ON NON-ABELIAN HIGHER SPECIAL ELEMENTS OF $p$-ADIC REPRESENTATIONS

DANIEL MACIAS CASTILLO AND KWOK-WING TSOI

ABSTRACT. We develop a theory of ‘non-abelian higher special elements’ in the non-commutative exterior powers of the Galois cohomology of $p$-adic representations. We explore their relation to the theory of organising matrices and thus to the Galois module structure of Selmer modules. In concrete applications, we relate our general theory to the formulation of refined conjectures of Birch and Swinnerton-Dyer type and to the Galois structure of Tate-Shafarevich and Selmer groups of abelian varieties.

1. INTRODUCTION

1.1. The general theory. Before discussing the main objects of study in this article we must recall the theory of organising matrices.

1.1.1. Organising matrices. In the study of the classical (commutative) Iwasawa theory of elliptic curves, Mazur and Rubin first suggested in [25] the possibility of a theory of ‘organising modules’ as a means of encoding detailed arithmetic information in a single matrix. A little later, Mazur and Rubin [28] successfully associated (under certain hypotheses) such matrices to the corresponding Selmer complexes that were introduced by Nekovář in [31]. Subsequently, Burns and the first author [11] have both refined, and extended, this theory, in a way which associates a canonical family of ‘organising matrices’ to general $p$-adic representations, considered with general (non-abelian) coefficients.

To be a little more precise, let $F/k$ be a finite Galois extension of global fields with Galois group $G$ and let $p$ be a prime number. Then to any $p$-adic Galois representation $T$ defined over $k$ one may associate certain étale cohomology complexes of $\mathbb{Z}_p[G]$-modules. These complexes are often ‘admissible’ in the sense of loc. cit. (see also §2.1.1 below) and in any such cases can be assigned a canonical family of organising matrices, with entries in $\mathbb{Z}_p[G]$, which encode a wide range of detailed information concerning the arithmetic of $T$ over $F/k$. 
In this article we will give a generalisation of the construction of organising matrices. In addition, we will clarify their relationship to the theory of non-commutative higher Fitting invariants that has recently been developed by Burns and Sano [16]. In this way we obtain a refinement of one of the main algebraic results (Corollary 3.3) of [11]. See §3.3 below for more details.

1.1.2. Non-abelian higher special elements. In the commutative setting Burns, Sano and the second author [17] have recently developed a theory of ‘higher special elements’ as a generalisation of the notion of higher rank Euler systems. Such elements are also associated to admissible complexes in the sense of [11] and live in the higher exterior powers of the cohomology modules of the complexes. We recall that in arithmetic applications these modules are thus strictly related to the Galois cohomology of $p$-adic representations.

Burns and Sano [16] have also recently defined a natural notion of non-commutative higher rank Euler systems for $p$-adic representations $T$, relative to arbitrary Galois extensions of a number field over which $T$ is defined. They have then proved, under mild hypotheses, the existence of such non-commutative Euler systems whose rank depends explicitly on $T$.

The importance of this development is supported by, among other factors, a growing interest in the study of leading term conjectures that are relevant to non-abelian Galois extensions. These include the equivariant Tamagawa number conjecture of Burns and Flach [8], the non-commutative Tamagawa number conjecture of Fukaya and Kato [20], the main conjecture of non-commutative Iwasawa theory for elliptic curves without complex multiplication of Coates, Fukaya, Kato, Sujatha and Venjakob [18], the non-abelian Brumer-Stark conjectures formulated independently by Burns [7] and by Nickel [33], or the recent formulation of a refined conjecture of Birch and Swinnerton-Dyer type by Burns and the first author [12].

In order to arrive at the relevant notion of non-commutative higher rank Euler systems, Burns and Sano [16] have also recently developed an algebraic theory of non-commutative exterior powers. The main objective of this article is to use this theory in order to define a completely general notion of ‘non-abelian higher special element’. The theory of non-commutative exterior powers comes naturally equipped with canonical duality pairings and our definition gives a direct relationship between the images of non-abelian higher special elements under these pairings and the reduced norms of the corresponding organising matrices.

By exploiting our understanding of the properties of organising matrices we are therefore able to prove that non-abelian higher special elements satisfy strong integrality properties and also encode delicate information regarding the Galois structure of Selmer modules of $p$-adic representations. These are the contents of our main algebraic result, given below as Theorem 5.1.

In this way, we hope to contribute to the future study of non-commutative higher rank Euler systems and of general leading term conjectures.

We emphasise that, exactly as in the commutative case considered in [17], our construction of higher special elements does not depend on fixing ‘separable’ tuples of elements (in the highest degree cohomology modules of admissible complexes) but rather arises from arbitrary choices of tuples. This fact makes potential arithmetic
applications of our theory significantly finer than any specialisations currently present in the literature. The degree of generality of our algebraic methods allows for subsequent applications in a wide range of natural arithmetic settings, including to the compact support cohomology complexes, the finite support cohomology complexes in the sense of Bloch and Kato [4] and the Nekovář-Selmer complexes, that arise from very general $p$-adic representations.

In this article we will however only focus on applications to certain classes of Selmer complexes associated to abelian varieties (see §2.2 below). Before discussing these applications let us however mention other settings in which our algebraic results will play a significant role in future work.

1.2. Arithmetic applications.

1.2.1. Refined Stark conjectures. In work in progress of Burns, Seo and the first author [13], our main algebraic result will be applied to the study of refined Stark conjectures and of the annihilation of ideal class groups by higher derivatives at $z = 0$ of Artin $L$-functions. A little more specifically, our main result will motivate the definition of canonical lattices of ‘non-abelian higher Stickelberger elements’, and lead to the prediction that all such elements should provide integral annihilators of suitable ideal class groups. These predictions will be shown to hold unconditionally in the setting of global function fields.

Let us also note that such predictions will significantly extend and refine the non-abelian Brumer-Stark conjectures due to Burns [7] and to Nickel [33]. In addition, in future work, we will also apply our algebraic results to study the annihilation of both suitable higher $K$-groups, and of wild kernels in higher $K$-theory, by higher derivatives at integer values of Artin $L$-functions. We aim to extend the constructions of conjectural annihilators of such modules that are carried out by Nickel in [34, 35].

1.2.2. Refined conjectures of Birch and Swinnerton-Dyer type. Burns and the first author [12] have formulated a completely general ‘refined Birch and Swinnerton-Dyer conjecture’ (or ‘refined BSD conjecture’ in the sequel) for the Hasse-Weil-Artin $L$-series associated to an abelian variety $A$ defined over a number field $k$ and to a finite Galois extension $F$ of $k$.

This conjecture is equivalent to the relevant case of the equivariant Tamagawa number conjecture and is thus also compatible with the main conjecture of non-commutative Iwasawa theory formulated by Coates et al. in [18]. Its formulation relies on a construction of canonical Nekovář-Selmer complexes associated to choices of semi-local points on $A$. Under certain hypotheses, it may also be reformulated in terms of ‘classical Selmer complexes’ that are closely related to the finite support cohomology that was introduced by Bloch and Kato in [4].

In [12] §8, assuming that $F/k$ is abelian, Burns and the first author then study the congruence relations between the values at $z = 1$ of higher derivatives of Hasse-Weil-Artin $L$-series, as well as their relation to the Galois structure of the Tate-Shafarevich and Selmer groups of $A$ over $F$, that are encoded in the refined BSD conjecture. (Both
in loc. cit and in the sequel, it is always assumed that the relevant Tate-Shafarevich are finite.)

Our algebraic results will now allow us to extend this study to general finite Galois
extensions $F/k$. In particular, in Theorem 6.1 and the remarks that follow it, we will obtain an explicit description of the predictions that are encoded in the refined BSD conjecture in the general case. We are hopeful that it may be possible in the future to numerically test such predictions in non-abelian examples.

In §6.2 we then specifically consider (generalised) dihedral twists of elliptic curves over general number fields. By combining our approach with a result of Mazur and Rubin we are able to obtain strikingly explicit predictions for the derivatives of Hasse-Weil-Artin $L$-series of such twists, as we briefly discuss in the next section.

1.2.3. Tate-Shafarevich groups of dihedral twists of elliptic curves. Let $A$ be an elliptic curve and let $F/k$ be generalised dihedral, in the sense of [29], of degree $2p^n$, say. Assume that $F/k$ is unramified at all places of $k$ at which $A$ has bad reduction. Let $K/k$ be the corresponding quadratic subextension of $F/k$, and assume that all $p$-adic places of $k$ split completely in $K/k$ and that the rank of $A(K)$ is odd. In this setting, we first derive from the work of Mazur and Rubin in loc. cit. the existence of a point $Q$ in $A(F)$ on which $\text{Gal}(F/k)$ acts in a specific manner.

Moreover, claim (ii) of Theorem 6.2 below (in combination with Theorem 6.1) gives a generalisation of the predictions studied by Burns, Wuthrich and the first author in [15, Thm. 5.8]. Namely we show that if the refined BSD conjecture is valid, then the derivatives of Hasse-Weil-Artin $L$-series, normalised by Néron-Tate heights associated to such a point $Q$, provide integral annihilators of the $p$-primary Tate-Shafarevich group $X(A_F)[p^\infty]$ of $A$ over $F$. We recall that, in addition to various other additional hypotheses, the group $\text{III}(A_F)[p^\infty]$ was assumed to vanish in [15, Thm. 5.8], and $A(K)$ was assumed to have rank equal to 1.

These predictions may be rendered strikingly explicit in many cases of interest and in various levels of generality.

Examples 1.1.

(i) By imposing some of the additional hypotheses of [15, Thm. 5.8], but still without forcing the vanishing of $\text{III}(A_F)[p^\infty]$, we are led in claim (iii) of Theorem 6.2 below to predict that the elements $Q_\psi$ that occur in [15, Thm. 5.8] (but constructed using our chosen point $Q$), as $\psi$ ranges over the irreducible complex character of $\text{Gal}(F/k)$, combine to provide integral annihilators of $\text{III}(A_F)[p^\infty]$.

(ii) As a concrete example of the discussion in the above paragraph, in Example 6.7 below we explain how further specialisation leads to conjectural annihilation predictions for the elements $Q_\psi$ corresponding to ‘higher Heegner points’ $Q$ in (generalised) dihedral extensions $F$ of $Q$ that contain an imaginary quadratic field.

(iii) In a different direction, Christian Wuthrich kindly supplied us with the following concrete applications of Theorem 6.2. Set $k = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{229})$ and write $F$ for the Galois closure of the field $L = \mathbb{Q}(\alpha)$ with $\alpha^3 - 4\alpha + 1 = 0$. Then $K \subset F$ and the group $G := \text{Gal}(F/\mathbb{Q})$ is dihedral of order six. Let $A$ denote either of the curves 3928b1 (with equation $y^2 = x^3 - x^2 + x + 4$) or 5864a1 (with equation $y^2 = x^3 - x^2 - 24x + 28$). Then $\text{rk}(A_Q) = 2$, $\text{rk}(A_K) = 3$ and $\text{rk}(A_L) = 3$ while $\text{III}(A_K)[3^\infty]$ vanishes. These facts combine with [14, Cor. 2.10(i)] to imply the $\mathbb{Z}_3[G]$-module $\mathbb{Z}_3 \otimes_2 A(F)$ is
isomorphic to
\[ Z_3[G](1 - \delta) \oplus Z_3 \oplus Z_3, \]
with \( \delta \) the unique non-trivial element in \( \text{Gal}(F/L) \). We let \( Q \) be the image of \((1 - \delta, 0, 0)\) under any such isomorphism. We also fix a non-trivial element \( \gamma \) of \( \text{Gal}(F/K) \) and then define elements \( T := 1 + \gamma + \gamma^2 \) and \( U := 2 - \gamma - \gamma^2 \) of \( \mathbb{Z}[G] \).

Then Theorem 6.2(ii) and Theorem 6.1 combine with the computation of ‘logarithmic resolvents’ carried out in [12, Prop. 8.11] to imply that, if the refined BSD conjecture is valid for \( A \) and \( F/\mathbb{Q} \), then the product
\[
\beta \cdot (\Omega_A)^{-1} \cdot \tau^*(F/\mathbb{Q}) \cdot \left( \frac{L'_\epsilon(A, A, 1)}{2(T(Q), T(Q))_{A_F}} \cdot (1 - \delta) T + 3 \frac{L'_\epsilon(A, \phi, 1)}{(U(Q), U(Q))_{A_F}} \cdot U \right)
\]
belongs to \( Z_3[G] \) and annihilates \( \text{III}(A_F)[3^\infty] \).

Here \( \beta \) is any choice of element of the ‘ideal of denominators’ associated to the order \( Z_3[G] \) by Burns and Sano [16, Def. 3.4]. Note also that the computations carried out by Johnston and Nickel [22, §6.4] easily lead to explicit choices of \( \beta \).

In addition \( \Omega_A \) is the complex period of \( A \), \( \tau^*(F/\mathbb{Q}) \) is the global Galois-Gauss sum of \( F/\mathbb{Q} \) defined in [12, §4.2.1], \( \epsilon \) is the sign character of \( G \) and \( \phi \) is the irreducible character of \( G \) of dimension 2,
\[ S = \{2, 3, 229, \ell\} \]
with \( \ell = 491 \) if \( A \) is 3928b1 or with \( \ell = 733 \) if \( A \) is 5864a1 and both values at 1 of derivatives are of the corresponding \( L \)-functions truncated by removing the Euler factors of primes in \( S \). Further \( \langle \cdot, \cdot \rangle_{A_F} \) denotes the Néron-Tate height pairing of \( A \) defined relative to \( F \).

1.3. Structure of the article. In §2 we shall first recall the definition of the category of admissible complexes from [11, and then also the construction of the specific admissible arithmetic complexes from [12 that will be relevant to our applications (as described in §1.2.2).

In §3 we then introduce the notion of a characteristic element, recall the theory of non-commutative Fitting invariants of Burns and Sano [16, and describe important links between both notions through a generalised construction of organising matrices that we give in §3.3.

In §4 we define our notion of non-abelian higher special elements after briefly recalling the theory of non-commutative exterior powers of Burns and Sano [16]. As a preliminary step for the study of their finer integrality properties, we prove in §4.3 that these elements are rational in a natural sense.

In §5 we first state our main algebraic result together with two additional corollaries. We then proceed to prove our main result in the rest of the section.

In §6 we finally discuss the applications of our general theory to the arithmetic of abelian varieties, as outlined in §1.2.2 and §1.2.3.

1.4. General notation. For any ring \( R \) we write \( Z(R) \) for its centre. Unless otherwise specified we regard all \( R \)-modules as left \( R \)-modules.

We write \( D(R) \) for the derived category of complexes of \( R \)-modules. If \( R \) is noetherian, then we write \( D^p(R) \) for the full triangulated subcategory of \( D(R) \) comprising
complexes that are ‘perfect’ (that is, isomorphic in $D(R)$ to a bounded complex of finitely generated projective $R$-modules).

For an abelian group $M$ we write $M_{\text{tor}}$ for its torsion submodule and set $M_{tf} := M/M_{\text{tor}}$, which we regard as embedded in the associated space $\mathbb{Q} \otimes_{\mathbb{Z}} M$.

For a prime $p$ and natural number $n$ we write $M[p^n]$ for the subgroup $\{ m \in M : p^n m = 0 \}$ of the Sylow $p$-subgroup $M[p^\infty]$ of $M_{\text{tor}}$. We set $M_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} M$ and write $M_p^\wedge$ for the pro-$p$ completion of $M$.

If $G$ is a finite group we write $\text{Ir}(G)$ for the set of irreducible complex characters of $G$. For a $G$-module $M$ we write $M^\vee$ for the Pontryagin dual of $M$, endowed with the natural contragredient action of $G$.

1.5. FUNDING. The first author acknowledges financial support from grants CEX2019-000904-S and PID2019-108936GB-C21 funded by MCIN/AEI/10.13039/501100011033.

1.6. ACKNOWLEDGEMENTS. The authors are very grateful to David Burns for many interesting discussions, his generous encouragement, and some helpful comments on an earlier version of the article.

The first author is also very grateful to Cornelius Greither, Henri Johnston, Andreas Nickel, Takamichi Sano, Stefano Vigni and Christian Wuthrich for many helpful conversations and correspondence. We particularly thank Andreas Nickel for pointing out a mistake in an earlier version of the proof of Lemma 4.5.

2. PRELIMINARIES

In this section we recall the category of admissible complexes and discuss specific arithmetic examples of such complexes that will play a key role in the sequel.

2.1. Admissible complexes. We first introduce the categories of complexes to which our main algebraic results apply. To do this we fix a Dedekind domain $R$ of characteristic 0 with field of fractions $\mathcal{F}$, a finite group $G$ and an $R$-order $\mathfrak{A}$ that spans a direct factor $A := \mathcal{F} \otimes_R \mathfrak{A}$ of the group ring $\mathcal{F}[G]$.

2.1.1. The category of admissible complexes. We write $D^a(\mathfrak{A})$ for the full subcategory of $D^p(\mathfrak{A})$ comprising complexes $C = (C^i)_{i \in \mathbb{Z}}$ which satisfy the following four assumptions:

- (ad$_1$) $C$ is an object of $D^p(\mathfrak{A})$;
- (ad$_2$) the Euler characteristic of $A \otimes_{\mathfrak{A}} C$ in the Grothendieck group $K_0(A)$ vanishes;
- (ad$_3$) $C$ is acyclic outside degrees one and two;
- (ad$_4$) $H^1(C)$ is $R$-torsion-free.

In the sequel we will refer to an object of $D^a(\mathfrak{A})$ as an ‘admissible complex of $\mathfrak{A}$-modules’.

Remark 2.1. In the case that $G$ is abelian, the category $D^a(\mathfrak{A})$ plays a key role in the theory of higher special elements developed by Burns, Sano and the second author in [17]. However, we caution the reader that there is a slight difference of terminology in that objects of the category $D^a(\mathfrak{A})$ defined above are in loc. cit. referred to as ‘strictly admissible’ complexes. In the general case, the category $D^a(\mathfrak{A})$ provided the
setting for the theory of organising matrices developed by Burns and the first author in [11].

