standard nontrivial character introduced in Section 5.2 and let $A \in J(\mathbb{Q})$. We define the character $\psi_A : \mathrm{N}(\mathbb{Q})\backslash\mathrm{N}(\mathbb{A}) \to \mathbb{C}^\times$ by $\psi_A(X) = e(\mathrm{Tr}(A \circ X))$, where $A \circ X = \frac{1}{2}(AX + XA)$ is the Jordan product. Recall from Section 5.2 that, for any $B \in J_3(\mathbb{Q})$, we define a character

$$\psi_B : U_3(\mathbb{Q})\backslash U_3(\mathbb{A}) \to \mathbb{C}^\times$$

by $\psi_B(n(X)) = e(\mathrm{Tr}(BX))$. In particular, we have denoted by ψ_D the character associated to

$$\alpha_D = \begin{pmatrix} 0 & & \\ & -D & \\ & & 1 \end{pmatrix} \in J_3(\mathbb{Q}).$$

Define

$$\omega(\mathbb{Q}) := \{A \in \Omega(\mathbb{Q}) \mid \psi_A|_{U_3(\mathbb{A})} = \psi_D\},$$

i.e., the set of rank-1 matrices in $J(\mathbb{Q})$ inducing the same character as α_D on the unipotent radical of the Siegel parabolic. In the following, we will always see $\omega(\mathbb{Q})$ inside $\overline{N}(\mathbb{Q})$. In particular, if $g \in \mathrm{GL}_3(\mathbb{Q}) \subseteq M(\mathbb{Q})$, its action on A is the dual action to (11), namely $g \cdot A = \det(g)(g^t)^{-1}Ag^{-1}$. Finally, denote by $A(x, y, z)$ the matrix

$$\begin{pmatrix} 0 & \bar{z} & y \\ z & -D & \bar{x} \\ \bar{y} & x & 1 \end{pmatrix} \in J.$$

Lemma 7.4. *We have*

$$\omega(\mathbb{Q}) = \{A(x, y, z) : \mathrm{Tr}(x) = \mathrm{Tr}(z) = 0, \mathrm{N}(x) = -D, \mathrm{N}(z) = 0, z \in x^\perp, y = -D^{-1}zx\}.$$

Proof. Let

$$A = \begin{pmatrix} d & \bar{z} & y \\ z & e & \bar{x} \\ \bar{y} & x & f \end{pmatrix} \in J.$$

Similarly to the proof of [Gross and Savin 1998, Lemma 3.4], the condition $\psi_A|_{U_3(\mathbb{A})} = \psi_D$ is equivalent to

$$d = 0, \qquad e = -D, \quad f = 1,$$
$$\bar{x} = -x, \quad \bar{y} = -y, \qquad \bar{z} = -z.$$

This together with the condition that A has rank 1 (equation (10)) give

$$\mathrm{N}(x) = -D, \quad \mathrm{N}(y) = \mathrm{N}(z) = 0,$$
$$yz = 0, \qquad zx = -Dy, \qquad xy = z.$$

We claim that these conditions imply that $z \in x^{\perp}$, which means that $z\bar{x} + x\bar{z} = 0$, or equivalently $zx = -xz$. Indeed, multiplying $z = xy$ on the left by x and using alternativity, we obtain

$$xz = x(xy) = (xx)y = Dy = -zx.$$

Finally, as $\mathrm{N}(x) = -D$ and $\mathrm{Tr}(x) = 0$, we have $x^2 = D$ and hence $x^{-1} = D^{-1}x$, which implies that

$$y = x^{-1}z = D^{-1}xz.$$

This shows one inclusion of the statement.

In the other direction let $x, z \in \mathbb{O}$ be as in the right-hand side of the statement. We have to show that $y := -D^{-1}zx$ has norm and trace equal to zero and that $xy = z$. We have

$$\mathrm{N}(y) = (-D)^{-2}\mathrm{N}(z)\mathrm{N}(x) = 0 \quad \text{and} \quad \mathrm{Tr}(y) = -D^{-1}\,\mathrm{Tr}(zx) = D^{-1}\,\mathrm{Tr}(z\bar{x}) = 0$$

as $z \in x^{\perp}$. Hence $\mathrm{Tr}(y) = 0$. Moreover

$$xy = -D^{-1}x(zx) = D^{-1}x(xz) = D^{-1}(xx)z = z.$$

This shows that $A \in \omega(\mathbb{Q})$ and concludes the proof of the lemma. □

As for any $A(x, y, z) \in \omega(\mathbb{Q})$, the octonion $y = -D^{-1}zx$ is determined by x and z and we will often denote $A(x, y, z)$ by $A(x, z)$. Note that there is an action of $G_2(\mathbb{Q})$ on the set $\omega(\mathbb{Q})$ given by the action on the coefficients. The following proposition describing the orbits of this action will be essential.

Proposition 7.5. *The group $G_2(\mathbb{Q})$ acts on $\omega(\mathbb{Q})$ with a finite number of orbits. Moreover, representatives of the orbits and their respective stabilizers are given as follows.*

(1) *If D is a square in $\mathbb{Q}^{\times}$:*

   (a) $A_3 = A(x, 0)$, *where* $x = (s_4 - t_4)\sqrt{D}$ *and* $\mathrm{Stab}_{G_2(\mathbb{Q})}(A(x, 0)) \cong \mathrm{SL}_3$, *where* SL_3 *is embedded into* G_2 *as Section 6.2.2.*

   (b) $A_2 = A(x, t_3)$ *with* $\mathrm{Stab}_{G_2}(A_2) = \mathrm{SL}_2 V \subset \mathrm{SL}_3$, *where* SL_2 *and* V *embed into* SL_3 *as in Section 7.1.*

(c) $A_1 = A(x, s_3)$ *with* $\mathrm{Stab}_{G_2}(A_1) = \mathrm{SL}_2\overline{V} \subset \mathrm{SL}_3$, *where* SL_2 *is as in* (1)(*b*) *and* $\overline{V}$ *is the opposite unipotent subgroup to V.*

(d) $A_0 = A(x, s_1 + t_3)$ *with* $\mathrm{Stab}_{G_2}(A_0) = U_D$, *where* U_D *denotes the unipotent radical of the upper-triangular Borel of* SL_3 (*denoted by* U_{SL_3} *in Section 7.1*).

(2) *If D is not square in* $\mathbb{Q}^\times$:

(a) $A_1 = A(x, 0) \in \omega(\mathbb{Q})$, *for any* $x \neq 0$ *for which* $N(x) = -D$, *with*

$$\mathrm{Stab}_{G_2(\mathbb{Q})}(A(x, 0)) \cong \mathrm{SU}_3^D,$$

where $\mathrm{SU}_3^D = \mathrm{SU}(x^\perp)$ *is the unitary group for the restriction of the norm form to the three-dimensional* $\mathbb{Q}(\sqrt{D})$*-subspace of* $\mathbb{O}^0$ *orthogonal to* x.[1]

(b) $A_0 = A(x, z)$, *for any norm zero* z *in* $x^\perp$, *with* $\mathrm{Stab}_{G_2}(A_0) \simeq U_D$, *where* U_D *denotes the unipotent radical of the upper-triangular Borel of* SU_3^D.

Proof. Step 1. By [Rallis and Schiffmann 1989, Theorem 1], the group G_2 acts transitively on the set of trace zero elements of norm $-D$ and hence on the sets $A(x, 0)$. The description of the stabilizer in (1)(a) follows from [Jacobson 1958, Theorem 4] or [Rallis and Schiffmann 1989, Lemma 2]. The description of the stabilizer in (2)(a) follows from [Jacobson 1958, Theorem 3] or [Rallis and Schiffmann 1989, Lemma 3]. More precisely, according to [Rallis and Schiffmann 1989, Lemma 3] the subspace $x^\perp$ of $\mathbb{O}^0$ of elements which are orthogonal to x has the structure of a three-dimensional $\mathbb{Q}(\sqrt{D})$-vector space and the action of $\mathrm{Stab}_{G_2}(x)$ on $x^\perp$ induces an isomorphism $\mathrm{Stab}_{G_2}(x) \simeq \mathrm{SU}_3^D$.

Step 2. We now study the remaining G_2-orbits when D is a square in $\mathbb{Q}$. Again, we can assume that $D = 1$. Recall from Section 6.2.2 that SL_3 embeds into G_2 as the stabilizer of $s_4 - t_4$. This identification is explicitly given as follows (see [Rallis and Schiffmann 1989, Lemma 2]). An element of $g \in \mathrm{SL}_3$ induces an action on $\mathbb{O}^0$ fixing $s_4 - t_4$ and given by the left multiplication by g on $\langle s_1, s_2, s_3\rangle$ and by $(g^t)^{-1}$ on $\langle t_1, t_2, t_3\rangle$. One verifies that this actions respects multiplication and hence defines an element in G_2. Assume $z \neq 0$ is such that $A(x, z) \in \omega(\mathbb{Q})$. Since z is trace zero and orthogonal to $x = s_4 - t_4$ we can write $z = z_1 + z_2$ with $z_1 = \sum_i \alpha_i s_i$ and $z_2 = \sum_i \beta_i t_i$. Since the group SL_3 acts transitively on the nonzero elements of $\langle s_1, s_2, s_3\rangle$ and $\langle t_1, t_2, t_3\rangle$, then the cases where $z_1 = 0$ or $z_2 = 0$ give rise to exactly two orbits. When $z_1 = 0$, taking $z_2 = t_3$ as a generator of this orbit, the corresponding stabilizer is

$$\left\{\begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{pmatrix}\right\} \subset \mathrm{SL}_3,$$

which coincides with SL_2V as in (1)(b). Similarly, when $z_2 = 0$, taking $z_1 = s_3$ as the generator of the orbit, then the stabilizer is

$$\left\{\begin{pmatrix} * & * & 0 \\ * & * & 0 \\ * & * & 1 \end{pmatrix}\right\} \subset \mathrm{SL}_3.$$

[1] The unitary group SU_3^D is a form of SL_3 which splits over $\mathbb{Q}(\sqrt{D})$ and which is isomorphic to $\mathrm{SU}(2, 1)$ (resp. SL_3) if $D < 0$ (resp. $D > 0$) over $\mathbb{R}$.

This is nothing but $\mathrm{SL}_2\overline{V}$, with SL_2 which again embeds in the Levi of the long root parabolic P_a and $\overline{V}$ is the opposite unipotent subgroup to V generated by the negative roots $-a-3b$, $-2a-3b$. Finally we treat the case $z_1, z_2 \neq 0$. Write

$$z = \alpha_1 s_1 + \alpha_2 s_2 + \alpha_3 s_3 + \beta_1 t_1 + \beta_2 t_2 + \beta_3 t_3.$$

The condition $N(z) = 0$ translates then in

$$\alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 = 0. \tag{15}$$

We can assume that $z_2 = t_3$. Then $\alpha_3 = 0$ by (15) and, using the action of the stabilizer of t_3, we can assume that $z_1 = s_1$. It is then immediate to check that the stabilizer of $A(s_4 - t_4, s_1 + t_3)$ is as in (1)(d). This concludes the proof of (1).

