

## ORGANISING MATRICES FOR ARITHMETIC COMPLEXES

*Preliminary version of September 2011*

DAVID BURNS AND DANIEL MACIAS CASTILLO

ABSTRACT. We extend and refine the theory of ‘organising modules’ of Mazur and Rubin to construct a canonical class of matrices that encodes a wide range of detailed information about certain natural families of complexes in arithmetic. We also describe a variety of concrete applications of the general theory including the proof of new results on the explicit structures of Galois groups, ideal class groups, wild kernels in higher algebraic  $K$ -theory and Mordell-Weil and Selmer groups of elliptic curves. Our approach also leads to the formulation of several explicit refinements of the Birch and Swinnerton-Dyer Conjecture for abelian varieties that predict, for example, precise integral congruence relations between the heights of distinguished points on a wide range of elliptic curves and the values at  $s = 1$  of derivatives of the Hasse-Weil  $L$ -functions of dihedral twists of these curves.

## INTRODUCTION

Let  $E$  be an elliptic curve defined over a number field  $K$ ,  $p$  a rational prime and  $K_\infty$  a  $\mathbb{Z}_p$ -power extension of  $K$ . The possibility of a theory of ‘organising modules’ for  $E$  over  $K_\infty$  was first mooted by Mazur and Rubin in [34, 35] as a means of encoding in a single skew-Hermitian matrix with entries drawn from the Iwasawa algebra of  $K_\infty/K$  detailed information about the Mordell-Weil groups and their  $p$ -adic height pairings, and the Tate-Shafarevich groups and their Cassels pairings, of  $E$  over all finite extensions of  $K$  in  $K_\infty$ . A little later, Mazur and Rubin successfully constructed such a theory in [36] under some not-too-stringent conditions on  $E$  and  $K$  by using the Selmer complexes that were introduced by Nekovář in [40].

In the present article we shall both extend and refine the above theory by associating a canonical family of ‘organising matrices’ to a wide variety of arithmetic complexes, including the compactly supported étale cohomology of general Tate modules and both the Nekovář-Selmer complexes and finite support cohomology complexes of a natural class of critical motives. We show that these matrices simultaneously encode a wide

range of detailed arithmetic information concerning, for example, the explicit Galois structure of Tate-Shafarevich and Selmer groups (in the sense of Bloch and Kato), the evaluation of canonical algebraic height pairings, the computation of canonical extension classes (for example, in class field theory) and the nature of explicit families of congruence relations between the characteristic elements (including, conjecturally, the special values of  $p$ -adic Zeta functions and complex  $L$ -functions) that are associated to the given arithmetic complexes. The methods that we develop can equally well be used to construct such classes of matrices in the context of arbitrary compact  $p$ -adic Lie extensions of number fields but in the present article we focus on the case of finite (possibly non-abelian) Galois extensions.

Not surprisingly, given the amount of data that they incorporate, the explicit computation of organising matrices is a difficult problem that retains scope for much future research. Nevertheless, at this stage our understanding of the theory does allow us to prove a generalisation (from results concerning the values of  $L$ -functions of motives twisted by abelian characters to results concerning the values of higher derivatives of  $L$ -functions of motives twisted by general characters) of both the theory of annihilators of Bloch-Kato Selmer modules developed by Barrett and the first author in [3] and of the theory of integral congruences for the values of motivic  $L$ -functions developed by the first author in [9, §9].

To give an idea of the usefulness of our general approach we then combine the appropriate special case together with recent results of Ritter and Weiss and of Kakde on the main conjecture of non-commutative Iwasawa theory for totally real fields and of the first author on the equivariant Tamagawa number conjecture for Tate motives to prove, modulo the assumed vanishing of certain classical  $\mu$ -invariants, several new and rather concrete results including an explicit analogue for general (non-abelian) Galois extensions of totally real fields of Brumer's Conjecture, a refinement and non-abelian generalisation of the main results of Oriat in [43] concerning the explicit structure of certain Galois groups and an analogue involving leading terms of  $p$ -adic Artin  $L$ -functions at strictly positive (rather than negative) integers of the refined version of the Coates-Sinnott conjecture studied by Greither and the first author in [15]. By using the same approach in a different setting we also formulate a 'strong main conjecture' for the values at  $s = 1$  of Hasse-Weil  $L$ -functions of abelian varieties over non-abelian Galois extensions of precisely the sort that Mazur and Tate explicitly ask for (in the abelian case) in [38, Remark after Conj. 3] and give an (unconditional) construction of a family of elliptic curves  $E$  and totally real dihedral extensions  $F_n$  of  $\mathbb{Q}$  of degree  $2p^n$  (for arbitrarily large  $n$ ) for which the Mordell-Weil group  $E(F_n)$  has exact rank  $p^n$ , the Galois structures of  $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F_n)$  and  $\mathbb{Z}_p \otimes_{\mathbb{Z}} \text{Hom}(\text{Sel}(E/F_n), \mathbb{Q}/\mathbb{Z})$  are explicitly known and the validity of the  $p$ -part of the equivariant Tamagawa number conjecture of [14, Conj. 4] for the pair  $(h^1(E/F_n)(1), \mathbb{Z}[\text{Gal}(F_n/\mathbb{Q})])$  is equivalent to a family of explicit integral congruence relations between the height of a distinguished point in  $E(F_n)$  and the values at  $s = 1$  of derivatives of the twisted Hasse-Weil  $L$ -functions that are associated to  $E/F_n$ . We note, in particular, that these examples are the first in which the predictions of [14, Conj. 4] have been made completely explicit for a class of extensions of arbitrary degree and a class of elliptic curves of arbitrarily large Mordell-Weil rank and that they have since enabled Wuthrich to provide the first numerical verifications of the  $p$ -part of [14, Conj. 4] in the technically most demanding

case of a prime  $p$  that divides the degree of  $F_n/\mathbb{Q}$  and an elliptic curve  $E$  for which  $E(F_n)$  is infinite (and has a non-trivial action of  $\text{Gal}(F_n/\mathbb{Q})$ ).

In a little more detail, the main contents of this article is as follows. In §1 we discuss preliminaries concerning homological algebra and Euler characteristics, introduce the categories of complexes to which our results apply, describe important examples of these complexes from arithmetic and introduce a suitable notion of ‘characteristic element’. In §2 we define several classes of organising matrices, describe their basic properties and discuss connections to a range of existing results and conjectures in arithmetic. In §3 we prove all of the main results that are stated in §2. In §4 we use the theory of organising matrices to show that the vanishing of certain  $\mu$ -invariants implies a variety of new and rather explicit results on the structures of Galois groups, ideal class groups and wild kernels in higher algebraic  $K$ -theory. In §5 we apply the theory of organising matrices to both the Nekovář-Selmer complexes and finite support cohomology complexes (in the sense of Bloch and Kato) of abelian varieties to prove some unconditional results concerning the explicit structure of classical Selmer and Tate-Shafarevich groups and also use it to show that the equivariant Tamagawa number conjecture (and non-commutative Tamagawa number conjecture of Fukaya and Kato) implies a range of explicit refinements of the Birch and Swinnerton-Dyer Conjecture.

The authors are very grateful indeed to Christian Wuthrich for several useful discussions and also for providing supporting numerical evidence for the refinement of the Birch and Swinnerton-Dyer Conjecture that is formulated in §5.3.2.

## 1. PRELIMINARIES

All modules are to be regarded, unless explicitly stated otherwise, as left modules. For any noetherian ring  $\Lambda$  we write  $D^{\text{P}}(\Lambda)$  for the derived category of perfect complexes of  $\Lambda$ -modules.

For any module  $N$  we write  $N_{\text{tor}}$  for its torsion submodule and set  $N_{\text{tf}} := N/N_{\text{tor}}$  which we regard as embedded in the associated space  $\mathbb{Q} \otimes_{\mathbb{Z}} N$ .

**1.1. Categories of 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  $F$ , a finite group  $G$  and a direct factor  $\mathfrak{A}$  of the group ring  $R[G]$  and we set  $A := F \otimes_R \mathfrak{A}$ .

**1.1.1. Admissible complexes.** We write  $D^{\text{wa}}(\mathfrak{A})$  for the full subcategory of  $D^{\text{P}}(\mathfrak{A})$  comprising complexes  $C = (C^i)_{i \in \mathbb{Z}}$  which satisfy the following four assumptions:

- (wa<sub>1</sub>)  $C$  is an object of  $D^{\text{P}}(\mathfrak{A})$ ;
- (wa<sub>2</sub>) the Euler characteristic of  $A \otimes_{\mathfrak{A}} C$  in the Grothendieck group  $K_0(A)$  vanishes;
- (wa<sub>3</sub>)  $C$  is acyclic outside degrees 1, 2 and 3;
- (wa<sub>4</sub>)  $H^1(C)$  is  $R$ -torsion-free.

We will refer to an object of  $D^{\text{wa}}(\mathfrak{A})$  as a ‘weakly-admissible complex of  $\mathfrak{A}$ -modules’. We will also refer to an object of  $D^{\text{wa}}(\mathfrak{A})$  that is acyclic outside degrees 1 and 2 as an ‘admissible complex of  $\mathfrak{A}$ -modules’ and we write  $D^{\text{a}}(\mathfrak{A})$  for the full subcategory of  $D^{\text{wa}}(\mathfrak{A})$  comprising admissible complexes.

1.1.2. *Gorenstein algebras.* We now assume that  $\mathfrak{A}$  is endowed with an  $R$ -linear anti-involution  $\iota$  and use it to regard the  $R$ -linear dual  $M^* := \text{Hom}_R(M, R)$  of each left  $\mathfrak{A}$ -module  $M$  as a left  $\mathfrak{A}$ -module by the rule  $a(f)(m) := f(\iota(a)(m))$  for each  $a \in \mathfrak{A}$ ,  $f \in M^*$  and  $m \in M$ . We assume also that  $\mathfrak{A}$  is Gorenstein (with respect to  $\iota$ ) in the sense that  $\mathfrak{A}^*$  is a projective  $\mathfrak{A}$ -module. To give an example of such an algebra we write  $\iota$  for the  $R$ -linear map on  $R[G]$  that inverts elements of  $G$ . Then for any idempotent  $e$  of  $\zeta(R[G])$  that is invariant under  $\iota$  the algebra  $\mathfrak{A} := R[G]e$  is Gorenstein with respect to the anti-involution obtained by restricting  $\iota$ .

Then for any finitely generated projective  $\mathfrak{A}$ -module  $Q$  the module  $Q^*$  is finitely generated and projective and so the category  $D^{\text{p}}(\mathfrak{A})$  is preserved by the functor  $C \mapsto C^* := \text{R Hom}_R(C, R)$ . Further, for each  $C$  in  $D^{\text{p}}(\mathfrak{A})$  the universal coefficient spectral sequence implies that in each degree  $i$  there is a canonical short exact sequence

$$0 \rightarrow \text{Hom}_R(H^{4-i}(C)_{\text{tor}}, F/R) \rightarrow H^i(C^*[-3]) \rightarrow \text{Hom}_R(H^{3-i}(C), R) \rightarrow 0.$$

These sequences imply that (if  $\mathfrak{A}$  is Gorenstein, then) the functor  $C \mapsto C^*[-3]$  preserves each of the categories  $D^{\text{wa}}(\mathfrak{A})$  and  $D^{\text{a}}(\mathfrak{A})$ .

1.1.3. *Symmetric admissible complexes.* In this subsection we continue to assume that  $\mathfrak{A}$  is Gorenstein (with respect to a given anti-involution  $\iota$ ). We define a ‘symmetric, resp. skew-symmetric, admissible complex of  $\mathfrak{A}$ -modules’ to be a pair  $(C, \delta)$  comprising an object  $C$  of  $D^{\text{a}}(\mathfrak{A})$  and an isomorphism  $\delta : C \cong C^*[-3]$  in  $D^{\text{p}}(\mathfrak{A})$  which lies in a commutative diagram in  $D^{\text{p}}(\mathfrak{A})$  of the form

$$(1) \quad \begin{array}{ccc} C & \xrightarrow{\delta} & C^*[-3] \\ \epsilon \downarrow & & \parallel \\ (C^*[-3])^*[-3] & \xrightarrow{\epsilon_\delta \cdot \delta^*[-3]} & C^*[-3] \end{array}$$

where  $\epsilon$  is the natural identification and  $\epsilon_\delta$  is equal to 1 if  $(C, \delta)$  is symmetric and to  $-1$  if  $(C, \delta)$  is skew-symmetric.

We shall say that two such pairs  $(C, \delta)$  and  $(C', \delta')$  are isomorphic if there exists a commutative diagram in  $D^{\text{p}}(\mathfrak{A})$  of the form

$$\begin{array}{ccc} C & \xrightarrow{\delta} & C^*[-3] \\ \kappa \downarrow & & \downarrow (\kappa^*[-3])^{-1} \\ C' & \xrightarrow{\delta'} & C'^*[-3] \end{array}$$

in which  $\kappa$ , and hence also  $(\kappa^*[-3])^{-1}$ , is an isomorphism.

1.1.4. *Annihilation idempotents.* If  $C$  is an object of  $D^{\text{wa}}(\mathfrak{A})$ , then for each integer  $i$  in  $\{1, 2, 3\}$  we write  $e_i = e_i(C)$  for the sum over all primitive idempotents of  $\zeta(A)$  that annihilate the module  $H^i(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} C)$ . We note that the conditions  $(\text{wa}_2)$  and  $(\text{wa}_3)$  combine to imply that  $e_2 = e_1 e_3$ .

**1.2. Arithmetic examples.** Each of the classes of complexes introduced in §1.1 arises naturally in arithmetic. To describe some important examples we set  $G_{L/K} := \text{Gal}(L/K)$  for any Galois extension of fields  $L/K$ . We also fix an algebraic closure  $K^c$  of  $K$  and set  $G_K := G_{K^c/K}$ . We assume to be given a finite Galois extension of number fields  $F/k$  that is unramified outside a finite set of places  $S$  and fix a continuous  $\mathbb{Z}_p[G_k]$ -module  $T$  that is both finitely generated and free over  $\mathbb{Z}_p$ . We set  $T^*(1) := \text{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p(1))$  and endow this with the following commuting actions of  $G_{F/k}$  and  $G_k$ : for each  $a \in \mathbb{Z}_p[G_{F/k}]$ ,  $\sigma \in G_k$ ,  $f \in T^*(1)$  and  $t \in T$  one has  $a(f)(t) = f(a(t))$  and  $\sigma(f)(t) = \sigma(f(\sigma^{-1}(t)))$ . We also set  $V := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$ ,  $V^*(1) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T^*(1)$ ,  $W := V/T$  and  $W^*(1) := V^*(1)/T^*(1) \cong \text{Hom}_{\mathbb{Z}_p}(T, (\mathbb{Q}_p/\mathbb{Z}_p)(1))$ , each endowed with the actions of  $\mathbb{Z}_p[G_{F/k}]$  and  $G_k$  that are induced from the respective actions on  $T$  and  $T^*(1)$ . For each closed subgroup  $U$  of  $G_k$  and each continuous  $\mathbb{Z}_p[U]$ -module  $M$  we set  $M_F := \mathbb{Z}_p[G_{F/k}] \otimes_{\mathbb{Z}_p} M$  and we regard this as a module over  $\mathbb{Z}_p[G_{F/k}] \times \mathbb{Z}_p[U]$  in the following way:  $G_{F/k}$  acts via multiplication on the left and each  $u \in U$  acts as  $x \otimes_{\mathbb{Z}_p} t \mapsto x\bar{u}^{-1} \otimes_{\mathbb{Z}_p} u(t)$  for each  $x \in \mathbb{Z}_p[G_{F/k}]$  and  $t \in T$  where  $\bar{u}$  denotes the image of  $u$  in  $G_{F/k}$ . For any finite group  $\Gamma$  and any  $\mathbb{Z}_p[\Gamma]$ -module  $M$  we write  $M^\vee$  for the Pontryagin dual  $\text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$  which we endow with the usual contragredient action of  $\mathbb{Z}_p[\Gamma]$ .

**1.2.1. Compactly supported étale cohomology.** The compactly supported étale cohomology complex  $C(T_F) := R\Gamma_c(\mathcal{O}_{k,S}[\frac{1}{p}], T_F)$  of  $T_F$  is always an object of  $D^{\text{wa}}(\mathbb{Z}_p[G])$  and there exists a natural surjection from  $H^2(C(T_F))$  to  $\text{Sel}(T^*(1)_F)^\vee$  where  $\text{Sel}(T^*(1)_F)$  is the Selmer module of  $T^*(1)_F$  (in the sense of Bloch and Kato). If the group  $H^0(k, W^*(1)_F)$  vanishes, then  $C(T_F)$ , and hence also  $C(T_F)^*$ , is an object of  $D^{\text{a}}(\mathbb{Z}_p[G])$ . (For proofs of all of these claims see [3, Lem. 3.1]).

**1.2.2. Nekovář-Selmer Complexes.** Let  $V$  be the  $p$ -adic realisation of a critical motive  $M$  over  $k = \mathbb{Q}$  that has good ordinary reduction at  $p$ . Then there exists a unique  $G_{\mathbb{Q}_p}$ -stable  $\mathbb{Q}_p$ -subspace  $V^0$  of  $V$  with the property that the natural map  $D_{\text{dR}}(\mathbb{Q}_p, V^0) \rightarrow D_{\text{dR}}(\mathbb{Q}_p, V) \twoheadrightarrow t_p(V)$  induces an identification  $D_{\text{dR}}(\mathbb{Q}_p, V^0) \cong t_p(V)$  (cf. [46]). We then fix a full  $G_{\mathbb{Q}}$ -stable  $\mathbb{Z}_p$ -sublattice  $T$  of  $V$  and thereby obtain a full  $G_{\mathbb{Q}_p}$ -stable  $\mathbb{Z}_p$ -sublattice of  $V^0$  by setting  $T^0 := T \cap V^0$ . We also fix a finite totally real Galois extension  $F$  of  $\mathbb{Q}$  and write  $C(T_F, T_F^0)$  for the Nekovář-Selmer complex  $\text{SC}(\mathcal{O}_{k,S}[\frac{1}{p}], T_F, T_F^0)$  that is considered by Fukaya and Kato in [26, §4.1.2.]. If the spaces  $H^0(\mathbb{Q}_p, V_F/V_F^0)$ ,  $H^0(\mathbb{Q}_p, (V_F^0)^*(1))$  and  $H^0(\mathbb{Q}_\ell, V_F)$  for each prime  $\ell \notin \Sigma$  all vanish, then [3, Prop. 4.1] shows that the vanishing of  $H^0(k, W_p^*(1)_F)$  implies  $C(T_F, T_F^0)$  is an object of  $D^{\text{a}}(\mathbb{Z}_p[G])$  and that the  $\mathbb{Z}_p[G]$ -module  $\text{Sel}(T_p^*(1))^\vee$  is isomorphic to a subquotient of  $H^2(C(T_F, T_F^0))$ .