Example 2.2. Write \( \iota_\# \) for the \( R \)-linear anti-involution on \( R[G] \) that satisfies \( \iota_\#(g) = g^{-1} \) for all \( g \) in \( G \). Then for any idempotent \( e \) of \( Z(R[G]) \) which is fixed by \( \iota_\# \) the algebra \( \mathfrak{A} := R[G]e \) is Gorenstein (in the sense of [11] \( \S 2.1.2 \)), and with respect to the anti-involution that is obtained by restricting \( \iota_\# \). In particular, the universal coefficient spectral sequence implies that the functor \( C \mapsto C^*[-3] \) preserves the category \( D^b(\mathfrak{A}) \).

2.1.2. Annihilation idempotents. If \( C \) is an object of \( D^b(\mathfrak{A}) \), then we write \( e_0 = e_0(C) \) for the sum over all primitive idempotents of \( Z(A) \) that annihilate the module \( H^1(A \otimes_\mathfrak{A} C) \). We note that the conditions (\( \text{ad}_2 \)) and (\( \text{ad}_3 \)) combine to imply that \( H^1(A \otimes_\mathfrak{A} C) \cong H^2(A \otimes_\mathfrak{A} C) \). We use identical notation for complexes that satisfy (\( \text{ad}_1 \))-(\( \text{ad}_3 \)) but do not satisfy the condition (\( \text{ad}_4 \)).

2.2. Arithmetic examples. For brevity we only discuss the specific arithmetic examples of admissible complexes that will be relevant to the applications of the general theory that will be given in this article. We refer the reader to both [11] \( \S 2.2 \) and [17] \( \S 2.2 \) for general discussions of how ubiquitous admissible complexes are in arithmetic. In particular, both the Weil-étale cohomology complexes of the multiplicative group, and the étale cohomology complexes of cyclotomic representations, that are defined and studied by Burns, Kurihara and Sano in [9] and in [10] respectively, constitute a source of natural and arithmetically significant admissible complexes. Considering our algebraic theory in these instances will lead to important arithmetic applications that will be developed in detail in future work, as mentioned in the introduction.

2.2.1. Nekovář-Selmer complexes for abelian varieties. In this section we describe a construction of admissible complexes due to Burns and the first author [12]. Let \( F/k \) be a finite Galois extension of number fields with Galois group \( G \). Let \( A \) be an abelian variety defined over \( k \). We write \( A' \) for the dual abelian variety.

In the following result we write \( X_Z(A_F) \) for the integral Selmer group of \( A \) over \( F \) defined by Mazur and Tate in [30].

We recall that, if the Tate-Shafarevich group \( III(A_F) \) of \( A \) over \( F \) is finite, then \( X_Z(A_F) \) is a finitely generated \( G \)-module and there exists an isomorphism of \( \mathbb{Z}[G] \)-modules

\[
\hat{\mathbb{Z}} \otimes_{\mathbb{Z}} X_Z(A_F) \cong \text{Sel}(A_F)^\vee
\]

that is unique up to automorphisms of \( X_Z(A_F) \) that induce the identity map on both the submodule \( X_Z(A_F)_{\text{tor}} \) and quotient module \( X_Z(A_F)_{\text{fr}} = \text{Hom}_{\mathbb{Z}}(A(F), \mathbb{Z}) \). (Here \( \hat{\mathbb{Z}} \) denotes the profinite completion of \( \mathbb{Z} \)).

In the sequel we write \( S_\infty(k) \) for the set of archimedean places of \( k \) and, for a given prime number \( p \), also \( S_p(k) \) for the set of places of \( k \) which are \( p \)-adic. We write \( S_{\text{bad}}(A) \) for the set of places of \( k \) at which \( A \) has bad reduction and \( S_{\text{ram}}(F/k) \) for the set of places of \( k \) which ramify in \( F/k \). For a fixed set of places \( S \) of \( k \) we denote by \( S(F) \) the set of places of \( F \) which lie above a place in \( S \).

In the following result we identify the category of finite \( \mathbb{Z}_2[G] \)-modules as an abelian subcategory of the category of \( \mathbb{Z}[G] \)-modules in the obvious way and write \( \text{Mod}^{*}(\mathbb{Z}[G]) \) for the associated quotient category.
**Proposition 2.3.** Assume that III($A_F$) is finite. Fix a ‘perfect Selmer structure’ $\mathcal{X}$ for $A$ and $F/k$ in the sense of [12] Def. 2.10, and any finite set $S$ of places of $k$ with

$$S_\infty(k) \cup S_{\text{ram}}(F/k) \cup S_{\text{bad}}(A) \subseteq S.$$  

Then there exists a ‘Nekovář-Selmer complex’ $\text{SC}_S(A_{F/k}; \mathcal{X})$ in $D^p(\mathbb{Z}[G])$, unique up to isomorphisms in $D^p(\mathbb{Z}[G])$ that induce the identity map in all degrees of cohomology, that has all of the following properties.

(i) $\text{SC}_S(A_{F/k}; \mathcal{X})$ is acyclic outside degrees $1, 2$ and $3$, and there is a canonical identification $H^3(\text{SC}_S(A_{F/k}; \mathcal{X})) = (A(F)_\text{tor})^\vee$.

(ii) In $\text{Mod}^* (\mathbb{Z}[G])$ there exists a canonical injective homomorphism

$$H^1(\text{SC}_S(A_{F/k}; \mathcal{X})) \to A^1(F)$$

that has finite cokernel and a canonical surjective homomorphism

$$H^2(\text{SC}_S(A_{F/k}; \mathcal{X})) \to X_2(A_F)$$

that has finite kernel.

(iii) For a given odd prime $\ell$ the object

$$\text{SC}_S(A_{F/k}; \mathcal{X}(\ell)) := \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \text{SC}_S(A_{F/k}; \mathcal{X})$$

of $D^p(\mathbb{Z}_\ell[G])$ lies in $D^a(\mathbb{Z}_\ell[G])$ if and only if $A(F)$ contains no point of order $\ell$.

**Remarks 2.4.** (i) Even for an odd prime $\ell$ for which $A(F)$ contains a point of order $\ell$, the general result [17] Prop. 2.8 leads to a natural modification of $\text{SC}_S(A_{F/k}; \mathcal{X}(\ell))$ which belongs to the category $D^a(\mathbb{Z}_\ell[G])$. See also [12] Lem. 8.13(ii) for more details.

(ii) The cohomology group $H^1(\text{SC}_S(A_{F/k}; \mathcal{X}(\ell)))$ is in general a Selmer group in the sense of Mazur and Rubin [27]. Moreover [12] Prop. 2.12 (v) and Rem. 2.14 give fully explicit descriptions of the groups $H^1(\text{SC}_S(A_{F/k}; \mathcal{X}))$ and $H^2(\text{SC}_S(A_{F/k}; \mathcal{X}))$ in important cases.

(iii) Any choice of set $S$ as above and of an ordered $\mathbb{Q}[G]$-basis $\omega_\bullet$ of the space of invariant differentials

$$H^0(A^1_F, \Omega^1_{A^p}) \cong F \otimes_k H^0(A^1, \Omega^1_{A^p})$$

defines a perfect Selmer structure $\mathcal{X}_S(\omega_\bullet)$. See [12] for the details of this construction.

The Nekovář-Selmer complexes obtained from such perfect Selmer structures play a key role in the formulation of the central conjecture of loc. cit..

2.2.2. The classical Selmer complex of an abelian variety. In this section we give an additional construction of admissible complexes due to Burns and the first author [12] which, under suitable hypotheses, provides a more explicit alternative to the general Nekovář-Selmer complexes discussed in the previous section. These complexes will play an important role, when combined with a result of Mazur and Rubin [29] Thm. B], in Theorem 6.2(iii) below.

We adopt the notation and setting of the previous section and also fix an odd prime number $p$. We will consider the following list of hypotheses on $A$, $F/k$ and $p$.

In this list we fix an intermediate field $K$ of $F/k$ with the property that $G_{F/K}$ is a Sylow $p$-subgroup of $G$. In the sequel, for any non-archimedean place $v$ of a number field we write $\kappa_v$ for its residue field.
(H₁) The Tamagawa number of $A/K$ at each place in $S_{\text{bad}}(A/K)$ is not divisible by $p$.
(H₂) $A/K$ has good reduction at all $p$-adic places of $K$;
(H₃) For all $p$-adic places $v$ of $K$ that ramify in $F/k$, the reduction is ordinary and $A(k_v)[p^\infty] = 0$;
(H₄) For all non-archimedean places $v$ of $K$ that ramify in $F/k$, we have $A(k_v)[p^\infty] = 0$;
(H₅) No place of bad reduction for $A/k$ is ramified in $F/k$, i.e. $S_{\text{bad}}(A/k) \cap S_{\text{ram}}(F/k) = \emptyset$.

We refer the reader to [12, Rem. 6.1] for a further discussion of these hypotheses.

We write $Y_{F/k}$ for the module $\prod \mathbb{Z}$, with the product running over all $k$-embeddings $F \to k^e$, endowed with its natural action of $G \times G_k$.

We write $T_p(A^t)$ for the $p$-adic Tate module of the dual variety $A^t$. Then the $p$-adic Tate module of the base change of $A^t$ through $F/k$ is equal to

$$T_{p,F}(A^t) := Y_{F/k,p} \otimes_{\mathbb{Z}_p} T_p(A^t),$$

where $G$ acts on the first factor and $G_k$ acts diagonally.

For any subfield $E$ of $k$ and each non-archimedean place $v$ of $E$ we obtain a $G$-module by setting

$$A^t(F_v) := \prod_{w|v} A^t(F_w),$$

with $w$ running over all places of $F$ which divide $v$.

**Definition 2.5.** We fix a finite set of non-archimedean places $\Sigma$ of $k$ with

$$S_p(k) \cup S_{\text{ram}}(F/k) \cup S_{\text{bad}}(A) \subseteq \Sigma.$$  

We define the ‘classical $p$-adic Selmer complex’ $\text{SC}_{\Sigma,p}(A_{F/k})$ to be the mapping fibre of the following morphism in $D(\mathbb{Z}_p[G])$:

$$R\Gamma(O_{k,S_{\infty}(k) \cup \Sigma}, T_{p,F}(A^t)) \oplus \left( \bigoplus_{v \in \Sigma} A^t(F_v)[p] \right)[-1] \xrightarrow{(-\lambda,\kappa)} \bigoplus_{v \in \Sigma} R\Gamma(k_v, T_{p,F}(A^t)).$$

Here $\lambda$ is the natural diagonal localisation morphism in étale cohomology and $\kappa$ is induced by the sum of the local Kummer maps $A^t(F_v)[p] \to H^1(k_v, T_{p,F}(A^t))$ (and the fact that for each $v \in \Sigma$ the group $H^0(k_v, T_{p,F}(A^t))$ vanishes).

**Remark 2.6.** By Lem. 2.5 (and Rem. 2.6) in [12], the classical $p$-adic Selmer complex is independent, in a natural sense, of the choice of set of places $\Sigma$ fixed in Definition 2.5. For this reason, in the sequel we shall usually simply denote it by $\text{SC}_p(A_{F/k})$.

In the following result we write $\text{Sel}_p(A_F)$ for the classical $p$-primary Selmer group of $A$ over $F$.

**Proposition 2.7.** Assume that $A$, $F/k$ and $p$ satisfy the hypotheses (H₁)-(H₅) and that $\text{III}(A_F)[p^\infty]$ is finite.
Then the classical $p$-adic Selmer complex $\text{SC}_p(A_{F/k})$ belongs to $D^0(\mathbb{Z}_p[G])$ and is acyclic outside degrees one, two and three, with canonical identifications

$$H^i(\text{SC}_p(A_{F/k})) = \begin{cases} A^i(F)_{p}, & i = 1, \\ \text{Sel}_p(A_2)^\vee, & i = 2, \\ A(F)[p^\infty]^\vee, & i = 3. \end{cases}$$

In particular, $\text{SC}_p(A_{F/k})$ belongs to $D^3(\mathbb{Z}_p[G])$ if and only if neither $A(F)$ nor $A^i(F)$ contains a point of order $p$.

3. Characteristic elements, Fitting invariants and organising matrices

3.1. Characteristic elements. In this section we follow [8] in order to associate a natural notion of characteristic element to complexes in $D^3(\mathfrak{A})$.

For any field $F$ and any $\mathfrak{A}$-module $M$, resp. homomorphism of $\mathfrak{A}$-modules $\phi$, we write $M_F$ for the associated $E \otimes_R \mathfrak{A}$-module $E \otimes_R M$, resp. $\phi_E$ for the associated homomorphism $E \otimes_R \phi$ of $E \otimes_R \mathfrak{A}$-modules. We also use similar abbreviations for complexes, and morphisms of complexes, of $\mathfrak{A}$-modules.

3.1.1. Relative $K$-theory. For any field $E$ as above, we write $K_0(\mathfrak{A}, \mathfrak{A}_E)$ for the relative algebraic $K_0$-group of the ring inclusion $\mathfrak{A} \subset \mathfrak{A}_E$. We recall that this group comprises elements of the form $[P_1, P_2, \theta]$ where $P_1$ and $P_2$ are finitely generated projective $\mathfrak{A}$-modules and $\theta$ is an isomorphism of $\mathfrak{A}_E$-modules from $P_{1,E}$ to $P_{2,E}$.

We further recall that there exists a canonical exact commutative diagram of abelian groups of the form

$$
\begin{array}{cccccc}
K_1(\mathfrak{A}) & \xrightarrow{\partial^2_{\mathfrak{A}, E}} & K_1(A) & \xrightarrow{\partial^2_{\mathfrak{A}, \mathfrak{A}} - \partial^1_{\mathfrak{A}, \mathfrak{A}}} & K_0(\mathfrak{A}, A) & \xrightarrow{\partial^1_{\mathfrak{A}, \mathfrak{A}}} & K_0(\mathfrak{A}) \\
\downarrow{\iota_E} & & \downarrow{\iota_E} & & \downarrow{\iota_E} & & \\
K_1(\mathfrak{A}_E) & \xrightarrow{\partial^2_{\mathfrak{A}_E}} & K_1(\mathfrak{A}_E) & \xrightarrow{\partial^2_{\mathfrak{A}_E} - \partial^1_{\mathfrak{A}_E}} & K_0(\mathfrak{A}_E, A) & \xrightarrow{\partial^1_{\mathfrak{A}_E}} & K_0(\mathfrak{A}_E) \\
\end{array}
$$

Here the homomorphisms $\iota_E, \iota_E'$ and $\iota'_E$ are induced by the inclusion $A \subset \mathfrak{A}_E$ and are injective (indeed, we shall often regard these maps as inclusions). The homomorphisms $\partial^2_{\mathfrak{A}, E}$ and $\partial^1_{\mathfrak{A}, E}$ are induced by the inclusion $\mathfrak{A} \subset \mathfrak{A}_E$, $\partial^1_{\mathfrak{A}, \mathfrak{A}}$ is the homomorphism that sends the class of an automorphism $\phi$ of $\mathfrak{A}_E^n$ to $[\mathfrak{A}^n, \mathfrak{A}^n, \phi]$ and $\partial^2_{\mathfrak{A}, \mathfrak{A}}$ sends each element $[P_1, P_2, \theta]$ to $[P_1] - [P_2]$.

For any such field $E$ that is large enough (to contain, say, either $\mathbb{Q}_p$ for some prime $p$, or to contain $\mathbb{R}$), we write

$$\delta_{\mathfrak{A}, E} : Z(\mathfrak{A}_E) \rightarrow K_0(\mathfrak{A}, \mathfrak{A}_E)$$

for the ‘extended boundary homomorphism’ that is defined in [8] and we recall that

$$\delta_{\mathfrak{A}, E} \circ \text{nr}_{\mathfrak{A}, E} = \partial^1_{\mathfrak{A}, E}$$

where $\text{nr}_{\mathfrak{A}, E}$ denotes the homomorphism $K_1(\mathfrak{A}_E) \rightarrow Z(\mathfrak{A}_E)^\times$ that is induced by taking reduced norms.
3.1.2. Characteristic elements. In the sequel, for any ring $\Lambda$ and any (left) $\Lambda$-modules $M$ and $N$ we write $\text{Is}_\Lambda(M, N)$ for the set of $\Lambda$-module isomorphisms $M \to N$. For each cohomologically-bounded complex of $\mathfrak{A}$-modules $C$ and each field $E$ that contains $F$ we define the set of ‘$E$-trivialisations’ of $C$ by setting

$$\tau(C_E) := \text{Is}_{\mathfrak{A}_E}(\bigoplus_{i \in \mathbb{Z}} H^{2i}(C)_E, \bigoplus_{i \in \mathbb{Z}} H^{2i+1}(C)_E).$$

Example 3.1. In the setting of both §2.2.1 and §2.2.2 the Néron-Tate height pairing of $A$, defined relative to the field $F$, defines an $\mathbb{R}[G]$-isomorphism

$$h_{A,F/k} : A^i(F)_{\mathbb{R}} \to \text{Hom}_{\mathbb{R}}(A(F)_{\mathbb{R}}, \mathbb{R}).$$

If $\Pi(A_F)$ is finite then, since $X\mathbb{Z}(A/F)_f = \text{Hom}_{\mathbb{Z}}(A(F), \mathbb{Z})$, the map $h_{A,F/k}$ gives an $\mathbb{R}$-trivialisation of the Nekovář-Selmer complexes discussed in Proposition 2.3. Under the relevant hypotheses it also induces, for each isomorphism $C \cong C_p$, a $C_p$-trivialisation of the classical $p$-adic Selmer complex.

We next recall that to each pair $(C, t)$ comprising a complex $C$ in $D^p(\mathfrak{A})$ and an $E$-trivialisation $t$ of $C$ one can associate a canonical ‘refined’ Euler characteristic $\chi^\text{ref}_{\mathfrak{A},E}(C, t)$ in $K_0(\mathfrak{A}, \mathfrak{A}_E)$. (For explicit details of this construction in the relevant special case see the argument given in [11 §4.1]; for details in a more general context see, for example, [8 §2.8].)

Definition 3.2. For $C$ in $D^p(\mathfrak{A})$ and $t$ in $\tau(C_E)$ we define a ‘characteristic element for the pair $(C, t)$’ to be any element $\mathcal{L}$ of $Z(\mathfrak{A}_E)^\times$ which satisfies

$$\delta_{\mathfrak{A},E}(\mathcal{L}) = -\chi^\text{ref}_{\mathfrak{A},E}(C, t).$$

We also define a ‘characteristic element for $C$’ to be a characteristic element for $(C, t)$ for any choice of field $E$ and of $E$-trivialisation $t$ of $C$.