Step 3. We finally deal with the case where D is not a square in $\mathbb{Q}$. By Witt's theorem, the group SU_3^D acts transitively on the isotropic vectors of the three-dimensional $\mathbb{Q}(\sqrt{D})$ vector space $x^\perp$. We thus have two orbits for $G_2(\mathbb{Q})$ on $\omega(\mathbb{Q})$, generated by $A(x, 0)$ and $A(x, z)$, where z is any nonzero vector in $x^\perp$ with zero norm. We are now left with calculating the stabilizer of the latter orbit. The action of SU_3^D on $x^\perp$ is given by its natural action on $\mathbb{Q}(\sqrt{D})^3$. More precisely, after extending scalars to $\mathbb{Q}(\sqrt{D})$, we can decompose

$$x^\perp \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D})\langle s_1, s_2, s_3\rangle \oplus \mathbb{Q}(\sqrt{D})\langle t_1, t_2, t_3\rangle.$$

The projection to the first component induces an isomorphism of $\mathbb{Q}(\sqrt{D})$-vector spaces

$$x^\perp \simeq \mathbb{Q}(\sqrt{D})\langle s_1, s_2, s_3\rangle$$

(see [Rallis and Schiffmann 1989, Lemma 3]), with SU_3^D acting naturally on the basis $\{s_1, s_2, s_3\}$. Here, we choose the Hermitian form (with respect to the extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$) defining SU_3^D given by

$$\begin{pmatrix} & & \sqrt{D}^{-1} \\ & 1 & \\ -\sqrt{D}^{-1} & & \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Q}(\sqrt{D})).$$

We can then suppose that z is sent to s_1 and the corresponding stabilizer is given by

$$\left\{\begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}\right\} \cap \mathrm{SU}_3^D = U_D. \qquad \square$$

7.3. ***Nonvanishing of Fourier coefficients, I.*** Recall that we have denoted by $\Pi = \bigotimes_v' \Pi_v$ the minimal representation of the group E_7. Moreover, in Section 6.3, for $f \in \Pi$ and $\varphi \in \mathcal{A}(G_2(\mathbb{Q})\backslash G_2(\mathbb{A}))$, we have defined the function $\Theta(f, \varphi)$ on $\mathrm{PGSp}_6(\mathbb{A})$ by

$$\Theta(f, \varphi)(g) = \int_{G_2(\mathbb{Q})\backslash G_2(\mathbb{A})} \theta(f)(g'g)\varphi(g')\, dg'. \tag{16}$$

For any $A \in J(\mathbb{Q})$ and $f \in \Pi$, consider the Fourier coefficient

$$\theta(f)_A(g) = \int_{N(\mathbb{Q})\backslash N(\mathbb{A})} \theta(f)(ng)\psi_A^{-1}(n)\, dn.$$

We then have the Fourier expansion (see [Harris et al. 2023, §A.3])

$$\theta(f)(g) = \theta(f)_0(g) + \sum_{A \in \Omega(\mathbb{Q})} \theta(f)_A(g), \tag{17}$$

where $\Omega(\mathbb{Q}) \subset J(\mathbb{Q})$ is the subset of rank-1 elements.

The following lemma will be used in the proof of Proposition 7.7. Its proof is similar to that of [Gross and Savin 1998, Lemma 4.6] but we give details for the convenience of the reader. Let A_0 be the representative of the open G_2-orbit on $\omega(\mathbb{Q})$ given in Proposition 7.5. Note that there is no harm in conjugating $A_0 \in J(\mathbb{Q})$ by an element of the Levi $\mathrm{GL}_3(\mathbb{Q})$ of the Siegel parabolic of PGSp_6. Thus, conjugating by $\mathrm{diag}(n, n, n)$, A_0 gets multiplied by n^2 and so we can assume that the entries x, y, z of A_0 are in $\mathbb{O}(\mathbb{Z})$.

Lemma 7.6. *Let S denote a finite number of places containing 2 and ∞, and let $f = \otimes'_v f_v \in \Pi$ be such that, for $v \notin S$, we have $f_v = f_v^0$, where f_v^0 denotes the spherical vector normalized such that $f_v^0(A_0) = 1$. Let $\mathbb{Q}_S = \prod_{v \in S} \mathbb{Q}_v$. If $g \in G_2(\mathbb{A})$, we write $g = g_S g^S$ where $g_S \in G_2(\mathbb{Q}_S)$ and $g^S \in \prod_{v \notin S} G_2(\mathbb{Q}_v)$. Then there exists a nonzero constant c_{A_0} such that for every $g \in G_2(\mathbb{A})$ we have*

$$\theta(f)_{A_0}(g) = c_{A_0} f_S(g_S^{-1} A_0) \prod_{v \notin S} \chi_v(g_v),$$

where $f_S = \bigotimes_{v \in S} f_v$ and χ_v is the characteristic function of $U_D(\mathbb{Z}_v)\backslash G_2(\mathbb{Z}_v)$.

Proof. By uniqueness of local functionals [Harris et al. 2023, Theorem A.4], there exists a nonzero scalar c_{A_0} such that, for any $g \in E_7(\mathbb{A})$, we have $\theta(f)_{A_0}(g) = c_{A_0}(\Pi(g)f)(A_0)$. For $g \in G_2(\mathbb{A})$ we have $(\Pi(g)f)(A_0) = f(g^{-1}A_0)$, where $g^{-1}A_0$ is the result of the natural action of g^{-1} on the off-diagonal entries of A_0. Hence $\theta(f)_{A_0}(g) = c_{A_0} f(g^{-1}A_0) = c_{A_0} \prod_v f_v(g_v^{-1}A_0)$ for $g \in G_2(\mathbb{A})$. Let us prove that for any $p \notin S$, we have $f_p(g_p^{-1}A_0) = \chi_p(g_p)$. So let $g_p \in G_2(\mathbb{Q}_p)$ be such that $f_p^0(g_p^{-1}A_0) \neq 0$ and let x', y', z' denote the off-diagonal entries of $g_p^{-1}A_0$. According to [Harris et al. 2023, Theorem A.5] the spherical vector f_p^0 is supported in $J(\mathbb{Z}_p)$. Hence $x', y', z' \in \mathbb{O}(\mathbb{Z}_p)$. Consider $\mathbb{O}(\mathbb{F}_p)$ the split octonion algebra over $\mathbb{F}_p$. The projections of (x, y, z) and (x', y', z') to $\mathbb{O}(\mathbb{F}_p)$ are $G_2(\mathbb{F}_p)$-conjugated by the proof of Step 1 in Proposition 7.5, which is still valid over the base field $\mathbb{F}_p$ as long as $p \neq 2$. It follows from Hensel's lemma that (x, y, z) and (x', y', z') are $G_2(\mathbb{Z}_p)$-conjugated. Therefore the function $g_p \mapsto f_p^0(g_p^{-1}A_0)$ is supported in $U_D(\mathbb{Z}_p)\backslash G_2(\mathbb{Z}_p) \subset U_D(\mathbb{Q}_p)\backslash G_2(\mathbb{Q}_p)$. Since f_p^0 is $G_2(\mathbb{Z}_p)$-invariant, for $g_p \in G_2(\mathbb{Z}_p)$ we have $f_p^0(g_p^{-1}A_0) = f_p^0(A_0) = 1$. This completes the proof. □

Proposition 7.7. *Let σ be a cuspidal automorphic representation of $G_2(\mathbb{A})$ as in Theorem 7.2 and let $\varphi \in \sigma^\vee$ be a cuspidal form. Then the following conditions are equivalent:*

(1) $\Theta(f, \varphi)_{U_P, \psi_D}(1) \neq 0$ *for some choice of f.*

(2) $\varphi^{U_D}(g) \neq 0$ *for some $g \in G_2(\mathbb{A})$.*

In particular, if any of the conditions holds then $\Theta(\sigma)$ is nonzero.

Proof. Recall first that, according to Proposition 5.7, we have $\Theta(f,\varphi)_{U_P,\psi_D}\neq 0$ if and only if $\Theta(f,\varphi)_{U_3,\alpha}\neq 0$ for some $\alpha\in\mathrm{Sym}^{\mathrm{rk}2}(3)(\mathbb{Q})$ with $\alpha\sim_{L(\mathbb{Q})}\alpha_D$. We write

$$\begin{aligned}\Theta(f,\varphi)_{U_3,\psi_D}(1)&=\int_{U_3(\mathbb{Q})\backslash U_3(\mathbb{A})}\Theta(f,\varphi)(u)\psi_D^{-1}(u)\,du\\&=\int_{G_2(\mathbb{Q})\backslash G_2(\mathbb{A})}\int_{U_3(\mathbb{Q})\backslash U_3(\mathbb{A})}\sum_{A\in\Omega(\mathbb{Q})}\theta(f)_A(ug)\varphi(g)\psi_D^{-1}(u)\,du\,dg,\end{aligned}$$

where in the second equality we used the definition (16) of $\Theta(f,\varphi)$ and the Fourier expansion (17) of $\theta(f)$. Since $U_3\subseteq N$, we have that $\theta(f)_A(ug)=\psi_A(u)\theta(f)_A(g)$ and

$$\int_{U_3(\mathbb{Q})\backslash U_3(\mathbb{A})}\psi_A(u)\psi_D^{-1}(u)=\begin{cases}\mathrm{vol}(U_3(\mathbb{Q})\backslash U_3(\mathbb{A})) & \text{if } \psi_D=\psi_A|_{U_3(\mathbb{A})},\\ 0 & \text{otherwise.}\end{cases}$$

Hence

$$\Theta(f,\varphi)_{U_3,\psi_D}(1)=\mathrm{vol}(U_3(\mathbb{Q})\backslash U_3(\mathbb{A}))\int_{G_2(\mathbb{Q})\backslash G_2(\mathbb{A})}\sum_{A\in\omega(\mathbb{Q})}\theta(f)_A(g)\varphi(g)\,dg. \tag{18}$$

Let $(A_i)_i$ be the finite representatives of the orbits of the action of $G_2(\mathbb{Q})$ on $\omega(\mathbb{Q})$ as given by Proposition 7.5, and write Stab_{A_i} for the stabilizers of A_i in G_2. The integral on the right-hand side of (18) becomes

$$\sum_i\int_{G_2(\mathbb{Q})\backslash G_2(\mathbb{A})}\sum_{g'\in\mathrm{Stab}_{A_i}(\mathbb{Q})\backslash G_2(\mathbb{Q})}\theta(f)_{A_i}(g'g)\varphi(g)\,dg=\sum_i\int_{\mathrm{Stab}_{\mathrm{A_i}}(\mathbb{Q})\backslash G_2(\mathbb{A})}\theta(f)_{A_i}(g)\varphi(g)\,dg.$$