**1.2.3. Finite Support Cohomology.** Let  $E$  be an elliptic curve that is defined over  $k$  and let  $K$  be an intermediate field of  $F/k$ . For each non-archimedean place  $v$  of  $F$  let  $\tilde{E}_v$  be the reduction of the minimal model of  $E/K$  at  $v$  and write  $\mathbb{F}_v$  for the residue field of  $v$ . Let  $S_r^K$ , resp.  $S_b^K$ , denote the finite sets of places of  $K$  which ramify in  $F/k$ , resp. at which  $E$  has bad reduction, and recall that for each  $v$  in  $S_b^K$  the index  $[E(K_v) : E_0(K_v)]$  is the Tamagawa number in the Birch and Swinnerton-Dyer Conjecture for  $E/K$ . We let  $p$  be an odd prime which satisfies both of the following conditions:

- $p \nmid \text{disc}(F/\mathbb{Q})\text{cond}(E)|E(K)_{\text{tor}}|\prod_{v \in S_F^K} |\tilde{E}_v(\mathbb{F}_v)|\prod_{v \in S_b^K} [E(K_v) : E_0(K_v)]$ .
- The extension  $F/K$  is of  $p$ -power degree and is unramified at all primes of bad reduction for  $E/K$ .

Under these conditions, a natural generalisation of the proof of [9, Lem. 12.1.2] shows that the complex  $C_f(T_F) := R\Gamma_f(k, T_F)$  of cohomology with finite support that is defined in [12] is an object of  $D^{\mathfrak{a}}(\mathbb{Z}_p[G])$  for which  $H^1(C_f(T_F))$  and  $H^2(C_f(T_F))$  are canonically isomorphic to  $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F)$  and  $\text{Sel}_p(E/F)^{\vee}$  respectively, where we write  $\text{Sel}_p(E/F)$  for the  $p$ -primary Selmer module of  $E/F$ . (It is also easy to see that for a given elliptic curve  $E$  there are infinitely many primes  $p$ , and for each such  $p$  infinitely many fields  $F$  and  $K$ , which satisfy all of the above conditions.)

**1.3. Characteristic elements.** In this section we associate a natural notion of characteristic element to complexes in  $D^{\text{wa}}(\mathfrak{A})$ .

**1.3.1. Relative  $K$ -theory.** For any field  $E$  that contains  $F$  and any  $\mathfrak{A}$ -module  $M$ , resp.  $\mathfrak{A}$ -homomorphism  $\phi$ , we write  $M_E$  for the associated  $E \otimes_R \mathfrak{A}$ -module  $E \otimes_R M$ , resp.  $\phi_E$  for the associated  $E \otimes_R \mathfrak{A}$ -homomorphism  $E \otimes_R \phi$ . For any such  $E$ , we write  $K_0(\mathfrak{A}, E \otimes_R \mathfrak{A})$  for the relative algebraic  $K$ -group of the ring inclusion  $\mathfrak{A} \subset E \otimes_R \mathfrak{A}$ , and recall that there exists a canonical exact commutative diagram

$$(2) \quad \begin{array}{ccccc} K_1(\mathfrak{A}) & \xrightarrow{\partial_{\mathfrak{A},F}^2} & K_1(A) & \xrightarrow{\partial_{\mathfrak{A},F}^1} & K_0(\mathfrak{A}, A) \\ \parallel & & \downarrow \iota_E & & \downarrow \iota'_E \\ K_1(\mathfrak{A}) & \xrightarrow{\partial_{\mathfrak{A},E}^2} & K_1(E \otimes_R \mathfrak{A}) & \xrightarrow{\partial_{\mathfrak{A},E}^1} & K_0(\mathfrak{A}, E \otimes_R \mathfrak{A}). \end{array}$$

Here the homomorphisms  $\iota_E$  and  $\iota'_E$  are induced by scalar extension and are both injections (indeed, we shall often regard these maps as inclusions). The homomorphism  $\partial_{\mathfrak{A},E}^2$  is induced by the inclusion  $\mathfrak{A} \subset E \otimes_R \mathfrak{A}$  and  $\partial_{\mathfrak{A},E}^1$  is the homomorphism that sends the class of an automorphism  $\phi$  of  $(E \otimes_R \mathfrak{A})^n$  to  $[\mathfrak{A}^n, \mathfrak{A}^n, \phi]$ . We also write  $\delta_{\mathfrak{A},A} : \zeta(A)^{\times} \rightarrow K_0(\mathfrak{A}, A)$  for the ‘extended boundary homomorphism’ that is defined in [14] and we recall that  $\delta_{\mathfrak{A},A} \circ \text{nr}_A = \partial_{\mathfrak{A},F}^1$  where  $\text{nr}_A$  denotes the homomorphism  $K_1(A) \rightarrow \zeta(A)^{\times}$  induced by taking reduced norms.

In the sequel, for any ring  $R$  and any (left)  $R$ -modules  $M$  and  $N$  we write  $\text{Is}_R(M, N)$  for the set of  $R$ -module isomorphisms  $M \rightarrow N$ .

**1.3.2. Characteristic elements and Fitting invariants.** Recall that to each pair  $(C, t)$  with  $C$  in  $D^{\text{p}}(\mathfrak{A})$  and  $t$  in  $\text{Is}_{E \otimes_R \mathfrak{A}}(\bigoplus_{i \in \mathbb{Z}} H^{2i}(C)_E, \bigoplus_{i \in \mathbb{Z}} H^{2i+1}(C)_E)$  one can associate a canonical Euler characteristic element  $\chi^{\text{ref}}(C, t)$  in  $K_0(\mathfrak{A}, E \otimes_R \mathfrak{A})$  (for details of this construction see, for example, [14, §2.8]). We shall say that an element  $\mathcal{L}$  of  $\zeta(A)^{\times}$  is a ‘characteristic element’ for such a pair  $(C, t)$  if one has

$$\iota'_E(\delta_{\mathfrak{A},A}(\mathcal{L})) = \chi^{\text{ref}}(C, t),$$

and that  $\mathcal{L}$  is a characteristic element for  $C$  if it is a characteristic element for  $(C, t)$  for any  $t$  as above.

From the lower exact sequence in (2) it is clear that characteristic elements for  $(C, t)$  are unique up to multiplication by elements of  $\text{nr}_{E \otimes_R \mathfrak{A}}(\text{im}(\partial_{\mathfrak{A},E}^2))$ . For later use we

also recall that if  $\mathfrak{A}$  is semi-local (which is automatic if  $R = \mathbb{Z}_p$ ), then the natural homomorphism  $\mathfrak{A}^\times \rightarrow K_1(\mathfrak{A})$  is surjective.

Note that, as the algebra  $A$  is semisimple, for any complex  $C$  that satisfies the conditions (wa<sub>2</sub>) and (wa<sub>3</sub>) the  $A$ -modules  $H^2(C)_F$  and  $H^1(C)_F \oplus H^3(C)_F$  are isomorphic. Hence, if  $C$  also satisfies (wa<sub>1</sub>), then there exist characteristic elements for  $C$  in the above sense.

The following result shows that in a special case these characteristic elements are related to the ‘non-commutative Fitting invariants’ that are introduced by Nickel in [41, §3] (and, in fact, earlier by Parker in [44]).

**Lemma 1.1.** *Let  $R$  be a discrete valuation ring. If  $M$  is any finite  $\mathfrak{A}$ -module that has finite projective dimension, then the complex  $M[-3]$  belongs to  $D^{\text{wa}}(\mathfrak{A})$  and the (non-commutative) Fitting invariant  $\text{Fitt}_{\mathfrak{A}}(M)$  is well-defined. Further, any generating element (in  $\zeta(A)^\times$ ) of  $\text{Fitt}_{\mathfrak{A}}(M)$  is a characteristic element for  $M[-3]$ .*

*Proof.* It is clear that  $M[-3]$  belongs to  $D^{\text{wa}}(\mathfrak{A})$ . In addition, since  $G$  is finite,  $R$  is a discrete valuation ring and  $\mathfrak{A}$  is a direct factor of  $R[G]$ , there exists a resolution of  $M$  of the form

$$(3) \quad 0 \rightarrow P \xrightarrow{h} P \rightarrow M \rightarrow 0$$

where  $P$  is a finitely generated free  $\mathfrak{A}$ -module. The invariant  $\text{Fitt}_{\mathfrak{A}}(M)$  is therefore well-defined by [41, Th. 3.2(2)] and indeed any generator of  $\text{Fitt}_{\mathfrak{A}}(M)$  is of the form  $\mathcal{L}_h := \text{Nrd}_A(F \otimes_R h)$  for an endomorphism  $h$  as above. On the other hand, the sequence (3) induces an isomorphism in  $D^{\text{p}}(\mathfrak{A})$  between  $M[-3]$  and the complex  $F \xrightarrow{h} F$ , where the first term is placed in degree 2, and so the definition of the connecting homomorphism  $\partial_{\mathfrak{A},A}^1$  implies that  $\delta_{\mathfrak{A},A}(\mathcal{L}_h) = \partial_{\mathfrak{A},A}^1(F \otimes_R h) = \chi^{\text{ref}}(M[-3], 0)$  and hence that  $\mathcal{L}_h$  is a characteristic element for  $M[-3]$ , as required.  $\square$

1.3.3. *Basic properties.* For later purposes, we record two useful results regarding characteristic elements. For any complex of  $A$ -modules  $X$  we set  $\tau(X) := \text{Is}_A(H^2(X), H^1(X) \oplus H^3(X))$ .

**Lemma 1.2.** *Let  $C_1 \rightarrow C_2 \rightarrow C_3 \rightarrow C_1[1]$  be an exact triangle in  $D(\mathfrak{A})$  in which each  $C_i$  satisfies the conditions (wa<sub>1</sub>), (wa<sub>2</sub>) and (wa<sub>3</sub>). Then there are characteristic elements  $\mathcal{L}_1$  and  $\mathcal{L}_3$  for  $C_1$  and  $C_3$  such that  $\mathcal{L}_1\mathcal{L}_3$  is a characteristic element for  $C_2$ .*

*Proof.* It suffices to construct elements  $t_j$  of  $\tau((C_j)_F)$  such that the pairs  $(C_j, t_j)$  for  $j \in \{1, 2, 3\}$  satisfy the additivity criterion of [8, Cor. 6.6]. Indeed, in any such case, one has  $\chi^{\text{ref}}(C_2, t_2) = \chi^{\text{ref}}(C_1, t_1) + \chi^{\text{ref}}(C_3, t_3)$  in  $K_0(\mathfrak{A}, A)$  and so it is clear that if  $\mathcal{L}_1$  and  $\mathcal{L}_3$  are characteristic elements for  $(C_1, t_1)$  and  $(C_3, t_3)$ , then  $\mathcal{L}_1\mathcal{L}_3$  is a characteristic element for  $(C_2, t_2)$ .

Let  $A = \prod_{i \in I} A_i$  be the decomposition of  $A$  as a product of simple algebras. This induces a decomposition  $\zeta(A)^\times = \prod_{i \in I} \zeta(A_i)^\times$  and  $\tau(C) = \bigoplus_{i \in I} \tau(C_i)$  for each complex of  $\mathfrak{A}$ -modules  $C$ , where we set  $C_i := A_i \otimes_{\mathfrak{A}}^{\mathbb{L}} C$ . In particular, since the criterion of [8, Cor. 6.6] takes the form of an equality in  $\zeta(A)^\times$ , it suffices to construct for each  $i \in I$  and  $j \in \{1, 2, 3\}$  an element  $t_{ji}$  of  $\tau(C_{ji})$  which together satisfy the projection to  $\zeta(A_i)^\times$  of the criterion of [8, Cor. 6.6]. Now if each complex  $\{C_{ji} : j \in \{1, 2, 3\}\}$  is acyclic, then the equality of [8, Cor. 6.6] is obviously satisfied. On the other hand, if  $C_{ji}$  is not acyclic for any given  $j$ , then for any  $t$  in  $\tau(C_{ji})$  and any  $\lambda$  in  $\zeta(A_i)^\times$  there

exists an element  $t'$  of  $\tau(C_{ji})$  with  $\text{Nrd}_{A_i}(t' \circ t^{-1}) = \lambda$ . The latter fact implies, in particular, that for any given choice of elements  $t_{ki}$  of  $\tau(C_{ki})$  for  $k \in \{1, 2, 3\} \setminus \{j\}$ , one can construct an element  $t_{ji}$  of  $\tau(C_{ji})$  so that  $\{t_{ki} : k \in \{1, 2, 3\}\}$  satisfies the criterion of [8, Cor. 6.6].  $\square$

**Remark 1.3.** Let  $C$  be a complex that satisfies (wa<sub>1</sub>), (wa<sub>2</sub>) and (wa<sub>3</sub>) and is also such that the  $\mathfrak{A}$ -module  $H^1(C)_{\text{tor}}$  has finite projective dimension. Then there is an exact triangle  $H^1(C)_{\text{tor}}[-1] \rightarrow C \rightarrow C' \rightarrow H^1(C)_{\text{tor}}[0]$  in  $D(\mathfrak{A})$ . Further, in this case the complex  $C'$  belongs to  $D^{\text{wa}}(\mathfrak{A})$  and Lemmas 1.1 and 1.2 combine to imply that if  $\Phi$  is any generator of  $\text{Fit}_{\mathfrak{A}}(H^1(C)_{\text{tor}})$  and  $\mathcal{L}'$  is a characteristic element for  $C'$ , then  $\Phi\mathcal{L}'$  is a characteristic element for  $C$ .

**Lemma 1.4.** *Let  $R$  be a complete discrete valuation ring. Fix a complex  $C$  in  $D^{\text{wa}}(\mathfrak{A})$ , write  $e_2$  for the idempotent  $e_2(C)$  defined in §1.1.4 and set  $\mathfrak{A}_2 := \mathfrak{A}e_2$ ,  $A_2 := Ae_2$  and  $C_2 := \mathfrak{A}_2 \otimes_{\mathfrak{A}}^{\mathbb{L}} C$ . Then  $C_2$  belongs to  $D^{\text{wa}}(\mathfrak{A}_2)$  and for any characteristic element  $\mathcal{L}_2$  (in  $\zeta(A_2)^{\times}$ ) of  $C_2$  there exists a characteristic element  $\mathcal{L}$  of  $C$  such that  $e_2\mathcal{L} = \mathcal{L}_2$ .*

*Proof.* Since  $R$  is complete the algebras  $\mathfrak{A}$  and  $\mathfrak{A}_2$  are semi-local, so the natural homomorphisms  $\mathfrak{A}^{\times} \rightarrow K_1(\mathfrak{A})$  and  $\mathfrak{A}_2^{\times} \rightarrow K_1(\mathfrak{A}_2)$  are surjective, and in addition the homomorphisms  $\text{nr}_{\mathfrak{A}}$  and  $\text{nr}_{\mathfrak{A}_2}$  are both bijective. The exact sequence (2) therefore gives rise to the central and lower rows in the following exact commutative diagram

$$(4) \quad \begin{array}{ccccccc} & & \zeta(A'_2)^{\times} & \xlongequal{\quad} & \zeta(A'_2)^{\times} & & \\ & & \subseteq \downarrow & & \alpha \downarrow & & \\ \mathfrak{A}^{\times} & \longrightarrow & \zeta(A)^{\times} & \xrightarrow{\delta} & K_0(\mathfrak{A}, A) & \longrightarrow & 0 \\ \pi'_2 \downarrow & & \pi_2 \downarrow & & \pi''_2 \downarrow & & \\ \mathfrak{A}_2^{\times} & \longrightarrow & \zeta(A_2)^{\times} & \xrightarrow{\delta_2} & K_0(\mathfrak{A}_2, A_2) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ 0 & & 0 & & 0 & & \end{array}$$

In this diagram we also set  $A'_2 := A(1 - e_2)$ , write  $\pi'_2$  and  $\pi_2$  for the homomorphisms induced by multiplication by  $e_2$  and define  $\alpha$  and  $\pi''_2$  by the commutativity of the upper and lower right hand squares. The central column of (4) is obviously exact and (since  $\mathfrak{A}$  is semi-local) the homomorphism  $\pi'_2$  is surjective as a consequence of Bass' Theorem (cf. [30, Chap. 7, (20.9)]) and so the Snake Lemma implies that the right hand column of (4) is also exact.

We now fix an element  $\mathcal{L}'$  of  $\zeta(A)^{\times}$  with  $\mathcal{L}'e_2 = \pi_2(\mathcal{L}') = \mathcal{L}_2$ . Then for any  $t$  in  $\text{Is}_A(H^2(C)_F, H^1(C)_F \oplus H^3(C)_F)$  one has  $\pi''_2(\chi^{\text{ref}}(C, t)) = \chi^{\text{ref}}(C_2, 0) = \delta_2(\mathcal{L}_2) = \pi''_2(\delta(\mathcal{L}'))$ , where the last equality follows from the commutativity of the lower right hand square in (4). The exactness of the right hand column in (4) therefore implies that there exists an element  $u$  of  $\zeta(A'_2)^{\times}$  with  $\chi^{\text{ref}}(C, t) = \delta(\mathcal{L}') + \alpha(u) = \delta(\mathcal{L}'u)$ . Since  $\pi_2(\mathcal{L}'u) = \pi_2(\mathcal{L}') = \mathcal{L}_2$  one therefore obtains an element of the required sort by setting  $\mathcal{L} := \mathcal{L}'u$ .  $\square$

## 2. ORGANISING MATRICES

In this section we associate to each admissible complex of  $\mathbb{Z}_p[G]$ -modules a class of ‘organising matrices’ that generalises and refines the ‘organising modules’ introduced in special cases by Mazur and Rubin in [36]. The observation made in Remark 1.3 allows one to extend many of the results proved both in this section and in §4 to a larger class of complexes, but for simplicity we shall leave the precise formulation of all such generalisations to an interested reader.

Throughout this section we use the following convention: if  $\Psi$  belongs to  $M_m(\mathbb{Z}_p[G])$  for any natural number  $m$ , then we use the standard basis of the direct sum  $\mathbb{Z}_p[G]^m$  of  $m$  copies of  $\mathbb{Z}_p[G]$  to regard  $\Psi$  as an element of  $\text{End}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G]^m)$ . For each normal subgroup  $J$  of  $G$  we also write  $\Psi_J$  for the image of  $\Psi$  in  $M_m(\mathbb{Z}_p[G/J])$  and for each  $C$  in  $D^{\text{p}}(\mathbb{Z}_p[G])$  we write  $C_J$  for the associated object  $\mathbb{Z}_p[G/J] \otimes_{\mathbb{Z}_p[G]}^{\mathbb{L}} C$  of  $D^{\text{p}}(\mathbb{Z}_p[G/J])$ . For any  $\mathbb{Z}_p[G]$ -module  $M$  we also set  $a_G(M) := \text{Ann}_{\zeta(\mathbb{Z}_p[G])}(M)$ .

**2.1. Weakly organising matrices.** In this subsection we assume to be given data of the following sort:

- a complex  $C$  in  $D^{\text{wa}}(\mathbb{Z}_p[G])$ ;
- a non-zero element  $\alpha = \beta\gamma$  with  $\beta \in a_G(H^3(C)) \cap \zeta(\mathbb{Q}_p[G]e_3)^\times$  and  $\gamma \in \zeta(\mathbb{Z}_p[G]) \cap \zeta(\mathbb{Q}_p[G]e_3)$ .