From the lower exact sequence in [11] it is then clear that characteristic elements for $(C, t)$ are unique up to multiplication by elements of $\text{nr}_{\mathfrak{A}_E}(\text{im}(\partial^2_{\mathfrak{A},E}))$. In this regard we also recall that if $\mathfrak{A}$ is semi-local (which is automatic if $R$ is a discrete valuation ring), then the natural homomorphism $\mathfrak{A}^\times \to K_1(\mathfrak{A})$ is surjective.

We next record a property of characteristic elements that will be useful in the proof of our main algebraic result. We refer to [11 §2.3.3] for the proof of this fact, which relies on Bass’ Theorem.

Lemma 3.3. Let $R$ be a discrete valuation ring and $E$ be any field that contains $F$. Fix a complex $C$ in $D^a(\mathfrak{A})$, write $e_0$ for the idempotent $e_0(C)$ defined in §2.1.2 and set $\mathfrak{A}_0 := \mathfrak{A}e_0$, $A_{E,0} := \mathfrak{A}_Ee_0$ and $C_0 := \mathfrak{A}_0 \otimes^L_{\mathfrak{A}} C$.

Then $C_0$ belongs to $D^a(\mathfrak{A}_0)$ and for any characteristic element $\mathcal{L}_0$ in $Z(A_{E,0})^\times$ of $C_0$ there exists a characteristic element $\mathcal{L}$ of $C$ such that $e_0\mathcal{L} = \mathcal{L}_0$.

3.2. Non-commutative higher Fitting invariants. In this section we briefly review the theory of non-commutative higher Fitting invariants introduced by Burns and Sano in [10]. The following definition of ‘Whitehead orders’ plays a key role in these constructions.
3.2.1. The Whitehead order. For any prime ideal \( p \) of \( R \) we write \( R_p \) for the localisation of \( R \) at \( p \) and for any \( \mathfrak{A} \)-module \( M \) we then set \( M_{(p)} := R_p \otimes_R M \).

**Definition 3.4.** For each prime ideal \( p \) of \( R \) the ‘Whitehead order’ \( \xi(\mathfrak{A}_{(p)}) \) is the \( R_{(p)} \)-submodule of \( Z(A) \) that is generated by the reduced norms \( \text{nr}_A(M) \) as \( M \) runs over the set \( \bigcup_{n \geq 0} M_n(\mathfrak{A}_{(p)}) \) of all square matrices with coefficients in \( \mathfrak{A}_{(p)} \).

The Whitehead order of \( \mathfrak{A} \) is then defined by the intersection

\[
\xi(\mathfrak{A}) := \bigcap_p \xi(\mathfrak{A}_{(p)}),
\]

where \( p \) runs over all prime ideals of \( R \).

By [10, Lem. 3.2] we know that \( \xi(\mathfrak{A}) \) is indeed an \( R \)-order in \( Z(A) \), which furthermore satisfies \( \xi(\mathfrak{A}_{(p)}) = \xi(\mathfrak{A}_{(p)}) \) for each prime ideal \( p \) of \( R \).

3.2.2. The higher Fitting invariants of a matrix. Let \( M \) be any matrix in \( M_{d \times d'}(A) \) with \( d \geq d' \). Then for any integer \( t \) with \( 0 \leq t \leq d' \) and any \( \varphi = (\varphi_i)_{1 \leq i \leq t} \in \text{Hom}_A(\mathfrak{A}^d, \mathfrak{A})^t \) we write \( \text{Min}_\varphi^d(M) \) for the set of all \( d' \times d' \)-minors of the matrices \( M(J, \varphi) \) that are obtained from \( M \) by choosing any \( t \times t \)-tuple of integers \( J = \{i_1, \ldots, i_t\} \) with \( 1 \leq i_1 \leq \ldots \leq i_t \leq d' \), and setting

\[
M(J, \varphi)_{ij} := \begin{cases} 
\varphi_a(b_i), & \text{if } j = i_a \text{ with } 1 \leq a \leq t, \\
M_{ij}, & \text{otherwise,}
\end{cases}
\]

where \( \{b_i\} \) denotes the standard basis of \( \mathfrak{A}^d \).

For any non-negative integer \( a \) the ‘\( a \)-th (non-commutative) Fitting invariant’ of \( M \) is defined to be the ideal of \( \xi(\mathfrak{A}) \) obtained by setting

\[
\text{Fit}^a_\mathfrak{A}(M) := \xi(\mathfrak{A}) \cdot \{\text{nr}_A(N) : N \in \text{Min}_\varphi^d(M), \varphi \in \text{Hom}_A(\mathfrak{A}^d, \mathfrak{A})^t, t \leq a\}.
\]

3.2.3. The higher Fitting invariants of a presentation. A ‘free presentation’ \( \Pi \) of a finitely generated \( \mathfrak{A} \)-module \( Z \) is an exact sequence of \( \mathfrak{A} \)-modules of the form

\[
F^1 \xrightarrow{\theta} F^2 \rightarrow Z \rightarrow 0
\]

in which the \( \mathfrak{A} \)-modules \( F^1 \) and \( F^2 \) are finitely generated and free and (without loss of generality) one has \( \text{rk}_\mathfrak{A} F^1 \geq \text{rk}_\mathfrak{A} F^2 \). The free presentation \( \Pi \) is said to be quadratic if \( \text{rk}_\mathfrak{A} F^1 = \text{rk}_\mathfrak{A} F^2 \).

Th \( a \)-th Fitting invariant \( \text{Fit}^a_\mathfrak{A}(\Pi) \) of \( \Pi \) is defined to be \( \text{Fit}^a_\mathfrak{A}(M_\theta) \) for any matrix \( M_\theta \) which represents \( \theta \) with respect to any choice of \( \mathfrak{A} \)-bases of \( F^1 \) and \( F^2 \).

We recall that a finitely generated \( \mathfrak{A} \)-module \( F \) is said to be locally-free if the localisation \( F_p \) is a free \( \mathfrak{A}_{(p)} \)-module (or equivalently if the completion \( F_p \) is a free \( \mathfrak{A}_{(p)} \)-module) for every prime ideal \( p \) of \( R \).

A ‘locally-free presentation’ \( \Pi \) of \( Z \) is an exact sequence of the form \( (2) \) in which the \( \mathfrak{A} \)-modules \( F^1 \) and \( F^2 \) are only assumed to be finitely generated and locally-free. The locally-free presentation \( \Pi \) is then said to be ‘locally-quadratic’ if \( \text{rk}_\mathfrak{A} F^1 = \text{rk}_\mathfrak{A} F^2 \) (we recall that the rank of a locally-free \( \mathfrak{A} \)-module is indeed a well-defined invariant).
By localising the sequence \( \Pi \) at a prime ideal \( p \) of \( R \) one obtains a free resolution \( \Pi_{(p)} \) of the \( A_{(p)} \)-module \( Z_{(p)} \) and one then defines the \( a \)-th Fitting invariant of \( \Pi \) to be

\[
\text{Fit}^a_{A}(\Pi) := \bigcap_p \text{Fit}^a_{A_{(p)}}(\Pi_{(p)}),
\]

where the intersection runs over all prime ideals \( p \) of \( R \) and takes place in \( Z(A) \).

We note in passing that, for \( a = 0 \), there is an explicit relationship between \( \text{Fit}^0_{A}(\Pi) \) and the Fitting invariant defined by Nickel in [32], as explained in [16, Prop. 3.13 (i)].

3.2.4. The total higher Fitting invariants. In order to associate to the module \( Z \) a finer invariant that will be crucial to our approach, we say that a free presentation \( \Pi' : F^1 \to F^2 \to Z' \to 0 \) of a finitely generated \( A \)-module \( Z' \) is ‘finer’ that the free presentation \( \Pi \) of \( Z \) given by (2) if both \( \text{rk}_A(F^1) = \text{rk}_A(F^1) \) and \( \text{rk}_A(F^2) = \text{rk}_A(F^2) \) and there exists an isomorphism \( F^2' \cong F^2 \) which induces a well-defined surjective homomorphism \( Z' \to Z \).

We define the ‘total \( a \)-th Fitting invariant’ of \( \Pi \) to be

\[
\text{Fit}^{a,\text{tot}}_{H}(\Pi) := \sum_{\Pi'} \text{Fit}^a_{H}(\Pi'),
\]

where in the sum \( \Pi' \) runs over all free presentations that are finer than \( \Pi \).

For a locally-free presentation \( \Pi \) we define the total \( a \)-th Fitting invariant of \( \Pi \) to be

\[
\text{Fit}^{a,\text{tot}}_{H}(\Pi) := \bigcap_p \text{Fit}^{a,\text{tot}}_{H_{(p)}}(\Pi_{(p)}).
\]

We recall an useful property of this invariant. In this result, we denote by \( D(A) \) the ‘ideal of denominators’ that is introduced by Burns and Sano in [16, Def. 3.4] (and denoted \( \delta(A) \) in loc. cit., which in this article could unfortunately clash with the standard notation for the extended boundary homomorphism). This result is then a consequence of the stronger [16, Thm. 3.17 (iii)].

Lemma 3.5. (Burns-Sano) Let \( \Pi \) be a locally-free presentation of an \( A \)-module \( Z \). Then one has

\[
D(A) \cdot \text{Fit}^0_{H}(\Pi) \subseteq D(A) \cdot \text{Fit}^{0,\text{tot}}_{H}(\Pi) \subseteq \text{Ann}_A(Z).
\]

3.3. A construction of organising matrices. If \( C \) is an object of \( D^a(Z_p[G]) \) then Burns and the first author associate in [11, Thm. 3.1] a family of ‘weakly-organising matrices’ to \( C \); an additional specification of data then also leads via Theorem 3.11 in loc. cit. to a more restrictive family of ‘organising matrices’ associated to \( C \). Let us recall that the original motivation of this theory lies in the construction by Mazur and Rubin of ‘organising modules’ in the (commutative) Iwasawa theory of elliptic curves (see [28]).

In this section we give a generalisation of the construction of such matrices that will play a key role in the proof of Theorem 5.1 below. We only discuss the properties of our organising matrices that will be of subsequent use in this article (but see also Remark 3.7 below for a comparison to one of the main results of [11]).
3.3.1. Statement of the main results. Throughout this section we assume that \( R \) is a discrete valuation ring. As a natural generalisation of admissible complexes, we assume to be given a complex \( D \) of \( \mathfrak{A} \)-modules of the form

\[
D^0 \xrightarrow{\delta^0} D^1 \xrightarrow{\delta^1} D^2
\]

in which the first term is placed in degree zero and each module is finitely generated and free of rank \( a \), \( d \) and \( d - a \) respectively, always assuming also that \( d \geq a \). We assume further that \( D \) is acyclic outside degrees one and two.

We then fix data of the following form:

(D1) an element \( z \) of the group \( \text{Ann}_{\mathfrak{A}}(\text{Ext}^2_{\mathfrak{A}}(H^2(D), \mathfrak{A})) \);

(D2) and an ordered \( a \)-tuple of homomorphisms

\[
\phi_\bullet = \{\phi_1, \ldots, \phi_a\} \subseteq \text{Hom}_{\mathfrak{A}}(\ker(\delta^1), \mathfrak{A}).
\]

Theorem 3.1. Assume that \( R \) is a discrete valuation ring and fix a complex of \( \mathfrak{A} \)-modules \( D \) and elements \( z \) and \( \phi_\bullet \) as above. We also fix any \( \mathfrak{A} \)-bases \( \{b^i_j\} \) of \( D_j \) for \( j = 0, 1, 2 \).

Then there exists a matrix \( \Phi = \Phi_{D, z, \phi_\bullet} \in M_d(\mathfrak{A}) \) that satisfies the following conditions:

(i) \( \Phi \) is of the form

\[
\left( \begin{array}{c} \Delta^1 \\ \end{array} \right)
\]

where \( \Delta^1 \in M_{d,d-a}(\mathfrak{A}) \) is the matrix of \( \delta^1 \) with respect to the chosen bases of \( D^1 \) and \( D^2 \).

(ii) We set \( \Lambda := (\phi_j(\delta^0(b_i^0)))_{1 \leq i,j \leq a} \in M_a(\mathfrak{A}) \). Then for any characteristic element \( \mathcal{L} \) of \( D \), the element

\[
\text{nr}_{\mathfrak{A}}(z)^a \cdot \text{nr}_{\mathfrak{A}}(\Lambda) \cdot \text{nr}_{\mathfrak{A}}(\Phi) \cdot \mathcal{L}
\]

belongs to \( \text{nr}_{\mathfrak{A}}(\mathfrak{A}^\times) \cdot \text{nr}_{\mathfrak{A}}(\Phi) \). (Here \( e_0(D) \) is the idempotent defined in §2.1.2).

Before proving Theorem 3.1, we state a direct consequence of this result.

Corollary 3.6. For any characteristic element \( \mathcal{L} \) of \( D \), the element \( \text{(4)} \) belongs to

\[
\text{Fit}^0_{\mathfrak{A}}(\Pi) \cap \text{Fit}^a_{\mathfrak{A}}\left( \begin{array}{c} I_a \\ 0 \\ \Delta^1 \\ \end{array} \right)
\]

where \( I_a \) is the identity \( a \times a \) matrix, \( 0 \) is the trivial \( (d-a) \times a \) matrix and \( \Pi \) denotes the canonical free presentation

\[
D^0 \oplus D^1 \xrightarrow{\text{id} \oplus \delta^1} D^0 \oplus D^2 \rightarrow H^2(D) \rightarrow 0
\]

of the \( \mathfrak{A} \)-module \( H^2(D) \).

Proof. Since claim (i) of Theorem 3.1 implies that \( \Phi \) coincides with

\[
M := \left( \begin{array}{c} I_a \\ 0 \\ \Delta^1 \\ \end{array} \right)
\]

in all but the first \( a \) columns, one has

\[
\text{nr}_{\mathfrak{A}}(\mathfrak{A}^\times) \cdot \text{nr}_{\mathfrak{A}}(\Phi) \subseteq \xi(\mathfrak{A}) \cdot \text{nr}_{\mathfrak{A}}(\Phi) \subseteq \text{Fit}^a_{\mathfrak{A}}(M).
\]
We next consider the following commutative diagram with exact rows:

\[
\begin{array}{cccccc}
D^0 & D^1 & D^0 & D^2 & \text{cok}(\Phi) & 0 \\
\Phi^0 & 0 & \text{id} & \epsilon & 0 \\
D^0 & D^1 & D^0 & D^2 & H^2(D) & 0
\end{array}
\]

Here \( \Phi \) is interpreted as a homomorphism \( D \) the group \( \text{Ext}^2 \) where \( \pi \) (under the simplifying assumption that \( D \)).

In fact, our ability to apply Corollary 3.6 over more general generalisation of [11, Cor. 3.3].

Remark 3.7. Let \( D \) be a complex of \( R[G] \)-modules which satisfies conditions (ad_1), (ad_2) and (ad_3). Then one may fix a representative of \( D \) of the form \( (3) \). Furthermore, the group \( \text{Ext}^2_{R[G]}(H^2(D), R[G]) \) vanishes so one may take \( z = 1 \) in \( (3) \).

If in addition \( D \) satisfies the condition (ad_4) then one may fix a representative of \( D \) of the form \( (3) \) for which \( D^0 \) is acyclic in degree 3) implies that there is \( \pi_0 \) denotes the projection to the \( D^0 \) component; the left-hand side square commutes by Theorem 3.1(i); and the surjective map \( \epsilon \) is defined by the commutativity of the right-hand side square.

We write \( \Pi' \) for the free presentation of the \( A \)-module \( \text{cok}(\Phi) \) that is given by the top row of this diagram. In particular, the presentation \( \Pi' \) is finer than the presentation \( \Pi \). It follows that \( \text{nr}_A(\mathfrak{A}^\times) \cdot \text{nr}_A(\Phi) \subseteq \xi(\mathfrak{A}) \cdot \text{nr}_A(\Phi) = \text{Fit}_A^0(\Pi') \subseteq \text{Fit}_A^{0,\text{tot}}(\Pi) \).

The inclusions \( (5) \) and \( (6) \) combine with claim (ii) of Theorem 3.1 to imply the validity of the claimed containment.

The differential \( \delta^0 \) is injective and, since the groups \( e_0(H^2(D)_F) \) and \( e_0(H^1(D)_F) \) both vanish, there exists a direct sum decomposition \( e_0D^0_F = V^1_1 \oplus V^1_2 \) so that the maps \( e_0\delta^0_F \) and \( e_0\delta^1_F \) give isomorphisms \( e_0D^0_F \cong V^1_1 \) and \( V^1_2 \cong e_0D^1_F \) respectively. We can therefore fix an isomorphism of \( A_E \)-modules

\[ t : (D^0 \oplus D^2)_E \to D^1_E \]

whose restriction coincides with the scalar extension of the isomorphism

\[ e_0D^0_F \oplus e_0D^1_F \cong e_0D^1_F = V^1_1 \oplus V^1_2 \]

given by \( (e_0\delta^0_F, (e_0\delta^1_F)^{-1}) \).

We now assume to be given \( t \) in \( \text{Is}_{A_E}(H^2(D)_E, H^1(D)_E) \) and a characteristic element \( \mathcal{L} \) for the pair \( (D, t) \). Then the same argument used to prove [11, Thm. 3.1(iv)] (under the simplifying assumption that \( D \) is acyclic in degree 3) implies that there is \( u_\mathcal{L} \in \text{nr}_A(\mathfrak{A}^\times) \) with the property that

\[ e_0\mathcal{L} = \text{nr}_{A_E}(t^{-1})u_\mathcal{L}. \]
We next apply the functor $\text{Hom}_{\mathfrak{A}}(-, \mathfrak{A})$ to the tautological short exact sequences

\[
\begin{align*}
0 & \to Z^1(D) \to D^1 \to B^2(D) \to 0 \\
0 & \to B^2(D) \to D^2 \to H^2(D) \to 0.
\end{align*}
\]

In particular, since the groups $\text{Ext}^2_{\mathfrak{A}}(D^i, \mathfrak{A})$ vanish for each $j \geq 1$ and each $i \in \{1, 2, 3\}$, we obtain an exact sequence

\[
\text{Hom}_{\mathfrak{A}}(D^1, \mathfrak{A}) \xrightarrow{\iota} \text{Hom}_{\mathfrak{A}}(Z^1(D), \mathfrak{A}) \to \text{Ext}^1_{\mathfrak{A}}(B^2(D), \mathfrak{A}) \to 0
\]

and an isomorphism

\[
\text{Ext}^1_{\mathfrak{A}}(B^2(D), \mathfrak{A}) \cong \text{Ext}^1_{\mathfrak{A}}(H^2(D), \mathfrak{A}).
\]

Hence for $1 \leq j \leq a$ there exist homomorphisms $\varphi_j$ in $\text{Hom}_{\mathfrak{A}}(D^1, \mathfrak{A})$ with

\[
\varphi_j|Z^1(D) = \kappa(\varphi_j) = z \cdot \varphi_j.
\]

We define $\phi$ to be the element of $\text{Hom}_{\mathfrak{A}}(D^1, D^0)$ that maps each element $w$ of $D^1$ to

\[
\sum_{i=1}^{a} \varphi_i(w) \cdot b_i^0
\]

where $\{b_i^0\}_{1 \leq i \leq a}$ is our fixed basis of $D^0$, and consider the homomorphism $D^1 \to D^0 \oplus D^2$ that is given by the direct sum $\phi \oplus \delta^1$.