Observe now that, by [Harris et al. 2023, Theorem A.4], we have $\theta(f)_{A_i}(g)=c_{A_i}f(g^{-1}A_i)$ for any $g\in G_2$. Hence, since $\mathrm{Stab}_{A_i}(\mathbb{A})$ fixes the matrix A_i, we deduce that the function $g\mapsto\theta(f)_{A_i}(g)$ is left $\mathrm{Stab}_{A_i}(\mathbb{A})$-invariant. Making an inner integration over $\mathrm{Stab}_{A_i}(\mathbb{Q})\backslash\mathrm{Stab}_{A_i}(\mathbb{A})$ in each term of the outer sum, we deduce that the above equals

$$\sum_i\int_{\mathrm{Stab}_{A_i}(\mathbb{A})\backslash G_2(\mathbb{A})}\theta(f)_{A_i}(g)\varphi^{\mathrm{Stab}_{A_i}}(g)\,dg,$$

where $\varphi^{\mathrm{Stab}_{A_i}}(g)$ denotes the period of φ over $\mathrm{Stab}_{A_i}(\mathbb{Q})\backslash\mathrm{Stab}_{A_i}(\mathbb{A})$. We now analyze two different possibilities. If D is not a square in $\mathbb{Q}$, then, by Proposition 7.5(2), $G_2(\mathbb{Q})$ acts on $\omega(\mathbb{Q})$ with two orbits, one closed and one open. Let A_0, A_1 denote representatives of these two orbits with stabilizers $\mathrm{Stab}_{A_0}=U_D$ and $\mathrm{Stab}_{A_1}=\mathrm{SU}_3^D$ in G_2. By the proof of Theorem 7.2, $\varphi^{\mathrm{SU}_3^D}(g)=0$, and hence the only surviving term is the one corresponding to the orbit represented by A_0. If D is a square in $\mathbb{Q}$, then by Proposition 7.5(1), $G_2(\mathbb{Q})$ acts on the set $\omega(\mathbb{Q})$ with four orbits, three closed and one open. Let A_i, $0\le i\le 3$ denote representatives of those orbits, with A_0 representing the open one. The corresponding stabilizers are U_D, SL_3, SL_2V and its conjugate $\mathrm{SL}_2\overline{V}$. By the proof of Theorem 7.2, we have $\varphi^{\mathrm{SL}_3}(g)=0$. By hypothesis σ (and $\sigma^\vee$) is not globally generic; hence Lemma 7.1 implies that $\varphi^{\mathrm{SL}_2V}(g)=\varphi^{\mathrm{SL}_2\overline{V}}(g)=0$. From this, we deduce that, for any D,

$$\Theta(f,\varphi)_{U_3,\psi_D}(1)=\int_{U_D(\mathbb{A})\backslash G_2(\mathbb{A})}\theta(f)_{A_0}(g)\varphi^{U_D}(g)\,dg, \tag{19}$$

where $\varphi^{U_D}(g)$ is the constant term of φ along U_D. This shows that if $\Theta(f,\varphi)_{U_3,\psi_D}(1)\neq 0$ then $\varphi^{U_D}\neq 0$ since the period appears as an inner integral of the Fourier coefficient.

We now show the converse, i.e., that if $\varphi^{U_D}\neq 0$ then, for some choice of $f\in\Pi$, the Fourier coefficient $\Theta(f,\varphi)_{U_3,\psi_D}$ does not vanish. Let S be as in Lemma 7.6. By enlarging S if necessary, we can assume that the cusp form φ is $G_2(\mathbb{Z}_v)$-invariant for all $v\notin S$. By Lemma 7.6, the integral of (19) equals

$$c_{A_0}\cdot\left(\int_{U_D(\mathbb{Q}_S)\backslash G_2(\mathbb{Q}_S)} f_S(g^{-1}A_0)\varphi^{U_D}(g)\,dg\right)\cdot\prod_{v\notin S}\mathrm{vol}(U_D(\mathbb{Z}_v)\backslash G_2(\mathbb{Z}_v),dg_v).$$

It remains to show that, when $\varphi^{U_D}\neq 0$, then for a good choice of f at the places in S, the integral satisfies

$$\int_{U_D(\mathbb{Q}_S)\backslash G_2(\mathbb{Q}_S)} f_S(g^{-1}A_0)\varphi^{U_D}(g)\,dg\neq 0.$$

It follows from [Harris et al. 2023, Theorem A.4] that f_S can be any smooth compactly supported function on $\Omega(\mathbb{Q}_S)$. Let $g_0\in G_2(\mathbb{Q}_S)$ be such that $\varphi^{U_D}(g_0)\neq 0$. We can take a nonnegative f supported in a sufficiently small neighborhood of g_0 to ensure the nonvanishing of the integral. This finishes the proof of the proposition. □

7.4. ***Nonvanishing of Fourier coefficients, II.*** The purpose of this section is to prove the following result.

Theorem 7.8. *Let F denote a quadratic étale algebra and $\sigma=\sigma_\infty\otimes\sigma_f$ be a cuspidal automorphic representation of $G_2(\mathbb{A})$ such that*

- *σ_∞ is a nongeneric discrete series with infinitesimal character $r\varepsilon_1+s\varepsilon_2$;*
- *there exists a finite prime p such that σ_p is Steinberg;*
- *the representation σ supports Fourier coefficient associated to the cubic algebra $\mathbb{Q}\times F$.*

The theta lift $\Theta(\sigma)=\otimes'_v\Theta(\sigma_v)$ is a nonzero cuspidal automorphic representation of $\mathrm{PGSp}_6(\mathbb{A})$. *Moreover, if π denotes any nonzero irreducible subquotient of $\Theta(\sigma)$, then*

- *π_∞ is a discrete series of infinitesimal character $\big(r,\tfrac12(r+s),\tfrac12(r-s)\big)$;*
- *π_p is Steinberg;*
- *the representation π supports a nontrivial Fourier coefficient of type* $(4\,2)$ *associated to F.*

Remark 7.9. As it will follow from the proof, the condition of σ_∞ being nongeneric can be replaced by σ not being locally generic, i.e., that there exists one local component of σ_v of σ which is not generic.

Let us first fix some notation first. Recall from Section 6.1.2 that the centralizer of G_2 in M is GL_3 and let

$$U_0=\left\{\begin{pmatrix}1&a&b\\0&1&0\\0&0&1\end{pmatrix}\right\}$$

be the unipotent radical of its Borel subgroup of upper triangular matrices. Note that the unipotent subgroup U_0U_3 is the unipotent radical of the parabolic subgroup P of PGSp_6 of Levi $\mathrm{GL}_2\times\mathrm{GL}_1^2$ appearing in Section 5.2.2.

Definition 7.10. Define the character $\psi_0 : U_0(\mathbb{Q})\backslash U_0(\mathbb{A}) \to \mathbb{C}^\times$ by sending

$$\psi_0(u) = e(a).$$

Note that $\psi_0\psi_D$ is the character (simply denoted by ψ_D) on $U_P(\mathbb{Q})\backslash U_P(\mathbb{A})$ introduced in Section 5.2.2.

As explained in Section 7.2, we view the space Ω of rank-1 elements in J inside $\overline{N}$ so that U_0 acts on Ω via the natural right action of $\mathrm{GL}_3 \subseteq M$ on $\overline{N}$. Then we let U_0 act on the left on ω and hence on the triples (x, y, z) of off-diagonal terms by the rule

$$u^{-1} \cdot (x, y, z) = (x + ay + bz, y, z). \tag{20}$$

7.4.1. *The relation between U_P and U_H.* In what follows, we relate the unipotent subgroup U_0 to the unipotent radical U_H of the Heisenberg parabolic. Such a relation will be employed in Proposition 7.13 to establish a relation between Fourier coefficients for the Heisenberg parabolic of G_2-cusp forms and Fourier coefficients of type $(4\,2)$ of their theta lifts.

Before stating our result, we make the following comments on the choice of representatives of the open orbits in Proposition 7.5. First, suppose that $D = d^2$, with $d \in \mathbb{Q}^\times$. There is no harm in assuming $d \in \mathbb{Z}$. Recall that the stabilizer in G_2 of the vector $s_4 - t_4$ can be identified with $\mathrm{SL}_3 = \mathrm{SL}(\langle s_1, s_2, s_3\rangle)$. Since the Heisenberg parabolic $H = L_H \cdot U_H$ is the stabilizer of the flag $\langle s_1, t_3\rangle$, its unipotent radical U_H contains $U_D = \mathrm{Stab}_{G_2}(A_0)$, where

$$A_0 = A(d(s_4 - t_4), s_1 - t_3, d(s_1 + t_3)) \in J(\mathbb{Z})$$

is the representative of the open orbit of the action of G_2 on $\omega(\mathbb{Q})$ as in Proposition 7.5. Moreover, U_H/U_D is two-dimensional and supported on the roots $a + b$ and $a + 2b$. Let us now suppose that D is not a square in $\mathbb{Q}^\times$. The vector $x = s_2 + Dt_2$ is a trace zero octonion of norm $-D$ and orthogonal to t_3. We choose the representative of the open orbit to be

$$A_0 = A(s_2 + Dt_2, s_1, t_3) \in J(\mathbb{Z}).$$

Lemma 7.11. *There is a natural surjection $p : U_H \to U_0$ inducing an isomorphism*

$$U_H/U_D \to U_0.$$

Proof. By the description of the action in (20) and the linear independence of the coordinates (x, y, z) of the representative of the open orbit, one sees that U_0 acts freely on it. Hence, the result follows from showing that any element in U_H acts on the triple (x, y, z) as an element of U_0 and vice versa.