**2.1.1. Statement of the main result.** In the following result we write  $I_{G,p}$  for the kernel of the natural augmentation homomorphism  $\mathbb{Z}_p[G] \rightarrow \mathbb{Z}_p$ . We also recall that a  $\mathbb{Z}_p[G]$ -module  $M$  is said to have a ‘quadratic presentation’ if there exists a natural number  $n$  and an exact sequence of  $\mathbb{Z}_p[G]$ -modules of the form  $\mathbb{Z}_p[G]^n \rightarrow \mathbb{Z}_p[G]^n \rightarrow M \rightarrow 0$ . We finally set  $I(\mathbb{Z}_p[G]e_3) := \mathbb{Z}_p[G] \cap \mathbb{Q}_p[G](1 - e_3)$ .

**Theorem 2.1.** *For each complex  $C$  and element  $\alpha$  as above there exists a natural number  $d$  and a matrix  $\Phi = \Phi_{C,\alpha}$  in  $M_d(\mathbb{Z}_p[G])$  that satisfies the following conditions.*

- (i) *The  $\mathbb{Z}_p[G]$ -module  $\ker(\Phi)$  is isomorphic to  $H^1(C) \oplus I(\mathbb{Z}_p[G]e_3)^{g_3(C)}$ , where  $g_3(C)$  is the minimal number of generators of  $H^3(C)$  as a  $\mathbb{Z}_p[G]$ -module.*
- (ii) *The  $\mathbb{Z}_p[G]$ -module  $\text{cok}(\Phi)$  lies in an exact sequence of the form*

$$0 \rightarrow H^2(C) \rightarrow \text{cok}(\Phi) \rightarrow M_\alpha \rightarrow 0$$

*where the module  $M_\alpha$  is annihilated by  $\alpha$ .*

- (iii) *If  $H^3(C)$  is finite, then one can take  $\alpha$  to be  $|H^3(C)|$  and in this case the  $\mathbb{Z}_p[G]$ -module  $H^2(C)$  is isomorphic to a finite index submodule of  $\text{cok}(\Phi)$  and  $\Phi$  can be chosen so that precisely  $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2(C_G))$  of its columns have all of their entries in  $I_{G,p}$ . In particular, if  $H^3(C)$  vanishes, then the  $\mathbb{Z}_p[G]$ -module  $H^2(C)$  is isomorphic to  $\text{cok}(\Phi)$  and so has a quadratic presentation.*
- (iv) *For each characteristic element  $\mathcal{L}$  of  $C$  one has  $\alpha^{g_3(C)} \mathcal{L}e_1 = \text{nr}_{\mathbb{Q}_p[G]}(\Phi)u_{\mathcal{L}}$  where  $u_{\mathcal{L}}$  belongs to  $\text{nr}_{\mathbb{Q}_p[G]}(\mathbb{Z}_p[G]^\times)$ .*

**Definition 2.2.** *We shall call any matrix  $\Phi_{C,\alpha}$  constructed as in Theorem 2.1 a ‘weakly-organising matrix’ for the complex  $C$  and element  $\alpha$ . If  $\alpha = 1$  (so that  $\beta$  belongs to  $\mathbb{Z}_p[G]^\times$  and  $H^3(C)$  vanishes), then we say that  $\Phi_{C,\alpha}$  is a weakly-organising matrix for  $C$ .*

In the rest of this section we derive several concrete consequences which follow from the existence of the matrices described in Theorem 2.1.

2.1.2. *The structure of  $H^2(C)$ .* It is immediately clear from Theorem 2.1(ii) and (iii) that weakly-organising matrices determine explicit aspects of the structure of  $H^2(C)$ . In this subsection we show that Theorem 2.1(iv) also provides an explicit link between characteristic elements for  $C$  and certain structural invariants of  $H^2(C)$ .

For each non-negative integer  $n$  we write  $I_{G,p}^{[n]}$  for the  $\zeta(\mathbb{Z}_p[G])$ -submodule of  $\zeta(\mathbb{Q}_p[G])$  that is generated by elements of the form  $\text{nr}_{\mathbb{Q}_p[G]}(N)$  where  $N$  belongs to  $M_m(\mathbb{Z}_p[G])$  for some  $m \geq n$  and all entries in the first  $n$  columns of  $N$  belong to  $I_{G,p}$ . For every matrix  $H$  in  $M_m(\mathbb{Z}_p[G])$  we also note that there is a unique matrix  $H'$  in  $M_m(\mathbb{Q}_p[G])$  with  $HH' = H'H = \text{nr}_{\mathbb{Q}_p[G]}(H)I_m$  and such that for every primitive central idempotent  $e$  of  $\mathbb{Q}_p[G]$  the matrix  $H'e$  is invertible if and only if  $\text{nr}_{\mathbb{Q}_p[G]}(H)e$  is non-zero. We follow Nickel [41] in defining the following  $\zeta(\mathbb{Z}_p[G])$ -submodule of  $\zeta(\mathbb{Q}_p[G])$

$$\mathcal{A}_p(G) := \{x \in \zeta(\mathbb{Q}_p[G]) : \text{if } m > 0 \text{ and } H \in M_m(\mathbb{Z}_p[G]) \text{ then } xH' \in M_m(\mathbb{Z}_p[G])\}.$$

For more details about the modules  $I_{G,p}^{[n]}$  and  $\mathcal{A}_p(G)$  see Remark 2.4 below.

Before stating the next result we note that if  $H^3(C)$  vanishes, then the  $\mathbb{Z}_p[G]$ -module  $H^2(C)$  has a quadratic presentation (by Theorem 2.1(iii)) and hence that the (non-commutative) Fitting invariant  $\text{Fitt}_{\mathbb{Z}_p[G]}(H^2(C))$  of  $H^2(C)$  is well-defined.

**Corollary 2.3.** *Let  $C$  and  $\mathcal{L}$  be as in Theorem 2.1.*

- (i) *Let  $\delta$  be any element of  $\mathcal{A}_p(G)$ ,  $\beta$  any element of  $a_G(H^3(C))$  and  $\gamma$  any element of  $\zeta(\mathbb{Z}_p[G]) \cap \zeta(\mathbb{Q}_p[G]e_3)$ . Then one has  $(\beta\gamma)^{g_3(C)}\delta\mathcal{L}e_1 \in a_G(H^2(C))$ .*
- (ii) *If  $H^3(C)$  is finite, then there exists a weakly organising matrix  $\Phi$  for  $C$  and  $|H^3(C)|$  with the property that  $|H^3(C)|^{g_3(C)}\mathcal{L}e_1 = \text{nr}_{\mathbb{Q}_p[G]}(\Phi) \in I_{G,p}^{[n]}$  with  $n = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2(C_G))$ .*
- (iii) *If  $H^3(C)$  vanishes, then  $\mathcal{L}e_1$  generates  $\text{Fit}_{\mathbb{Z}_p[G]}(H^2(C))$ .*

*Proof.* Regarding claim (i), we may clearly assume that  $\beta\gamma$  is non-zero. The definition of  $e_3$  implies that  $\beta \in \mathbb{Q}_p[G]e_3$ , so that actually  $\beta = \beta e_3$ . We may and will now choose a large enough multiple  $m$  of  $|G||H^3(C)_{\text{tor}}||H^2(C)_{\text{tor}}|$  to ensure that  $\beta' := \beta + me_3$  belongs to  $\zeta(\mathbb{Q}_p[G]e_3)^\times \cap a_G(H^3(C))$ . Set  $\alpha := \beta'\gamma$ . Theorem 2.1(iv) implies that  $\alpha^{g_3(C)}\delta\mathcal{L}e_1 = \delta\text{nr}_{\mathbb{Q}_p[G]}(\Phi_{C,\alpha})u_{\mathcal{L}}$  and Theorem 2.1(ii) implies that  $a_G(\text{cok}(\Phi_{C,\alpha})) \subseteq a_G(H^2(C))$ . Since  $\beta'^{g_3(C)}e_1 = (\beta + m)^{g_3(C)}e_2$ , the binomial theorem implies that  $(\beta\gamma)^{g_3(C)}\delta\mathcal{L}e_1$  belongs to  $a_G(H^2(C))$  if and only if  $\alpha^{g_3(C)}\delta\mathcal{L}e_1$  does. It is thus enough to prove that  $\delta\text{nr}_{\mathbb{Q}_p[G]}(\Phi_{C,\alpha})$  belongs to  $a_G(\text{cok}(\Phi_{C,\alpha}))$  and this is proved by Nickel in [41, Th. 4.2].

Claim (ii) follows directly by combining the equality in Theorem 2.1(iv) together with the following two facts: one has  $u_{\mathcal{L}} = \text{nr}_{\mathbb{Q}_p[G]}(U_{\mathcal{L}})$  for some matrix  $U_{\mathcal{L}}$  in  $\text{GL}_d(\mathbb{Z}_p[G])$ ; if  $\Phi'$  is any weakly organising matrix for  $C$  and  $|H^3(C)|$  with the property that precisely  $n$  of its columns have all entries in  $I_{G,p}$  (as constructed in Theorem 2.1(iii)), then  $\Phi := \Phi' \cdot U_{\mathcal{L}}$  is also a weakly organising matrix for  $C$  and  $|H^3(C)|$  which has precisely  $n$  of its columns with all entries in  $I_{G,p}$ .

Claim (iii) follows directly by combining the equality in Theorem 2.1(iv) with the isomorphism  $\text{cok}(\Phi_{C,1}) \cong H^2(C)$  in Theorem 2.1(iii) and the very definition of non-commutative Fitting invariants.  $\square$

**Remark 2.4.**

(i) In the context of Corollary 2.3 we note that for each natural number  $n$  the projection map  $G \rightarrow G^{\text{ab}}$  induces a surjective homomorphism of finite abelian groups  $\pi_{G,n} : I_{G,p}^{[n]} / I_{G,p}^{[n+1]} \rightarrow I_{G^{\text{ab}}}^n / I_{G^{\text{ab}}}^{n+1}$ . Groups of the form  $I_{G^{\text{ab}},p}^n / I_{G^{\text{ab}},p}^{n+1}$  are extensively studied in the literature (see, for example, the survey article [45]) but it seems likely that  $\ker(\pi_{G,n})$  is in general non-trivial.

(ii) If  $H = I_d$ , then  $H' = I_d$  and so  $\mathcal{A}_p(G) \subseteq \zeta(\mathbb{Z}_p[G])$ . This inclusion is an equality if  $G$  is abelian. In general, for each  $H$  in  $M_d(\mathbb{Z}_p[G])$  the matrix  $H'$  belongs to  $M_d(\mathcal{M})$  for any maximal order  $\mathcal{M}$  in  $\mathbb{Q}_p[G]$  that contains  $\mathbb{Z}_p[G]$  (cf. [41, Lem. 4.1]) and so Jacobinski's description in [28] of the central conductor of  $\mathcal{M}$  in  $\mathbb{Z}_p[G]$  implies that for any  $\mathbb{Q}_p^c$ -valued character  $\psi$  of  $G$  the element  $\psi(1)^{-1}|G|e_\psi$  belongs to  $\mathbb{Z}_p[\rho] \otimes_{\mathbb{Z}_p} \mathcal{A}_p(G)$  where  $\mathbb{Z}_p[\rho]$  is the subring of  $\mathbb{Q}_p^c$  that is generated over  $\mathbb{Z}_p$  by the values of  $\rho$ .

(iii) If  $G$  is abelian, then Corollary 2.3(iii) recovers the result of [9, Th. 8.2.1]. In particular, it follows from [9, Rem. 8.2.5] that Corollary 2.3(iii) gives in the setting of §1.2.3 a (non-commutative generalization of a) 'strong main conjecture' of the kind that Mazur and Tate ask for in [38, Remark after Conj. 3]. For a more general version of this result in the setting of §1.2.2 see Remark 5.2(ii).

(iv) Corollary 2.3(i) both refines and generalizes the main algebraic result of Snaith in [49] (which, amongst other conditions, required  $G$  to be abelian).

2.1.3. *The structure of  $H^1(C)$ .* Theorem 2.1(i) implies that weakly-organising matrices completely determine, at least in theory, the structure of  $H^1(C)$ . In this subsection we show that, in certain cases, the elementary properties of such matrices can also give some remarkably explicit information about  $H^1(C)$ .

For any subgroup  $J$  of  $G$  and any  $\Phi$  in  $M_d(\mathbb{Z}_p[G])$  we set  $d_J := d[G : J]$  and write  $\Phi^J$  for the image of  $\Phi$  under the homomorphism  $M_d(\mathbb{Z}_p[G]) \rightarrow M_{d_J}(\mathbb{Z}_p[J]) \rightarrow M_{d_J}(\mathbb{Z}_p)$ , where the first map is induced by a set of coset representatives of  $J$  in  $G$  and the second by the natural ring homomorphism  $\mathbb{Z}_p[J] \rightarrow \mathbb{Z}_p$ . We say that  $\Phi^J$  is 'saturated' if it is conjugate to a block matrix  $(\Psi \mid 0_{d_J, d_J - \text{rk}(\Phi^J)})$  where, for any natural numbers  $m$  and  $n$ , we write  $0_{m,n}$  for the  $m \times n$  zero-matrix. (This notion is independent of the choice of coset representatives and corresponds to the assumption that  $\text{im}(\Phi^J)$  is  $\mathbb{Z}_p$ -saturated as a submodule of  $\mathbb{Z}_p^{d_J}$ .)

For any  $H$  we also write  $\mathbb{Z}_p[G/H]$  for  $\mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[H]} \mathbb{Z}_p$ , regarded as a left  $\mathbb{Z}_p[G]$ -module in the obvious way. We will see in §5.3 that the following result has some important consequences in the context of §1.2.2 and §1.2.3.

**Corollary 2.5.** *Assume that the Sylow  $p$ -subgroups of  $G$  are cyclic. Assume also that  $H^3(C)$  vanishes and fix a weakly-organising matrix  $\Phi$  for  $C$ . If  $\Phi^J$  is saturated for each non-trivial subgroup  $J$  of a given Sylow  $p$ -subgroup  $P$ , then the  $\mathbb{Z}_p[G]$ -module  $H^1(C)$  decomposes as a finite direct sum of modules, each of which is isomorphic to a direct summand of  $\mathbb{Z}_p[G/J]$  for some subgroup  $J$  of  $P$ .*

*Proof.* Fix a Sylow  $p$ -subgroup  $P$  of  $G$ . Let  $\{c_i : 1 \leq i \leq d\}$  be the standard  $\mathbb{Z}_p[G]$ -basis of  $\mathbb{Z}_p[G]^d$ , with  $d$  as specified by Theorem 2.1 and, by abuse of notation, denote by  $\Phi$  the endomorphism of  $\mathbb{Z}_p[G]^d$  which is represented by the matrix  $\Phi$  with respect to this basis. For any non-trivial subgroup  $J$  of  $P$ , fix a set of coset representatives  $\{j_k : 1 \leq k \leq [G : J]\}$ , let  $\{c_{(i,k)} : 1 \leq i \leq d, 1 \leq k \leq [G : J]\}$  be the standard

$\mathbb{Z}_p$ -basis of  $\mathbb{Z}_p^{d_J}$  (ordered lexicographically) and, by abuse of notation, denote by  $\Phi^J$  the endomorphism of  $\mathbb{Z}_p^{d_J}$  which is represented by the matrix  $\Phi^J$ , defined by our choice of coset representatives of  $J$ , with respect to this basis. We have for each such  $J$  a commutative diagram of  $\mathbb{Z}_p$ -modules

$$\begin{array}{ccc} \mathbb{Z}_p \otimes_{\mathbb{Z}_p[J]} \mathbb{Z}_p[G]^d & \xrightarrow{\mathbb{Z}_p \otimes_{\mathbb{Z}_p[J]} \Phi} & \mathbb{Z}_p \otimes_{\mathbb{Z}_p[J]} \mathbb{Z}_p[G]^d \\ \cong \downarrow & & \downarrow \cong \\ \mathbb{Z}_p^{d_J} & \xrightarrow{\Phi^J} & \mathbb{Z}_p^{d_J} \end{array}$$

in which the vertical arrows send each product  $j_k c_i$  to  $c_{(i,k)}$ . The modules  $\text{cok}(\Phi^J)$  are by assumption  $\mathbb{Z}_p$ -torsion-free, and hence so are the modules  $\text{cok}(\mathbb{Z}_p \otimes_{\mathbb{Z}_p[J]} \Phi) \cong \mathbb{Z}_p \otimes_{\mathbb{Z}_p[J]} \text{cok}(\Phi) \cong \mathbb{Z}_p \otimes_{\mathbb{Z}_p[J]} H^2(C)$ , where the last isomorphism follows from the final sentence in Theorem 2.1(iii). But for each subgroup  $J$  of  $P$ , the Tate cohomology group  $\widehat{H}^{-1}(J, H^2(C))$  is a finite group of  $p$ -power order (which is trivial if  $J$  is the trivial group) and hence identifies with a finite submodule of  $\mathbb{Z}_p \otimes_{\mathbb{Z}_p[J]} H^2(C)$ . We deduce that  $\widehat{H}^{-1}(J, H^2(C))$  vanishes for all subgroups  $J$  of  $P$ . Since  $C$  is perfect and acyclic outside degrees 0 and 1, one easily shows that  $\widehat{H}^1(J, H^1(C))$  vanishes for all  $J$ , and since  $J$  is cyclic, its Tate cohomology is periodic of order 2 and hence  $\widehat{H}^{-1}(J, H^1(C))$  also vanishes for each subgroup  $J$  of  $P$ . Now Yakovlev proves in [53, Th. 2.4] that every indecomposable  $\mathbb{Z}_p[G]$ -module  $M$  which is both free of finite rank as a  $\mathbb{Z}_p$ -module and such that  $\widehat{H}^{-1}(J, M)$  vanishes for each subgroup  $J$  of  $P$  is isomorphic to a direct summand of  $\mathbb{Z}_p[G/J]$  for some such  $J$ . Since  $H^1(C)$  is  $\mathbb{Z}_p$ -torsion-free by assumption (wa<sub>4</sub>), and every finitely generated  $\mathbb{Z}_p[G]$ -module is noetherian, we can therefore deduce that it decomposes as a finite direct sum of  $\mathbb{Z}_p$ -torsion-free, indecomposable modules, each of which is isomorphic to a direct summand of  $\mathbb{Z}_p[G/J]$  for some subgroup  $J$  of  $P$ , as required.  $\square$

**2.2. Organising matrices.** In this section we use the following general notation concerning a finitely generated  $\mathbb{Z}_p[G]$ -module  $M$ : for each character  $\chi$  in  $\text{Irr}_p(G)$  we fix a left  $\mathbb{Q}_p^c[G]$ -module  $V_\chi$  which realises  $\chi$  and then set  $M_\chi := \text{Hom}_{\mathbb{Q}_p^c[G]}(V_\chi, M_{\mathbb{Q}_p^c})$  and  $r_\chi(M) := \dim_{\mathbb{Q}_p^c}(M_\chi)$ .