Now, by explicitly comparing this map to the isomorphism $\iota$ defined in (7) one computes that on $e_0D^0_E \oplus e_0D^2_E$ there is an equality of functions

\[
(e_0(\phi \oplus \delta^1)|E \circ \iota(\phi) = (e_0(\phi \oplus \delta^0)E, \text{id}_{e_0D^1_E})
\]

and for each basis element $b_i^0$ one has

\[
(\phi \oplus \delta^0)(b_i^0) = \sum_{j=1}^{a} \varphi_j(\delta^0(b_i^0)) \cdot b_j^0 = \sum_{j=1}^{a} z(\varphi_j \circ \delta^0)(b_i^0) \cdot b_j^0.
\]

We set $\lambda_{ij} := (\varphi_j \circ \delta^0)(b_i^0)$.

For any fixed choice of bases $\{b_i^1\}$ and $\{b_i^2\}$ of $D^1$ and $D^2$ respectively we write $\Delta^1$ for the matrix of $\delta^1$ and $\Phi$ for the matrix of $\phi \oplus \delta^1$, as computed with respect to these choices and $\{b_i^0\}$. Claim (i) is then trivially satisfied.

We next note that $\text{cok}(\phi \oplus \delta^1)$ surjects canonically onto $H^2(D) = \text{cok}(\delta^1)$. In particular, for any primitive central idempotent $e$ of $A$ one has that $e(\Phi)$ is invertible over $Ae$ only if $e = ee_0$, so we deduce that $\text{nr}_A(\Phi) = e_0\text{nr}_A(\Phi)$. Combining this equality with (3), (4) and (6) we finally find that

\[
\text{nr}_A(z^a \text{nr}_A(A)e_0L) = \text{nr}_A((z\lambda_{ij})_{1 \leq i,j \leq a})e_0\text{nr}_{A_E}(\iota^{-1})u_L
\]

\[
= \text{nr}_{Ae_0}(e_0(\phi \circ \delta^0)|_E)\text{nr}_{Ae_0}(e_0(\iota^{-1}))u_L
\]

\[
= e_0\text{nr}_A((\phi \oplus \delta^1)|_E)u_L
\]

\[
= e_0\text{nr}_A(\Phi)u_L
\]

\[
= \text{nr}_A(\Phi)u_L.
\]

Here each reduced norm is computed with respect to our fixed bases. This equality completes the proof.
4. Non-abelian higher special elements

In this section we use the theory of non-commutative exterior powers to introduce our notion of a ‘non-abelian higher special element’. We also establish its basic rationality properties.

4.1. Non-commutative exterior powers. In this section we review the construction of non-commutative exterior powers due to Burns and Sano [16].

The ring $A$ is semisimple and so there is a direct product Wedderburn decomposition

$$A \cong \prod_{i \in I} A_i,$$

in which the index set $I$ is finite each ring $A_i$ is simple (and unique up to isomorphism). For any choice of splitting fields $E_i$ for the rings $A_i$ over $Z(A_i)$ and of simple $E_i \otimes Z(A_i)$ $A_i$-modules $V_i$, and for any non-negative integer $r$, there is an $r$-th reduced exterior power functor $\bigwedge^r_A$ from the category of finitely generated $A$-modules to that of $Z(A)$-modules.

If $A$ is commutative then one may take $V_i = E_i = A_i$ and then this functor coincides with the standard $r$-th exterior power. In general, there are canonical choices of splitting fields $E_i$ and then, since all simple $E_i \otimes Z(A_i)$ $A_i$-modules are isomorphic, different choices of such modules $\{V_i\}_{i \in I}$ are easily seen to give naturally equivalent reduced exterior powers. See [16, Rem. 4.4] for more details.

Reduced exterior powers also behave well under scalar extension, in that for any algebraic extension $\mathcal{F}'$ of $\mathcal{F}$ and any finitely generated $A$-module $M$, there is an injective homomorphism $\bigwedge^r_A M \to \bigwedge^r_{(A \otimes \mathcal{F})} (M \otimes \mathcal{F})$.

For any $0 \leq s \leq r$ there are natural duality pairings

$$(\bigwedge_A M) \times \bigwedge^{r-s}_{A \otimes \mathcal{F}} \text{Hom}_A(M, A) \to \bigwedge^s_A M$$

for every finitely generated $A$-module $M$. In the sequel we shall denote this pairing by $(m, \varphi) \mapsto \varphi(m)$.

In addition, for fixed ordered $E_i$-bases of the spaces $V_i$, each $r$-tuples $(m_j)_{1 \leq j \leq r}$ of elements of $M$ and $(\varphi_j)_{1 \leq j \leq r}$ of elements of $\text{Hom}_A(M, A)$ have associated elements $\bigwedge_{j=1}^r m_j$ of $\bigwedge^r_A M$ and $\bigwedge_{j=1}^{r-s} \varphi_j$ of $\bigwedge_{j=1}^{r-s} \text{Hom}_A(M, A)$. If $A$ is commutative and the required bases are specified to be the identity elements of each $V_i = E_i = A_i$ then these definitions coincide with the classical definitions of exterior products. In general, it is proved in [16, Lem. 4.10] that one always has

$$(\bigwedge_{i=1}^r \varphi_i)(\bigwedge_{j=1}^{j=r} m_j) = \mathfrak{n}_{M_\varphi(A \otimes \mathcal{F})}((\varphi_i(m_j))_{1 \leq i,j \leq m})$$

so that, in particular, this element belongs to $Z(A)$ and only depends on the $r$-tuples $(m_j)_{1 \leq j \leq r}$ and $(\varphi_j)_{1 \leq j \leq r}$. These properties will often be useful throughout the sequel.

Remark 4.1. Let $k$ be a field with algebraic closure $k^c$ and set $G_k := \text{Gal}(k^c/k)$. For each irreducible complex character $\chi$ of $G_k$ that has open kernel, we write $k(\chi)$ for the subfield of $k^c$ that is fixed by $\ker(\chi)$ and $n_\chi$ for the exponent of $\text{Gal}(k(\chi)/k)$. We also write $E_\chi$ for the field generated over $\mathbb{Q}$ by a primitive $n_\chi$-th root of unity. Then there exists a representation

$$\rho_\chi : \text{Gal}(k(\chi)/k) \to \text{GL}_{\chi(1)}(E_\chi)$$
of character \( \chi \).

For a given finite Galois extension \( L/k \) in \( k^c \) with Galois group \( \mathcal{G}_L := \text{Gal}(L/k) \) we write \( E_L \) for the composite of the fields \( E_\chi \), as \( \chi \) runs over \( \text{Ir}(\mathcal{G}_L) \). Then, for a fixed choice of representations \( \rho_\chi \) for each \( \chi \in \text{Ir}(\mathcal{G}_L) \), the induced homomorphisms \( \rho_\chi,* : E_L[\mathcal{G}_L] \to M_{\chi(1)}(E_L) \) combine to give an isomorphism

\[
E_L[\mathcal{G}_L] \cong \prod_{\chi \in \text{Ir}(\mathcal{G}_L)} M_{\chi(1)}(E_L).
\]

This decomposition shows that \( E_L \) is a splitting field for \( \mathbb{Q}[\mathcal{G}_L] \), that the spaces \( V_\chi := E^{(1)}_\chi \), considered as the first columns of the component \( M_{\chi(1)}(E_L) \), are a set of representatives of the simple \( E_L[\mathcal{G}_L] \)-modules and that one can specify the standard basis of \( E^{(1)} \) to be the ordered basis of \( V_\chi \).

In this way, the specification of a representation \( \rho_\chi \) for each irreducible complex character \( \chi \) of \( G_k \) that has open kernel leads to a canonical choice of the data necessary to define reduced exterior powers over any algebra of the form \( F[\text{Gal}(L/k)] \), with \( L \) a finite Galois extension of \( k \). We assume throughout the sequel and without further explicit comment that, whenever we have fixed a field \( k \), all such reduced exterior powers are defined relative to such a fixed choice of representations.

4.2. Definitions. In this section we first construct the necessary idempotents and then finally define our non-abelian higher special elements.

**Definition 4.2.** Let \( C \) be an object of \( D^a(\mathfrak{A}) \). For any non-negative integer \( a \) we define a central idempotent \( e_a = e_{C,a} \) of \( A \) to be the sum of all primitive central idempotents \( e \) of \( A \) with the property that the free \( Ae \)-module \( eH^2(C)_F \) has rank \( a \). We also set \( e(a) = e_{C,(a)} := \sum b \geq a e_b \).

We now fix an object \( C \) of \( D^a(\mathfrak{A}) \) as well as a surjective homomorphism of \( \mathfrak{A} \)-modules

\[
\pi : H^2(C) \to Y_\pi.
\]

**Definition 4.3.** We define a central idempotent \( e_\pi(a) \) of \( A \) as the sum of all primitive central idempotents \( e \) of \( A \) for which \( e(\ker(\pi)_F) \) vanishes.

The isomorphism

\[
e_\pi \cdot \pi_F : e_\pi H^2(C)_F \to e_\pi Y_{\pi,F}
\]

then induces, for each non-negative integer \( a \), a canonical isomorphism of \( Z(Ae_\pi) \)-modules

\[
(e_\pi \cdot \pi_F)^{(a)} : e_\pi(\bigwedge^a H^2(C)_F) \to e_\pi(\bigwedge^a Y_{\pi,F}).
\]

For a given \( E \)-trivialisation \( t \in \tau(C_E) \) of \( C \), its inverse \( t^{-1} \) induces, together with the map \( (e_\pi \cdot \pi_F)^{(a)} \) for any non-negative integer \( a \), a composite isomorphism \( t_a \) of \( Z(\mathfrak{A}_E e_\pi) \)-modules

\[
e_\pi(\bigwedge^a H^1(C)_E) \sim e_\pi(\bigwedge^a H^2(C)_E) \sim e_\pi(\bigwedge^a Y_{\pi,E}).
\]

**Definition 4.4.** Let \( L \) be a characteristic element for the pair \((C,t)\) and \( \pi \) be any surjective homomorphism as in [13].
Let $\mathcal{X}$ be a finite ordered subset of $Y_{\pi}$ of cardinality $a \geq 0$. The 'non-abelian higher special element' associated to the data $(C, t, \mathcal{L}, \pi, \mathcal{X})$ is

$$
\eta_{\mathcal{X}} := (t^a)^{-1}(e_{\pi} \cdot e_{C,a} \cdot \mathcal{L} \cdot \wedge_{x \in \mathcal{X}} x) \in (e_{\pi} \cdot e_{C,a})(\bigwedge_{x \in \mathcal{X}} H^1(C)_E).
$$

4.3. Rationality of non-abelian higher special elements. Before studying the finer integrality properties of non-abelian higher special elements we must establish that they live in rational non-commutative exterior powers.

**Lemma 4.5.** For any data $(C, t, \mathcal{L}, \pi, \mathcal{X})$ as in Definition 4.4 one has

$$
\eta_{\mathcal{X}} \in (e_{\pi} \cdot e_{C,a}) \bigwedge_{\mathcal{X}} H^1(C)_F.
$$

**Proof.** We set $\eta := \eta_{\mathcal{X}}$. It is enough to prove, for each primitive central idempotent $e$ of $A$, that $e(\eta) \in (e \cdot e_{\pi} \cdot e_{C,a}) \bigwedge_{\mathcal{X}} H^1(C)_F$.

If $e \cdot e_{\pi} \cdot e_{C,a} = 0$ then $e(\eta) = 0$ and this containment is clear. So we henceforth assume that $e \cdot e_{\pi} \cdot e_{C,a} \neq 0$, so that $e \cdot e_{\pi} \cdot e_{C,a} = e$, $e(\ker(\pi)_F)$ vanishes and

$$
\eta = (e \cdot t^a)^{-1}(e \cdot \mathcal{L} \cdot \wedge_{x \in \mathcal{X}} x) \in e \cdot \bigwedge_{\mathcal{X}} H^1(C)_F.
$$

It is enough to prove that $e(\eta)$ belongs to $e \cdot \bigwedge_{\mathcal{X}} H^1(C)_F$. In addition, the $Ae$-module $eY_{\pi,F}$ is free of rank $a$ (since so is $eH^2(C)_F$) and, if the set $\{e \cdot x : x \in \mathcal{X}\}$ is not a basis for this module, then [12] implies that

$$
eq \cdot \wedge_{x \in \mathcal{X}} x = 0
$$
in $e \cdot \bigwedge_{\mathcal{X}} Y_{\pi,F}$. In this case also $e(\eta) = 0$ and the required containment is clear. We thus assume henceforth that $\{e \cdot x : x \in \mathcal{X}\}$ is an $Ae$-basis of $eY_{\pi,E}$.

Now, the $A$-modules $H^1(C)_F$ and $H^2(C)_F$ are (non-canonically) isomorphic, so we may and will fix an isomorphism $t': H^1(C)_F \rightarrow H^2(C)_F$.

After enlarging $E$ if necessary, we may assume that the reduced norm map $nr_{Ae,F} : \mathcal{K}(Ae) \rightarrow \mathcal{Z}(Ae)_F$ is bijective, and this implies that $\ker(\delta_{Ae,F}) \subseteq \mathcal{Z}(Ae)_F$. Since

$$
\delta_{Ae,F}(e \cdot \mathcal{L}) = -\chi_{\delta_{Ae,F}}(Ae) \otimes 1_{C,F} (e \cdot t) = \delta_{Ae,F}(nr_{Ae,F}(e \cdot t^{-1} \circ e \cdot t')^{-1})
$$

we thus deduce that

$$
eq \cdot \mathcal{L} \cdot nr_{Ae,F}(e \cdot t \circ e \cdot t') \in \mathcal{Z}(Ae)_F.
$$

It follows that the element

$$
eq \cdot \mathcal{L} \cdot nr_{Ae,F}(e \cdot t \circ e \cdot t') \cdot ((e \cdot t^{-1} \circ e \cdot (\pi_F)^{-1})(e \cdot \wedge_{x \in \mathcal{X}} x))
$$

belongs to $e \cdot \bigwedge_{\mathcal{X}} H^1(C)_F$. Since [13] combines with [16] Lem. 4.13 to imply that the last displayed expression is equal to $e(\eta)$, this containment completes the proof.

5. THE MAIN ALGEBRAIC RESULT

In this section we state our main algebraic result under the specification $\mathfrak{A} := R[G]$. We recall that $\mathcal{D}(R[G])$ denotes the 'ideal of denominators' that is introduced by Burns and Sano in [16 Def. 3.4].
5.1. **The statements.** Fix any data \((C, t, \mathcal{L}, \pi, \mathcal{X})\) as in Definition 4.4 and set \(a := \lVert \mathcal{X} \rVert\). For any \(R[G]\)-module \(M\) we set
\[
M' := R[G] \pi_{C, (a)} \otimes_{R[G]} M.
\]
The statement of our main result will require data of the following type:
(i) an element
\[
x \in (R[G] \cap R[G']) \cdot \mathcal{D}(R[G]');
\]
(ii) an element
\[
z \in \text{Ann}_{R[G]'}(\text{Ext}^2_{R[G]'}(H^2(C)', R[G]'));
\]
(iii) an \(a\)-tuple of homomorphisms
\[
\varphi_1, \ldots, \varphi_a \in \text{Hom}_{R[G]}(H^1(C), R[G]).
\]
The proof of this result will be given in \(\S 5.3\) below.

**Theorem 5.1.** The \(R[G]'-\text{module} H^2(C)'\) admits a locally-free, locally-quadratic presentation \(\Pi\) with the property that
\[
\text{nr}_{F[G]'}(z)^a \cdot (\text{nr}_{F[G]'}(z)^a) \in \text{Fil}^a_{R[G]'}(\Pi)
\]
and
\[
x \cdot \text{nr}_{F[G]'}(z)^a \cdot (\text{nr}_{F[G]'}(z)^a) \in \text{Ann}_{R[G]}((Y_\pi)_{\text{tor}}).
\]

**Remark 5.1.** Let \(C\) be a complex in \(D^a(R[G])\) which, as an strengthening of condition (ad2), satisfies the condition that the Euler characteristic of \(C\) in the Grothendieck group \(K_0(R[G])\) vanishes. Then one may take the presentation \(\Pi\) to be free (quadratic) rather than just locally-free.

As explained in Example 2.2, \(R[G]\) is Gorenstein with respect to the anti-involution \(\iota_{\#}\) that satisfies \(\iota_{\#}(g) = g^{-1}\) for all \(g\) in \(G\), and therefore the group \(\text{Ext}^2_{R[G]}(M, R[G])\) vanishes for any finitely generated \(R[G]\)-module \(M\).

As an immediate consequence one thus obtains the following simplification of Theorem 5.1.

**Corollary 5.2.** Fix \((C, t, \mathcal{L}, \pi)\). Fix any non-negative integer \(a\) for which the \(F[G]\)-module \(F \otimes_R H^2(C)\) contains a free submodule of rank \(a\).
Then for any subset \(\mathcal{X}\) of \(Y_\pi\) of cardinality \(a\), any \(a\)-tuple of homomorphisms \(\varphi_1, \ldots, \varphi_a \in \text{Hom}_{R[G]}(H^1(C), R[G])\) and any \(x \in \mathcal{D}(R[G])\) one has
\[
(\text{nr}_{F[G]'}(z)^a) \in \text{Fil}^a_{R[G]}(\Pi) \quad \text{and} \quad x \cdot (\text{nr}_{F[G]'}(z)^a) \in \text{Ann}_{R[G]}((Y_\pi)_{\text{tor}}).
\]

The following additional consequence of Theorem 5.1 will also, in the sequel, lead to relatively simper statements in our arithmetic applications.