Case 1. We start with the case where D is a square in $\mathbb{Q}^\times$. The action of U_0 is given by

$$u^{-1} \cdot (d(s_4 - t_4), s_1 - t_3, d(s_1 + t_3)) = (d(s_4 - t_4) + (a + db)s_1 + (db - a)t_3, s_1 - t_3, d(s_1 + t_3)). \tag{21}$$

Since any element of U_H fixes s_1 and t_3, it suffices to show that U_H acts on $(s_4 - t_4)$ as an element of U_0. We verify this by studying the action of the Lie algebra. By (13), we know that the Lie algebra of U_H is generated by the Lie algebra of the unipotent upper-triangular subgroup U_D in SL_3 and by the vectors v_1 and δ_3. Using the explicit action of the action of the Lie algebra given in Section 6.2.3, one checks that

$$E_{ij} \cdot (s_4 - t_4) = 0, \quad v_1 \cdot (s_4 - t_4) = s_1, \quad \delta_3 \cdot (s_4 - t_4) = t_3.$$

The above equations show that, for $u_1 = x_{a+b}(\lambda_1)$ and $u_2 = x_{a+2b}(\lambda_2)$ for some scalars λ_1, λ_2, we have

$$u_1 \cdot (d(s_4 - t_4)) = d(s_4 - t_4 + \lambda_1 s_1), \quad u_2 \cdot (d(s_4 - t_4)) = d(s_4 - t_4 + \lambda_2 t_3).$$

This gives the desired isomorphism: if $u \in U_H/U_D$ is identified with the product of $x_{a+b}(\lambda_1)x_{a+2b}(\lambda_2)$, then, from (21), we see that it gets sent to the element

$$\begin{pmatrix} 1 & \frac{1}{2}d(\lambda_1 - \lambda_2) & \frac{1}{2}(\lambda_1 + \lambda_2) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in U_0.$$

Case 2. We now suppose that D is not a square in $\mathbb{Q}^\times$. Similarly to Case 1, it suffices to calculate $u \cdot (s_2 + Dt_2)$ for any $u \in U_H$. As above, one checks that

$$E_{12} \cdot (s_2 + Dt_2) = s_1, \quad E_{23} \cdot (s_2 + Dt_2) = Dt_3, \quad E_{13} \cdot (s_2 + Dt_2) = 0,$$
$$v_1 \cdot (s_2 + Dt_2) = t_3, \quad \delta_3 \cdot (s_2 + Dt_2) = -Ds_1.$$

This implies that if $u \in V_H = U_H/[U_H, U_H]$ is equal to $x_a(\lambda_1)x_{a+b}(\lambda_2)x_{a+2b}(\lambda_3)x_{a+3b}(\lambda_4)$, then

$$u \cdot (s_2 + Dt_2) = s_2 + Dt_2 + (\lambda_1 - \lambda_3 D)s_1 + (\lambda_2 + D\lambda_4)t_3.$$

In particular, U_D embeds into U_H as the subgroup of matrices with $\lambda_1 = \lambda_3 D$ and $\lambda_2 = -\lambda_4 D$, and the map $p : U_H/U_D \to U_0$ sends u to the element

$$\begin{pmatrix} 1 & \lambda_1 - \lambda_3 D & \lambda_2 + \lambda_4 D \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in U_0. \qquad \square$$

Corollary 7.12. *Under the isomorphism $p : U_H/U_D \to U_0$, we have*

$$\psi_{H,D} = \psi_0 \circ p,$$

where $\psi_{H,D} : U_H(\mathbb{Q})\backslash U_H(\mathbb{A}) \to \mathbb{C}^\times$ is the character corresponding to the étale cubic algebra $\mathbb{Q} \times \mathbb{Q}(\sqrt{D})$.

Proof. We start with the case where D is a square in $\mathbb{Q}^\times$. For simplicity, we can (and do) assume that $D = 1$. From Lemma 7.11, if $n \in U_H/U_D$ is identified with the product of $x_{a+b}(\lambda_1)x_{a+2b}(\lambda_2)$, it is sent via p to

$$\begin{pmatrix} 1 & \frac{1}{2}(\lambda_1 - \lambda_2) & \frac{1}{2}(\lambda_1 + \lambda_2) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in U_0.$$

Hence, the character $\psi_0 \circ p : U_H(\mathbb{Q})\backslash U_H(\mathbb{A}) \to \mathbb{C}^\times$ sends $n \mapsto e\big(\frac{1}{2}(\lambda_1 - \lambda_2)\big)$. We now show that this corresponds to the character $\psi_{H,D}$ associated to $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$ as in Section 6.2.4. Recall that each character on $U_H(\mathbb{Q})\backslash U_H(\mathbb{A})$ is of the form $n \mapsto e(\langle w, \bar{n}\rangle)$, where $\bar{n}$ denotes the projection of n to $U_H/[U_H, U_H]$ and $w \in U_H(\mathbb{Q})/[U_H(\mathbb{Q}), U_H(\mathbb{Q})]$ corresponds to a binary cubic form

$$f_w(x, y) = \lambda_1 x^3 + \lambda_2 x^2 y + \lambda_3 x y^2 + \lambda_4 y^3,$$

with $\lambda_i \in \mathbb{Q}$. Furthermore, as $\bar{n} = x_a(\lambda'_1)x_{a+b}(\lambda'_2/3)x_{a+2b}(\lambda'_3/3)x_{a+3b}(\lambda'_4)$ corresponds to $f'(x, y) = \lambda'_1 x^3 + \lambda'_2 x^2 y + \lambda'_3 x y^2 + \lambda'_4 y^3$, the pairing is

$$\langle w, \bar{n}\rangle = \lambda_1\lambda'_4 - \tfrac{1}{3}\lambda_2\lambda'_3 + \tfrac{1}{3}\lambda_3\lambda'_2 - \lambda_4\lambda'_1.$$

Then, the character $\psi_0 \circ p$ corresponds to an element w_D for which $\lambda_1, \lambda_4 = 0$ and $\lambda_2, \lambda_3 = \frac{1}{2}$, namely the binary cubic polynomial $f_D(x, y) = \frac{1}{2}(x^2 y + x y^2)$. The latter is in the $L_H(\mathbb{Q})$-orbit corresponding to the cubic algebra $\mathbb{Q}^3$. Indeed, if we let $g = \left(\begin{smallmatrix} 2 & \\ & -2 \end{smallmatrix}\right) \in L_H(\mathbb{Q})$ act on f_D, we get

$$g \cdot f_D(x, y) = -\tfrac{1}{4} f_D(2x, -2y) = \tfrac{1}{8}(8x^2 y - 8x y^2) = x^2 y - x y^2,$$

which corresponds to $\mathbb{Q}^3$ by Example 6.1(1).

We now suppose that D is not a square in $\mathbb{Q}^\times$. Then, by Lemma 7.11, if

$$n \equiv x_a(\lambda_1)x_{a+b}(\lambda_2)x_{a+2b}(\lambda_3)x_{a+3b}(\lambda_4) \bmod [U_H, U_H],$$

the character $\psi_0 \circ p : U_H(\mathbb{Q})\backslash U_H(\mathbb{A}) \to \mathbb{C}^\times$ sends $n \mapsto e(\lambda_1 - \lambda_3 D)$. This character is associated to the binary cubic polynomial $f_D(x, y) = D x^2 y - y^3$, which corresponds to $\mathbb{Q} \times \mathbb{Q}(\sqrt{D})$ by Example 6.1(2). □

7.4.2. *Comparison of Fourier coefficients.* The following proposition can be paired with Proposition 7.7 to give three equivalent ways of proving that the theta lift of an automorphic representation of G_2 does not vanish.

Proposition 7.13. *Let σ be a cuspidal automorphic representation of $G_2(\mathbb{A})$ as in Theorem 7.2 and let $\varphi \in \sigma^\vee$ be a cuspidal form. The following conditions are equivalent*:

(1) $\Theta(f, \varphi)_{U_P,\psi_D}(1) \neq 0$ *for some choice of* $f \in \Pi$.

(2) $\varphi_{U_H,\psi_{H,D}}(g) \neq 0$ *for some* $g \in G_2(\mathbb{A})$.

In particular, if any of the conditions holds then $\Theta(\sigma)$ is nonzero.

Proof. Decomposing $U_P = U_0 U_3$, we have

$$\Theta(f, \varphi)_{U_P,\psi_D}(1) = \int_{U_0(\mathbb{Q})\backslash U_0(\mathbb{A})} \int_{U_3(\mathbb{Q})\backslash U_3(\mathbb{A})} \Theta(f, \varphi)(u u')\psi_D^{-1}(u')\psi_{U_0}^{-1}(u)\, du'\, du.$$

As in the proof of Proposition 7.7, this equals

$$\int_{U_0(\mathbb{Q})\backslash U_0(\mathbb{A})} \int_{U_D(\mathbb{A})\backslash G_2(\mathbb{A})} \theta(f)_{A_0}(u g)\varphi^{U_D}(g)\psi_{U_0}^{-1}(u)\, dg\, du.$$

Exchanging integrals and making an inner integration over $U_D(\mathbb{A})\backslash U_H(\mathbb{A})$, we get

$$\int_{U_H(\mathbb{A})\backslash G_2(\mathbb{A})} \int_{U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \left(\int_{U_0(\mathbb{Q})\backslash U_0(\mathbb{A})} \theta(f)_{A_0}(u u' g)\psi_{U_0}^{-1}(u)\, du \right) \varphi^{U_D}(u' g)\, du'\, dg.$$

The isomorphism $p : U_H/U_D \cong U_0$ of Lemma 7.11 induces

$$U_0(\mathbb{Q})\backslash U_0(\mathbb{A}) \cong U_H(\mathbb{Q})U_D(\mathbb{A})\backslash U_H(\mathbb{A})$$

such that $\psi_{H,D} = \psi_0 \circ p$ (see Corollary 7.12). Thus, we can write the integral as

$$\int_{U_H(\mathbb{A})\backslash G_2(\mathbb{A})} \int_{U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \left(\int_{U_H(\mathbb{Q})U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \theta(f)_{A_0}(uu'g)\psi_{H,D}^{-1}(u)\,du \right) \varphi^{U_D}(u'g)\,du'\,dg.$$

Exchanging integrals, we have

$$\begin{aligned}
&\int_{U_H(\mathbb{A})\backslash G_2(\mathbb{A})} \int_{U_H(\mathbb{Q})U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \left(\int_{U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \theta(f)_{A_0}(uu'g)\varphi^{U_D}(u'g)\,du' \right) \psi_{H,D}^{-1}(u)\,du\,dg \\
&\quad = \int_{U_H\backslash G_2(\mathbb{A})} \int_{U_H(\mathbb{Q})U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \left(\int_{U_H(\mathbb{Q})U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \sum_{\gamma \in U_D\backslash U_H(\mathbb{Q})} \theta(f)_{A_0}(u\gamma u'g)\varphi^{U_D}(\gamma u'g)\,du' \right) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cdot \psi_{H,D}^{-1}(u)\,du\,dg \\
&\quad = \int_{U_H\backslash G_2(\mathbb{A})} \int_{U_H(\mathbb{Q})U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \sum_{\gamma} \left(\int_{U_H(\mathbb{Q})U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \theta(f)_{A_0}(\gamma uu'g)\varphi^{U_D}(\gamma u'g)\,du' \right) \psi_{H,D}^{-1}(u)\,du\,dg
\end{aligned}$$