By a ‘permutation module’ we shall then mean a direct sum of (left)  $\mathbb{Z}_p[G]$ -modules of the form  $\bigoplus_{i=1}^{i=n} \Pi_i$  where each  $\Pi_i$  is a direct summand of  $\mathbb{Z}_p[G/H_i]$  for some subgroup  $H_i$  of  $G$ . We note in passing that if the group  $H_i$  is both normal and of  $p$ -power index in  $G$ , then a result of Coleman (cf. [19, Th. 32.13]) implies that  $\Pi_i = \mathbb{Z}_p[G/H_i]$ .

**2.2.1. The assumptions.** In the rest of §2.2 we assume to be given the following data:

- a complex  $C$  in  $D^a(\mathbb{Z}_p[G])$ ;
- a permutation module  $\Pi = \bigoplus_{i=1}^{i=n} \Pi_i$  and a surjective homomorphism of  $\mathbb{Z}_p[G]$ -modules  $\pi : H^2(C) \rightarrow \Pi$  which induces, upon passage to  $G$ -coinvariants, an isomorphism  $H^2(C)_{G,\text{tf}} \cong \Pi_G$ .

We will also assume that there exists a non-negative integer  $r$  (with  $r \leq n$ ) so that the  $\mathbb{Z}_p[G]$ -module  $\Pi_i$  is projective for each  $i$  with  $1 \leq i \leq r$  and we then set  $\Pi^{\text{pr}} := \bigoplus_{i=1}^{i=r} \Pi_i$  and  $\Pi^{\text{np}} := \bigoplus_{i=r+1}^{i=n} \Pi_i$ . We note, in particular, that  $\pi$  induces a composite surjection

$$(5) \quad \lambda_{\Pi} : H^2(C) \rightarrow \Pi = \Pi^{\text{pr}} \oplus \Pi^{\text{npr}} \rightarrow \Pi^{\text{pr}}$$

and hence implies that  $r_{\chi}(H^2(C)) \geq r_{\chi}(\Pi^{\text{pr}})$  for each character  $\chi$  in  $\text{Ir}_p(G)$ .

Before proceeding we give three examples to show that input data of the above kind exists in a wide variety of interesting cases.

**Example 2.6.** *The general case* For any given complex  $C$  in  $D^a(\mathbb{Z}_p[G])$  one obtains data of the above kind by setting  $\Pi := H^2(C)_{G,\text{tf}}$  and  $r := 0$  (so that  $\Pi^{\text{pr}}$  is trivial) and taking  $\pi$  to be the canonical homomorphism  $\pi_C : H^2(C) \rightarrow H^2(C)_{G,\text{tf}}$ .

**Example 2.7.** *Tate motives* In this example we assume that  $p$  is odd, we use the notation and hypotheses of §1.2.1 and for any integer  $m$  we set  $C_m := C(\mathbb{Z}_p(m)_F)^*[-3]$ . We also assume that  $H^0(k, W_F^*(1))$  vanishes and hence (by the arguments of §1.1.2) that  $C_m$  belongs to  $D^a(\mathbb{Z}_p[G])$ .

(i)  $m = 0$ . In this case  $H^0(k, W_F^*(1))$  vanishes if and only if  $F$  contains no non-trivial  $p$ -th roots of unity. In addition, Kummer theory and class field theory give identifications of  $H^1(C_0)$ ,  $H^2(C_0)_{\text{tor}}$  and  $H^2(C_0)_{\text{tf}}$  with  $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_{F,S}^{\times}$ ,  $\mathbb{Z}_p \otimes_{\mathbb{Z}} \text{Cl}(\mathcal{O}_{F,S})$  and the kernel  $X_{F,S}$  of the homomorphism  $\prod_{w \in S(F)} \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  that sends each  $(n_w)_w$  to  $\sum_{w \in S(F)} n_w$  respectively. We assume  $|S| > 1$ , set  $n := |S| - 1$ , label the elements of  $S$  as  $\{v_i : 0 \leq i \leq n\}$  and let  $r_{\text{sp}}$  be any integer such that each place  $v_i$  with  $1 \leq i \leq r_{\text{sp}}$  splits completely in  $F/k$ . Then there is a canonical surjective homomorphism from  $X_{F,S}$  to the permutation module  $Y_{F,S \setminus \{v_0\}} := \bigoplus_{i=1}^{i=n} (\bigoplus_{w|v_i} \mathbb{Z}_p)$ . We can thus set  $\Pi := Y_{F,S \setminus \{v_0\}}$ , define  $\Pi^{\text{pr}}$  to be the free  $\mathbb{Z}_p[G]$ -module  $\bigoplus_{i=1}^{i=r_{\text{sp}}} (\bigoplus_{w|v_i} \mathbb{Z}_p)$ , set  $r := r_{\text{sp}}$  and take  $\pi$  to be the canonical surjective homomorphism  $H^2(C_0) \rightarrow H^2(C_0)_{\text{tf}} = X_{F,S} \rightarrow Y_{F,S \setminus \{v_0\}}$ .

(ii)  $m < 0$ . In this case  $H^0(k, W_F^*(1))$  vanishes if and only if any abelian extension of  $F$  of exponent  $-m$  contains no non-trivial  $p$ -th roots of unity. In addition, the modules  $H^1(C_m)$  and  $H^2(C_m)_{\text{tor}}$  identify with  $\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{1-2m}(\mathcal{O}_F)$  and  $\mathbb{Z}_p \otimes_{\mathbb{Z}} K_{-2m}(\mathcal{O}_{F,S})$  respectively (see Remark 2.9 below). Also, if we write  $s_1$  and  $s_2$  for the number of real and complex places of  $k$  and set  $d_{k,m} := s_2 + \frac{1}{2}(1 + (-1)^m)s_1$ , then the  $\mathbb{Z}_p[G]$ -module  $H^2(C_m)_{\text{tf}}$  is isomorphic to a direct sum of  $d_{k,m}$  modules, each of which is a direct summand of  $\mathbb{Z}_p[G]$  (cf. [9, Lem. 11.1.1(iii)]) and so we can set  $\Pi = \Pi^{\text{pr}} := H^2(C_m)_{\text{tf}}$  and  $r = d_{k,m}$  and take  $\pi$  to be the canonical homomorphism  $H^2(C_m) \rightarrow H^2(C_m)_{\text{tf}}$ .

**Example 2.8.** *Cyclic Sylow  $p$ -subgroups* We now assume that Sylow  $p$ -subgroups of  $G$  are cyclic. Then in certain cases one can deduce from Corollary 2.5 that the  $\mathbb{Z}_p[G]$ -module  $H^2(C)_{\text{tf}}$  is a permutation module and hence one can take  $\pi$  to be the canonical homomorphism  $H^2(C) \rightarrow H^2(C)_{\text{tf}} =: \Pi$ . Such examples arise naturally in the setting of elliptic curves and either cyclic or dihedral extensions of number fields and in many of these cases one can also take  $r > 0$  so that  $\Pi^{\text{pr}}$  is non-trivial. (For more details about such examples see §5.3.)

**Remark 2.9.** Assume the notation of Example 2.7(ii). Then for each  $i \in \{0, 1\}$  the Quillen-Lichtenbaum Conjecture predicts that the  $p$ -adic étale Chern class homomorphism  $K_{2(1-m)-i}(\mathcal{O}_{F,S})_p \rightarrow H^i(\mathcal{O}_{F,S}, \mathbb{Z}_p(1-m))$  is bijective. It is known, by work of Suslin, that this conjecture is a consequence of the conjecture of Bloch and Kato relating Milnor  $K$ -theory to étale cohomology. Following fundamental work of Voevodsky

and Rost, Weibel has recently completed the proof of the Bloch-Kato Conjecture and hence also of the Quillen-Lichtenbaum Conjecture (cf. [51]). The explicit description of the modules  $H^1(C_m)$  and  $H^2(C_m)_{\text{tor}}$  given above relies on this fundamental result. (The authors are very grateful to Chuck Weibel for advise in this regard.)

2.2.2. *Regulators.* For each isomorphism  $t$  in  $\text{Is}_{\mathbb{C}_p[G]}(H^1(C)_{\mathbb{C}_p}, H^2(C)_{\mathbb{C}_p})$  and each homomorphism  $\theta$  in  $\text{Hom}_{\mathbb{Z}_p[G]}(H^1(C), H^2(C))$  we define a  $\zeta(\mathbb{C}_p[G])$ -valued regulator by setting

$$R_t(\theta) := \text{nr}_{\mathbb{C}_p[G]}(\theta_{\mathbb{C}_p} \circ t^{-1}).$$

We note that  $R_t(\theta)$  belongs to  $\zeta(\mathbb{C}_p[G])^\times$  if and only if  $\theta$  is injective.

2.2.3. *Statement of the main results.* For each integer  $i$  with  $1 \leq i \leq n$  we write  $N(H_i)$  for the normaliser of  $H_i$  in  $G$  and  $I(\Pi_i)$  for the kernel of the natural composite homomorphism  $\mathbb{Z}_p[G] \twoheadrightarrow \mathbb{Z}_p[G/H_i] \twoheadrightarrow \Pi_i$ .

We also write  $\Upsilon_{\text{pr}}$  for the subset of  $\text{Ir}_p(G)$  comprising characters  $\chi$  for which the inequality  $r_\chi(H^2(C)) \geq r_\chi(\Pi^{\text{pr}})$  in §2.2.1 is an equality. We note that  $\Upsilon_{\text{pr}}$  is a union of conjugacy classes under the natural action of  $\text{Gal}(\mathbb{Q}_p^c/\mathbb{Q}_p)$  on  $\text{Ir}_p(G)$  and hence that the associated idempotent  $e_{\text{pr}} := \sum_{\chi \in \Upsilon_{\text{pr}}} e_\chi$  belongs to  $\zeta(\mathbb{Q}_p[G])$ .

**Theorem 2.10.** *We fix a complex  $C$  and homomorphism  $\pi$  as in §2.2.1 and also use the notation of §2.2.2. Then there exists a natural number  $d$  (with  $d \geq n$ ) and a canonical family  $\text{M}(C, \pi)$  of weakly-organising matrices  $\Phi$  for  $C$  that belong to  $\text{M}_d(\mathbb{Z}_p[G])$  and in addition satisfy all of the following conditions.*

- (i) *If  $J$  is a normal subgroup of  $G$ , then  $\Phi_J$  is a relation matrix for the  $\mathbb{Z}_p[G/J]$ -module  $H^2(C_J)$ . In addition, if  $G$  is a  $p$ -group, then  $\Phi_G$  is a block matrix  $\begin{pmatrix} 0_{d,n} & \Psi \end{pmatrix}$  where  $\Psi$  is a relation matrix for the  $\mathbb{Z}_p$ -module  $H^2(C_G)_{\text{tor}}$ .*
- (ii) *If  $i$  is any integer with  $1 \leq i \leq n$ , then every element of the  $i$ -th column of  $\Phi$  belongs to  $I(\Pi_i)$ . Further, if  $r < i \leq n$ , then the  $i$ -th column of  $\Phi$  computes a natural algebraic height pairing*

$$H^1(C_{N(H_i)}) \otimes_{\mathbb{Z}_p[G/N(H_i)]} \text{Hom}_{\mathbb{Z}_p}(H^2(C_{N(H_i)}), \mathbb{Z}_p) \rightarrow N(H_i)^{\text{ab}}.$$

- (iii) *For each  $\theta$  in  $\text{Hom}_{\mathbb{Z}_p[G]}(H^1(C), H^2(C))$  there exists an ‘augmented’ matrix  $\Phi(\theta)$  in  $\text{M}_d(\mathbb{Z}_p[G])$  which agrees with  $\Phi$  in all but the first  $r$  columns and has the following property: for each  $t$  in  $\text{Is}_{\mathbb{C}_p[G]}(H^1(C)_{\mathbb{C}_p}, H^2(C)_{\mathbb{C}_p})$  and each characteristic element  $\mathcal{L}_t$  for the pair  $(C, t)$  one has  $R_t(\theta)\mathcal{L}_t e_{\text{pr}} = \text{nr}_{\mathbb{Q}_p[G]}(\Phi(\theta))u_{\mathcal{L}_t}$  where  $u_{\mathcal{L}_t}$  belongs to  $\text{nr}_{\mathbb{Q}_p[G]}(\mathbb{Z}_p[G]^\times)$ .*
- (iv) *If  $\Phi$  and  $\Phi'$  belong to  $\text{M}(C, \pi)$ , then  $\Phi' = U\Phi V$  for suitable matrices  $U$  and  $V$  in  $\text{GL}_d(\mathbb{Z}_p[G])$ .*

**Definition 2.11.** We shall call any matrix that belongs to the family  $\text{M}(C, \pi)$  constructed in Theorem 2.10 an ‘organising matrix’ for  $C$  and  $\pi$ .

The following result (which will be proved in §3.2.6) describes an important consequence of the existence of organising matrices. We will see that this result has several interesting arithmetic consequences.

**Corollary 2.12.** *We use the hypotheses and notation of Theorem 2.10. Then for every  $a$  in  $\mathcal{A}_p(G)$ ,  $t$  in  $\text{Is}_{\mathbb{C}_p[G]}(H^1(C)_{\mathbb{C}_p}, H^2(C)_{\mathbb{C}_p})$  and  $\theta$  in  $\text{Hom}_{\mathbb{Z}_p[G]}(H^1(C), H^2(C))$ ,*

the element  $aR_t(\theta)\mathcal{L}_te_{\text{pr}}$  belongs to  $a_G(\ker(\lambda_\Pi))$ . In particular, every such element  $aR_t(\theta)\mathcal{L}_te_{\text{pr}}$  belongs to  $\zeta(\mathbb{Z}_p[G])$  and annihilates the module  $H^2(C)_{\text{tor}} \oplus \Pi^{\text{apr}}$ .

**Remark 2.13.** The containment  $aR_t(\theta)\mathcal{L}_te_{\text{pr}} \in \zeta(\mathbb{Z}_p[G])$  that occurs in Corollary 2.12 can be interpreted as a family of explicit congruence relations between the elements  $aR_t(\theta)\mathcal{L}_te_\rho$  as  $\rho$  varies. To explain this we define for each  $\rho$  in  $\text{Ir}_p(G)$  an element  $A(\rho)$  of  $\mathbb{C}_p$  by the equality

$$A(\rho)e_\rho = \begin{cases} aR_t(\theta)\mathcal{L}_te_\rho, & \text{if } e_\rho e_{\text{pr}} = e_\rho \\ 0, & \text{otherwise.} \end{cases}$$

We write  $E$  for the field generated over  $\mathbb{Q}_p$  by  $\{\psi(g) : g \in G, \psi \in \text{Ir}_p(G)\}$ . Then the containment  $aR_t(\theta)\mathcal{L}_te_{\text{pr}} \in \zeta(\mathbb{Z}_p[G])$  implies that each  $A(\rho)$  belongs to the valuation ring  $\mathcal{O}$  of  $E$  and also satisfies  $\omega(A(\rho)) = A(\omega \circ \rho)$  for all  $\omega \in G_{E/\mathbb{Q}_p}$ . Further, for differing  $\rho$ , the elements  $A(\rho)$  must satisfy a family of mutual congruence relations that are together equivalent to the condition that an element of the integral closure of  $\mathbb{Z}_p$  in  $\zeta(\mathbb{Q}_p[G])$  should actually belong to  $\zeta(\mathbb{Z}_p[G])$ . For example, if  $|G| = p$ , then the required condition is that  $A(\rho) \equiv A(\rho_0) \pmod{\mathfrak{p}}$  for every  $\rho \in \text{Ir}_p(G)$ , where  $\rho_0$  is the trivial character of  $G$  and  $\mathfrak{p}$  the maximal ideal of  $\mathcal{O}$ . However, explicating these congruences in any very general setting seems to be a difficult algebraic problem.

**Remark 2.14.** Let  $\Phi$  be an organising matrix for  $C$  and  $\pi$  as in Theorem 2.10 and (since  $H^3(C)$  vanishes) use Theorem 2.1(i) and (ii) (with  $\alpha = 1$ ) to fix identifications of  $\ker(\Phi)$  and  $\text{cok}(\Phi)$  with  $H^1(C)$  and  $H^2(C)$  respectively. Then the tautological exact sequence

$$0 \rightarrow \ker(\Phi) \rightarrow \mathbb{Z}_p[G]^d \xrightarrow{\Phi} \mathbb{Z}_p[G]^d \rightarrow \text{cok}(\Phi) \rightarrow 0$$

determines an element  $\epsilon(C)$  of the Yoneda ext-group  $\text{YExt}_{\mathbb{Z}_p[G]}^2(H^2(C), H^1(C))$  that can be shown to depend only upon  $C$ . Such extension classes can encode highly significant arithmetic data. For example, if  $C = C_0$  (as in Example 2.7(i)), and  $S$  is sufficiently large to ensure that  $\text{Cl}(\mathcal{O}_{F,S})$  is trivial, then [13, Prop. 3.5] shows that  $\epsilon(C_0)$  is equal to the ‘canonical class’ that is defined by Tate in [50] by using class field theory.

**2.2.4. Arithmetic examples.** In §4 and §5 we will show that Theorem 2.10 and Corollary 2.12 give rise to a variety of new results and conjectures in the setting of the arithmetic examples discussed in §1.2. In this subsection we give an early indication of the usefulness of our approach by discussing links between the theory discussed above and several results and conjectures in the literature.

**Example 2.15. The general case.** In this example we fix an arbitrary complex  $C$  in  $D^a(\mathbb{Z}_p[G])$  and use the same notation as in Example 2.6. In this case the  $\mathbb{Z}_p[G]$ -module  $\Pi$  is isomorphic to  $\mathbb{Z}_p^n$  with  $n = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2(C)_G)$  and Theorem 2.10 can be applied with  $r = 0$  (so that  $e_{\text{pr}} = e_1 = e_2$  in the notation of §1.1.4 and also  $R_t(\theta)e_{\text{pr}} = e_{\text{pr}}$ ) and both  $N(H_i) = G$  and  $I(\Pi_i) = I_{G,p}$  for each integer  $i$  with  $1 \leq i \leq n$ . In particular, if  $G$  is abelian, then Corollary 2.3(ii) (with  $h = 1$ ) implies that  $\mathcal{L}e_1$  belongs to  $I_{G,p}^n$  for any characteristic element  $\mathcal{L}$  of  $C$  and the same argument that deduces [9, Th. 9.2.2] from the equality of [9, (36)] shows that Theorem 2.10(ii) and (iii) combine to imply a formula for the residue class of  $\mathcal{L}e_1$  modulo  $I_{G,p}^{n+1}$  in terms

of the discriminant of a natural algebraic height pairing. Specialising to the setting of §1.2.3 this result combines with the equivariant Tamagawa number conjecture to predict a refinement of the Birch and Swinnerton-Dyer conjecture that is in precisely the same spirit as (but more general than) the congruences for modular symbols that are conjectured by Mazur and Tate in [38]. (In this context we also believe, but have not yet been able to prove, that the height pairings that occur in Theorem 2.10(ii) coincide with the  $G$ -valued height pairings defined in [38].) For a version of this conjectural framework in the setting of §1.2.2 see Remark 5.2(ii).