**Corollary 5.3.** In the notation and setting of Theorem 5.1, and for any
\[
y \in (R[G] \cap R[G']'),
\]
one has
\[
\text{nr}_{F[G]'}(y)^{2a} \cdot (\text{nr}_{F[G]'}(y)^{2a}) \in \text{Fil}^a_{R[G]'}(\Pi)
\]
and
\[
x \cdot \text{nr}_{F[G]'}(y)^{2a} \cdot (\text{nr}_{F[G]'}(y)^{2a}) \in \text{Ann}_{R[G]}((Y_\pi)_{\text{tor}}).
Proof. We set \( M := H^2(G)^f \). To deduce the claimed result from Theorem \ref{thm:main_theorem} it is then enough to show that \( y^2 \) annihilates \( \operatorname{Ext}^2_{R[G]}(M, R[G]^f) \). We adapt an argument used in the proof of \cite[Thm. 8.6]{12}.

To do this we use the existence of a convergent first quadrant cohomological spectral sequence

\[
E_2^{pq} = \operatorname{Ext}^p_{R[G]}(M, \operatorname{Ext}^q_{R[G]}(R[G], R[G]^f)) \Rightarrow \operatorname{Ext}^{p+q}_{R[G]}(M, R[G]^f)
\]

(cf. \cite[Exer. 5.6.3]{32}).

In particular, since the long exact sequence of low degree terms of this spectral sequence gives an exact sequence of \( R[G] \)-modules

\[\operatorname{Hom}_{R[G]}(M, \operatorname{Ext}^1_{R[G]}(R[G], R[G]^f)) \rightarrow \operatorname{Ext}^2_{R[G]}(M, R[G]^f) \rightarrow \operatorname{Ext}^2_{R[G]}(M, R[G]^f),\]

we find that it is enough to show that the element \( y \) annihilates both \( \operatorname{Ext}^1_{R[G]}(R[G], R[G]^f) \) and \( \operatorname{Ext}^2_{R[G]}(M, R[G]^f) \).

To verify this we write \( R[G]^1 \) for the ideal \( \{ x \in R[G] : x \cdot e_{C,a} = 0 \} \) so that there is a natural short exact sequence of \( R[G] \)-modules

\[0 \rightarrow R[G]^1 \rightarrow R[G] \rightarrow R[G]^1 \rightarrow 0.\]

Then by applying the exact functor \( \operatorname{Ext}^1_{R[G]}(-, R[G]^f) \) to this sequence one obtains a surjective homomorphism

\[\operatorname{Hom}_{R[G]}(R[G]^1, R[G]^f) \rightarrow \operatorname{Ext}^1_{R[G]}(R[G]^f, R[G]^f).\]

In addition, since as explained in Example \ref{ex:valuation_ring} \( R[G] \) is Gorenstein with respect to the anti-involution \( \tau_\# \) that satisfies \( \tau_\#(g) = g^{-1} \) for all \( g \) in \( G \), by applying the exact functor \( \operatorname{Ext}^1_{R[G]}(M, -) \) to the above sequence one finds that there is a natural isomorphism

\[\operatorname{Ext}^3_{R[G]}(M, R[G]^1) \cong \operatorname{Ext}^2_{R[G]}(M, R[G]^f).\]

To complete the proof it is thus enough to note that the left hand modules in both of the last two displays are annihilated by \( y \) since the definition of \( R[G]^1 \) implies immediately that \( y \cdot R[G]^1 = 0 \).

\[\square\]

5.2. Reduction results. In order to prove Theorem \ref{thm:main_theorem} in the next section, we begin by making the following helpful reductions.

Lemma \ref{lem:discrete_valuation_ring}. It is enough to prove Theorem \ref{thm:main_theorem} in the case that \( R \) is a discrete valuation ring.

Proof. This is clear from the definition of a locally-free presentation, and of the associated higher Fitting invariants, in terms of the localised rings \( R_{(p)}[G] \) as \( p \) ranges over the prime ideals of \( R \).

\[\square\]

Lemma \ref{lem:image_free_module}. Assume that \( R \) is a discrete valuation ring. Then it is enough to prove Theorem \ref{thm:main_theorem} in the case that the image of \( \mathcal{X} \) in \( Y_{\pi, F}^f \) generates a free \( R[G]^f \)-module of rank \( a \).

Proof. Let \( p \) denote the residue characteristic of \( R \). We set \( e_{\pi,a} := e_\pi \cdot e_{C,a} \).

We label the elements of \( \mathcal{X} \) as \( \{x_i\}_{1 \leq i \leq a} \) and fix an ordered subset \( \mathcal{Y} := \{y_i\}_{1 \leq i \leq a} \) of \( Y_\pi \), of cardinality \( a \), that generates a free \( R[G]^f \)-submodule of rank \( a \) of \( Y_{\pi, F}^f \). By the argument of \cite[Lem. 3.16]{17}, for any large enough integer \( N \) the set

\[\mathcal{Y}_N := \{x_i + p^N y_i\}_{1 \leq i \leq a} \]
generates a free $R[G]'$-submodule of rank $a$ of $Y'_{π,Γ}$. For any such integer $N$ we set $η_N := η_{Y'_{π,Γ}}$.

Now, in each simple component $Δ_{Γ}[e_{Γ,Γ}Y_{π,Γ}]$ of $e_{π,Γ}Δ_{Γ}[e_{Γ,Γ}Y_{π,Γ}]$, the difference
\begin{equation}
\bigwedge_{i=1}^a (x_i + p^N y_i) - \bigwedge_{i=1}^a x_i
\end{equation}
begins to $p^N \cdot L_e$ where $L_e$ is the $R$-sublattice of $Δ_{Γ}[e_{Γ,Γ}Y_{π,Γ}]$ generated by $Z := \{\bigwedge_{i=1}^a z_i : z_i \in \{x_i, y_i\}\}$.

In fact, in $e_{π,Γ}Δ_{Γ}[e_{Γ,Γ}Y_{π,Γ}]$ the difference $\langle 15 \rangle$ therefore belongs to $p^N \cdot L$ where $L$ is the $R$-sublattice generated by $Z$. Defining an $R$-sublattice $L' := e_{π,Γ} \cdot L \cdot (t_{π})^{-1}(L)$ of $e_{π,Γ}Δ_{Γ}[H^1(Γ)]$ one then finds that $η_N - η \in p^N \cdot L'$.

We next define an $R$-sublattice $L'' := \{\bigwedge_{j=1}^a ϕ_j(L') : ϕ \in \text{Hom}_{R[G]}(H^1(Γ), R[Γ])^a\}$ of $Z(Δ_{Γ}[e_{Γ,Γ}]) \subseteq Z(Δ_{Γ}[Γ'])$, so that $\{((\bigwedge_{j=1}^a ϕ_j)(η_N) - (\bigwedge_{j=1}^a ϕ_j)(η)) : ϕ \in \text{Hom}_{R[G]}(H^1(Γ), R[Γ])^a\} \subseteq p^N \cdot L''$.

We note that, for any large enough choice of $N$, one has
\begin{align*}
(R[G] \cap R[Γ']) \cdot D(R[Γ']) \cdot p^N \cdot L'' \subseteq (R[G] \cap R[Γ']) \cdot \text{Ann}_{R[G]}((Y'_{π,Γ})_{tor}) \\
\subseteq \text{Ann}_{R[G]}((Y'_{π,Γ})_{tor}),
\end{align*}
where the first inclusion holds because $(Y'_{π,Γ})_{tor}$ is finite and the second inclusion follows from $\langle 13 \rangle$ below.

It is now enough to prove that, for any large enough choice of $N$ and any free, quadratic $R[G]'$-presentation $Π$ of $H^2(Γ)'$ one has
\begin{equation}
p^N \cdot L'' \subseteq \text{Fit}_{R[G]}^a(Π),
\end{equation}
and this would follow from the fact that $\text{Fit}_{R[G]}^a(Π) \cap Z(Δ_{Γ}[e_{Γ,Γ}])$ has finite index in $Z(Δ_{Γ}[e_{Γ,Γ}])$. It is thus enough to prove that
\begin{equation}
e_{π,Γ} \cdot (Δ_{Γ}[R[Γ]]^a) = Z(Δ_{Γ}[e_{Γ,Γ}])
\end{equation}
and this is what we proceed to do.

The presentation $Π$ is of the form
\begin{equation}
R[G]' \xrightarrow{θ} R[G]'^d \rightarrow H^2(Γ)' \rightarrow 0
\end{equation}
and induces a free presentation of $Δ_{Γ}[e_{Γ,Γ}]$-modules
\begin{equation}
(Δ_{Γ}[e_{Γ,Γ}]^d)^{e_{π,Γ} \cdot θ} \rightarrow (Δ_{Γ}[e_{Γ,Γ}]^d)^{e_{π,Γ} \cdot H^2(Γ)_{Γ'}} \rightarrow 0.
\end{equation}
It is enough to prove that, for some matrix $B \in M_d(Δ_{Γ}[e_{Γ,Γ}])$ that coincides with $M_{e_{π,Γ} \cdot θ_{Γ'}}$ in all but $a$ columns, the reduced norm of $B$ is a unit in $Z(Δ_{Γ}[e_{Γ,Γ}])$.

Here $M_{e_{π,Γ} \cdot θ_{Γ'}} \in M_d(Δ_{Γ}[e_{Γ,Γ}])$ denotes the matrix of $e_{π,Γ} \cdot θ_{Γ'}$ with respect to any choice of $Δ_{Γ}[e_{Γ,Γ}]$-bases.
But the \( \mathcal{F}[G][e, \alpha, \theta] \cdot H^2(C) \) is free of rank \( a \). Fixing a section to \( \varpi \) induces a direct sum decomposition
\[
(\mathcal{F}[G][e, \alpha, \theta])^d = \text{im}(e, \alpha, \theta) \oplus e, \alpha, \theta \cdot H^2(C)
\]
where \( \text{im}(e, \alpha, \theta) \) is free of rank \( d - a \). It is now clear that one may find bases with respect to which \( M_{e, \alpha, \theta} \) is a block matrix of the form
\[
\begin{pmatrix}
I_{d-a} & \\
0 & *
\end{pmatrix}.
\]

The identity matrix in \( M_d(\mathcal{F}[G][e, \alpha, \theta]) \) therefore coincides with such a choice \( M_{e, \alpha, \theta} \) in all but the last \( a \) columns, and is thus a valid choice of matrix \( B \). This fact completes the proof. \( \square \)

5.3. The proof of Theorem 5.1 In this section we complete the proof of Theorem 5.1. In view of Lemmas 5.3 and 5.5 in the rest of this proof we may and will assume that \( R \) is a discrete valuation ring and that the image of \( \mathcal{X} \) in \( Y_{\pi, \mathcal{X}} \) generates a free \( R[G] \cdot \) module \( X \) of rank \( a \).

We consider the object
\[
C' := R[G][e, \alpha] \otimes_{\mathcal{R}[G]} C
\]
of \( D^p(R[G]) \). We fix, as we may, an (injective) \( R[G]' \)-lift \( \iota_2 : X \to H^2(C)' = H^2(C') \) of the inclusion \( X \subseteq Y' \) via \( \pi' = e(a) \pi \). We also fix any injective homomorphism \( \iota_1 : X \to H^1(C') \).

Since \( R \) is a discrete valuation ring and \( C \) is an admissible complex of \( R[G] \)-modules, a standard argument in homological algebra implies that one may fix a representative of \( C \) of the form
\[
F^1 \xrightarrow{\partial} F^2,
\]
where \( F^1 \) and \( F^2 \) are finitely generated free \( R[G] \)-modules of the same rank and \( F^1 \) is placed in degree one.

We fix any such choice of explicit representative for \( C \) and associate to it an explicit complex
\[
D : X \xrightarrow{\partial} X \oplus F^1, (\iota_2(\partial')) F^2',
\]
of \( R[G]' \)-modules. Here the first term is placed in degree zero, \( \partial' = e(a) \partial \) and, by abuse of notation, \( \iota_1 \) is the composition
\[
X \xrightarrow{\partial} H^1(C') = \ker(\partial') \subseteq F^1,
\]
while \( \iota_2 : X \to F^2' \) is any lift of \( \iota_2 \) via the canonical surjection \( F^2' \to \text{cok}(\partial') = H^2(C') \).

By [17, Lem. 3.22], modifying our given \( a \)-tuple of homomorphisms \( \varphi_1, \ldots, \varphi_a \) by setting \( \varphi_j' := e(a) \varphi_j \) gives a well-defined \( a \)-tuple of homomorphisms in \( \text{Hom}_{R[G]}(H^1(C'), R[G]) \). After setting \( \mathcal{X} = \{x_1, \ldots, x_a\} \) one then computes
\[
(\lambda_{i,j}^{a, \alpha}) (\eta x) = (\lambda_{i,j}^{a, \alpha}) (\eta x)
\]
\[
= \text{nr}_{F[G]}((\varphi_j')(\iota_1(x_i))) \cdot e \cdot \mathcal{L} \cdot \text{nr}_{E[G]}((\iota_1^1 E \circ e(a) \circ e(a) \pi E^1)).
\]

This computation uses the equality [12] and the result [16, Lem. 4.13], as well as the linearity of the duality pairing [11].
We may now apply Corollary 3.6 to the complex of \( R[G]' \)-modules \( D \), the \( a \)-tuple of homomorphisms \( \varphi'_1, \ldots, \varphi'_a \), the element \( z \) of
\[
\text{Ann}_{R[G]}'(\text{Ext}^2_{R[G]}(H^2(C)', R[G]')) \cong \text{Ann}_{R[G]}'(\text{Ext}^2_{R[G]}(H^2(D), R[G]'))
\]
and the characteristic element \( \mathcal{L}_D \) for \( D \) provided by Lemma 5.5 below. In order to do so, we fix \( R[G]' \)-bases \( b_1^\bullet \) and \( b_2^\bullet \) of \( F^1 \) and \( F^2 \) respectively, write \( \Delta \) for the matrix of \( \partial \) as computed with respect to these bases and write \( \Gamma \) for the matrix of \( \iota_2 : X \to F^2' \) as computed with respect to \( X \) and \( e_{(\alpha)} \cdot b_2^\bullet \).

These results then combine with (10) to imply that there exists a canonical free presentation \( \Pi_D \) of the \( R[G]' \)-module \( H^2(D) = H^2(C')/\iota_2(X) \) with the property that
\[
\eta_{R[G]'}(z^a) \cdot (\lambda_j^{\alpha_a}(\varphi_j))(\eta_X) \in \left( \text{Fit}_{R[G]}'(\Pi_D) \cap \text{Fit}_{R[G]}'(\Pi_D) \right)
\]
We next construct the free quadratic presentation \( II \) of \( H^2(C)' \) that is claimed to exist in Theorem 5.1. We define
\[
\theta : X \oplus F^1' \to X \oplus F^2'
\]
by setting
\[
\theta(\alpha, \beta) := (\alpha, \iota_2(\alpha) + \partial'(\beta)).
\]
If we then define a map
\[
\rho : X \oplus F^2' \to \text{cok}(\partial') = H^2(C')
\]
by setting
\[
\rho(\gamma, \delta) := (-\iota_2(\gamma) + \delta) + \text{im}(\partial')
\]
then the sequence
\[
\Pi : X \oplus F^1' \overset{\delta}{\to} X \oplus F^2' \overset{\rho}{\to} H^2(C)' \to 0
\]
is exact. It is in addition clear that
\[
\text{Fit}_{R[G]}' \left( \left( \begin{array}{cc} I_a & \Gamma \\ 0 & e_{(\alpha)} \Delta \end{array} \right) \right) = \text{Fit}_{R[G]}'(\Pi).
\]
The proof of Theorem 5.1 is now completed upon combining (17) with the following result.

**Lemma 5.6.** For any free presentation \( \Pi_D \) of the \( R[G]' \)-module \( H^2(C')/\iota_2(X) \) one has
\[
(R[G] \cap R[G]') \cdot D(R[G]') \cdot \text{Fit}_{R[G]}'(\Pi_D) \subseteq \text{Ann}_{R[G]}'((Y_\pi)_{\text{tor}}).
\]

**Proof.** One has that \( D(R[G]') \cdot \text{Fit}_{R[G]}'(\Pi_D) \) is contained in \( \text{Ann}_{R[G]}'(H^2(C')/\iota_2(X)) \) by Lemma 3.3. Since, by choice of \( \iota_2 \), the surjective map \( \pi \) induces a surjection
\[
H^2(C')/\iota_2(X) = (R[G]' \otimes_{R[G]} H^2(C))/\iota_2(X) \to (R[G]' \otimes_{R[G]} Y_\pi)/X,
\]
and since \( X \) is a free \( R[G]' \)-module, we find that \( D(R[G]') \cdot \text{Fit}_{R[G]}'(\Pi_D) \) is also contained in \( \text{Ann}_{R[G]}'((R[G]' \otimes_{R[G]} Y_\pi)_{\text{tor}}) \).

To conclude the proof, it is thus enough to note that
\[
(R[G] \cap R[G]') \cdot \text{Ann}_{R[G]}'((R[G]' \otimes_{R[G]} Y_\pi)_{\text{tor}}) \subseteq \text{Ann}_{R[G]}'((Y_\pi)_{\text{tor}}).
\]
Indeed, if we set $R[G]^{\#} := R[G] \cap R[G](1 - e_{(a)})$, the tautological exact sequence $0 \to R[G]^{\#} \to R[G] \to R[G]' \to 0$ gives rise to an exact sequence of $R[G]$-modules

$$R[G]^{\#} \otimes_{R[G]} Y_\pi \to Y_\pi \to R[G]' \otimes_{R[G]} Y_\pi \to 0.$$  

The required inclusion then follows from the fact the first term in this sequence is annihilated by $R[G] \cap R[G]'$ and the fact that any element in the kernel of the induced map

$$(Y_\pi)_{tor} \to (R[G]' \otimes_{R[G]} Y_\pi)_{tor}$$

is contained in the image of this first term.

We finally prove the intermediate result that was used in the course of the proof of Theorem 5.1.