Changing variable $u' \mapsto u'' = \gamma uu' = u\gamma u''$ in the inner integral, the above becomes

$$\int_{U_H(\mathbb{A})\backslash G_2(\mathbb{A})} \int_{U_H(\mathbb{Q})U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \left(\int_{U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \theta(f)_{A_0}(u''g)\varphi^{U_D}(u^{-1}u''g)\,du'' \right) \psi_{H,D}^{-1}(u)\,du\,dg$$

which, after rearranging the integrals, is equal to

$$\int_{U_H(\mathbb{A})\backslash G_2(\mathbb{A})} \int_{U_D(\mathbb{A})\backslash U_H(\mathbb{A})} \theta(f)_{A_0}(u''g)\varphi_{U_H,\psi_{H,D}}(u''g)\,du''\,dg = \int_{U_D(\mathbb{A})\backslash G_2(\mathbb{A})} \theta(f)_{A_0}(g)\varphi_{U_H,\psi_{H,D}}(g)\,dg.$$

This shows that (1) implies (2). The proof of the converse is identical as the one given in Proposition 7.7. □

Proof of Theorem 7.8. Let σ be a cuspidal automorphic representation satisfying the hypotheses of the Theorem. We first apply Corollary 7.3 to deduce that $\Theta(\sigma)$ is cuspidal. Moreover, by Proposition 7.13, the theta lift supports a Fourier coefficient of type $(4\,2)$ and, in particular, it is nonzero. Let π be an irreducible subquotient of $\Theta(\sigma)$. Its component at p is the Steinberg representation by the compatibility between the global and local correspondences (Proposition 6.5) and by Proposition 6.10(2). We are now left to prove the statement on its archimedean component. As π is unitary, π_∞ is a unitarizable Harish-Chandra module by [Flath 1979, Theorem 4]. Moreover, as σ_∞ is a discrete series with infinitesimal character $r\varepsilon_1 + s\varepsilon_2$, it follows from the discussion in [Li 1997, p. 204] and by Table 1 on [Li 1999, p. 375] that $\Theta(\sigma_\infty)$ has infinitesimal character $\bigl(r, \tfrac{1}{2}(r+s), \tfrac{1}{2}(r-s)\bigr)$, which is strongly regular in the sense of [Salamanca-Riba 1999, Definition 1.5]. By another application of Proposition 6.5, π_∞ is a subquotient of $\Theta(\sigma_\infty)$, and hence has a strongly regular infinitesimal character. As a consequence, we can apply [Salamanca-Riba 1999, Theorem 1.8] to deduce that π_∞ is cohomological. By [Kret and Shin 2023, Corollary 2.8], since π_p is Steinberg and π_∞ is cohomological, π_∞ is a discrete series with infinitesimal character $\bigl(r, \tfrac{1}{2}(r+s), \tfrac{1}{2}(r-s)\bigr)$. □

Remark 7.14. Suppose that σ_∞ is a discrete series in $\mathcal{D}_{3,1}$. If $\Theta(\sigma_\infty)$ admits a unique irreducible quotient $\theta(\sigma_\infty)$, then by the results of [Li 1997], $\theta(\sigma_\infty)$ is a discrete series of Hodge type $(3, 3)$. This implies that $\pi_\infty = \theta(\sigma_\infty)$ is a discrete series of Hodge type $(3, 3)$. Although Howe duality conjecture for the pair (G_2, PGSp_6) is known at nonarchimedean places [Gan and Savin 2023], the conjecture is still open at the archimedean place.

8. The cycle class formula and the standard motive for G_2

We conclude this article with the arithmetic applications described in the introduction.

8.1. ***The relation between L-functions of G_2 and*** $\mathbf{PGSp_6}$**.** The dual group of G_2 is $G_2(\mathbb{C})$, which can be realized as the intersection $\mathrm{SO}_7(\mathbb{C}) \cap \mathrm{Spin}_7(\mathbb{C})$. More precisely, we have the commutative diagram

$$\begin{tikzcd}
G_2(\mathbb{C}) \arrow[r, hook] \arrow[d, hook, "\zeta"'] \arrow[rr, bend left, "\mathrm{Std}"] & \mathrm{SO}_7(\mathbb{C}) \arrow[r, hook] \arrow[d, hook] & \mathrm{GL}_7(\mathbb{C}) \arrow[d, hook] \\
\mathrm{Spin}_7(\mathbb{C}) \arrow[r, hook] \arrow[rr, bend right, "\mathrm{Spin}"'] & \mathrm{SO}_8(\mathbb{C}) \arrow[r, hook] & \mathrm{GL}_8(\mathbb{C})
\end{tikzcd} \tag{22}$$

where $\mathrm{Std} : G_2(\mathbb{C}) \to \mathrm{GL}(V_7)$ is the standard representation given by trace zero octonions, $\mathrm{Spin} : \mathrm{Spin}_7(\mathbb{C}) \to \mathrm{GL}(V_8)$ is the eight-dimensional spin representation, while the embedding ζ is defined from the fact that the stabilizer in $\mathrm{Spin}_7(\mathbb{C})$ of a generic vector of V_8 is isomorphic to $G_2(\mathbb{C})$. From the commutative diagram, one immediately sees that

$$V_{8|_{G_2}} = V_7 \oplus \mathbf{1}.$$

In particular, if π_ℓ is an unramified smooth representation of $\mathrm{PGSp}_6(\mathbb{Q}_\ell)$ with Satake parameter s_{π_ℓ} belonging to $\zeta(G_2(\mathbb{C}))$, then

$$L(s, \pi_\ell, \mathrm{Spin}) = L(s, \pi_\ell, \mathrm{Std})\zeta_\ell(s),$$

where

$$L(s, \pi_\ell, \mathrm{Std}) := \frac{1}{\det(1 - \ell^{-s}\,\mathrm{Std}(s_{\pi_\ell}))}$$

denotes the Euler factor at ℓ of the seven-dimensional standard L-function for G_2.

Let now π be a cuspidal automorphic representation of PGSp_6, which is unramified outside a finite set of places S containing the archimedean place. As a special case of Langlands functoriality, one expects that if $L^S(s, \pi, \mathrm{Spin})$ has a simple pole at $s = 1$, then π is a functorial lift from either G_2 or G_2^c, recalling that G_2^c denotes the form of G_2 which is compact at ∞ and split at all finite places of $\mathbb{Q}$. We invite the reader to consult [Ginzburg and Jiang 2001; Gan and Gurevich 2009; Pollack and Shah 2018; Gan and Savin 2020] for results in this direction. Moreover, the existence of a pole is usually related to the nonvanishing of a certain period. The following result,[2] summarizing and complementing known results in this direction, gives equivalence conditions for π to be a weak functorial lift from G_2.

Proposition 8.1. *Suppose that π satisfies the hypotheses* (DS) *and* (St) *of Section 2.7. Then π is tempered and the following statements are equivalent*:

(1) *The partial L-function $L^S(s,\pi,\mathrm{Spin})$ has a simple pole at $s=1$.*

(2) *For almost all ℓ, the Satake parameter $s_{\pi_\ell}\in\zeta(G_2(\mathbb{C}))$.*

(3) *There exists a cuspidal automorphic representation σ of either G_2 or G_2^c such that π is a weak functorial lift of σ.*

Moreover, *if π supports a Fourier coefficient of rank-2 associated to the quadratic extension F these conditions are equivalent to*

(4) *π is $\boldsymbol{H}$-distinguished*, *with $\boldsymbol{H}=\mathrm{GL}_2\boxtimes\mathrm{GL}_{2,F}^*$, i.e., that there exists a cusp form Ψ in π such that*

$$\int_{\mathbb{Z}(\mathbb{A})\boldsymbol{H}(\mathbb{Q})\backslash\boldsymbol{H}(\mathbb{A})}\Psi(h)\,dh\neq 0.$$

If one of the first three conditions hold, *the residue at $s=1$ of the partial L-function $L^S(s,\pi,\mathrm{Spin})$ is given by*

$$\mathrm{Res}_{s=1}L^S(s,\pi,\mathrm{Spin})=L^S(1,\sigma,\mathrm{Std})\prod_{\ell\in S}(1-\ell^{-1}).$$

Proof. Since π is cohomological and it is Steinberg at a finite place, we can apply [Kret and Shin 2023, Lemma 2.7] to deduce that π is essentially tempered at all places. As π has trivial central character, this is equivalent to being tempered. The equivalence between (2) and (3) and the implication (1) $\Longrightarrow$ (3) follow from [Gan and Savin 2020, Theorem 1.1]. By [Gan and Gurevich 2009, Proposition 5.2], if π is $\boldsymbol{H}$-distinguished then its big theta lift to G_2 is nonzero and is contained in the space of cusp forms on G_2. By the compatibility between the local and global theta correspondence, this implies that every local component π_v appears in the local theta correspondence. When v is a finite unramified place for π, [Gan and Gurevich 2009, Proposition 5.1] implies that $s_{\pi_v}\in\zeta(G_2(\mathbb{C}))$. This shows (4) $\Longrightarrow$ (3).

We next prove that (1) $\Longrightarrow$ (4), for which we'll use the hypothesis on the existence of a Fourier coefficient of rank-2. By [Pollack and Shah 2018, Theorem 2.7] (see Theorem 5.8), given a cusp form Ψ in π, there exists a cusp form $\widetilde{\Psi}$ and a Schwartz–Bruhat function Φ such that

$$\mathcal{I}(\Phi,\widetilde{\Psi},s)=\mathcal{I}_\infty(\Phi,\Psi,s)L^S(s,\pi,\mathrm{Spin}).$$

By Proposition 5.10, taking residues at $s=1$ on both sides we have

$$\frac{\widehat{\Phi}(0)}{2}\cdot\int_{\mathbb{Z}(\mathbb{A})\boldsymbol{H}(\mathbb{Q})\backslash\boldsymbol{H}(\mathbb{A})}\widetilde{\Psi}(h)\,dh=\mathrm{Res}_{s=1}\big(\mathcal{I}_\infty(\Phi,\Psi,s)L^S(s,\pi,\mathrm{Spin})\big),$$

[2] We point out that Proposition 8.1 is not really needed in the following (it is cited in the proof of Theorem 8.6, but only to show that the L-function of the lift from G_2 to PGSp_6 has a pole at $s=1$), but it might be of independent interest.

where $c > 0$ is the constant of Lemma 5.1. We now use [Gan and Gurevich 2009, Proposition 12.1] to deduce that there exists local data Φ_∞ and Ψ_∞ such that $\mathcal{I}_\infty(\Phi, \Psi, 1) \neq 0$. Hence, up to modifying Ψ and Φ at ∞, we obtain

$$\widehat{\Phi}(0) \cdot \int_{\mathbb{Z}(\mathbb{A})\boldsymbol{H}(\mathbb{Q})\backslash \boldsymbol{H}(\mathbb{A})} \widetilde{\Psi}(h)\,dh = C \cdot \mathrm{Res}_{s=1} L^S(s, \pi, \mathrm{Spin}),$$

with C a certain nonzero constant in $\mathbb{C}$. Note finally that we have the freedom to choose Φ such that $\widehat{\Phi}(0) \neq 0$. This follows from the fact that, given the two nonzero linear maps

$$l_1 : \mathcal{S}(\mathbb{A}^2) \to \mathbb{C},\ \Phi \mapsto \mathcal{I}_\infty(\Phi, \Psi, 1) \quad \text{and} \quad l_2 : \mathcal{S}(\mathbb{A}^2) \to \mathbb{C},\ \Phi \mapsto \widehat{\Phi}(0), \quad \ker(l_1) \cup \ker(l_2) \neq \mathcal{S}(\mathbb{A}^2).$$

This shows that if $L^S(s, \pi, \mathrm{Spin})$ has a simple pole and π supports a Fourier coefficient of rank 2, then π is $\boldsymbol{H}$-distinguished.