**Example 2.16.** *Tate motives.* In this example we use the same hypotheses and notation as in Example 2.7.

(i)  $m = 0$ . We write  $t_0$  for the isomorphism  $\mathbb{C}_p \otimes_{\mathbb{Z}} \mathcal{O}_{F,S}^{\times} \rightarrow \mathbb{C}_p \otimes_{\mathbb{Z}_p} X_{F,S}$  induced by the Dirichlet regulator map. Then [10, Th. 4.1.1] shows that the equivariant Tamagawa number conjecture implies the existence of a characteristic element  $\mathcal{L}_0$  for  $(C_0, t_0)$  such that  $\mathcal{L}_0 e_{\text{pr}}$  is equal, up to multiplication by an element of  $\zeta(\mathbb{Z}_p[G])^{\times}$ , to the image in  $\zeta(\mathbb{C}_p[G])^{\times}$  of the ' $r$ -th order (non-abelian) Stickelberger element' that is introduced in [10]. In addition, the result of [10, Th. 7.5.1] shows that the height pairings that occur in Theorem 2.10(ii) with  $C = C_0$  coincide with the pairings

$$(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_{F^{N(H_i)}, S}^{\times}) \otimes_{\mathbb{Z}_p} \bigoplus_{w \in S_{v_i}(F^{N(H_i)})} \mathbb{Z}_p \rightarrow N(H_i)^{\text{ab}}$$

that are induced by local reciprocity maps. In this way the results of Theorem 2.10 and Corollary 2.12 specialise to recover the main results of [10]. In this regard we recall that the central conjectures of [10] constitute a universal refinement of Stark's Conjecture that incorporates simultaneous strengthenings of well-known conjectures of Gross, of Rubin and of Tate.

(ii)  $m < 0$ . In this case we write  $t_m$  for the isomorphism  $H^1(C_m)_{\mathbb{C}_p} \rightarrow H^2(C_m)_{\mathbb{C}_p}$  that is induced by combining the descriptions of  $H^1(C_m)$  and  $H^2(C_m)$  given in Example 2.7(ii) together with  $-1$  times the Beilinson regulator map. Then the argument of [9, §11.1] shows that the equivariant Tamagawa number conjecture implies the existence of a characteristic element for  $(C_m, t_m)$  that is constructed from the leading terms at  $m$  of the Artin  $L$ -functions of characters of  $G$ . In this context the result of Corollary 2.12 can be used to give a different proof of the main result (Theorem 4.1) of Nickel in [42].

**2.3. Symmetric organising matrices.** Given a symmetric, resp. skew-symmetric, admissible complex  $(C, \delta)$  as defined in §1.1.3 it is natural to ask if the family  $M(C, \pi)$  that is constructed in Theorem 2.10 (with  $\pi$  specified as, for instance, in Example 2.15) contains a matrix that is symmetric, resp. skew-symmetric? If this is the case, then Theorem 2.10 would provide a strong restriction on the structure of both Tate-Shafarevich and Selmer groups as  $\mathbb{Z}_p[G]$ -modules. We are not yet able to answer this question. Nevertheless, in the following result we do associate to  $(C, \delta)$  a canonical family of symmetric, resp. skew-symmetric, matrices which, whilst having fewer properties than the matrices in  $M(C, \pi)$ , does provide a natural generalisation of the constructions made by Mazur and Rubin in [36].

For any finitely generated projective  $\mathbb{Z}_p[G]$ -module  $Q$  that is self-dual (that is, isomorphic to its  $\mathbb{Z}_p$ -linear dual  $Q^*$ ) we write  $Q^{\bullet}$  for the complex  $Q \xrightarrow{0} Q^*$  where the

first term is placed in degree 1, and  $\delta_Q$  for the isomorphism of complexes  $Q^\bullet \rightarrow Q^{\bullet,*}$  that is induced by the canonical identification  $(Q^*)^* \cong Q$ . Then for any such module  $Q$ , and any symmetric, resp. skew-symmetric, admissible complex of  $\mathbb{Z}_p[G]$ -modules  $(C, \delta)$ , the pair  $(C \oplus Q^\bullet, \delta \oplus \delta_Q)$  is also a symmetric, resp. skew-symmetric, admissible complex of  $\mathbb{Z}_p[G]$ -modules.

**Theorem 2.17.** *Assume that  $p$  is odd and let  $(C, \delta)$  be a symmetric, resp. skew-symmetric, admissible complex of  $\mathbb{Z}_p[G]$ -modules.*

- (i) *If  $G$  is a  $p$ -group, then there exists a natural number  $d$  (with  $d \geq n$ ) and a canonical family  $M(C, \delta)$  of matrices  $\Phi$  in  $M_d(\mathbb{Z}_p[G])$  that have all of the properties described in Theorem 2.1 (with  $\alpha = 1$ ) and in addition satisfy all of the conditions listed below.*
  - (a)  *$\Phi$  is symmetric, resp. skew-symmetric, and any other matrix in  $M(C, \delta)$  has the form  $U\Phi U^{\text{tr}}$  with  $U$  in  $\text{GL}_d(\mathbb{Z}_p[G])$ .*
  - (b) *For each normal subgroup  $J$  of  $G$  the matrix  $\Phi_J$  is a relation matrix for the  $\mathbb{Z}_p[G/J]$ -module  $H^2(C_J)$ .*
  - (c) *For each normal subgroup  $J$  of  $G$  there is a canonical non-degenerate symmetric, resp. skew-symmetric,  $G/J$ -invariant pairing*

$$\rho_J : \text{cok}(\Phi_J)_{\text{tor}} \times \text{cok}(\Phi_J^{\text{tr}})_{\text{tor}} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

*The pairing  $H^2(C_J)_{\text{tor}} \times H^2(C_J)_{\text{tor}} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$  that sends  $(x, y)$  to the image of  $x$  under  $H^2(R\text{Hom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G/J], \delta))(y)$  is induced by  $\rho_J$ .*

- (ii) *In general, there exists a finitely generated projective self-dual  $\mathbb{Z}_p[G]$ -module  $Q$  that is unique up to isomorphism and such that all of the assertions in claim (i) are valid after one replaces  $(C, \delta)$  by  $(C \oplus Q^\bullet, \delta \oplus \delta_Q)$ .*

**Definition 2.18.** We call any matrix in the set  $M(C, \delta)$  a ‘symmetric organising matrix’, resp. ‘skew-symmetric organising matrix’, for the symmetric, resp. skew-symmetric, admissible complex  $(C, \delta)$ .

**Remark 2.19.** If one specialises to the cases considered by Mazur and Rubin in [36], then our proof of Theorem 2.17(i) will show that elements of  $M(C, \delta)$  are simply the matrix representatives of the differential that occurs in the complex  $\Phi^\bullet$  that is defined in [36, Def. 6.3] for any basic skew-Hermitian module  $\Phi$  that is associated to a skew-symmetric admissible complex  $(C, \delta)$  by [36, Prop. 6.5]. It follows in particular that [36, Rem. 7.9] provides concrete examples of the construction of Theorem 2.17 in this particular situation.

### 3. THE PROOFS OF THEOREMS 2.1, 2.10 AND 2.17

**3.1. The proof of Theorem 2.1.** Since  $C$  is both perfect (by assumption (wa<sub>1</sub>)) and acyclic outside degrees 1, 2 and 3 (by assumption (wa<sub>3</sub>)) a standard argument shows that it is isomorphic in  $D^{\text{p}}(\mathbb{Z}_p[G])$  to a complex of the form  $F^\bullet : F^1 \xrightarrow{d^1} F^2 \xrightarrow{d^2} F^3$  where  $F^1$  occurs in degree 1,  $F^2$  and  $F^3$  are finitely generated free  $\mathbb{Z}_p[G]$ -modules with  $\text{rk}_{\mathbb{Z}_p[G]}(F^3)$  equal to the minimal number  $g_3(C)$  of generators of  $H^3(C)$  as a  $\mathbb{Z}_p[G]$ -module, and  $F^1$  is a finitely generated  $\mathbb{Z}_p[G]$ -module that has finite projective dimension (cf. [20, Rapport, Lem. 4.7]). Set  $d := \text{rk}_{\mathbb{Z}_p[G]}(F^2)$ . Now  $\ker(d^1) \cong H^1(C)$  is  $\mathbb{Z}_p$ -free (by assumption (wa<sub>4</sub>)) and  $\text{im}(d^1)$  is a submodule of the free  $\mathbb{Z}_p$ -module

$F^2$  and so the tautological exact sequence  $0 \rightarrow \ker(d^1) \rightarrow F^1 \rightarrow \text{im}(d^1) \rightarrow 0$  implies that  $F^1$  is  $\mathbb{Z}_p$ -free. It follows that  $F^1$  is a projective  $\mathbb{Z}_p[G]$ -module since any finitely generated  $\mathbb{Z}_p[G]$ -module that is both  $\mathbb{Z}_p$ -free and of finite projective dimension is projective (cf. [1, Th. 8]). In addition, since  $\mathbb{Q}_p[G] \otimes_{\mathbb{Z}_p[G]} F^2$  and  $\mathbb{Q}_p[G] \otimes_{\mathbb{Z}_p[G]} F^3$  are both free  $\mathbb{Q}_p[G]$ -modules and the Euler characteristic of  $\mathbb{Q}_p[G] \otimes_{\mathbb{Z}_p[G]} F^\bullet$  in  $K_0(\mathbb{Q}_p[G])$  vanishes (by assumption (wa<sub>2</sub>)) the  $\mathbb{Q}_p[G]$ -module  $\mathbb{Q}_p[G] \otimes_{\mathbb{Z}_p[G]} F^1$  is also free and of rank  $d - g_3(C)$ . By Swan's Theorem [19, (32.1)], this implies that  $F^1$  is a (finitely generated) free  $\mathbb{Z}_p[G]$ -module of rank  $d - g_3(C)$ .

Let  $\alpha = \beta\gamma$  with  $\beta \in a_G(H^3(C)) \cap \zeta(\mathbb{Q}_p[G]e_3)^\times$  and  $\gamma \in \zeta(\mathbb{Z}_p[G]) \cap \zeta(\mathbb{Q}_p[G]e_3)$ . Fix a  $\mathbb{Z}_p[G]$ -basis  $\{b_1, \dots, b_{g_3(C)}\}$  of  $F^3$ . Then there exists a subset  $\{c_1, \dots, c_{g_3(C)}\}$  of  $F^2$  such that  $d^2(c_i) = \beta b_i$  for each  $i$ . Let  $\eta : F_{\mathbb{Q}_p}^3 \rightarrow F_{\mathbb{Q}_p}^2$  be the associated homomorphism which sends each element  $b_i$  to  $\beta^{-1}c_i$  (where  $\beta^{-1}$  denotes the inverse of  $\beta$  in  $\zeta(\mathbb{Q}_p[G]e_3)$ ). Then the restriction of  $\eta$  to  $F_{\mathbb{Q}_p}^3 e_3$  is a section to the restriction of  $d_{\mathbb{Q}_p}^2$  to  $F_{\mathbb{Q}_p}^2 e_3$ , and one has  $\eta(\alpha F^3) = (\gamma\beta)\eta(F^3) \subseteq (\gamma e_3)F^2 \subseteq F^2$ , where the last inclusion is valid since our choice of  $\gamma$  implies that  $\gamma e_3 \in \mathbb{Z}_p[G]$ . We now define

$$\varphi = \varphi_{C,\alpha} : F^1 \oplus F^3 \rightarrow F^2$$

by setting  $\varphi((f^1, f^3)) := d^1(f^1) + \eta(\alpha f^3)$  for any  $(f^1, f^3) \in F^1 \oplus F^3$ . This map is a homomorphism between free  $\mathbb{Z}_p[G]$ -modules (of rank  $d$ ) and we shall define  $\Phi = \Phi_{C,\alpha}$  to be a matrix representative of  $\varphi$  with respect to a suitable choice of  $\mathbb{Z}_p[G]$ -bases.

Suppose first that  $(f^1, f^3) \in \ker(\varphi)$ . Then one has  $0 = d^2(\varphi((f^1, f^3))) = d^2(d^1(f^1)) + d^2(\eta(\alpha f^3)) = \alpha f^3$ , and hence also  $0 = \varphi((f^1, f^3)) = d^1(f^1)$ . So, if by abuse of notation, we let  $\alpha : F^3 \rightarrow F^3$  denote the map given by the action of  $\alpha$ , then one has  $\ker(\varphi) = H^1(C) \oplus \ker(\alpha) \cong H^1(C) \oplus I(\mathbb{Z}_p[G]e_3)^{g_3(C)}$ .

Note now that the natural map from  $H^2(C)$  to  $\text{cok}(\varphi)$  is an injection; indeed, if  $d^1(f^1) + \eta(\alpha f^3) \in \ker(d^2)$  for some  $(f^1, f^3) \in F^1 \oplus F^3$ , then  $\alpha f^3 = 0$  and hence  $d^1(f^1) + \eta(\alpha f^3) = d^1(f^1) \in \text{im}(d^1)$ . Furthermore,  $\alpha(\text{cok}(\varphi)/\text{im}(H^2(C))) = 0$ ; indeed, for any  $f \in F^2$ , we have that  $\alpha f - \eta(\alpha d^2(f)) \in \ker(d^2)$ . Claim (ii) is hence satisfied with  $M_\alpha := \text{cok}(\varphi)/\text{im}(H^2(C))$ .

We now suppose given  $t$  in  $\text{Is}_{\mathbb{Q}_p[G]}((H^1(C) \oplus H^3(C))_{\mathbb{Q}_p}, H^2(C)_{\mathbb{Q}_p})$  and a characteristic element  $\mathcal{L}$  for the pair  $(C, t)$ . To proceed we first recall that  $\chi^{\text{ref}}(C, t)$  is defined to be equal to  $[F^1 \oplus F^3, F^2, \lambda] \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G])$  where  $\lambda$  is any composite isomorphism of  $\mathbb{Q}_p[G]$ -modules of the form

$$\begin{aligned} (6) \quad (F^1 \oplus F^3)_{\mathbb{Q}_p} &\xrightarrow{\sim} (\text{im}(d^1) \oplus \text{im}(d^2) \oplus H^1(C) \oplus H^3(C))_{\mathbb{Q}_p} \\ &\xrightarrow{\sim} (\text{im}(d^1) \oplus \text{im}(d^2) \oplus H^2(C))_{\mathbb{Q}_p} \\ &\xrightarrow{\sim} (\text{im}(d^2) \oplus \ker(d^2))_{\mathbb{Q}_p} \\ &\xrightarrow{\sim} F_{\mathbb{Q}_p}^2. \end{aligned}$$

Here the first, third and fourth arrows are induced by a choice of splitting of the short exact sequences of  $\mathbb{Q}_p[G]$ -modules that are obtained by scalar extension of the following tautological sequences

$$\begin{aligned}
0 &\rightarrow H^1(C) \rightarrow F^1 \xrightarrow{d^1} \text{im}(d^1) \rightarrow 0, \\
0 &\rightarrow \text{im}(d^2) \rightarrow F^3 \rightarrow H^3(C) \rightarrow 0, \\
0 &\rightarrow \text{im}(d^1) \rightarrow \ker(d^2) \rightarrow H^2(C) \rightarrow 0, \\
0 &\rightarrow \ker(d^2) \rightarrow F^2 \xrightarrow{d^2} \text{im}(d^2) \rightarrow 0,
\end{aligned}$$

and the second arrow in (6) is induced by the given isomorphism  $t$ . It is straightforward to show that the element  $[F^1 \oplus F^3, F^2, \lambda]$  is indeed independent of all these choices. Further, since the restriction of  $\eta$  to  $F_{\mathbb{Q}_p}^3 e_3$  is a section to the restriction of  $d_{\mathbb{Q}_p}^2$  to  $F_{\mathbb{Q}_p}^2 e_3$ , we may and will make the relevant choices of section so that the restriction of  $\lambda$  to  $(F_{\mathbb{Q}_p}^1 \oplus F_{\mathbb{Q}_p}^3) e_2$  coincides with the restriction of  $d_{\mathbb{Q}_p}^1 \oplus \eta$ .

In the sequel we (choose bases and so) fix identifications of  $F^1 \oplus F^3$  and  $F^2$  with  $\mathbb{Z}_p[G]^d$  and hence regard  $\lambda$  and  $\varphi$  as elements of  $\text{Aut}_{\mathbb{Q}_p[G]}(\mathbb{Q}_p[G]^d)$  and  $\text{End}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G]^d) \subset \text{End}_{\mathbb{Q}_p[G]}(\mathbb{Q}_p[G]^d)$  respectively. Then

$$\partial_{\mathbb{Z}_p[G], \mathbb{Q}_p}^1(\text{nr}_{\mathbb{Q}_p[G]}^{-1}(\mathcal{L})) = [F^1 \oplus F^3, F^2, \lambda] = \partial_{\mathbb{Z}_p[G], \mathbb{Q}_p}^1([\mathbb{Q}_p[G]^d, \lambda])$$

and so the exactness of (the top row of) (2) implies that  $\text{nr}_{\mathbb{Q}_p[G]}^{-1}(\mathcal{L}) - [\mathbb{Q}_p[G]^d, \lambda]$  belongs to  $\ker(\partial_{\mathbb{Z}_p[G], \mathbb{Q}_p}^1) = \text{im}(\partial_{\mathbb{Z}_p[G], \mathbb{Q}_p}^2)$ , and hence that  $\mathcal{L} \cdot \text{nr}_{\mathbb{Q}_p[G]}(\lambda)^{-1}$  belongs to  $\text{nr}_{\mathbb{Q}_p[G]}(\text{im}(\partial_{\mathbb{Z}_p[G], \mathbb{Q}_p}^2))$ . But, since  $\mathbb{Z}_p[G]$  is semi-local, the natural homomorphism  $\mathbb{Z}_p[G]^\times \rightarrow K_1(\mathbb{Z}_p[G])$  is surjective and so there exists an element  $U_{\mathcal{L}}$  of  $\mathbb{Z}_p[G]^\times$  such that

$$(7) \quad \mathcal{L} = \text{nr}_{\mathbb{Q}_p[G]}(U_{\mathcal{L}}) \text{nr}_{\mathbb{Q}_p[G]}(\lambda).$$

We set  $u_{\mathcal{L}} := \text{nr}_{\mathbb{Q}_p[G]}(U_{\mathcal{L}})$ .