**Lemma 5.7.** There exists a characteristic element $L_D \in Z(E[G'])^\infty$ for $D$ with the property that

$$e_a \cdot L_D = e_a \cdot L \cdot \text{nr}_{E[G']}(t_{1,E}^{-1} \circ e_{(a)} t \circ e_{(a)} \pi_E^{-1}).$$

**Proof.** It is easy to see that there is a canonical exact triangle in $D^p(R[G'])$ of the form

$$X[-2] \oplus X[-1] \xrightarrow{=} C' \to D \to X[-1] \oplus X[0]$$

in which $H^1(t) = t_1$ and $H^2(t) = t_2$.

Since $t^{-1}$ induces an isomorphism of $E[G]$-modules between $e_a H^1(C) = e_a t_1(X) E$ and $e_a H^2(C) = e_a t_2(X) E$ we can fix a commutative diagram of $E[G]$-modules

$$
\begin{array}{cccccc}
0 & \longrightarrow & X_E & \xrightarrow{t_{1,E}} & H^1(C')_E & \longrightarrow & H^1(D)_E & \longrightarrow & 0 \\
& & \downarrow{t_1} & & \downarrow{t_2} & & \downarrow{t_3} & & \\
0 & \longrightarrow & X_E & \xrightarrow{t_{2,E}} & H^2(C')_E & \longrightarrow & H^2(D)_E & \longrightarrow & 0
\end{array}
$$

where the maps $t_1$, $t_2$ and $t_3$ are bijective and satisfy

$$e_a \pi_E^{-1} \circ e_{a} t_1 \circ e_{a} t_{1,E}^{-1} = e_a (t_{2,E} \circ t_1 \circ t_{1,E}^{-1}) = e_a t_2 = e_a t^{-1}.$$  

We consider the object

$$D_a := R[G] e_a \otimes_{R[G']} D$$

of $D^p(R[G] e_a)$. Then, since the definition of $e_a = e_{a,C}$ implies that, in the notation of [2,12] it is equal to $e_0(D) = e_{D,0}$, Lemma 3.3 implies that it is enough to prove that

$$e_{(a)} \cdot L \cdot \text{nr}_{E[G']}(t_{1,E}^{-1} \circ e_{(a)} t \circ e_{(a)} \pi_E^{-1}))$$

in $K_0(R[G] e_a, E[G'])$. Since one has

$$\chi_{R[G],E}(C', t_{1,E}^{-1}) = \chi_{R[G],E}(D, t_{3,E}^{-1}) + \chi_{R[G'],E}(X[-2] \oplus X[-1], t_{1,E}^{-1})$$

in $K_0(R[G'], E[G'])$, the required equality (20) now follows from the following explicit computation that uses (19):

$$- \chi_{R[G],E}(D_a, e_{a} t_{3,E}^{-1}) = \chi_{R[G],E}(e_{a} X[-2] \oplus e_{a} X[-1], e_{a} t_{1,E}^{-1} \circ e_{a} t \circ (e_{a} \pi_E^{-1}))$$

$$\quad - \chi_{R[G],E}(R[G] e_a \otimes_{R[G']} C, e_{a} t)$$

$$\quad = [e_{a} X, e_{a} X, e_{a} t_{1,E}^{-1} \circ e_{a} t \circ (e_{a} \pi_E^{-1})] + \delta_{R[G],E}(e_{a} L)$$

$$\quad = \delta_{R[G],E}(e_{a} \cdot L \cdot \text{nr}_{E[G']}(t_{1,E}^{-1} \circ e_{(a)} t \circ e_{(a)} \pi_E^{-1})).$$
6. Selmer and Tate-Shafarevich groups and refined BSD conjectures

In this section we extend the result [12, Thm. 8.6] of Burns and the first author, concerning the Galois structures of Selmer and Tate-Shafarevich groups of abelian varieties, and their relations to the formulation of refined conjectures of Birch and Swinnerton-Dyer type, from the setting of abelian extensions of number fields to the setting of general Galois extensions.

In §6.2 we will then consider dihedral twists of elliptic curves over general number fields. By combining our general approach with a result of Mazur and Rubin [29, Thm. B] we are able to obtain strikingly explicit predictions for the first derivatives of Hasse-Weil-Artin $L$-series of such twists. In Example 6.7 below we discuss how further specialisation leads to conjectural relationships between the arithmetic of ‘higher Heegner points’ in (generalised) dihedral extensions of $\mathbb{Q}$ and the Galois module structure of Tate-Shafarevich and Selmer groups.

6.1. The general case. Let $F/k$ be a finite Galois extension of number fields with Galois group $G$. We set $n := [k : \mathbb{Q}]$. Let $A$ be an abelian variety of dimension $d$ defined over $k$. We write $A^t$ for the dual abelian variety and in general use the notation introduced in §2.2.1 and in §2.2.2. In particular, we always assume in the sequel that the Tate-Shafarevich group $X(A_F)$ of $A$ over $F$ is finite.

We recall that Burns and the first author have recently formulated a general ‘refined conjecture of Birch and Swinnerton-Dyer type’ [12, Conj. 3.3], and that this conjecture decomposes naturally into $p$-primary components for each rational prime $p$. In the sequel we fix an odd prime number $p$ and refer to the $p$-primary component of this conjecture as BSD$_p(A_F/F/k)$. See Lemma 3.11 in loc. cit. for a precise statement of the conjecture BSD$_p(A_F/F/k)$.

Throughout this section we give ourselves a fixed odd prime $p$ and an isomorphism of fields $\mathbb{C} \cong \mathbb{C}_p$ (that we will use to make certain implicit identifications but usually avoid mentioning explicitly). We recall that the Néron-Tate height pairing for $A$ over $F$ combines with this isomorphism to induce a canonical isomorphism of $\mathbb{C}_p[G]$-modules

$$h_{A_{F/k}} : A^t(F)_{\mathbb{C}_p} \cong \text{Hom}_{\mathbb{C}_p}(A(F)_{\mathbb{C}_p}, \mathbb{C}_p) = \text{Hom}_{\mathbb{Z}_p[G]}(A(F)_{\mathbb{Z}_p}, \mathbb{Z}_p[G])_{\mathbb{C}_p}.$$

The formulation of the conjecture BSD$_p(A_{F/k})$ relies on fixing a finite set $S$ of places of $k$ as well as a basis $\omega$ of global differentials. Its validity, however, is independent of these choices (see [12, Rem. 3.9(i)]).

We thus fix a finite set $S$ of places of $k$ with

$$S_{\infty}(k) \cup S_p(k) \cup S_{\text{ram}}(F/k) \cup S_{\text{bad}}(A) \subseteq S.$$

We also fix an ordered $k$-basis $\{\omega_j : j \in [d]\}$ of $H^0(A^t, \Omega^1_A)$ and we use this basis to define an explicit ‘classical period’ $\Omega^F_A$ in $\mathbb{Z}(\mathbb{C}[G])^\times$ as in [12] (42)].

We also denote by $w_{F/k}$ the ‘root number’ defined in [12] (43)].

In order to state the main result of this section we need to introduce some additional preliminary notation.
For each non-archimedean place \( p \). \( \text{Here } \Phi_v \text{ has a zero of order equal to the multiplicity } A \).

Then for any ordered subset
\[
x_\bullet := \{ x_{(i, \sigma)} : (i, \sigma) \in \{1, \ldots, d\} \times \Sigma(k) \}
\]
of \( A^t(F_p) \), we define a logarithmic resolvent element of \( Z(\mathbb{C}_p[G]) \) by setting
\[
\mathcal{LR}_v^G(x_\bullet) := \text{nr}_{\mathbb{Q}_p[G]} \left( \left( \sum_{g \in G} \hat{\sigma}^{-1}(\log \omega'_j(x_{(j', \sigma')})) \cdot g \right)_{(j, \sigma), (j', \sigma')} \right)
\]
where the indices \((j, \sigma)\) and \((j', \sigma')\) run over \( \{1, \ldots, d\} \times \Sigma(k) \), \( \hat{\sigma} \) is the scalar extension to \( F_p \) of a fixed extension to \( F \) of \( \sigma \in \Sigma(k) \), and \( \text{nr}_{\mathbb{Q}_p[G]}(\cdot) \) denotes the reduced norm of the given matrix in \( M_{dn}(\mathbb{Q}_p[G]) \).

6.1.2. Higher derivatives of Hasse-Weil-Artin L-series. For each \( \psi \in \text{Ir}(G) \) we write \( L_S(A, \psi, z) \) for the Hasse-Weil-Artin L-function of \( A \) and \( \psi \), truncated by removing the Euler factors corresponding to places in \( S \).

We always assume that this function has an analytic continuation to \( z = 1 \), where it has a zero of order equal to the multiplicity \( r(A, \psi) \) with which the character \( \psi \) occurs in the representation \( \mathbb{C} \cdot A^t(F) \) of \( G \), as is conjectured by Deligne and Gross (cf. [36 p. 127]).

For each non-archimedean place \( v \) of \( k \) that does not ramify in \( F/k \) and at which \( A \) has good reduction we define an element of \( Z(\mathbb{Q}[G]) \) by setting
\[
P_v(A_{F/k}, 1) := \text{nr}_{\mathbb{Q}_p[G]}(1 - \Phi_v \cdot a_v + \Phi_v^2 \cdot Nv^{-2}).
\]
Here \( \Phi_v \in G \) denotes the Frobenius automorphism of (a fixed place of \( F \) above) \( v \) while \( Nv \) denotes its absolute norm and \( a_v \) is the integer \( 1 + Nv - |A(\kappa_v)| \) where \( \bar{A} \) is the reduction of \( A \) to the residue field \( \kappa_v \) of \( v \).

For a non-negative integer \( a \) we write \( \text{Ir}(G)_{A,(a)} \) for the subset of \( \text{Ir}(G) \) comprising characters \( \psi \) for which \( r(A, \psi) \geq a \). This definition ensures that the \( Z(\mathbb{C}[G]) \)-valued function
\[
L_S^{(a)}(A_{F/k}, z) := \sum_{\psi \in \text{Ir}(G)_{A,(a)}} z^{-a} L_S(A, \psi, z) \cdot e_\psi
\]
is holomorphic at \( z = 1 \).

6.1.3. Idempotents. For each \( a \) we also define idempotents in \( Z(\mathbb{Q}[G]) \) by setting
\[
e_{(a)} = e_{F,(a)} := \sum_{\psi \in \text{Ir}(G)_{A,(a)}} e_\psi
\]
and
\[
e_a = e_{F,a} := \sum_{\psi \in \text{Ir}(G)_{A,(a)} \setminus \text{Ir}(G)_{A,(a+1)}} e_\psi
\]
(so that \( e_{(a)} = \sum_{b \geq a} e_b \)). We also set \( R_{(a)} := Z_p[G]e_{(a)} \) and \( I_{(a)} := Z_p[G] \cap R_{(a)} \).

6.1.4. The main result. The proof of this result will be given in \([6,1.5]\) below.

**Theorem 6.1.** Fix an ordered maximal subset \( X_\bullet := \{ x_{(i, \sigma)} : (i, \sigma) \in \{1, \ldots, d \} \times \Sigma(k) \} \) of \( A^i(F_p)^F_\sigma \) that is linearly independent over \( Z_p[G] \) and any finite non-empty set \( T \) of places of \( k \) that is disjoint from \( S \).

If the conjecture BSD\(_p\)(\( A_{F/k} \)) of \([12]\) is valid, then for any non-negative integer \( a \), for any \( a \)-tuples \( \theta_\bullet \) in \( \text{Hom}_{Z_p[G]}(A^i(F_p), Z_p[G]) \) and \( \phi_\bullet \) in \( \text{Hom}_{Z_p[G]}(A(F)_p, Z_p[G]) \), any element \( \alpha \) of \( I_{(a)} \), \( \mathcal{D}(R_{(a)}) \) and any element \( y \) of \( I_{(a)} \), the product

\[
\alpha \cdot \text{nr}_{Q_p[G]e_{(a)}}(y)^{2a} \cdot \left( \prod_{v \in T} \mathcal{T}_{P_v}(A_{F/k}, 1) \right) \cdot \frac{L_S^{(a)}(A_{F/k}, 1)}{\Omega_{A/F}^{(a)} \cdot w_{F/k}^{(a)}} \cdot \mathcal{L}_R_{A_{F/k}}(x_\bullet) \cdot (\lambda_j^{\phi} \cdot (\lambda_j^{\phi})^{-1}) (ht_{A_{F/k}}(\lambda_j^{\phi}))
\]

belongs to \( Z_p[G] \) and annihilates \( \text{III}(A_{F/k}^a)[p^\infty] \).

**Remark 6.1.** If \( C \in D^a(Z_p[G]) \) is the Nekovář-Selmer complex (associated to \( X_\bullet \) and \( T \)) constructed in \([12]\) Lem. 8.13 (ii), then our methods will show that the \( R_{(a)} \)-module \( R_{(a)} \otimes_{Z_p[G]} H^2(C) \) admits a free, quadratic presentation \( \Pi \) with the property that, if BSD\(_p\)(\( A_{F/k} \)) is valid, then the product \([22]\) with the term \( \alpha \) omitted, belongs to \( \text{Fit}_{R_{(a)}}(\Pi) \).

We remark on several ways in which Theorem 6.1 either simplifies or becomes more explicit.

**Remark 6.2.** If \( A(F) \) does not contain an element of order \( p \), then our methods will show that the prediction in Theorem 6.1 should remain true if the term \( \prod_{v \in T} \mathcal{T}_{P_v}(A_{F/k}, 1) \) is omitted from the product \([22]\). Indeed, in this case one may apply Corollary 5.3 directly to the Nekovář-Selmer complex that occurs in Proposition 2.3 (iii) rather than to its \( T \)-modification.

**Remarks 6.3.**

(i) In special cases one can either show, or is led to predict, that the idempotent \( e_{(a)} \) belongs to \( Z_p[G] \) and hence that the term

\[
\alpha \cdot \text{nr}_{Q_p[G]e_{(a)}}(y)^{2a}
\]

in the product \([22]\) can be taken to be any element of \( \mathcal{D}(R_{(a)}) \).

This is, for example, the case if \( a = 0 \), since each function \( L(A, \psi, z) \) is holomorphic at \( z = 1 \) and thus \( e_{(0)} = 1 \). This situation can also arise naturally in cases with \( a = 1 \) thanks to the existence of Heegner points or, more generally, to the result of Mazur and Rubin in \([29]\) Th. B. We shall consider the latter cases in detail in \([6,2]\) below.

(ii) If in addition \( e_{(a)} = 1 \), there exist \( a \)-tuples in \( A^i(F) \) and \( A(F) \) that are each linearly independent over \( \mathbb{Q}[G] \) and this fact implies the expressions \( (\lambda_j^{\phi})^{-1} \cdot (ht_{A_{F/k}}(\lambda_j^{\phi})) \) in Theorem 6.1 can be interpreted in terms of classical Néron-Tate heights.

To be a little more precise we use the following notation: for ordered \( a \)-tuples \( P_\bullet = \{ P_i : i \in [a] \} \) of \( A^i(F)_p \) and \( Q_\bullet = \{ Q_j : j \in [a] \} \) of \( A(F)_p \) we define a matrix in
Let \( M_a(C_p[G]) \) by setting
\[
h_{F/k}(P_\bullet, Q_\bullet) := (\sum_{g \in G} \langle g(P_i), Q_j \rangle_{A_F} \cdot g^{-1})_{1 \leq i,j \leq a},
\]
where \( \langle -,- \rangle_{A_F} \) denotes the Neron-Tate height pairing for \( A \) over \( F \) (and we have again used our fixed isomorphism \( C \cong C_p \)).

Then a direct generalisation of the argument used to prove [12 Lem. 8.10] gives a direct relationship between the reduced norm of the matrix \( e_a \cdot h_{F/k}(P_\bullet, Q_\bullet) \) of \( \text{GL}_a(C_p[G]e_a) \) and the set
\[
\xi(\mathbb{Z}_p[G]e_a) \cdot \left\{ (\hat{\lambda}_{j=1}^a \theta_j)(\text{ht}_{A_{F/k}}^{(a)}(\hat{\lambda}_{i=1}^a \phi_i)) \mid \theta_\bullet \subset A_t'(F)_p, \phi_\bullet \subset A(F)_p \right\}.
\]

In a related direction, Theorem 5.2 (ii) below also gives a similar explicit computation in cases with \( a = 1 \) but without necessarily assuming that \( e(1) = 1 \).

Finally we note that the result [12 Prop. 8.11] allows one to explicitly compute the relevant logarithmic resolvents occurring in (22) in many situations of interest.

**Remark 6.4.** Under suitable additional hypotheses it is also possible to obtain considerably more explicit versions of the containment predicted by Theorem 6.1, avoiding the use of logarithmic resolvents, which we expect should be amenable to numerical testing in (non-abelian) examples.

To be more precise, assume that neither \( A(F) \) nor \( A'(F) \) has a point of order \( p \), that \( p \) is unramified in \( k \), that all \( p \)-adic places of \( k \) are at most tamely ramified in \( F \) and that \( A, F/k \) and \( p \) satisfy the hypotheses (H1)-(H5) that are listed in §2.2.2.

Then, after taking account of the equality in [12 Rem. 6.6], the argument that is used to prove Theorem 6.1 can be directly applied to the classical Selmer complex \( SC_p(A_{F/k}) \) rather than to the Nekovář-Selmer complex associated to \( S \) and to our choice of semi-local points \( x_\bullet \).

In any such situations, one finds that the \( \hat{R}_{(\alpha)} \)-module \( \hat{R}_{(\alpha)} \otimes_{\mathbb{Z}_p[G]} \text{Sel}_p(A_{F'})^\vee \) admits a free, quadratic presentation \( \Pi_{\text{Sel}} \), and that BSD\(_p(A_{F/k}) \) predicts that for any given non-negative integer \( a \) and any data as in Theorem 6.1 the product
\[
\text{nr}_{\mathbb{Z}_p[G]e_a}(y)^{2a} \cdot \frac{L_{\text{ram}}^{(a)}(A_{F/k}, 1)}{\Omega_{A_{F/k}}^{(a)} \cdot y_{D_{F/k}}^{(a)}} \cdot (\tau^*(F/k) \cdot \prod_{v \in S_{\text{ram}}} \langle \theta_v \rangle^d) \cdot (\hat{\lambda}_{j=1}^a \theta_j)(\text{ht}_{A_{F/k}}^{(a)}(\hat{\lambda}_{i=1}^a \phi_i))
\]
should belong to \( \text{Fit}_{\hat{R}_{(\alpha)}}(\Pi_{\text{Sel}}) \), and then also to \( \text{Ann}_{\mathbb{Z}_p[G]!}(\Pi'(A_{F'}), [p^\infty]) \) after multiplication by any element \( \alpha \) in \( I_{(\alpha)} \cdot \mathcal{D}(R_{(\alpha)}) \).