We finally show the implication (2) $\Longrightarrow$ (1). The commutative diagram (22) implies that

$$L^S(s, \pi, \mathrm{Spin}) = L^S(s, \pi, \mathrm{Std})\zeta^S(s),$$

where $L^S(s, \pi, \mathrm{Std})$ is the partial L-function of π associated to the standard seven-dimensional representation of Spin_7. By [Labesse and Schwermer 2019, Theorem 1.1.1], the restriction to $\mathrm{Sp}_6(\mathbb{A})$ of π contains a cuspidal automorphic representation $\pi^\flat$, such that (up to possibly enlarging S)

$$L^S(s, \pi, \mathrm{Std}) = L^S(s, \pi^\flat, \mathrm{Std}).$$

By [Kret and Shin 2023, Corollary 2.2 & Lemma 2.3], there exists a cuspidal automorphic representation $\pi^\sharp$ of $\mathrm{GL}_7(\mathbb{A})$ such that

$$L^S(s, \pi^\flat, \mathrm{Std}) = L^S(s, \pi^\sharp),$$

where $L^S(s, \pi^\sharp)$ denotes the standard L-function of $\pi^\sharp$. We claim that $L^S(1, \pi^\sharp) \neq 0$. By [Jacquet and Shalika 1976, Theorem (1.3)], $L(s, \pi^\sharp) \neq 0$ for any s with $\mathrm{Re}(s) = 1$. If we write

$$L^S(s, \pi^\sharp) = L(s, \pi^\sharp) \prod_{\ell \in S} L(s, \pi^\sharp_\ell)^{-1},$$

then our claim follows from the fact that each $L(s, \pi^\sharp_\ell)$ has no pole at $s = 1$ (see [Rudnick and Sarnak 1996, p. 317]). This implies that

$$L^S(1, \pi, \mathrm{Std}) \neq 0.$$

Thus, $L^S(s, \pi, \mathrm{Spin})$ has a simple pole at $s = 1$. This proves that (2) implies (1).

If now we assume (3), i.e., that π is a weak functorial lift of σ, then (up to possibly enlarging S)

$$L^S(1, \sigma, \mathrm{Std}) = L^S(1, \pi, \mathrm{Std}) \neq 0,$$

where the first equality is a consequence of the fact that the Satake parameters of σ and π agree almost everywhere. In particular

$$\mathrm{Res}_{s=1} L^S(s, \pi, \mathrm{Spin}) = L^S(1, \sigma, \mathrm{Std})\, \mathrm{Res}_{s=1} \zeta^S(s) = L^S(1, \sigma, \mathrm{Std}) \prod_{\ell \in S} (1 - \ell^{-1}),$$

showing the final claim. □

Remark 8.2. Let π be as in Corollary 5.12. Assuming (St), π is a weak functorial lift of σ as in Proposition 8.1 and Theorem 5.11 reads as

$$\langle \mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{H}}, [\omega_\Psi]\rangle_{\mathcal{H}} = C \cdot \mathcal{I}_S(\Phi, \Psi^{[\lambda,\mu]}, 1) \cdot \prod_{\ell \in S}(1-\ell^{-1}) \cdot L^S(1, \sigma, \mathrm{Std}).$$

8.2. ***Galois representations of G_2-type.*** The following result for the compact form of G_2 is shown in [Kret and Shin 2023, Theorem 11.1 and Corollary 11.3]. The same proof works for the split form of G_2 as long as one has some information on its lift to PGSp$_6$, and we only sketch it for the convenience of the reader.

Theorem 8.3. *Let σ be a cuspidal automorphic representation of $G_2(\mathbb{A})$ or $G_2^c(\mathbb{A})$ which lifts to a nonzero cuspidal automorphic representation π of $\boldsymbol{G}(\mathbb{A})$ such that*

- *π_∞ is cohomological,*
- *π_p is the Steinberg representation at some finite prime p.*

Then, for each prime ℓ and $\iota : \mathbb{C} \cong \overline{\mathbb{Q}}_\ell$, there exists a Galois representation $\rho_\sigma = \rho_{\sigma,\iota} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to G_2(\overline{\mathbb{Q}}_\ell)$ such that:

- *For every finite place $v \neq \ell$ where σ is unramified, ρ_σ is unramified at v. Moreover, the semisimple part of $\rho_\sigma(\mathrm{Frob}_v)$ is conjugate to the Satake parameter $\iota(s_{\sigma_v})$ in $G_2(\overline{\mathbb{Q}}_\ell)$.*
- *ρ_{σ_ℓ} is de Rham, and it is crystalline if σ is unramified at ℓ.*
- *$\zeta \circ \rho_\sigma = \rho_\pi$, where π is a theta lift of σ, and $\zeta : G_2(\mathbb{C}) \to \mathrm{Spin}_7(\mathbb{C})$ is the embedding appearing in* (22).
- *The Zariski closure of the image of ρ_σ maps onto either the image of a principal* SL$_2$ *in G_2 or onto G_2.*

Proof. By [Kret and Shin 2023, Theorem A], there exists a representation $\rho_\pi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Spin}_7(\overline{\mathbb{Q}}_\ell)$ attached to π. By the proof of [Kret and Shin 2023, Theorem 11.1], one has that the image of ρ_π is contained in $G_2(\overline{\mathbb{Q}}_\ell)$, and thus we have ρ_σ such that $\zeta \circ \rho_\sigma = \rho_\pi$ for a suitable choice of embedding $\zeta : G_2(\mathbb{C}) \to \mathrm{Spin}_7(\mathbb{C})$ fitting in the diagram (22). Hence, by [Kret and Shin 2023, Theorem A] and Proposition 6.10(1), the representation $\rho_\sigma : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to G_2(\overline{\mathbb{Q}}_\ell)$ satisfies the desired first three properties. Finally, by [Kret and Shin 2023, Theorem A(v)], the Zariski closure of ρ_π must map onto either a principal SL$_2$ in SO$_7 \cap$ G$_2$, or G_2. □

In the following proposition, we describe several cases where Theorem 8.3 applies. Before doing that, we need to introduce some notation. Let ω_1, ω_2 denote the two fundamental weights for G_2, where ω_1 is the highest weight of the standard representation and ω_2 of the fourteen-dimensional adjoint representation. According to our convention on the root system for G_2 in Section 6.2.1, $\omega_1 = a + 2b$ and $\omega_2 = 2a + 3b$.

Proposition 8.4. *Let σ be a cuspidal automorphic representation of $G_2^\circ(\mathbb{A})$ with $\circ \in \{\varnothing, c\}$ such that σ_∞ is a discrete series of infinitesimal character (r, s), where $r - 3 \geq s - 1 \geq 0$ and $r - s$ is even $\big($if $\circ = c$ then σ_∞ is the irreducible algebraic representation of $G_2^c(\mathbb{R})$ of highest weight $(s-1)\omega_1 + \frac{1}{2}(r-s-2)\omega_2\big)$ and σ_p is Steinberg at some finite place p. Suppose that one of the following conditions holds.*

(1) *We have $\circ = c$ and there exists $\alpha \in \sigma$ and a quaternion subalgebra D of the nonsplit octonions $\mathbb{O}^c$ such that*

$$P_\alpha^C := \int_{C(\mathbb{Q})\backslash C(\mathbb{A})} \alpha(v)\,dv \neq 0,$$

where C is the centralizer of D in G_2^c.

(2) *We have $\circ = \varnothing$ and either σ is globally generic or σ_∞ is nongeneric and σ supports a Fourier coefficient of type* (4 2) *corresponding to $\mathbb{Q} \times F$, where F is a real quadratic étale $\mathbb{Q}$-algebra.*

Then there exists a nontrivial small theta lift π of σ to $\boldsymbol{G}(\mathbb{A})$ which is a cuspidal automorphic representation, such that π_∞ is a discrete series with infinitesimal character $\bigl(r, \tfrac{1}{2}(r+s), \tfrac{1}{2}(r-s)\bigr)$ and π_p is Steinberg.

Proof. Let σ be as in assumption (1). Since the Steinberg representation is generic, then by [Gross and Savin 1998, Corollary 4.9] the big theta lift of σ to $\boldsymbol{G}(\mathbb{A})$ has a nontrivial cuspidal irreducible subquotient π, which is unramified at almost all places. The infinitesimal character of its archimedean component is given in [Gross and Savin 1998, Theorem 3.5], and by Propositions 6.5 and 6.10 we have that π_p is Steinberg. Under the assumption (2), if σ is globally generic, the result follows from [Harris et al. 2023, Theorem 1.7], and if σ_∞ is not generic and σ supports a Fourier coefficient as in the statement, the result follows from Theorem 7.8. □

By construction, the composition of the Galois representation ρ_π (and thus ρ_σ) with the spin representation appears in $H^6_{\text{ét}}(\mathrm{Sh}_{\boldsymbol{G},\overline{\mathbb{Q}}}, \mathcal{V}_\ell^\lambda(3))$, where the latter denotes the direct limit of the cohomology at level U in coefficients in the ℓ-adic lisse sheaf associated to an irreducible algebraic representation V^λ of $\boldsymbol{G}$, as U varies. This direct limit is a smooth admissible $\overline{\mathbb{Q}}_\ell$-representation of $\boldsymbol{G}(\mathbb{A}_f)$, endowed with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ commuting with the one of $\boldsymbol{G}(\mathbb{A}_f)$. Let σ and π be as in the statement of Theorem 8.3. Choose an embedding of the rationality field L of π in $\overline{\mathbb{Q}}_\ell$. Then by Lemma 2.8, the $\pi_f^\vee$-isotypic component of $H^6_{\text{ét},!}(\mathrm{Sh}_{\boldsymbol{G},\overline{\mathbb{Q}}}, \mathcal{V}_\ell^\lambda(3))$ is eight-dimensional $\overline{\mathbb{Q}}_\ell$-vector space, and we have

$$H^6_{\text{ét},!}(\mathrm{Sh}_{\boldsymbol{G},\overline{\mathbb{Q}}}, \mathcal{V}_\ell^\lambda(3))[\pi_f^\vee] = V_{\mathrm{Spin}\circ\rho_\pi} \otimes \pi_f^\vee = V_{\mathrm{Spin}\circ\zeta\circ\rho_\sigma} \otimes \pi_f^\vee.$$