Now if  $e_\chi$  is any primitive idempotent of  $\zeta(\mathbb{Q}_p[G])$  such that  $H^1(C)_{\mathbb{Q}_p} e_\chi$  is non-trivial, then our explicit description of  $\ker(\varphi)$  implies that  $\ker(\varphi)_{\mathbb{Q}_p} e_\chi$  is also non-trivial and hence that  $e_\chi \text{nr}_{\mathbb{Q}_p[G]}(\varphi) = 0$ . It follows that  $e_1 \text{nr}_{\mathbb{Q}_p[G]}(\varphi) = \text{nr}_{\mathbb{Q}_p[G]}(\varphi)$ . Combining this equality with (7), our choice of  $\lambda$  and our definitions of  $u_{\mathcal{L}}$  and of  $\varphi$ , we deduce that

$$\begin{aligned}
\alpha^{g_3(C)} \mathcal{L} e_1 &= e_2 \alpha^{g_3(C)} \mathcal{L} \\
&= u_{\mathcal{L}} \alpha^{g_3(C)} e_2 \text{nr}_{\mathbb{Q}_p[G]}(\lambda) \\
&= u_{\mathcal{L}} \alpha^{g_3(C)} \text{nr}_{\mathbb{Q}_p[G]}(\lambda | (F^1 \oplus F^3)_{\mathbb{Q}_p} e_2) \\
&= u_{\mathcal{L}} \alpha^{g_3(C)} \text{nr}_{\mathbb{Q}_p[G]}(d_{\mathbb{Q}_p}^1 \oplus \eta | (F^1 \oplus F^3)_{\mathbb{Q}_p} e_2) \\
&= u_{\mathcal{L}} e_2 \alpha^{g_3(C)} \text{nr}_{\mathbb{Q}_p[G]}(d_{\mathbb{Q}_p}^1 \oplus \eta) \\
&= u_{\mathcal{L}} e_1 \alpha^{g_3(C)} \text{nr}_{\mathbb{Q}_p[G]}(d_{\mathbb{Q}_p}^1 \oplus \eta) \\
&= u_{\mathcal{L}} e_1 \text{nr}_{\mathbb{Q}_p[G]}(\varphi) \\
&= \text{nr}_{\mathbb{Q}_p[G]}(\varphi) u_{\mathcal{L}},
\end{aligned}$$

as required to prove claim (ii).

All that is now left is to prove Theorem 2.1(iii). To do this we assume that  $H^3(C)$  is finite and let  $h$  be any integer multiple of  $|H^3(C)|$ , so that  $H^2(C)_{\mathbb{Q}_p} \cong \text{cok}(\varphi_{C,h})_{\mathbb{Q}_p}$ . Then  $(\varphi_{C,h})_G : (F^1 \oplus F^3)_G \rightarrow F_G^2$  is a homomorphism of free  $\mathbb{Z}_p$ -modules of rank  $d$ , and it is clear that one can choose  $\mathbb{Z}_p$ -bases of  $(F^1 \oplus F^3)_G$  and  $F_G^2$  so that the corresponding matrix in  $M_d(\mathbb{Z}_p)$  has precisely  $n' := \dim_{\mathbb{Q}_p}(\text{cok}((\varphi_{C,h})_G)_{\mathbb{Q}_p})$  zero columns. In particular, if we assume (as we may) that the  $\mathbb{Z}_p[G]$ -bases of  $F^1 \oplus F^3$  and  $F^2$  that we fixed above map under the natural projections to our chosen bases of  $(F^1 \oplus F^3)_G$  and  $F_G^2$ , then the matrix  $\Phi = \Phi_{C,h}$  in  $M_d(\mathbb{Z}_p[G])$  that represents  $\varphi_{C,h}$  with respect to this choice of bases has precisely  $n'$  columns that have all of their entries in  $I_{G,p}$ . It therefore only remains to check that  $n = n'$  and this is true because  $H^3(C)$  is finite and so

$$\begin{aligned} n &:= \dim_{\mathbb{Q}_p}(H^2(C_G)_{\mathbb{Q}_p}) = \dim_{\mathbb{Q}_p}((H^2(C)_G)_{\mathbb{Q}_p}) \\ &= \dim_{\mathbb{Q}_p}(\text{cok}(\varphi_{C,h})_G)_{\mathbb{Q}_p} \\ &= \dim_{\mathbb{Q}_p}(\text{cok}((\varphi_{C,h})_G)_{\mathbb{Q}_p}) =: n'. \end{aligned}$$

The assertion of claim (iii) is now obtained by setting  $\alpha = h = |H^3(C)|$ . This completes the proof of Theorem 2.1.

**3.2. The proofs of Theorem 2.10 and of Corollary 2.12.** In this section we set  $R := \mathbb{Z}_p[G]$  and write  $J(R)$  for the Jacobson radical of  $R$  and  $A$  for the semisimple algebra  $R/J(R)$ . We recall that  $R$  is semiperfect (cf. [19, p. 132]) so [19, Th. (6.23)] implies that for every finitely generated  $R$ -module  $M$  there exists a ‘projective cover’  $\varpi : P \rightarrow M$  in which  $P$  is a finitely generated projective  $R$ -module and  $\varpi$  is a homomorphism of  $R$ -modules such that  $A \otimes_R \varpi$  is bijective. We recall that any such homomorphism is unique up to isomorphism in the sense that if  $\varpi' : P' \rightarrow M$  is any other projective cover of  $M$ , then Nakayama’s Lemma implies that there exists a commutative diagram of  $R$ -modules

$$(8) \quad \begin{array}{ccc} P & \xrightarrow{\varpi} & M \\ \iota \downarrow & & \parallel \\ P' & \xrightarrow{\varpi'} & M \end{array}$$

in which  $\iota$  is an isomorphism.

**3.2.1. A convenient resolution.** In the following result we use the surjective homomorphism  $\pi : H^2(C) \rightarrow \Pi$  that is assumed to be given in Theorem 2.10. We recall that  $\Pi = \bigoplus_{i=1}^{i=n} \Pi_i$  and that each module  $\Pi_i$  is a direct summand of  $\mathbb{Z}_p[G/H_i]$  for some subgroup  $H_i$  of  $G$ .

**Lemma 3.1.** *There exists a class  $\mathcal{C}(H^2(C))$  of surjective homomorphisms of  $R$ -modules  $\varpi : F \rightarrow H^2(C)$  with all of the following properties:*

- (i)  $F$  is a finitely generated free  $R$ -module of rank  $d$  (for some integer  $d \geq n$ ).
- (ii) There exists an  $R$ -basis  $\underline{b} := \{b_i : 1 \leq i \leq d\}$  of  $F$  with the following two properties:
  - (a) For each integer  $i$  with  $1 \leq i \leq n$  the element  $\pi(\varpi(b_i))$  is an  $R$ -generator of  $\Pi_i$ .

- (b) For each integer  $i$  with  $n < i \leq d$  one has  $\pi(\varpi(b_i)) = 0$ .
- (iii) If  $\tilde{\varpi} : \tilde{F} \rightarrow H^2(C)$  is any other homomorphism in  $\mathcal{C}(H^2(C))$ , then there exists a commutative diagram of  $R$ -modules

$$(9) \quad \begin{array}{ccc} F & \xrightarrow{\varpi} & H^2(C) \\ \iota \downarrow & & \parallel \\ \tilde{F} & \xrightarrow{\tilde{\varpi}} & H^2(C) \end{array}$$

in which  $\iota$  is an isomorphism.

*Proof.* We first choose for each integer  $i$  a projective cover  $\varrho'_{1i} : P_{1i} \rightarrow \Pi_i$  of  $\Pi_i$ . Since each  $\Pi_i$  is a cyclic  $R$ -module, each module  $P_{1i}$  is isomorphic to a direct summand of  $R$ . Setting  $P_1 := \bigoplus_{i=1}^{i=n} P_{1i}$  we thus obtain a projective cover  $\varrho'_1 := \bigoplus_{i=1}^{i=n} \varrho'_{1i}$  of  $\Pi$  and we then choose a lift  $\varrho_1 : P_1 \rightarrow H^2(C)$  of  $\varrho'_1$  through  $\pi$ . We next choose a projective cover  $\varrho_2 : P_2 \rightarrow \ker(\pi)$  of  $\ker(\pi)$ , set  $P := P_1 \oplus P_2 = (\bigoplus_{i=1}^{i=n} P_{1i}) \oplus P_2$  and write  $\varrho : P \rightarrow H^2(C)$  for the homomorphism that is equal to  $\varrho_1$  on  $P_1$  and to  $\varrho_2$  on  $P_2$ . It is straightforward to see that  $\varrho$  is surjective (but is not in general a projective cover of  $H^2(C)$ ).

We claim that for any other set of data  $\{\tilde{\varrho}_{1i}\}_{1 \leq i \leq n}$ ,  $\tilde{P} := \bigoplus_{i=1}^{i=n} \tilde{P}_{1i}$ ,  $\tilde{\varrho}_1 : \tilde{P}_1 \rightarrow \Pi$ ,  $\tilde{\varrho}_2 : \tilde{P}_2 \rightarrow \ker(\pi)$ ,  $\tilde{P} := \tilde{P}_1 \oplus \tilde{P}_2$  and  $\tilde{\varrho} : \tilde{P} \rightarrow H^2(C)$  that is constructed as above, there exists a commutative diagram of  $R$ -modules

$$(10) \quad \begin{array}{ccc} P & \xrightarrow{\varrho} & H^2(C) \\ \iota' \downarrow & & \parallel \\ \tilde{P} & \xrightarrow{\tilde{\varrho}} & H^2(C) \end{array}$$

in which  $\iota'$  is an isomorphism. To show this we first use the property (8) of projective covers to deduce that there is a commutative diagram

$$\begin{array}{ccc} P_2 & \xrightarrow{\varrho_2} & \ker(\pi) \\ \iota'_2 \downarrow & & \parallel \\ \tilde{P}_2 & \xrightarrow{\tilde{\varrho}_2} & \ker(\pi) \end{array}$$

in which  $\iota'_2$  is an isomorphism. We next choose a lift  $\iota'_1 : P_1 \rightarrow \tilde{P}$  of  $\varrho_1$  through the surjection  $\tilde{\varrho} : \tilde{P} \rightarrow H^2(C)$  and write  $\iota' : P \rightarrow \tilde{P}$  for the homomorphism that is equal to  $\iota'_1$  on  $P_1$  and to  $\iota'_2$  on  $P_2$ . It is then clear that  $\iota'$  lies in a commutative diagram of the form (10) and also easy to check (since  $\varrho_1$  and  $\tilde{\varrho}_1$  are projective covers of  $\Pi$ ) that the composite homomorphism  $P_1 \rightarrow \tilde{P} \rightarrow \tilde{P}_1$  induced by  $\iota'_1$  is bijective. This implies that  $\iota'$  is itself an isomorphism and hence gives us the required diagram (10).

We now choose a projective  $R$ -module  $Q_2$  of minimal  $\mathbb{Z}_p$ -rank such that  $F_2 := P_2 \oplus Q_2$ , and hence also  $\tilde{F}_2 := \tilde{P}_2 \oplus Q_2$ , is a free  $R$ -module and for each integer  $i$  a projective  $R$ -module  $Q_{1i}$  such that  $F_{1i} := P_{1i} \oplus Q_{1i}$ , and hence also  $\tilde{F}_{1i} := \tilde{P}_{1i} \oplus Q_{1i}$ , is a free rank one  $R$ -module, and we set  $Q := (\bigoplus_{i=1}^{i=n} Q_{1i}) \oplus Q_2$ , resp.  $\tilde{Q} := (\bigoplus_{i=1}^{i=n} \tilde{Q}_{1i}) \oplus \tilde{Q}_2$ . We also then set  $F := (\bigoplus_{i=1}^{i=n} F_{1i}) \oplus F_2 = P \oplus Q$  and  $\tilde{F} := (\bigoplus_{i=1}^{i=n} \tilde{F}_{1i}) \oplus \tilde{F}_2 = \tilde{P} \oplus \tilde{Q}$

and write  $\varpi : F \rightarrow H^2(C)$ , resp.  $\tilde{\varpi} : \tilde{F} \rightarrow H^2(C)$ , for the surjective homomorphism of  $R$ -modules that is equal to  $\varrho$  on  $P$ , resp. to  $\tilde{\varrho}$  on  $\tilde{P}$  and to the zero map on  $Q$ , resp.  $\tilde{Q}$ . It is then clear that (10) extends to give a commutative diagram of  $R$ -modules of the form (9) in which  $\iota$  is the isomorphism that restricts to give the map  $\iota' : P \rightarrow \tilde{P} \subset \tilde{F}$  on  $P$  and to give the inclusion map  $Q \subset \tilde{F}$  on  $Q$ .

To obtain an  $R$ -basis of  $F$  of the required sort we write  $d$  for the rank of the free  $R$ -module  $F$ , choose for each integer  $i$  a generator  $b_i$  of the free rank one  $R$ -module  $F_{1i}$  and fix an  $R$ -basis  $\{b_i : n < i \leq d\}$  of  $F_2$ . The set  $\{b_i : 1 \leq i \leq d\}$  is then an  $R$ -basis of  $F$  which has the properties described in claim (ii).  $\square$

**3.2.2. Basic complexes.** In the following result we construct an analogue of the notion of ‘basic complex’ that is introduced by Mazur and Rubin in [36, Def. 5.2 and Lem. 5.3] in the special case that  $G$  is abelian. (We remark that the explicit methods used in loc. cit. do not generalise to the non-abelian case and so we have had to use a different approach.) We continue to write  $R$  in place of  $\mathbb{Z}_p[G]$ .

**Proposition 3.2.** *Let  $C$  be an object of  $D^a(R)$ . Then there exists a class  $\mathcal{C}(C)$  of bounded complexes of finitely free  $R$ -modules  $F^\bullet$  with each of the following properties.*

- (i)  $F^\bullet$  has the form  $F \xrightarrow{\phi} F$ , where  $F$  is the domain of a homomorphism  $\varpi$  that belongs to the class  $\mathcal{C}(H^2(C))$  and the first term is placed in degree 1.
- (ii) One has  $H^1(F^\bullet) = \ker(\phi) = H^1(C)$  and  $H^2(F^\bullet) = \text{cok}(\phi) = H^2(C)$ .
- (iii) There exists an isomorphism  $\vartheta : F^\bullet \rightarrow C$  in  $D^p(R)$  such that for both  $i = 1, 2$  the map  $H^i(\vartheta)$  is the identity map (with respect to the identification  $H^i(F^\bullet) = H^i(C)$  given in claim (ii)).
- (iv) If  $\tilde{F}^\bullet$  is any other complex in  $\mathcal{C}(C)$  that is constructed by using a homomorphism  $\tilde{\varpi} : \tilde{F} \rightarrow H^2$  in  $\mathcal{C}(H^2(C))$ , then there exists a commutative diagram of  $R$ -modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(F^\bullet) & \longrightarrow & F & \xrightarrow{\phi} & F & \longrightarrow & H^2(F^\bullet) & \longrightarrow & 0 \\ & & \parallel & & \downarrow \iota^1 & & \downarrow \iota^2 & & \parallel & & \\ 0 & \longrightarrow & H^1(\tilde{F}^\bullet) & \longrightarrow & \tilde{F} & \xrightarrow{\tilde{\phi}} & \tilde{F} & \longrightarrow & H^2(\tilde{F}^\bullet) & \longrightarrow & 0 \end{array}$$

in which both  $\iota^1$  and  $\iota^2$  are isomorphisms.

*Proof.* We set  $H^i := H^i(C)$  for both  $i = 1, 2$ . Since  $C$  is acyclic outside degrees 1 and 2 we can assume without loss of generality that  $C$  has the form  $C^1 \xrightarrow{d} C^2$ . Since  $H^1 = \ker(d)$  and  $H^2 = \text{cok}(d)$  the complex  $C$  thus gives rise to a tautological exact sequence  $0 \rightarrow H^1 \rightarrow C^1 \xrightarrow{d} C^2 \rightarrow H^2 \rightarrow 0$  and hence corresponds to an element  $\epsilon(C)$  of  $\text{YExt}_R^2(H^2, H^1)$ .

We next choose a surjective homomorphism of  $R$ -modules  $\varpi : F \rightarrow H^2$  from the class  $\mathcal{C}(H^2)$  that is constructed in Lemma 3.1 and then consider the following exact commutative diagram of  $R$ -modules

$$(11) \quad \begin{array}{ccccccccc} 0 & \longrightarrow & \ker(d') & \xrightarrow{\subseteq} & F' & \xrightarrow{d'} & F & \xrightarrow{\varpi} & H^2 & \longrightarrow & 0 \\ & & \phi \downarrow & & \phi' \downarrow & & \parallel & & \parallel & & \\ 0 & \longrightarrow & H^1 & \xrightarrow{\eta} & P & \xrightarrow{d''} & F & \xrightarrow{\varpi'} & H^2 & \longrightarrow & 0. \end{array}$$

In this diagram we use the following notation:  $F'$  is a finitely generated free  $R$ -module and  $d'$  is such that  $\text{im}(d') = \ker(\varpi)$ ;  $\phi$  is a homomorphism which represents  $\epsilon(C)$  when the group  $\text{YExt}_R^2(H^2, H^1) \cong \text{Ext}_R^2(H^2, H^1)$  is computed by using the truncated free resolution of  $H^2$  given by the upper row in (11);  $P$  is the module obtained as the push out of  $\phi$  and the inclusion  $\ker(d') \subset F'$  and the homomorphisms  $\eta$ ,  $\phi'$  and  $d''$  are induced by the push-out construction. In particular, our choice of  $\phi$  implies that the lower row of (11) represents  $\epsilon(C)$ . This implies that the complexes  $C$  and  $P \xrightarrow{d''} F$  (in which the first term occurs in degree 1) are isomorphic in  $D(R)$ ; the complex  $P \xrightarrow{d''} F$  therefore belongs to  $D^p(R)$  and since  $F$  is both finitely generated and projective this implies that  $P$  is finitely generated over  $R$  and also cohomologically-trivial as a  $G$ -module. In addition, since  $H^1$  and  $F$  are both free  $\mathbb{Z}_p$ -modules (the former by condition (wa<sub>4</sub>) in the definition of admissible complexes), it follows from the exactness of the lower row of (11) that  $P$  is  $\mathbb{Z}_p$ -free and hence from [1, Th. 8] that  $P$  is a finitely generated projective  $R$ -module. Now, since the  $\mathbb{Q}_p[G]$ -modules  $H_{\mathbb{Q}_p}^1$  and  $H_{\mathbb{Q}_p}^2$  are isomorphic (by condition (wa<sub>2</sub>) and the fact that  $C$  is acyclic outside degrees 1 and 2), the exactness of the lower row of (11) combines with the Krull-Schmidt theorem to imply that the  $\mathbb{Q}_p[G]$ -modules  $P_{\mathbb{Q}_p}$  and  $F_{\mathbb{Q}_p}$  are isomorphic. Since both  $P$  and  $F$  are also projective  $R$ -modules Swan's Theorem [19, Th. 32.1] thus implies that there exists an isomorphism  $\kappa : P \rightarrow F$  of  $R$ -modules. The resulting exact sequence  $0 \rightarrow H^1 \xrightarrow{\kappa \circ \eta} F \xrightarrow{d'' \circ \kappa^{-1}} F \xrightarrow{\varpi'} H^2 \rightarrow 0$  gives a complex  $F^\bullet$  with the properties described in claims (i) and (ii) in which  $\phi = d'' \circ \kappa^{-1}$ . Since the latter sequence represents the Yoneda extension class  $\epsilon(C)$  it is also clear that the property in claim (iii) is satisfied.