Here \( L_{\text{ram}}^{(a)}(A_{F/k}, 1) \) is as defined above but with each \( L \)-function truncated only at the set of non-archimedean places \( S_{\text{ram}}(F/k) \) which ramify in \( F/k \) rather than at all places in \( S \) (as in the expression (22)). In addition, \( \tau^*(F/k) \) is the (modified) global Galois-Gauss sum of \( F/k \) defined in [12 §4.2.1], we have used the notation \( S_{p,\text{ram}} := S_p(k) \cap S_{\text{ram}}(F/k) \) and, for each \( v \) in this intersection, we have also set
\[
\theta_v := \sum_{\psi \in I_v(G)} \det(Nv \mid V^*_\psi) \cdot e_\psi.
\]

Here \( Nv \) denotes the absolute norm of \( v \), \( I_v \) is the inertia subgroup of \( v \) in \( G \) and \( V_\psi \) is any fixed complex representation of \( G \) of character \( \psi \).
This special case of Theorem 6.1 is thus itself a strong generalisation and refinement of [15] Prop. 5.2 and of [24] Cor. 3.5 (ii)]. We shall also make products of the form (24) fully explicit for dihedral twists of elliptic curves in Theorem 6.2 (iii) below.

**Remark 6.5.** One may obtain concrete congruences from the integrality claims of Theorem 6.1 or its variant in Remark 6.4 exactly as in [12] Pred. 8.5. In this regard see also Theorem 6.2 (ii) below.

6.1.5. The proof of Theorem 6.1 Fix an ordered subset \( x_{\bullet} \) of \( A^i(F_p)^{\pm} \) as well as a set \( T \) of places of \( k \) as in Theorem 6.1. Write \( X \) for the \( \mathbb{Z}[G] \)-module generated by \( x_{\bullet} \). Then we shall consider the \( T \)-modified Nekovář-Selmer complex \( C_{S,X,T} \in D^a(\mathbb{Z}_p[G]) \) that is constructed in [12] Lem. 8.13 (ii)], together with the \( \mathbb{C}_p \)-trivialisation \( (h^{T,F}_A)^{-1} \) and, under the assumption that \( \text{BSD}_p(A_{F/k}) \) is valid, characteristic element \( \mathcal{L}_T \in \zeta(\mathbb{C}_p[G])^x \), that are constructed in [12] Lem. 8.13 (iii)]. We recall that for any non-negative integer \( a \) one has

\[
e_a \cdot \mathcal{L}_T = \left( \prod_{v \in T} t_#(P_v(A_{F/k},1)) \right) \frac{L_S^{(a)}(A_{F/k},1)}{\Omega^{(a)}_A, w_{F/k}} \cdot \mathcal{L}R_{A_{F/k}}^{(a)}(x_{\bullet}).
\]

(We note that a different normalisation in the notion of a characteristic element justifies the disparities in sign between the above equality and the one occurring in [12] Lem. 8.13 (ii)]).

We also recall that from [12] Lem. 8.13 (ii)] that there exists a surjective homomorphism

\[
\pi : H^2(C_{S,X,T}) \to Y_{\pi}
\]

with finite kernel and the property that \( Y_{\pi} \) contains \( \text{Sel}_p(A_F)^{\vee} \) as a submodule of finite index. There also exists a canonical injective homomorphism \( \iota : H^1(C_{S,X,T}) \to A^i(F_p) \)

with finite cokernel. We will apply Corollary 5.3 to the triple given by \( (C_{S,X,T}, (h^{T,F}_A)^{-1}, \mathcal{L}_T), \pi, \phi_{\bullet} \) together with the surjective homomorphism \( \pi \).

In order to do so, we fix a non-negative integer \( a \) and an \( a \)-tuple \( \phi_{\bullet} \) in \( \text{Hom}_{\mathbb{Z}_p[G]}(A(F_p), \mathbb{Z}_p[G]) \). We fix a pre-image \( \phi_{\bullet}' \) of each \( \phi_i \) under the surjective homomorphism occurring in the canonical short exact sequence

\[
\begin{align*}
0 & \longrightarrow \text{III}(A_F)[p^\infty]^{\vee} \longrightarrow \text{Sel}_p(A_F)^{\vee} \longrightarrow \text{Hom}_{\mathbb{Z}_p}(A(F_p), \mathbb{Z}_p) \longrightarrow 0.
\end{align*}
\]

We set \( \phi_{\bullet}' := (\phi_{\bullet}')_{1 \leq i \leq a} \) and view this \( a \)-tuple as comprising elements of \( Y_{\pi} \).

Then the non-abelian higher special element associated to the data \( (C_{S,X,T}, (h^{T,F}_A)^{-1}, \mathcal{L}_T, \pi, \phi_{\bullet}') \) coincides with the pre-image under the bijective map \( \bigwedge_{C_{S,X,T}} \iota \) of the element

\[
\left( \prod_{v \in T} t_#(P_v(A_{F/k},1)) \right) \cdot \frac{L_S^{(a)}(A_{F/k},1)}{\Omega^{(a)}_A, w_{F/k}} \cdot \mathcal{L}R_{A_{F/k}}^{(a)}(x_{\bullet}) \cdot \text{ht}_{A_{F/k}}^{(a)}(w_{F/k}^{i=0} \phi_{i}).
\]

We fix an \( a \)-tuple \( \theta_{\bullet} \) in \( \text{Hom}_{\mathbb{Z}_p[G]}(A^i(F_p), \mathbb{Z}_p[G]) \), and identify it with its image under the injective map

\[
\text{Hom}_{\mathbb{Z}_p[G]}(A^i(F_p), \mathbb{Z}_p[G]) \to \text{Hom}_{\mathbb{Z}_p[G]}(H^1(C_{S,X,T}), \mathbb{Z}_p[G])
\]

induced by \( \iota \).
Then Corollary 6.3 implies that any element of the form \( p \) belongs to
\[
\text{Ann}_{\mathbb{Z}[G]}((Y_\tau)_{\text{tor}}) \subseteq \text{Ann}_{\mathbb{Z}[G]}((\text{Sel}_p(A_F)\uparrow)_{\text{tor}}).
\]
To complete the proof of Theorem 6.1 it is therefore enough to note that the exact sequence (24) identifies \((\text{Sel}_p(A_F)\uparrow)_{\text{tor}}\) with \(\text{III}(A_F)[p^\infty]\uparrow\) and that the Cassels-Tate pairing identifies \(\text{III}(A_F)[p^\infty]\uparrow\) with \(\text{III}(A'_F)[p^\infty]\).

6.2. Dihedral twists of elliptic curves. In this section we assume that \(A\) is an elliptic curve and that \(F/k\) is a generalised dihedral extension in the sense of Mazur and Rubin [29].

We recall that this condition means that \(G\) has an abelian normal Sylow \(p\)-subgroup \(P\) of index two (where \(p\) still denotes an odd prime) and that the conjugation action of any lift to \(G\) of the generator of \(G/P\) inverts elements of \(P\). In the sequel we fix such a lift \(\tau \in G\) and also set \(K := F^P\). We write \(\epsilon\) for the unique linear non-trivial character of \(G\).

6.2.1. Statement of the main result. For any \(G\)-module \(M\) we set \(M' := \mathbb{Z}^{[1]} \otimes \mathbb{Z} M\). For any \(\psi \in \text{Ir}(G)\) we write \(T_\psi\) for the element \(\sum_{g \in G} \psi(g^{-1}) \cdot g\) of \(Z(\mathbb{C}_p[G])\) and also use the product of periods \(\Omega_\psi^A\) and Artin root number \(w_\psi\) specified in [12 §4.1]. We recall that, in particular, one has
\[
\Omega_\psi^A = \Omega_\psi^A := \prod_{v \in S_C(k)} \Omega_{A,v} \cdot \prod_{v \in S_h(k)} \Omega_{A,v}^+
\]
and
\[
\Omega_\psi^A = \Omega_\psi^{-A} := \prod_{v \in S_C(k)} \Omega_{A,v} \cdot \prod_{v \in S_h(k)} \Omega_{A,v}^-
\]
with each individual term \(\Omega_{A,v}, \Omega_{A,v}^+, \Omega_{A,v}^-\) defined in loc. cit. as a fully explicit classical period.

We still assume to be given a set \(S\) of places of \(k\) as in [21]. We again abbreviate \(S_{\text{ram}}(F/k)\) to \(S_{\text{ram}}\), while \(S_{\text{ram}}'\) will denote the subset of \(S_{\text{ram}}(F/k)\) comprising places which split in \(K/k\). In addition \(d_k\) and \(d_K\) denote the discriminants of \(k\) and of \(K\) respectively while \(Nf(\phi)\) is be the absolute norm of the Artin conductor of any \(\phi\) in \(\text{Ir}(P)\). In addition we will use the ‘unramified characteristic’
\[
u_\psi := \prod_{v \in S_{\text{ram}}} \text{det}(-\Phi_{\psi}^{-1} | V_{\psi}^I)
\]
for each \(\psi \in \text{Ir}(G)\).

If \(Q\) is a given point in \(A(F)\) which satisfies \(\tau(Q) = (-1)^{i_Q} Q\) with \(i_Q \in \{0,1\}\) then for any \(\psi \in \text{Ir}(G)\) we set
\[
h_{F,\psi}(Q) := \begin{cases} 1, & \text{if either } \psi = 1_G \text{ and } i_Q = 1, \text{ or } \psi = \epsilon \text{ and } i_Q = 0, \\ \psi(1) | G |^{-1} \langle T_\psi(Q), T_\psi(Q) \rangle_{A_F}, & \text{otherwise.} \end{cases}
\]
and then also

\[ Q_\psi := \begin{cases} 
(-1)^{S_{\text{ram}}} \cdot \sqrt{|d_K|} \cdot \frac{L'_{\text{ram}}(A,1)}{\Omega_A h_{F,F/k}(Q)}, & \text{if } \psi = 1_G, \\
(-1)^{S_{\text{ram}}} \cdot \sqrt{|d_K/d_k|} \cdot \frac{L'_{\text{ram}}(A,\epsilon,1)}{\Omega_A h_{F,k}(Q)}, & \text{if } \psi = \epsilon, \\
u_\psi \cdot \sqrt{|d_K|} \cdot N f(\phi) \cdot \frac{L'_{\text{ram}}(A,\psi,1)}{\Omega_A h_{F,k}(Q)}, & \text{if } \psi = \text{Ind}_F^G(\phi) \text{ with } \phi \in \text{Ir}(P).
\end{cases} \]

The proof of this result will be given in [3] below.

**Theorem 6.2.** Let \( F/k \) be a generalised dihedral extension, with \( K := F^P \) as above, and let \( A \) be an elliptic curve. Assume that \( F/k \) is unramified at all places of \( k \) at which \( A \) has bad reduction, that all \( p \)-adic places of \( k \) split completely in the quadratic extension \( K/k \) and that the rank of \( A(K) \) is odd.

(i) Then there exists a point \( Q \) in \( A(F) \) which satisfies \( \tau(Q) = (-1)^iQ \) with \( i_1 \in \{0,1\} \) and generates a \( \mathbb{Z}[G] \)-submodule \( (Q) \) of \( A(F)^\vee \) isomorphic to \( \mathbb{Z}[G](1 + (-1)^i\tau) \).

If in addition one has \( A(K)[p] = 0 \) and also

\[ (1 + (-1)^i\tau) \text{Tr}_{F/k}(A(F)) \not\equiv p \cdot A(K) \]

for some \( i \in \{0,1\} \), then one may choose the point \( Q \) so that \( i_1 = i \) and \( (Q) \)

is a direct summand of the \( \mathbb{Z}_p[G] \)-module \( A(F)_p = A(F)_{p,\text{tr}} \).

In the sequel fix a point \( Q \) as in claim (i) and write \( t_Q \) for the exponent of the group \( (A(F)_{p,\text{tr}}/(Q))_{\text{tor}} \).

(ii) There is an element \( \phi_Q \) of \( \text{Hom}_{\mathbb{Z}_p[G]}(A(F)_p, \mathbb{Z}_p[G]) \) with the property that

\[ e(1) \cdot (\lambda^{i_1}_j \cdot 1_Q \cdot \phi_Q)(\lambda^{i_1}_1 \cdot (\lambda^{i_1}_j \cdot 1_Q \cdot \phi_Q)) = e(1) \cdot \sum_{\psi \in \text{Ir}(G)} t_Q^{2\psi(1)} \cdot h_{F,\psi}(Q)^{-1} \cdot e_\psi. \]

In the sequel we assume that \( A(K)[p] = 0 \) and that the hypotheses \((H_1)-(H_4)\) that are listed in [3] are satisfied.

(iii) The \( R_{(1)} \)-module \( R_{(1)} \otimes_{\mathbb{Z}_p[G]} \text{Sel}_p(A_F)^\vee \) admits a free, quadratic presentation \( \Pi_{\text{Sel}} \) with the property that, if \( p \) is unramified in \( F/Q \) and the conjecture \( \text{BSD}(A_{F/k}) \) of [12] is valid, then the product

\[ \text{nr}_{Q_p[G]}(y)^2 \cdot \left( \sum_{\psi \in \text{Ir}(G)} t_Q^{2\psi(1)} \cdot Q_\psi \cdot e_\psi \right) \]

belongs to \( \text{Fit}_{R_{(1)}}^1(\Pi_{\text{Sel}}) \) for any \( y \in I_{(1)} \) and, after multiplication by any element of \( \alpha \in I_{(1)} \cdot D(R_{(1)}) \), also to \( \text{Ann}_{\mathbb{Z}_p[G]}(\text{III}(A_{F})[p^\infty]) \).

In particular, we fix any elements \( \delta_\psi \) in the inverse different of the fields generated over \( Q_p \) by the values of each \( \psi \) in \( \text{Ir}(G) \). We set \( m_\psi := n(2\psi(1)+1) \).

Then if \( \text{rk}(A(k)) = 0 \), one has

\[ \sum_{\psi \neq 1_G} p^m \cdot t_Q^{2\psi(1)} \cdot \hat{\psi} \cdot Q_\psi \delta_\psi \in \mathbb{Z}_p \]

for every \( g \in G \).
If instead \( \text{rk}(A(k)) = \text{rk}(A(K)) = 1 \), one has
\[
\sum_{\psi \neq \epsilon} p^{e_{\psi}t_{Q}^{2(1)}}(g) \delta_{\psi} Q_{\psi} \in \mathbb{Z}_p
\]
for every \( g \in G \).

In all other cases, one has
\[
\sum_{\psi \in \text{Ir}(G)} t_{Q}^{2(1)}(g) \delta_{\psi} Q_{\psi} \in \mathbb{Z}_p
\]
for every \( g \in G \).

(iv) If \( P \) is cyclic and for every subgroup \( H \) of \( P \) the restriction map \( \text{I}_{\Pi}(A_{F,F}) \to \text{I}_{\Pi}(A_{F}) \) is injective, then one may choose the point \( Q \) so that \( \langle Q \rangle_p \) is a direct summand of the \( \mathbb{Z}_p[G] \)-module \( A(F)_p = A(F)_{p,tt} \), so in particular \( t_Q = 1 \).

Remarks 6.6.

(i) The proof of the final assertions of claim (iii) will rely on making explicit choices of \( \gamma \in \text{I}(1) \) and of \( \alpha \in \text{I}(1) \cdot \mathcal{D}(R_{(1)}) \) which would also determine fully explicit elements of \( \text{Ft}_{\Pi}(\Pi_{\text{Sel}}) \) and of \( \text{Ann}_{\mathbb{Z}_p[G]}(\text{I}_{\Pi}(A_{F})) \).

(ii) Both claim (ii) of Theorem 6.2, when combined with Theorem 6.1, and claim (iii) of Theorem 6.2 extend the congruence relations predicted by Burns, Wuthrich and the first author in Theorem 5.8 of [15]. We recall that in loc. cit., in addition to all the hypotheses of claim (iii), it was assumed that the rank of \( A(K) \) is equal to 1 and that \( \text{I}_{\Pi}(A_{K})[p^\infty] \) vanishes. In particular, the assertions of claim (iii) hold unconditionally for the families for which the conjecture BSD(\( A_{F/k} \)) was verified, either theoretically or numerically, via Theorem 5.8 of loc. cit..

(iii) Moreover, our methods lead to more general, albeit less explicit, versions of claim (iii) which do not require \( p \) to be unramified in \( F/Q \) while at the same time circumventing the need for the logarithmic resolvents occurring in the much more general claim (ii).

For instance, if \( p \) is unramified in \( k/Q \) rather than in \( F/Q \) (so in particular if \( k = Q \)), then under the assumed compatibility of specific cases of the ‘local epsilon constant conjecture’, and the assumed validity of a conjecture of Breuning [8, Conj. 3.2], the given claims for the element \( \{25\} \) would remain true after multiplying it by the product, over all \( p \)-adic places of \( k \) that are wildly ramified in \( F \), of the fully explicit elements occurring in the display [12, (51)].

In this regard we recall that work of Breuning [5, 6], of Bley and Debeerst [3] and of Bley and Cobbe [1] provides verifications of Breuning’s conjecture for natural families of dihedral extensions of \( Q \) in which \( p \) is wild ramified. Similarly, Bley and Cobbe [2] have proved the compatibility of the relevant cases of the local epsilon constant conjecture for certain families of wildly ramified extensions. See [12, Rem. 6.7, Rem. 6.8, §5.3] for a more detailed account.

Example 6.7. Assume that the elliptic curve \( A \) is defined over \( k = Q \) and has conductor \( N \). We fix a modular parametrisation \( \varphi_A : X_0(N) \to A \) of minimal degree. We assume that the given generalised dihedral extension \( F \) of \( Q \) contains an imaginary quadratic field \( K \) in which all prime divisors of \( N \) split, and in addition that the
Conductor $c$ of $F$ is a square-free product of primes that are both inert in $K$ and coprime to $N$.

We write $K_c$ for the ring class field of $K$ of conductor $c$ and set $G_c := \text{Gal}(K_c/K)$. Then a standard construction described in [12] §12.1 gives a canonical point $x_c$ on $X_0(N)/(K_c)$ and we follow loc. cit. in defining a 'higher Heegner point' $y_c := \varphi_A(x_c)$ of $A(K_c)$.