If the image of ρ_σ is Zariski dense in $G_2(\overline{\mathbb{Q}}_\ell)$, we have $\mathrm{Spin}\circ\zeta\circ\rho_\sigma = \mathrm{Std}\circ\rho_\sigma \oplus \mathbf{1}$, where $\mathrm{Std}\circ\rho_\sigma$ is the irreducible "standard" Galois representation attached to σ. If not, by Theorem 8.3, the image of ρ_σ is Zariski dense onto a principal $\xi : \mathrm{SL}_2(\overline{\mathbb{Q}}_\ell) \to G_2(\overline{\mathbb{Q}}_\ell)$. Then the branching law of [Gross 2000, (7.1)] gives that $\mathrm{Spin}\circ\zeta\circ\rho_\sigma = \mathrm{Sym}^6\circ\rho_\sigma \oplus \mathbf{1}$, where $\mathrm{Sym}^6\circ\rho_\sigma$ is the irreducible symmetric sixth power Galois representation attached to σ. Denote by $M_\ell(\pi_f)$ the Galois representation $V_{\mathrm{Spin}\circ\rho_\pi}$ and let $M_\ell(\sigma_f)$ be either the Galois representation $V_{\mathrm{Std}\circ\rho_\sigma}$ or $V_{\mathrm{Sym}^6\circ\rho_\sigma}$. Then we have that $M_\ell(\sigma_f)^{G_\mathbb{Q}} = 0$ and $M_\ell(\pi_f)$ decomposes as the direct sum

$$M_\ell(\pi_f) = M_\ell(\sigma_f) \oplus \mathbf{1}, \tag{23}$$

where $\mathbf{1}$ denotes the one-dimensional trivial representation.

Remark 8.5. In the case where ρ_σ is not Zariski dense in $G_2(\overline{\mathbb{Q}}_\ell)$, the Satake parameter $s_{\sigma_p} \in \xi(\mathrm{SL}_2(\mathbb{C}))$ for any unramified prime p. By Langlands reciprocity principle, σ should be the functorial lift of a cuspidal automorphic representation τ of $\mathrm{PGL}_2(\mathbb{A})$, while $V_{\mathrm{Sym}^6\circ\rho_\sigma}$ should be a geometric realization of the motive of the symmetric sixth power of τ.

8.3. ***On a question of Gross and Savin.*** Tate conjecture predicts the existence of a cycle which gives rise to the trivial representation appearing in the decomposition of (23). Gross and Savin [1998], inspired by local computations, conjectured that this cycle should come from a Hilbert modular 3-fold inside $\mathrm{Sh}_{\boldsymbol{G}}$. Theorem 8.6 below supports this expectation for certain cuspidal automorphic representations σ of G_2 and G_2^c.

Let σ be a cuspidal automorphic representation of $G_2^\circ(\mathbb{A})$ with $\circ\in\{\varnothing, c\}$ such that σ_∞ is a discrete series of infinitesimal character (r, s) with $r-3\geq s-1\geq 0$ and $r-s$ even and σ_p is Steinberg at some finite place p and let π be the small theta lift of σ given by Proposition 8.4. Let V^λ denote an irreducible algebraic representation of $\boldsymbol{G}$ of highest weight $\lambda=\big(r-3, \frac{1}{2}(r+s)-2, \frac{1}{2}(r-s)-1, 0\big)$. Note that $V^\lambda|_{\boldsymbol{H}}$ contains the trivial representation by Lemma 3.2. Let $U\subset\boldsymbol{G}(\mathbb{A}_f)$ denote a neat compact open subgroup such that $\pi_f^U\neq 0$. For any $\frac{1}{2}(r+s)-2\geq\mu\geq\frac{1}{2}(r-s)-1$, let

$$\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\text{ét}} := \mathrm{cl}_{\text{ét}}(\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{M}}) \in \mathrm{H}^6_{\text{ét}}(\mathrm{Sh}_{\boldsymbol{G}}(\mathrm{U})_{\overline{\mathbb{Q}}}, \mathcal{V}^\lambda_\ell(3))^{\mathrm{G}_\mathbb{Q}}$$

be the étale realization of the motivic class $\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\mathcal{M}}$ (see Definition 3.9), where $\boldsymbol{H}=\mathrm{GL}_2\boxtimes\mathrm{GL}^*_{2,F}$. Fix a vector $\Psi_f\in\pi_f^U$. By composing the projection to the $\pi_f^\vee$-isotypic component together with the projection given by the vector Ψ_f, we get

$$\mathcal{Z}^{\sigma}_{\boldsymbol{H},\text{ét}} := \Psi_f(\mathrm{pr}_{\pi^\vee}(\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\text{ét}})) \in (M_\ell(\sigma_f)\oplus\mathbf{1})^{G_\mathbb{Q}}=\mathbf{1}.$$

By (the proof of) Lemma 2.8, there exists a cuspidal automorphic representation $\pi^{3,3}=\pi^{3,3}_\infty\otimes\pi_f$ of $\boldsymbol{G}(\mathbb{A})$ whose archimedean component is a discrete series of Hodge type (3, 3) with the same infinitesimal character of π_∞ and whose nonarchimedean part π_f is the same as the one of π. Let $\Psi=\Psi_\infty\otimes\Psi_f$ be the cusp form in the space of $\pi^{3,3}$ such that Ψ_∞ is a highest weight vector of the minimal K_∞-type of $\pi^{3,3}_{\infty,1}\subseteq\pi^{3,3}_\infty|_{\mathrm{Sp}_6(\mathbb{R})}$. For any μ as above, recall that we denote $\Psi^{[\lambda,\mu]}=A^{[\lambda,\mu]}\cdot\Psi_\infty\otimes\Psi_f$, where $A^{[\lambda,\mu]}$ is the operator that appeared in Proposition 4.8.

Theorem 8.6. *Assume that the integral $\mathcal{I}_S(\Phi, \Psi^{[\lambda,\mu]}, 1)$ is nonzero for some Schwartz–Bruhat function Φ. Then the class $\mathcal{Z}^\sigma_{\boldsymbol{H},ét}$ generates the trivial subrepresentation $\mathbf{1}$ of $M_\ell(\pi_f)$.*

Proof. By the comparison theorem between étale and Betti cohomology [SGA 4_3 1973, Exposé XI, Theorem 4.4(iii)], Proposition 8.1 and Corollary 5.12, we know that the projection $\mathrm{pr}_{\pi^\vee}\mathcal{Z}^{[\lambda,\mu]}_{\boldsymbol{H},\text{ét}}$ to $M_\ell(\pi_f)\otimes(\pi_f^U)^\vee$ generates a one-dimensional subspace, which is trivial for the action of the Galois group. As we have explained above, the image of ρ_σ is either dense in $G_2(\overline{\mathbb{Q}}_\ell)$ or in $\mathrm{SL}_2(\overline{\mathbb{Q}}_\ell)\to\mathrm{PGL}_2(\overline{\mathbb{Q}}_\ell)\hookrightarrow G_2(\overline{\mathbb{Q}}_\ell)$. In either case, the representation $M_\ell(\sigma_f)$ is irreducible and the trivial factor $\mathbf{1}$ in $M_\ell(\pi_f)$ is hence generated by the image of $\mathcal{Z}^\sigma_{\boldsymbol{H},\text{ét}}$. □

Acknowledgements

We would like to heartily thank David Ginzburg for sharing with us the proof of Lemma 7.1. We also thank Nadir Matringe, Aaron Pollack and Armando Gutierrez Terradillos for fruitful exchanges. We thank Marc-Hubert Nicole and Vincent Pilloni for comments on an earlier draft of the article. Finally, we thank the referee for a careful reading of the manuscript, comments and corrections which have significantly improved the content of this article.

References

[Ancona 2015] G. Ancona, "Décomposition de motifs abéliens", *Manuscripta Math.* **146**:3-4 (2015), 307–328. MR Zbl

[Beĭlinson 1986] A. A. Beĭlinson, "Notes on absolute Hodge cohomology", pp. 35–68 in *Applications of algebraic K-theory to algebraic geometry and number theory*, *I* (Boulder, CO, 1983), edited by S. J. Bloch et al., Contemp. Math. **55**, Amer. Math. Soc., Providence, RI, 1986. MR Zbl

[Blasius and Rogawski 1994] D. Blasius and J. D. Rogawski, "Zeta functions of Shimura varieties, II", pp. 525–571 in *Motives* (Seattle, WA, 1991), edited by U. Jannsen et al., Proc. Sympos. Pure Math. **55**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Borel 1980] A. Borel, "Stable and L^2-cohomology of arithmetic groups", *Bull. Amer. Math. Soc.* (*N.S.*) **3**:3 (1980), 1025–1027. MR Zbl

[Borel 1981] A. Borel, "Stable real cohomology of arithmetic groups, II", pp. 21–55 in *Manifolds and Lie groups* (Notre Dame, IN, 1980), edited by S. Murakami et al., Progr. Math. **14**, Birkhäuser, Boston, MA, 1981. MR Zbl

[Borel and Wallach 1980] A. Borel and N. R. Wallach, *Continuous cohomology*, *discrete subgroups*, *and representations of reductive groups*, Ann. of Math. Stud. **94**, Princeton Univ. Press, 1980. MR Zbl

[Burgos Gil et al. 2007] J. I. Burgos Gil, J. Kramer, and U. Kühn, "Cohomological arithmetic Chow rings", *J. Inst. Math. Jussieu* **6**:1 (2007), 1–172. MR Zbl

[Burgos Gil et al. 2024] J. I. Burgos Gil, A. Cauchi, F. Lemma, and J. Rodrigues Jacinto, "Tempered currents and Deligne cohomology of Shimura varieties, with an application to GSp_6", *Camb. J. Math.* **12**:4 (2024), 831–902. MR Zbl

[Cauchi and Rodrigues Jacinto 2020] A. Cauchi and J. Rodrigues Jacinto, "Norm-compatible systems of Galois cohomology classes for GSp_6", *Doc. Math.* **25** (2020), 911–954. MR Zbl

[Deligne 1971] P. Deligne, "Théorie de Hodge, II", *Inst. Hautes Études Sci. Publ. Math.* **40** (1971), 5–57. MR Zbl

[Deninger and Murre 1991] C. Deninger and J. Murre, "Motivic decomposition of abelian schemes and the Fourier transform", *J. Reine Angew. Math.* **422** (1991), 201–219. MR Zbl

[Flath 1979] D. Flath, "Decomposition of representations into tensor products", pp. 179–183 in *Automorphic forms*, *representations and L-functions*, *I* (Corvallis, OR, 1977), edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, RI, 1979. MR Zbl

[Fulton and Harris 1991] W. Fulton and J. Harris, *Representation theory: a first course*, Grad. Texts in Math. **129**, Springer, 1991. MR Zbl