To prove claim (iv) we consider the following diagram

$$(12) \quad \begin{array}{ccccccccc} 0 & \longrightarrow & H^1 & \longrightarrow & F & \xrightarrow{\phi} & F & \xrightarrow{\varpi} & H^2 & \longrightarrow & 0 \\ & & \parallel & & \iota' \downarrow & & \downarrow \iota & & \parallel & & \\ 0 & \longrightarrow & H^1 & \longrightarrow & \tilde{F} & \xrightarrow{\tilde{\phi}} & \tilde{F} & \xrightarrow{\tilde{\varpi}} & H^2 & \longrightarrow & 0. \end{array}$$

In this diagram the lower row is constructed as above but with the role of  $\varpi$  replaced by  $\tilde{\varpi}$  and  $\iota$  is the isomorphism of  $R$ -modules constructed in Lemma 3.1(iii). Since both rows of this diagram represent the same element of  $\text{YExt}_R^2(H^2, H^1)$  there is then a homomorphism of  $R$ -modules  $\iota'$  that makes the diagram commute. By an easy application of the Five Lemma it follows that  $\iota'$  is an isomorphism, as required.  $\square$

**3.2.3. The matrices.** We define  $M(C, \pi)$  to be the set of matrix representatives, with respect to the basis  $\underline{b}$  of  $F$  as codomain and a suitably chosen basis of  $F$  as domain, of any of the homomorphisms  $\phi$  that occur in Proposition 3.2. In this subsection we show that any such matrix  $\Phi$  satisfies the conditions of Theorem 2.10(i) and (iv).

We note first that Proposition 3.2(iv) implies that any such matrix is unique up to pre- and post-multiplication by elements of  $\mathrm{GL}_d(R)$ , as required by Theorem 2.10(iv). We note next that for such a matrix  $\Phi$  the first assertion of Theorem 2.10(i) is also clear since  $\Phi_J$  is a representative of the endomorphism  $\phi^J$  of  $F^J$  induced by  $\phi_J$  and the associated complex  $F^J \xrightarrow{\phi^J} F^J$  is isomorphic to  $C_J$  in  $D(\mathbb{Z}_p[G/J])$ . This gives an exact sequence of  $\mathbb{Z}_p[G/J]$ -modules  $F^J \xrightarrow{\phi^J} F^J \rightarrow H^2(C_J) \rightarrow 0$  which in turn implies that  $\phi^J$  is a relation matrix for the module  $H^2(C_J)$ .

To prove the second assertion of claim (i) we note that if  $G$  is a  $p$ -group, then  $\Pi_i = R \otimes_{\mathbb{Z}_p[H_i]} \mathbb{Z}_p$  for each integer  $i$  and so  $\varpi$  induces both an identification  $F_1^G \cong F_{1,G} \cong \Pi_G \cong H_{G,\mathrm{tf}}^2$  and a surjection  $F_2^G \cong F_{2,G} \rightarrow \ker(H_G^2 \rightarrow H_{G,\mathrm{tf}}^2) = H_{G,\mathrm{tor}}^2$ . This implies that  $\mathrm{im}(\phi^G) \subseteq F_2^G$  and hence that  $\Phi_G$  is a block matrix  $(0_{d,n} \mid \Phi')$  where  $\Phi'$  is the matrix of the homomorphism  $\theta$  in the exact sequence  $F^G \xrightarrow{\theta} F_2^G \rightarrow H_{G,\mathrm{tor}}^2 \rightarrow 0$  that is induced by  $\phi^G$ . This proves that  $\Phi$  satisfies the second assertion of claim (i).

**3.2.4. Height pairings.** In this subsection we show that any matrix  $\Phi$  as above has the properties described in Theorem 2.10(ii). We first fix an element  $x$  in  $F$  and write  $\phi(x) = \sum_{i=1}^{i=d} \mu_i b_i$ , with  $\mu_i \in R$  for each  $i$ . Then, since  $\phi(x) \in \ker(\varpi)$ , Lemma 3.1(ii)(b) implies  $0 = \pi(\varpi(x)) = \sum_{i=1}^{i=d} \mu_i \pi(\varpi(b_i)) = \sum_{i=1}^{i=n} \mu_i \pi(\varpi(b_i))$ . From Lemma 3.1(ii)(a) it thus follows that  $\mu_i$  belongs to  $I(\Pi_i)$  for each integer  $i$  with  $1 \leq i \leq n$ . This shows that  $\Phi$  satisfies the first assertion in Theorem 2.10(ii).

We now fix an integer  $i$  with  $r < i \leq n$  and define an algebraic height pairing of the form described in Theorem 2.10(ii). (This construction is motivated by the general formalism of algebraic height pairings introduced by Nekovář in [40, §11].) To do this we set  $N_i := N(H_i)$ ,  $\mathcal{G}_i := G/N_i$ ,  $R_i := \mathbb{Z}_p[\mathcal{G}_i]$ ,  $I_i$  for the two-sided ideal  $\{n-1 : n \in N_i\}$  of  $R$  and  $C_i$  for the complex  $C_{N_i}$ . Then the natural projection homomorphism  $R \rightarrow R_i$  gives rise to short exact sequence  $0 \rightarrow I_i \rightarrow R \rightarrow R_i \rightarrow 0$  and by tensoring this sequence with  $C$  we obtain an exact triangle in  $D(R)$  of the form

$$I_i \otimes_R^{\mathbb{L}} C \rightarrow C \rightarrow C_i \rightarrow I_i \otimes_R^{\mathbb{L}} C[1].$$

Since  $C$  is acyclic in degrees greater than 2 there are identifications  $H^2(I_i \otimes_R^{\mathbb{L}} C) \cong I_i \otimes_R H^2(C)$  and  $H^2(C)_{N_i} \cong H^2(C_i)$ . The cohomology sequence of the above triangle therefore induces a ‘Bockstein homomorphism’ of  $R$ -modules

$$\beta_{C,i} : H^1(C_i) \rightarrow H^2(I_i \otimes_R^{\mathbb{L}} C) \cong I_i \otimes_R H^2(C) \rightarrow I_i/I_i^2 \otimes_R H^2(C_i),$$

where the last arrow is induced by passing to  $N_i$ -coinvariants, and hence also a pairing

$$H^1(C_i) \otimes_R \mathrm{Hom}_{\mathbb{Z}_p}(H^2(C_i), \mathbb{Z}_p) \rightarrow I_i/I_i^2 \cong N_i^{\mathrm{ab}}.$$

where the last map is the isomorphism induced by sending each element  $n-1$  with  $n$  in  $N_i$  to the image of  $n$  in  $N_i^{\mathrm{ab}}$ .

The following result justifies the second assertion of Theorem 2.10(ii). In this result we set  $T_i := \sum_{g \in J} g \in R$  and often identify  $F^{N_i}$  and  $F_{N_i}$  by the map which sends each  $T_i(b_j)$  to the image  $b_{ji}$  of  $b_j$  in  $F_{N_i}$ . We also write  $\rho'_i$  for the projection  $I_i \rightarrow I_i/I_i^2$  and  $\rho_i$  for the composite  $F_{i,N_i} \subset F_{N_i} \xrightarrow{\varpi_{N_i}} H^2(C)_{N_i} = H^2(C_i)$ .

**Lemma 3.3.** *We fix the  $R$ -basis  $\underline{b}$  of  $F$  as codomain and assume that  $\underline{b}'$  is the basis of  $F$  (as domain) that is used when the matrix  $\Phi = (\Phi_{kl})_{1 \leq k, l \leq d}$  represents  $\phi$ . For each  $i$  with  $r < i \leq n$  we set  $F_i := R \cdot b_i$  and write  $\phi_i$  for the element of  $\text{Hom}_R(F^{N_i}, F_{i, N_i})$  that sends each element  $T_i(b'_k)$  to  $\Phi_{ki} b_{ii}$ . Then for each  $x$  in  $H^1(C_i) \subseteq F_{N_i} \cong F^{N_i}$  one has  $\phi_i(x) \in I_i \otimes_R F_{i, N_i}$  and  $\beta_{C, i}(x) = (\rho'_i \otimes_R \rho_i)(\phi_i(x))$ .*

*Proof.* We write  $\pi_i$  for the natural projection  $F \rightarrow F_{i, N_i}$ . Then  $\beta_{C, i}$  is equal to the connecting homomorphism which arises when applying the Snake lemma to the following commutative diagram (in which both rows and the third column are exact and the first column is a complex)

$$\begin{array}{ccccccc}
 & & & & \ker(\phi^{N_i}) & & \\
 & & & & \downarrow & & \\
 0 & \longrightarrow & I_i \otimes_R F & \xrightarrow{\subseteq} & F & \xrightarrow{T_i} & F^{N_i} \longrightarrow 0 \\
 & & \downarrow \text{id} \otimes_{\mathbb{Z}[G]} \phi & & \downarrow \phi & & \downarrow \phi^{N_i} \\
 0 & \longrightarrow & I_i \otimes_R F & \xrightarrow{\subseteq} & F & \xrightarrow{T_i} & F^{N_i} \longrightarrow 0 \\
 & & \downarrow \rho'_i \otimes_R (\rho_i \circ \pi_i) & & & & \\
 & & I_i / I_i^2 \otimes_R H^2(C_i) & & & & 
 \end{array}$$

We may write the given element  $x$  of  $H^1(C_i) = \ker(\phi^{N_i})$  as  $\sum_{s=1}^{s=d} \mu_s T_i(b'_s)$  with  $\mu_s$  in  $R$  for each index  $s$ . Then the commutativity of the above diagram implies the element

$$\sum_{s=1}^{s=d} \mu_s \phi(b'_s) = \sum_{u=1}^{u=d} \left( \sum_{s=1}^{s=d} \mu_s \Phi_{su} \right) \otimes_R b_u$$

belongs to  $I_i \otimes_R F$ , and hence that  $\phi_i(x) = \sum_{s=1}^{s=d} \mu_s \Phi_{si} \otimes_R b_{ii}$  belongs to  $I_i \otimes_R F_{i, N_i}$ , as claimed. An explicit computation of the connecting homomorphism in the above diagram also then shows that

$$\begin{aligned}
 \beta_{C, i}(x) &= (\rho'_i \otimes_R (\rho_i \circ \pi_i)) \left( \sum_{s=1}^{s=d} \mu_s \phi(b'_s) \right) \\
 &= (\rho'_i \otimes_R (\rho_i \circ \pi_i)) \left( \sum_{u=1}^{u=d} \left( \sum_{s=1}^{s=d} \mu_s \Phi_{su} \right) \otimes_R b_u \right) \\
 &= (\rho'_i \otimes_R \rho_i) \left( \sum_{s=1}^{s=d} \mu_s \Phi_{si} \otimes_R b_{ii} \right) \\
 &= (\rho'_i \otimes_R \rho_i)(\phi_i(x)),
 \end{aligned}$$

as claimed.  $\square$

**3.2.5. Semisimplicity.** In this subsection we refine the choice of  $\Phi$  in order to satisfy the condition described in Theorem 2.10(iii). The key observation is provided by the following result.

**Lemma 3.4.** *There exists an  $R$ -basis  $\underline{b}'$  of  $F$  with the following property: if  $\Phi$  is the matrix of the homomorphism  $\phi$  in Proposition 3.2 with respect to  $\underline{b}'$  and  $\underline{b}$  (as bases of  $F$  as domain and codomain respectively), then for every character  $\chi$  in  $\Upsilon_{\text{pr}}$  the subspaces  $\ker(\Phi)_\chi$  and  $\text{im}(\Phi)_\chi$  of  $F_\chi$  are linearly-disjoint.*

*Proof.* We write  $\text{Ir}'(G)$  for the set of irreducible  $\mathbb{Q}_p$ -valued characters of  $G$  and for any  $R$ -module  $M$  and  $\psi$  in  $\text{Ir}'(G)$  we write  $M'_\psi$  for the  $\mathbb{Q}_p[G]$ -module  $e_\psi(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} M)$ . We write  $g(W)$  for the minimal number of generators of a finitely generated  $\mathbb{Q}_p[G]$ -module  $W$ . For natural numbers  $m$  and  $m'$  we also set  $\langle m \rangle := \{a \in \mathbb{Z} : 1 \leq a \leq m\}$  and  $\langle m, m' \rangle := \langle m \rangle \times \langle m' \rangle$  and we order elements of the latter set lexicographically.

We recall the homomorphism  $\lambda_\Pi$  from (5) and note that  $\chi$  belongs to  $\Upsilon_{\text{pr}}$  if and only if  $\text{im}(\phi)_\chi = \ker(\lambda_\Pi \circ \varpi)_\chi$ . Since the homomorphisms  $\phi$ ,  $\varphi$  and  $\lambda_\Pi$  are all defined over  $\mathbb{Z}_p$  it is thus enough to construct an automorphism  $\epsilon$  in  $\text{Aut}_R(F)$  for which

$$(13) \quad F'_\psi = \ker(\phi \circ \epsilon)'_\psi \oplus \text{im}(\phi \circ \epsilon)'_\psi$$

for each  $\psi$  in  $\text{Ir}'(G)$  with  $\text{im}(\phi)'_\psi = \ker(\lambda_\Pi \circ \varpi)'_\psi$ . (The claimed result then follows by taking  $\underline{b}'$  to be the image of  $\underline{b}$  under  $\epsilon^{-1}$ .)

We set  $I := \ker(\phi) \cap \text{im}(\phi)$  and write  $\Upsilon$  for the subset of  $\text{Ir}'(G)$  comprising characters  $\psi$  for which  $\text{im}(\phi)'_\psi = \ker(\lambda_\Pi \circ \varpi)'_\psi$  but  $F'_\psi \neq \ker(\phi)'_\psi \oplus \text{im}(\phi)'_\psi$  (or equivalently  $I'_\psi \neq \{0\}$ ).

For each  $\psi$  in  $\Upsilon$  we write  $e_\psi$  as a sum  $\sum_{i=1}^{i=d_\psi} f_{i,\psi}$  of primitive (mutually orthogonal) idempotents of  $e_\psi \mathbb{Q}_p[G]$ . For each  $\underline{x} \in \langle d, d_\psi \rangle$  we set  $b_{\underline{x},\psi} := f_{x_2,\psi} b_{x_1}$  and  $V_{\underline{x},\psi} := \mathbb{Q}_p[G] \cdot b_{\underline{x},\psi}$ . Then  $F'_\psi = \bigoplus_{\underline{x} \in \langle d, d_\psi \rangle} V_{\underline{x},\psi}$  and  $\text{im}(\phi)'_\psi = \ker(\lambda_\Pi \circ \varpi)'_\psi = \bigoplus_{\underline{x} \in \Sigma_\psi^*} V_{\underline{x},\psi}$  for some subset  $\Sigma_\psi^*$  of  $\langle d, d_\psi \rangle$ . We set  $\Sigma_\psi := \langle d, d_\psi \rangle \setminus \Sigma_\psi^*$  and  $W_\psi := \bigoplus_{\underline{x} \in \Sigma_\psi} V_{\underline{x},\psi}$ , so that  $F'_\psi = W_\psi \oplus \text{im}(\phi)'_\psi$ . We write  $\varrho_\psi$  and  $\varrho_{\underline{x},\psi}$  for each  $\underline{x}$  for the projections  $F'_\psi \rightarrow W_\psi$  and  $F'_\psi \rightarrow V_{\underline{x},\psi}$ .

We next set  $g_\psi := g(I'_\psi)$  and  $Z_\psi := \varrho_\psi(\ker(\phi)'_\psi)$ . Then  $g(Z_\psi) = g(\ker(\phi)'_\psi) - g_\psi = g(W_\psi) - g_\psi$  and so [10, Lem. 6.4.2] (with  $W = W_\psi$  and  $V = V_{\underline{x},\psi}$  for any  $\underline{x} \in \Sigma_\psi$ ) implies there exists a subset  $\Sigma'_\psi$  of  $\Sigma_\psi$  with  $|\Sigma'_\psi| = g_\psi$  and such that the  $\mathbb{Q}_p[G]$ -module  $X_\psi := \bigoplus_{\underline{x} \in \Sigma'_\psi} V_{\underline{x},\psi}$  is a direct complement of  $Z_\psi$  in  $W_\psi$ .

We now choose a minimal set of generators  $\{w_{i,\psi} : i \in \langle g_\psi \rangle\}$  of the  $\mathbb{Q}_p[G]$ -module  $I'_\psi$ . For each  $i$  in  $\langle g_\psi \rangle$  and each  $\underline{x}$  in  $\Sigma_\psi^*$  we then choose an element  $\mu_{i,\underline{x},\psi}$  of  $\mathbb{Q}_p[G]$  such that  $w_{i,\psi} = \sum_{\underline{x} \in \Sigma_\psi^*} \mu_{i,\underline{x},\psi} b_{\underline{x},\psi}$  and consider the associated  $g_\psi \times |\Sigma_\psi^*|$ -matrix  $M = (\mu_{i,\underline{x},\psi})$ , where the rows are indexed by  $i \in \langle g_\psi \rangle$  and the columns by  $\underline{x} \in \Sigma_\psi^*$ . After changing the elements  $w_{i,\psi}$  (using ‘elementary row operations’) if necessary, we can assume  $M$  contains  $g_\psi$  columns which together form an identity matrix. We then fix a subset  $\Sigma_\psi^{*'} of  $\Sigma_\psi^*$  corresponding to a set of columns of  $M$  which together constitute a  $g_\psi \times g_\psi$  identity matrix, a bijection of sets  $\iota_\psi : \Sigma_\psi^{*'} \rightarrow \Sigma'_\psi$  and for each  $\underline{x} \in \Sigma_\psi^{*'}$  an element  $\theta_{\underline{x},\psi}$  of  $\text{Is}_{\mathbb{Q}_p[G]}(V_{\underline{x},\psi}, V_{\iota_\psi(\underline{x}),\psi})$  (such isomorphisms exist since each  $\mathbb{Q}_p[G]f_{x_i,\psi}$  is a minimal left ideal of the simple algebra  $e_\psi \mathbb{Q}_p[G]$ ). We also fix a natural number  $m_{\underline{x},\psi}$  large enough to ensure that  $m_{\underline{x},\psi} \cdot \text{im}(\theta_{\underline{x},\psi} \circ \varrho_{\underline{x},\psi}) \subset F$ . We now define mutually-inverse elements  $\epsilon_{(\psi)}^+$  and  $\epsilon_{(\psi)}^-$  of  $\text{Aut}_R(F)$  by setting$

$$\epsilon_{(\psi)}^\pm := \text{id} \pm \sum_{\underline{y} \in \Sigma_\psi^{*'}} m_{\underline{y},\psi} \theta_{\underline{y},\psi} \circ \varrho_{\underline{y},\psi}$$

(Since  $\varrho_{\underline{y},\psi} \circ \theta_{\underline{y}',\psi} \circ \varrho_{\underline{y}',\psi} = 0$  for any elements  $\underline{y}$  and  $\underline{y}'$  of  $\Sigma_{\psi}^{*'}$  it is clear that  $\epsilon_{(\psi)}^+ \circ \epsilon_{(\psi)}^- = \text{id}_F$ .) We finally define  $\epsilon$  to be the composite (in any order) of the automorphisms  $\epsilon_{(\psi)}^-$  as  $\psi$  varies over  $\Upsilon$  and in the remainder of the proof we verify that this automorphism has the property (13). To do this we fix  $\kappa$  in  $\text{Ir}'(G)$  for which  $\text{im}(\phi)'_{\kappa} = \bigoplus_{\underline{x} \in \Sigma_{\kappa}^*} V_{\underline{x},\kappa}$ . If firstly  $\kappa \notin \Upsilon$ , then  $F'_{\kappa} = \ker(\phi)'_{\kappa} \oplus \text{im}(\phi)'_{\kappa}$  (by definition of  $\Upsilon$ ) and  $e_{\kappa}(\epsilon) = \text{id}_{F'_{\kappa}}$  (because  $e_{\kappa} V_{\underline{x},\chi}$  vanishes for all  $\chi \in \Upsilon$ ). The equality (13) is thus clear.