Assuming $L(A_K, z)$ vanishes to order one at $z = 1$, Zhang’s generalisation [38] 39 of the seminal results of Gross and Zagier in [21] implies that for every $\phi$ in $\text{Ir}(G_c)$ the function $L(A_K, \phi, z)$ vanishes to order one at $z = 1$ and that the number $\langle T_\phi(y_c), T_\phi(y_c) \rangle_{A_k}$ is non-zero.

In this setting one therefore knows that the rank of $A(K)$ is equal to 1 and, via the proof of this result given in §2.2.2 below, also that the point $Q := \text{Tr}_{K_c/F}(y_c)$ of $A(F)$ satisfies the conditions of claim (i) of Theorem 6.2.

If we now assume that $A(K)[p] = 0$ (with the prime $p$ determined by the generalised dihedral extension $F/\mathbb{Q}$), that the hypotheses (H1)-(H4) that are listed in §2.2.2 are satisfied and that the point $\text{Tr}_{K_c/K}(y_1)$ of $A(K)$ is not divisible by $p$, then it is easy to see that the number $t_Q$ occurring in the expression (25) is equal to 1. It follows that claim (iii) of Theorem 6.2 describes explicit relationships, between the arithmetic of higher Heegner points of $A$ in generalised dihedral extensions $F/\mathbb{Q}$ and the Galois module structure of Tate-Shafarevich and Selmer groups in $F/\mathbb{Q}$, that are encoded in the refined Birch and Swinnerton-Dyer conjecture BSD($A_{F/\mathbb{Q}}$) of [12].

In particular, this claim extends the description of such relationships that is given in Theorem 12.2 (ii) of loc. cit., which is instead solely concerned with the $\text{Gal}(F/K)$-module structure of $\text{III}(A_F)$.

In fact in the setting of this Example, it is straightforward to prove a converse to Theorem 6.2 (iii) that gives an explicit criterion to verify the validity of (the $p$-component) of conjecture BSD($A_{F/\mathbb{Q}}$) in terms of the properties of the point $Q = \text{Tr}_{K_c/F}(y_c)$.

This approach will be developed in greater generality in future work.

6.2.2. The proof of Theorem 6.2. To prove claim (i) we use the result [29, Thm. B] of Mazur and Rubin, which implies that the $\mathbb{Q}_p[P]$-module $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \text{Sel}_p(A_F)^{\vee} \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} A(F)_p^*$ has a direct summand that is isomorphic to $\mathbb{Q}_p[P]^\cdot$. The same is thus true of the $\mathbb{Q}_p[P]$-module $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} A(F)_p$.

The $\mathbb{Q}_p[G]$-submodule generated by this summand inside of $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} A(F)_p$ must then contain a copy of either $\mathbb{Q}_p[G](1 + \tau)$ or of $\mathbb{Q}_p[G](1 - \tau)$. Setting $e \pm := \frac{1 - \pm}{\mp}$ we then deduce the existence of an injective homomorphism of $\mathbb{Z}_p[G]$-modules $\mathbb{Z}_p[G]e \pm \rightarrow A(F)_p$. The existence of the claimed point $Q$ then follows easily from Roiter’s Lemma [13] (31.6).

Now, if one has $(1 + (-1)^i \tau) \text{Tr}_p(A(F)) \not\subseteq p \cdot A(K)$ for some $i \in \{0, 1\}$, proving that one may choose the point $Q$ with $i_Q = i$ is a relatively straightforward exercise which we leave to the reader. Moreover, after replacing such a point $Q$ by $(1 + (-1)^i \tau) Y + p^N Q$ if necessary, for any given point $Y$ of $A(F)$ with $(1 + (-1)^i \tau) \text{Tr}_p(Y) \not\subseteq p \cdot A(K)$ and a large enough positive integer $N$, one may assume in addition that $\text{Tr}_p(Q) \not\subseteq p \cdot A(K)$. 
To conclude the proof of claim (i) we shall now use this condition, together with the assumption $A(K)[p] = 0$, to verify that $\langle Q \rangle_p$ is a direct summand of the $\mathbb{Z}_p[G]$-module $A(F)_p$. We first observe that the two given conditions imply that the quotient $A(K)_p/\mathbb{Z}_p \cdot \text{Tr}_P(Q)$ is $\mathbb{Z}_p$-free.

But $\langle Q \rangle_p$ is a cohomologically-trivial $P$-module and so one has a canonical isomorphism

$$A(K)_p/\langle Q \rangle_p^P \cong (A(F)_p/\langle Q \rangle_p)^P.$$ 

Since in addition $\langle Q \rangle_p^P = \mathbb{Z}_p \cdot \text{Tr}_P(Q)$ we deduce that $(A(F)_p/\langle Q \rangle_p)^P$ is also $\mathbb{Z}_p$-free. Since $P$ is a $p$-group, the quotient $A(F)_p/\langle Q \rangle_p$ must itself be $\mathbb{Z}_p$-free.

This last fact implies that there is a canonical isomorphism

$$\text{Ext}^1_{\mathbb{Z}_p[G]}(A(F)_p/\langle Q \rangle_p, \langle Q \rangle_p) \cong H^1(G, \text{Hom}_{\mathbb{Z}_p}(A(F)_p/\langle Q \rangle_p, \langle Q \rangle_p))$$ 

and, since the latter group vanishes (because $\langle Q \rangle_p$ is a projective $\mathbb{Z}_p[G]$-module), we finally find that $\langle Q \rangle_p$ is indeed a direct summand of the $\mathbb{Z}_p[G]$-module $A(F)_p$. This completes the proof of claim (i).

We now consider claim (ii). We observe first that there is a canonical exact sequence

$$\text{Hom}_{\mathbb{Z}_p[G]}(A(F)_p, \mathbb{Z}_p[G]) \to \text{Hom}_{\mathbb{Z}_p[G]}((\langle Q \rangle_p), \mathbb{Z}_p[G]) \to (A(F)_p, \langle Q \rangle_p) \to (A(F)_p, \langle Q \rangle_p)_{\text{cor}}.$$ 

We define $Q^* \in \text{Hom}_{\mathbb{Z}_p[G]}((\langle Q \rangle_p), \mathbb{Z}_p[G])$ by setting $Q^*(Q) := 1$ and also $Q^*(\pi \cdot Q) := 0$ for each $\pi \in P$. We then let $\phi_Q$ be any element of $\text{Hom}_{\mathbb{Z}_p[G]}(A(F)_p, \mathbb{Z}_p[G])$ whose restriction to $\langle Q \rangle_p$ is equal to $t_Q \cdot Q^*$.

Then an explicit computation shows that

$$e(1) \cdot (\Lambda^\varphi=1 \phi_Q)(\lambda^\varphi=1) = e(1) \cdot \text{nr}_{\mathbb{Z}_p[G]}(t_Q)^2 \cdot \text{nr}_{\mathbb{Z}_p[G]}(c_{\mathbb{Z}_p}[p]) (e(1) \cdot (g(Q, Q)_A \cdot g^{-1}))^{-1}$$

as required.

We now assume that $A(K)[p] = 0$ and that the hypotheses $(H_1)$–$(H_4)$ that are listed in \S2.2.2 are satisfied, and proceed to deduce the validity of claim (iii) from the variant of Theorem B.1 that is given in Remark D.4.

In fact, in view of the computation (26) and of the explicit definitions of $L^{(1)}_S(A_{F/k}, 1)$, of $\Omega^\psi_A := \sum_{\psi \in \text{Ir}(G)} \Omega^\psi_A \cdot e_\psi$ and of $w_{F/k} := \sum_{\psi \in \text{Ir}(G)} w_\psi \cdot e_\psi$, the first assertion of claim (iii) is valid because if $p$ is unramified in $F/Q$ then

$$\frac{L^{(1)}_S(A_{F/k}, 1)}{\Omega^\psi_A \cdot w_{F/k}} \cdot \tau^*(F/k) \cdot \left( \sum_{\psi \in \text{Ir}(G)} h_{F, \psi}(Q) \cdot e_\psi \right)^{-1} = \sum_{\psi \in \text{Ir}(G)} Q_\psi \cdot e_\psi.$$ 

This equality is itself an immediate consequence of the computation of the term $\tau^*(F/k) \cdot w_{F/k}^{-1}$ that is carried out in [15] (21).

As for the final assertion of claim (iii), we use the fact that, for any family $(C_\psi)_{\psi \in \text{Ir}(G)}$ of elements of $\mathbb{C}_p$, the sum

$$\sum_{\psi \in \text{Ir}(G)} C_\psi \cdot e_\psi = \sum_{g \in G} (|G|^{-1} \sum_{\psi \in \text{Ir}(G)} \psi(1) \tilde{\psi}(g) C_\psi) \cdot g$$

where $\tilde{\psi}(g)$ is the non-abelian higher special elements of $\mathbb{C}_p$. This is a consequence of the fact that $\tilde{\psi}(g)$ is a cohomologically-trivial $P$-module for any $P$-extension $P \to G$.
belongs to $\mathbb{Z}_p[G]$ if and only if, for each $g \in G$, the sum $\sum_{\psi \in \text{Ir}(G)} \psi(1) \psi(g) C_\psi$ belongs to $|G| \cdot \mathbb{Z}_p$.

We will combine this observation with the first assertion of claim (iii). We first observe that from claim (i) one easily deduces that

$$e_{(1)} = \begin{cases} 1 - e_{1_G}, & \text{if } \text{rk}(A(k)) = 0, \\ 1 - e_{e}, & \text{if } \text{rk}(A(k)) = \text{rk}(A(K)) = 1, \\ 1, & \text{otherwise}. \end{cases}$$

We may thus use the element

$$y = \begin{cases} p^n(1 - e_{1_G}), & \text{if } \text{rk}(A(k)) = 0, \\ p^n(1 - e_{e}), & \text{if } \text{rk}(A(k)) = \text{rk}(A(K)) = 1, \\ 1, & \text{otherwise} \end{cases}$$

of $I_{(1)}$ to construct the product (25). In addition, for any given elements $\delta_\psi$ as in the statement of this final assertion, the arguments of Johnston and Nickel in [22, §6.4] then imply that we may use the element

$$\alpha := y \cdot |G| \sum_{\psi \in \text{Ir}(G)} (1) - 1 \delta_\psi e_\psi$$

of $I_{(1)} \cdot D(R_{(1)})$.

From the first assertion of claim (iii) we then know that the element

$$\alpha \cdot \text{nrt}_p[|G|]_{(1)} \cdot (y)^2 \cdot \left( \sum_{\psi \in \text{Ir}(G)} \iota_Q^{2\psi(1)} \cdot Q_\psi \cdot e_\psi \right)$$

$$= y \cdot \text{nrt}_p[|G|]_{(1)} \cdot (y)^2 \cdot \left( |G| \cdot \iota_Q^{2\psi(1)} \cdot (1)^{-1} \cdot \delta_\psi \cdot Q_\psi \cdot e_\psi \right)$$

belongs to $\text{Ann}_{\mathbb{Z}_p[G]}(\Pi(A_F)[p^\infty]) \subseteq \mathbb{Z}_p[G]$.

Now for our chosen element $y$ we have

$$y \cdot \text{nrt}_p[|G|]_{(1)} \cdot (y)^2 = \begin{cases} \sum_{\psi \neq 1_G} p^{n(2\psi(1) + 1)} e_\psi, & \text{if } \text{rk}(A(k)) = 0, \\ \sum_{\psi \neq e} p^{n(2\psi(1) + 1)} e_\psi, & \text{if } \text{rk}(A(k)) = \text{rk}(A(K)) = 1, \\ 1, & \text{otherwise}, \end{cases}$$

and so the claimed explicit integrality conditions follow from the general argument given just below (27).

We finally note that the validity of claim (iv) follows directly upon combining the result [29, Thm. B] of Mazur and Rubin used above with a (dual) variant of [14, Thm. 2.7 (ii)] that replaces the dependence of this result on Proposition 3.1 from loc. cit. (which is formulated in terms of cokernels of norm maps on $p$-primary Tate-Shafarevich groups) by the use of the result [23, Lem. 3.3] (formulated instead in terms of kernels of restriction maps).

**References**

[1] W. Bley, A. Cobbe, Equivariant epsilon constant conjectures for weakly ramified extensions, Math. Zeit. 283 (2016) 1217-1244.
[2] W. Bley, A. Cobbe, The equivariant local epsilon constant conjecture for unramified twists of $\mathbb{Z}_p(1)$, Acta Arith. 178 (2017) 313-383.
[3] W. Bley, R. Debeerst, Algorithmic proof of the epsilon constant conjecture, Math. Comp. 82 (2013) 2363-2387.
[4] S. Bloch, K. Kato, $L$-functions and Tamagawa numbers of motives, In: ‘The Grothendieck Festschrift’ vol. 1, Prog. Math. 86, Birkhäuser, Boston, (1990) 333-400.
[5] M. Breuning, On equivariant global epsilon constants for certain dihedral extensions, Math. Comp. 73 (2004) 881-898.
[6] M. Breuning, Equivariant local epsilon constants and étale cohomology, J. London Math. Soc. (2) 70 (2004), 289-306.
[7] D. Burns, On derivatives of Artin $L$-series, Invent. Math. 186 (2011) 291-371.
[8] D. Burns, M. Flach, Tamagawa numbers for motives with (non-commutative) coefficients, Doc. Math. 6 (2001) 501-570.
[9] D. Burns, M. Kurihara, T. Sano, On zeta elements for $\mathbb{G}_m$, Documenta Math. 21 (2016) 555-626.
[10] D. Burns, M. Kurihara, T. Sano, On Stark elements of arbitrary weight and their $p$-adic families, to appear in Proceedings of Iwasawa 2017.
[11] D. Burns, D. Macias Castillo, Organising matrices for arithmetic complexes, Int. Math. Res. Notices 2014 10 (2014) 2814-2883.
[12] D. Burns, D. Macias Castillo, On refined conjectures of Birch and Swinnerton-Dyer type for Artin-Hasse-Weil $L$-series, to appear in Memoirs of the Amer. Math. Soc..
[13] D. Burns, D. Macias Castillo, S. Seo On special elements for $\mathbb{G}_m$, preprint (2021), arXiv:2111.11109.
[14] D. Burns, D. Macias Castillo, C. Wuthrich, On the Galois structure of Selmer groups, Int. Math. Res. Notices 2015 (2015) 11909-11933.
[15] D. Burns, D. Macias Castillo, C. Wuthrich, On Mordell-Weil groups and congruences between derivatives of twisted Hasse-Weil $L$-functions, J. reine angew. Math. 734 (2017) 187-228.
[16] D. Burns, D. Macias Castillo, K.-W. Tsai, On non-commutative Euler systems, preprint (2020), arXiv:2004.10564.
[17] D. Burns, T. Sano, K.-W. Tsai, On higher special elements of $p$-adic representations, to appear in Int. Math. Res. Notices.
[18] J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, The $GL_2$ main conjecture for elliptic curves without complex multiplication, Publ. IHES 101 (2005) 163-208.
[19] C. W. Curtis, I. Reiner, Methods of Representation Theory, Vol. I, John Wiley and Sons, New York, 1981.
[20] T. Fukaya, K. Kato, A formulation of conjectures on $p$-adic zeta functions in non-commutative Iwasawa theory, Proc. St. Petersbg Math. Soc. Vol. XII, 1–85, Amer. Math. Soc. Transl. Ser. 2, 219, Amer. Math. Soc., Providence, RI, 2006.
[21] B. H. Gross, D. B. Zagier, Heegner points and derivatives of $L$-series, Invent. Math. 84 (1986) 225-320.
[22] H. Johnston, A. Nickel, Noncommutative Fitting invariants and improved annihilation results, J. London Math. Soc. 88 (2013) 137-160.
[23] D. Macias Castillo, On the Krull-Schmidt decomposition of Mordell-Weil groups, Tokyo J. Math. 40 (2017) 353-378.
[24] D. Macias Castillo, Congruences for critical values of higher derivatives of twisted Hasse-Weil $L$-functions, II, Acta Arith. 195 (2020) 327-365.
[25] B. Mazur, K. Rubin, Elliptic curves and class field theory, In: Ta Tsien Li (Ed.), Proceedings of the International Congress of Mathematicians 2002, vol. II, Higher Education Press, Beijing, 2002, pp. 185-195.
[26] B. Mazur, K. Rubin, Pairings in the theory of elliptic curves, In: J. Cremona et al (Eds.), Modular Curves and Abelian Varieties, Progress in Math. 224, 2004, pp. 151-163.
[27] B. Mazur, K. Rubin, Kolyvagin systems, Mem. Amer. Math. Soc. 799 (2004).
[28] B. Mazur, K. Rubin, Organizing the arithmetic of elliptic curves, Adv. Math. 198 (2005) 504-546.
[29] B. Mazur, K. Rubin, Finding large Selmer rank via an arithmetic theory of local constants, Ann. Math. 166 (2007) 579-612.
[30] B. Mazur, J. Tate, Refined Conjectures of the Birch and Swinnerton-Dyer Type, Duke Math. J. 54 (1987) 711-750.
[31] J. Nekovář, Selmer complexes, Astérisque 310, S.M.F., Paris, 2006.
[32] A. Nickel, Non-commutative Fitting invariants and annihilation of class groups, J. Algebra 323 (2010) 2756-2778.
[33] A. Nickel, On non-abelian Stark-type conjectures, Ann. Inst. Fourier 61 (2011) 2577-2608.
[34] A. Nickel, Leading terms of Artin $L$-series at negative integers and annihilation of higher $K$-groups, Math. Proc. Camb. Philos. Soc. 151 (2011) 1-22.
[35] A. Nickel, Annihilating wild kernels, Documenta Math. 24 (2019) 2381-2422.
[36] D. Rohrlich, The vanishing of certain Rankin-Selberg convolutions, Automorphic forms and analytic number theory (University of Montréal, 1990) 123-133.
[37] C. Weibel, An introduction to homological algebra, Cambridge Studies in Advanced Mathematics 38. Cambridge University Press, Cambridge, 1994.
[38] S-W Zhang, Heights of Heegner points on Shimura curves, Ann. of Math. 153 (2001) 27-147.
[39] S-W Zhang, Gross-Zagier Formula for $GL(2)$, II, in Heegner Points and Rankin $L$-Series, Math. Sci. Res. Inst. Publ. 49, Cambridge Univ. Press, Cambridge, 2004, 191-214.