[Gan 2005] W. T. Gan, "Multiplicity formula for cubic unipotent Arthur packets", *Duke Math. J.* **130**:2 (2005), 297–320. MR Zbl

[Gan and Gurevich 2009] W. T. Gan and N. Gurevich, "CAP representations of G_2 and the spin L-function of PGSp_6", *Israel J. Math.* **170** (2009), 1–52. MR Zbl

[Gan and Savin 2020] W. T. Gan and G. Savin, "An exceptional Siegel–Weil formula and poles of the Spin L-function of PGSp_6", *Compos. Math.* **156**:6 (2020), 1231–1261. MR Zbl

[Gan and Savin 2023] W. T. Gan and G. Savin, "Howe duality and dichotomy for exceptional theta correspondences", *Invent. Math.* **232**:1 (2023), 1–78. MR Zbl

[Gan et al. 2002] W. T. Gan, B. Gross, and G. Savin, "Fourier coefficients of modular forms on G_2", *Duke Math. J.* **115**:1 (2002), 105–169. MR Zbl

[Ginzburg 1993] D. Ginzburg, "On the standard L-function for G_2", *Duke Math. J.* **69**:2 (1993), 315–333. MR Zbl

[Ginzburg and Jiang 2001] D. Ginzburg and D. Jiang, "Periods and liftings: from G_2 to C_3", *Israel J. Math.* **123** (2001), 29–59. MR Zbl

[Ginzburg et al. 1997a] D. Ginzburg, S. Rallis, and D. Soudry, "On the automorphic theta representation for simply laced groups", *Israel J. Math.* **100** (1997), 61–116. MR Zbl

[Ginzburg et al. 1997b] D. Ginzburg, S. Rallis, and D. Soudry, "A tower of theta correspondences for G_2", *Duke Math. J.* **88**:3 (1997), 537–624. MR Zbl

[Gross 1998] B. H. Gross, "On the Satake isomorphism", pp. 223–237 in *Galois representations in arithmetic algebraic geometry* (Durham, 1996), edited by A. J. Scholl and R. L. Taylor, Lond. Math. Soc. Lect. Note Ser. **254**, Cambridge Univ. Press, 1998. MR Zbl

[Gross 2000] B. H. Gross, "On minuscule representations and the principal SL_2", *Represent. Theory* **4** (2000), 225–244. MR Zbl

[Gross and Lucianovic 2009] B. H. Gross and M. W. Lucianovic, "On cubic rings and quaternion rings", *J. Number Theory* **129**:6 (2009), 1468–1478. MR Zbl

[Gross and Savin 1998] B. H. Gross and G. Savin, "Motives with Galois group of type G_2: an exceptional theta-correspondence", *Compos. Math.* **114**:2 (1998), 153–217. MR Zbl

[Gross and Wallach 1994] B. H. Gross and N. R. Wallach, "A distinguished family of unitary representations for the exceptional groups of real rank $= 4$", pp. 289–304 in *Lie theory and geometry*, edited by J.-L. Brylinski et al., Progr. Math. **123**, Birkhäuser, Boston, MA, 1994. MR Zbl

[Gross and Wallach 1996] B. H. Gross and N. R. Wallach, "On quaternionic discrete series representations, and their continuations", *J. Reine Angew. Math.* **481** (1996), 73–123. MR Zbl

[Harris 1990] M. Harris, "Automorphic forms and the cohomology of vector bundles on Shimura varieties", pp. 41–91 in *Automorphic forms, Shimura varieties, and L-functions, II* (Ann Arbor, MI, 1988), edited by L. Clozel and J. S. Milne, Perspect. Math. **11**, Academic Press, Boston, MA, 1990. MR Zbl

[Harris 1997] M. Harris, "L-functions and periods of polarized regular motives", *J. Reine Angew. Math.* **483** (1997), 75–161. MR Zbl

[Harris et al. 2023] M. Harris, C. B. Khare, and J. A. Thorne, "A local Langlands parameterization for generic supercuspidal representations of p-adic G_2", *Ann. Sci. École Norm. Sup.* (4) **56**:1 (2023), 257–286. With an appendix by Gordan Savin. MR Zbl

[Huang et al. 1996] J.-S. Huang, P. Pandžić, and G. Savin, "New dual pair correspondences", *Duke Math. J.* **82**:2 (1996), 447–471. MR Zbl

[Ikeda 1994] T. Ikeda, "On the theory of Jacobi forms and Fourier–Jacobi coefficients of Eisenstein series", *J. Math. Kyoto Univ.* **34**:3 (1994), 615–636. MR Zbl

[Jacobson 1958] N. Jacobson, "Composition algebras and their automorphisms", *Rend. Circ. Mat. Palermo* (2) **7** (1958), 55–80. MR Zbl

[Jacquet 1972] H. Jacquet, *Automorphic forms on* GL(2)*, II*, Lecture Notes in Math. **278**, Springer, 1972. MR Zbl

[Jacquet and Shalika 1976] H. Jacquet and J. A. Shalika, "A non-vanishing theorem for zeta functions of GL_n", *Invent. Math.* **38**:1 (1976), 1–16. MR Zbl

[Jacquet and Shalika 1981] H. Jacquet and J. A. Shalika, "On Euler products and the classification of automorphic representations, I", *Amer. J. Math.* **103**:3 (1981), 499–558. MR Zbl

[Knapp 1986] A. W. Knapp, *Representation theory of semisimple groups: an overview based on examples*, Princeton Math. Series **36**, Princeton Univ. Press, 1986. MR Zbl

[Kobayashi and Savin 2015] T. Kobayashi and G. Savin, "Global uniqueness of small representations", *Math. Z.* **281**:1-2 (2015), 215–239. MR Zbl

[Kret and Shin 2023] A. Kret and S. W. Shin, "Galois representations for general symplectic groups", *J. Eur. Math. Soc.* **25**:1 (2023), 75–152. MR Zbl

[Labesse 1999] J.-P. Labesse, *Cohomologie, stabilisation et changement de base*, Astérisque **257**, Soc. Math. France, Paris, 1999. MR Zbl

[Labesse and Schwermer 2019] J.-P. Labesse and J. Schwermer, "Central morphisms and cuspidal automorphic representations", *J. Number Theory* **205** (2019), 170–193. MR Zbl

[Lemma 2017] F. Lemma, "On higher regulators of Siegel threefolds, II: The connection to the special value", *Compos. Math.* **153**:5 (2017), 889–946. MR Zbl

[Li 1997] J.-S. Li, "On the discrete spectrum of (G_2, PGSp_6)", *Invent. Math.* **130**:1 (1997), 189–207. MR Zbl

[Li 1999] J.-S. Li, "The correspondences of infinitesimal characters for reductive dual pairs in simple Lie groups", *Duke Math. J.* **97**:2 (1999), 347–377. MR Zbl

[Morel 2010] S. Morel, *On the cohomology of certain noncompact Shimura varieties*, Ann. of Math. Stud. **173**, Princeton Univ. Press, 2010. MR Zbl

[Piatetski-Shapiro and Rallis 1987] I. Piatetski-Shapiro and S. Rallis, "Rankin triple L functions", *Compos. Math.* **64**:1 (1987), 31–115. MR Zbl

[Pollack 2021] A. Pollack, "Modular forms on G_2 and their standard L-function", pp. 379–427 in *Relative trace formulas*, edited by W. Müller et al., Springer, 2021. MR Zbl

[Pollack and Shah 2018] A. Pollack and S. Shah, "The spin L-function on GSp_6 via a non-unique model", *Amer. J. Math.* **140**:3 (2018), 753–788. MR Zbl

[Rallis and Schiffmann 1989] S. Rallis and G. Schiffmann, "Theta correspondence associated to G_2", *Amer. J. Math.* **111**:5 (1989), 801–849. MR Zbl

[Rudnick and Sarnak 1996] Z. Rudnick and P. Sarnak, "Zeros of principal L-functions and random matrix theory", *Duke Math. J.* **81**:2 (1996), 269–322. MR Zbl

[Saito 1990] M. Saito, "Mixed Hodge modules", *Publ. Res. Inst. Math. Sci.* **26**:2 (1990), 221–333. MR Zbl

[Salamanca-Riba 1999] S. A. Salamanca-Riba, "On the unitary dual of real reductive Lie groups and the $A_g(\lambda)$ modules: the strongly regular case", *Duke Math. J.* **96**:3 (1999), 521–546. MR Zbl

[Schneider 1988] P. Schneider, "Introduction to the Beĭlinson conjectures", pp. 1–35 in *Beĭlinson's conjectures on special values of L-functions*, edited by M. Rapoport et al., Perspect. Math. **4**, Academic Press, Boston, MA, 1988. MR Zbl

[SGA 4_3 1973] M. Artin, A. Grothendieck, and J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 3: Exposés IX–XIX* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Math. **305**, Springer, 1973. MR Zbl

[Shin and Templier 2014] S. W. Shin and N. Templier, "On fields of rationality for automorphic representations", *Compos. Math.* **150**:12 (2014), 2003–2053. MR Zbl

[Sun 2017] B. Sun, "The nonvanishing hypothesis at infinity for Rankin–Selberg convolutions", *J. Amer. Math. Soc.* **30**:1 (2017), 1–25. MR Zbl

[Torzewski 2020] A. Torzewski, "Functoriality of motivic lifts of the canonical construction", *Manuscripta Math.* **163**:1-2 (2020), 27–56. MR Zbl

[Vogan and Zuckerman 1984] D. A. Vogan, Jr. and G. J. Zuckerman, "Unitary representations with nonzero cohomology", *Compos. Math.* **53**:1 (1984), 51–90. MR Zbl

[Waldspurger 1997] J.-L. Waldspurger, "Cohomologie des espaces de formes automorphes (d'après J. Franke)", exposé 809, pp. 139–156 in *Séminaire Bourbaki*, 1995/1996, Astérisque **241**, Soc. Math. France, Paris, 1997. MR Zbl

[Wallach 2003] N. R. Wallach, "Generalized Whittaker vectors for holomorphic and quaternionic representations", *Comment. Math. Helv.* **78**:2 (2003), 266–307. MR Zbl

[Wedhorn 2000] T. Wedhorn, "Congruence relations on some Shimura varieties", *J. Reine Angew. Math.* **524** (2000), 43–71. MR Zbl

Communicated by Wee Teck Gan
Received 2023-04-26 Revised 2024-01-25 Accepted 2024-04-29

cauchi.a.aa@m.titech.ac.jp *Deptartment of Mathematics, Tokyo Institute of Technology, Tokyo, Japan*

francesco.lemma@imj-prg.fr *Université Paris Cité, CNRS, IMJ–PRG, Paris, France*

joaquin.rodrigues-jacinto@univ-amu.fr *Aix–Marseille Université, Marseille, France*

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and 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

Volume 19 No. 3 2025