We henceforth assume that  $\kappa \in \Upsilon$ . We define an automorphism  $\xi := e_{\kappa}(\epsilon) = e_{\kappa}(\epsilon_{(\kappa)}^-)$  of  $F'_{\kappa}$  and note that  $\ker(\phi \circ \epsilon)'_{\kappa} = \xi^{-1}(\ker(\phi)'_{\kappa})$ . For each  $\underline{x}$  in  $\Sigma'_{\kappa}$  we write  $\underline{x}' = (x'_1, x'_2)$  for the element  $\iota_{\kappa}^{-1}(\underline{x})$  of  $\Sigma_{\psi}^{*'}$  and we recall that (by our assumptions on  $M$ ) there is a unique integer  $i$  in  $\langle g_{\kappa} \rangle$  such that  $w_{i,\kappa} = b_{\underline{x}',\kappa}$ . Since  $b_{\underline{x}',\kappa} \in \ker(\varrho_{\underline{y},\kappa})$  for all  $\underline{y} \in \Sigma_{\kappa}^{*'} \setminus \{\underline{x}'\}$  one therefore has

$$\begin{aligned} \xi^{-1}(w_{i,\kappa}) &= e_{\kappa}(\epsilon_{(\kappa)}^+)(b_{\underline{x}',\kappa}) \\ &= b_{\underline{x}',\kappa} + \sum_{\underline{y} \in \Sigma_{\kappa}^{*'}} m_{\underline{y},\kappa} \theta_{\underline{y},\kappa} \circ \varrho_{\underline{y},\kappa}(b_{\underline{x}',\kappa}) \\ &= b_{\underline{x}',\kappa} + m_{\underline{x}',\kappa} \theta_{\underline{x}',\kappa}(b_{\underline{x}',\kappa}) \end{aligned}$$

and so  $m_{\underline{x}',\kappa} \theta_{\underline{x}',\kappa}(b_{\underline{x}',\kappa}) = \varrho_{\kappa}(\xi^{-1}(w_{i,\kappa}))$  belongs to  $\varrho_{\kappa}(\ker(\phi \circ \epsilon)'_{\kappa})$ . Since the  $\mathbb{Q}_p[G]$ -module  $X_{\kappa}$  is generated by the set  $\{m_{\underline{x}',\kappa} \theta_{\underline{x}',\kappa}(b_{\underline{x}',\kappa}) : \underline{x}' \in \Sigma_{\kappa}^{*'}\}$  it follows that  $X_{\kappa} \subseteq \varrho_{\kappa}(\ker(\phi \circ \epsilon)'_{\kappa})$ . But for every  $w \in \ker(\phi)'_{\kappa}$  the definition of  $e_{\kappa}(\epsilon)$  implies that  $\varrho_{\kappa}(\xi^{-1}(w)) - \varrho_{\kappa}(w) \in X_{\kappa}$  and so  $\varrho_{\kappa}(\ker(\phi \circ \epsilon)'_{\kappa}) = \varrho_{\kappa}(\ker(\phi)'_{\kappa}) + X_{\kappa} = Z_{\kappa} + X_{\kappa} = W_{\kappa}$ . Since  $g(W_{\kappa}) = g(\ker(\phi \circ \epsilon)'_{\kappa})$  this implies that  $\ker(\phi \circ \epsilon)'_{\kappa}$  is disjoint from  $\ker(\varrho_{\kappa})'_{\kappa} = \text{im}(\phi)'_{\kappa} = \text{im}(\phi \circ \epsilon)'_{\kappa}$  and hence that (13) is valid, as required.  $\square$

In the rest of this section we assume that  $\Phi$  represents  $\phi$  with respect to the bases specified in Lemma 3.4, or equivalently, that  $\Phi$  represents  $\phi \circ \epsilon$  with respect to the basis  $\underline{b}$  of  $F$  for  $\epsilon$  in  $\text{Aut}_R(F)$  constructed as in the proof of Lemma 3.4. Let  $\epsilon^0$  denote the isomorphism from  $\ker(\phi \circ \epsilon)$  to  $\ker(\phi) = H^1(C)$  given by the restriction of  $\epsilon$ , and  $\epsilon^1$  denote the obvious isomorphism from  $\text{cok}(\phi \circ \epsilon)$  to  $\text{cok}(\phi) = H^2(C)$ . Fix  $\theta \in \text{Hom}_R(H^1(C), H^2(C))$ . We write  $\rho$  for the surjective restriction homomorphism  $\text{Hom}_R(F, \Pi^{\text{pr}}) \rightarrow \text{Hom}_R(\ker(\phi \circ \epsilon), \Pi^{\text{pr}})$  and fix  $\bar{\theta} \in \text{Hom}_R(F, \Pi^{\text{pr}})$  such that  $\rho(\bar{\theta}) = \lambda_{\Pi} \circ \theta \circ \epsilon^0$ . Fix also an  $R$ -section  $\iota_3$  to the surjective homomorphism  $\lambda_{\Pi} \circ \varpi : F \rightarrow \Pi^{\text{pr}}$ . We define the augmented matrix  $\Phi(\theta)$  in  $M_d(R)$  to be the matrix of

$$(14) \quad \iota_3 \circ \bar{\theta} + \phi \circ \epsilon \in \text{Hom}_R(F, F)$$

with respect to the basis  $\underline{b}$  of  $F$ . By Lemma 3.1(ii),  $\Phi(\theta)$  agrees with  $\Phi$  in all but the first  $r$  columns.

The algebra  $\mathbb{Q}_p[G]$  is semisimple and so there are  $\mathbb{Q}_p[G]$ -equivariant sections  $\iota_1$  and  $\iota_2$  to the surjections  $F_{\mathbb{Q}_p} \rightarrow \text{im}(\phi \circ \epsilon)_{\mathbb{Q}_p}$  and  $F_{\mathbb{Q}_p} \rightarrow H^2(C)_{\mathbb{Q}_p} \cong \text{cok}(\phi \circ \epsilon)_{\mathbb{Q}_p}$  that are induced by  $\phi \circ \epsilon$  and  $\epsilon^1 \circ \varpi$  respectively. If we let  $E$  denote either  $\mathbb{Q}_p$  or  $\mathbb{C}_p$ , this induces a direct sum decomposition of  $E[G]$ -modules

$$F_E = \ker(\phi \circ \epsilon)_E \oplus (E \otimes_{\mathbb{Q}_p} \iota_1)(\text{im}(\phi \circ \epsilon)_E)$$

and so for  $\tau$  in  $\text{Hom}_{E[G]}(H^1(C)_E, H^2(C)_E)$  there is a unique  $\langle \tau, \phi \circ \epsilon, \iota_1, \iota_2 \rangle$  in  $\text{Hom}_{E[G]}(F_E, F_E)$  that is equal to  $(E \otimes_{\mathbb{Q}_p} \iota_2) \circ (\epsilon^1)_E^{-1} \circ \tau \circ \epsilon_E^0$  on  $\ker(\phi \circ \epsilon)_E$  and to  $(\phi \circ \epsilon)_E$  on  $(E \otimes_{\mathbb{Q}_p} \iota_1)(\text{im}(\phi \circ \epsilon)_E)$ .

**Lemma 3.5.** *Fix  $t$  in  $\text{Is}_{\mathbb{C}_p[G]}(H^1(C)_{\mathbb{C}_p}, H^2(C)_{\mathbb{C}_p})$  and a characteristic element  $\mathcal{L}_t$  for the pair  $(C, t)$ . Then for any choice of sections  $\iota_1$  and  $\iota_2$ , the endomorphism  $\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle$  is invertible and, furthermore, there exists an element  $u_{\mathcal{L}_t}$  of  $\text{nr}_{\mathbb{Q}_p[G]}(R^\times)$  with  $\mathcal{L}_t = u_{\mathcal{L}_t} \text{nr}_{\mathbb{C}_p[G]}(\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle)$ .*

*Proof.* The definition of  $\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle$  implies that  $\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle((\mathbb{C}_p \otimes_{\mathbb{Q}_p} \iota_1)(\text{im}(\phi \circ \epsilon)_{\mathbb{C}_p})) = \text{im}(\phi \circ \epsilon)_{\mathbb{C}_p}$  and  $\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle(\ker(\phi \circ \epsilon)_{\mathbb{C}_p}) = (\mathbb{C}_p \otimes_{\mathbb{Q}_p} \iota_2)(\text{cok}(\phi \circ \epsilon)_{\mathbb{C}_p})$ . Since  $F_{\mathbb{C}_p}$  is equal to the direct sum of  $\text{im}(\phi \circ \epsilon)_{\mathbb{C}_p}$  and  $(\mathbb{C}_p \otimes_{\mathbb{Q}_p} \iota_2)(\text{cok}(\phi \circ \epsilon)_{\mathbb{C}_p})$  one therefore has  $\text{im}(\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle) = F_{\mathbb{C}_p}$  and so  $\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle$  is invertible.

After identifying  $F$  with  $R^d$  and recalling the notation of §1.3, we have by commutativity of the diagram (2) that  $\partial_{R, \mathbb{C}_p}^1(\iota_{\mathbb{C}_p}(\text{nr}_{\mathbb{Q}_p[G]}^{-1}(\mathcal{L}_t))) = \iota'_{\mathbb{C}_p}(\partial_{R, \mathbb{Q}_p}^1(\text{nr}_{\mathbb{Q}_p[G]}^{-1}(\mathcal{L}_t))) = \chi^{\text{ref}}(C, t) = \partial_{R, \mathbb{C}_p}^1([\mathbb{C}_p[G], \langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle])$  (independently of our choices of sections  $\iota_1$  and  $\iota_2$ ) and hence, by the exactness of the bottom row of the diagram (2), that  $\iota_{\mathbb{C}_p}(\text{nr}_{\mathbb{Q}_p[G]}^{-1}(\mathcal{L}_t)) - [\mathbb{C}_p[G], \langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle] \in \ker(\partial_{R, \mathbb{C}_p}^1) = \text{im}(\partial_{R, \mathbb{C}_p}^2)$ , so that  $\mathcal{L}_t \cdot \text{nr}_{\mathbb{C}_p[G]}(\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle)^{-1} \in \text{nr}_{\mathbb{C}_p[G]}(\text{im}(\partial_{R, \mathbb{C}_p}^2))$ . Since the natural map  $\text{GL}_d(R) \rightarrow K_1(R)$  is surjective (by [19, (40.41), (40.42)]), there is a matrix  $U_{\mathcal{L}_t}$  in  $\text{GL}_d(R)$  such that  $\mathcal{L}_t = \text{nr}_{\mathbb{Q}_p[G]}(U_{\mathcal{L}_t}) \text{nr}_{\mathbb{C}_p[G]}(\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle)$ . Setting  $u_{\mathcal{L}_t} := \text{nr}_{\mathbb{Q}_p[G]}(U_{\mathcal{L}_t})$  completes the proof of the lemma.  $\square$

Comparing now the explicit definitions of  $\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle$  and  $\langle \theta_{\mathbb{C}_p}, \phi \circ \epsilon, \iota_1, \iota_2 \rangle$  one finds that  $\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle^{-1} \circ \langle \theta_{\mathbb{C}_p}, \phi \circ \epsilon, \iota_1, \iota_2 \rangle$  is the identity on  $(\mathbb{C}_p \otimes_{\mathbb{Q}_p} \iota_1)(\text{im}(\phi \circ \epsilon)_{\mathbb{C}_p})$  and equal to  $(\epsilon^0)_{\mathbb{C}_p}^{-1} \circ t^{-1} \circ \theta_{\mathbb{C}_p} \circ \epsilon_{\mathbb{C}_p}^0$  on  $\ker(\phi \circ \epsilon)_{\mathbb{C}_p}$ . This fact combines with Lemma 3.5 to imply that

$$\begin{aligned} \mathcal{L}_t R_t(\theta) &= u_{\mathcal{L}_t} \text{nr}_{\mathbb{C}_p[G]}(\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle) \text{nr}_{\mathbb{C}_p[G]}((\epsilon^0)_{\mathbb{C}_p}^{-1} \circ t^{-1} \circ \theta_{\mathbb{C}_p} \circ \epsilon_{\mathbb{C}_p}^0) \\ &= u_{\mathcal{L}_t} \text{nr}_{\mathbb{C}_p[G]}(\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle) \text{nr}_{\mathbb{C}_p[G]}(\langle t, \phi \circ \epsilon, \iota_1, \iota_2 \rangle^{-1} \circ \langle \theta_{\mathbb{C}_p}, \phi \circ \epsilon, \iota_1, \iota_2 \rangle) \\ &= u_{\mathcal{L}_t} \text{nr}_{\mathbb{Q}_p[G]}(\langle \theta_{\mathbb{Q}_p}, \phi \circ \epsilon, \iota_1, \iota_2 \rangle). \end{aligned}$$

The proof of Theorem 2.10(iii) will hence be completed if we prove the following:

**Lemma 3.6.**  $e_{\text{pr}} \text{nr}_{\mathbb{Q}_p[G]}(\langle \theta_{\mathbb{Q}_p}, \phi \circ \epsilon, \iota_1, \iota_2 \rangle) = \text{nr}_{\mathbb{Q}_p[G]}(\Phi(\theta))$ .

*Proof.* It suffices to prove that  $e_\chi e_{\text{pr}} \text{nr}_{\mathbb{Q}_p[G]}(\langle \theta_{\mathbb{Q}_p}, \phi \circ \epsilon, \iota_1, \iota_2 \rangle) = e_\chi \text{nr}_{\mathbb{Q}_p[G]}((\iota_3 \circ \bar{\theta} + \phi \circ \epsilon)_{\mathbb{Q}_p})$  for all  $\chi \in \text{Ir}_p(G)$ . If  $\chi$  does not belong to  $\Upsilon_{\text{pr}}$  then  $e_\chi e_{\text{pr}} = 0$  and so we must show  $(\iota_3 \circ \bar{\theta} + \phi \circ \epsilon)_\chi$  is singular. But in this case the inclusion  $\text{im}(\phi)_\chi \subset \ker(\lambda_\Pi \circ \varpi)_\chi$  is strict and so  $\dim_{\mathbb{C}_p}(\text{im}((\iota_3 \circ \bar{\theta} + \phi \circ \epsilon)_\chi)) \leq \dim_{\mathbb{C}_p}(\text{im}(\iota_3)_\chi) + \dim_{\mathbb{C}_p}(\text{im}(\phi)_\chi) < \dim_{\mathbb{C}_p}(F_\chi) - \dim_{\mathbb{C}_p}(\ker(\lambda_\Pi \circ \varpi)_\chi) + \dim_{\mathbb{C}_p}(\ker(\lambda_\Pi \circ \varpi)_\chi) = \dim_{\mathbb{C}_p}(F_\chi)$  and hence  $(\iota_3 \circ \bar{\theta} + \phi \circ \epsilon)_\chi$  is not surjective, as required.

In the rest of the argument we fix  $\chi \in \Upsilon_{\text{pr}}$ . In this case  $e_\chi e_{\text{pr}} = e_\chi$  and the map  $\lambda_{\Pi, \chi}$  is bijective. Since  $\text{nr}_{\mathbb{Q}_p[G]}(\langle \theta_{\mathbb{Q}_p}, \phi \circ \epsilon, \iota_1, \iota_2 \rangle)$  is independent of the choice of sections  $\iota_1$  and  $\iota_2$ , we assume henceforth that  $\iota_2$  is chosen so that  $\iota_{2, \chi} = \iota_{3, \chi} \circ \lambda_{\Pi, \chi} \circ \epsilon_\chi^1$ . The endomorphism  $\langle \theta_{\mathbb{Q}_p}, \phi \circ \epsilon, \iota_1, \iota_2 \rangle_\chi$  is then equal to  $\xi_\chi$  with

$$(15) \quad \xi := (\iota_3 \circ \bar{\theta})_{\mathbb{Q}_p} \circ \widehat{\iota}_1 + (\phi \circ \epsilon)_{\mathbb{Q}_p} \in \text{Hom}_{\mathbb{Q}_p[G]}(F_{\mathbb{Q}_p}, F_{\mathbb{Q}_p}),$$

where we write  $\widehat{\iota}_1$  for the homomorphism  $F_{\mathbb{Q}_p} \rightarrow \ker(\phi \circ \epsilon)_{\mathbb{Q}_p}$  that is induced by the decomposition  $F_{\mathbb{Q}_p} = \ker(\phi \circ \epsilon)_{\mathbb{Q}_p} \oplus \iota_1(\text{im}(\phi \circ \epsilon)_{\mathbb{Q}_p})$ . By Lemma 3.4, we have that  $F_\chi = \ker(\phi \circ \epsilon)_\chi \oplus \text{im}(\phi \circ \epsilon)_\chi$  and so we obtain an ordered  $\mathbb{C}_p$ -basis  $\mathfrak{B}$  of  $F_\chi$  by

concatenating ordered  $\mathbb{C}_p$ -bases  $\mathfrak{B}_1$  of  $\ker(\phi \circ \epsilon)_\chi$  and  $\mathfrak{B}_2$  of  $\text{im}(\phi \circ \epsilon)_\chi$  (in this order). This also implies that the restriction  $(\phi \circ \epsilon)'_\chi : \text{im}(\phi \circ \epsilon)_\chi \rightarrow \text{im}(\phi \circ \epsilon)_\chi$  of  $(\phi \circ \epsilon)_\chi$  is bijective and so we may assume that the section  $\iota_1$  is chosen so that  $\iota_{1,\chi} = ((\phi \circ \epsilon)'_\chi)^{-1}$ . The direct sum decomposition  $F_\chi = \iota_{2,\chi}(\text{cok}(\phi \circ \epsilon)_\chi) \oplus \text{im}(\phi \circ \epsilon)_\chi$  also shows that we obtain an ordered  $\mathbb{C}_p$ -basis  $\mathfrak{B}'$  of  $F_\chi$  by concatenating an ordered  $\mathbb{C}_p$ -basis  $\mathfrak{B}'_1$  of  $\iota_{2,\chi}(\text{cok}(\phi \circ \epsilon)_\chi)$  with the basis  $\mathfrak{B}_2$  of  $\text{im}(\phi \circ \epsilon)_\chi$ . Now, using the above choice of  $\iota_1$ , the matrices with respect to the bases  $\mathfrak{B}$  and  $\mathfrak{B}'$  of the endomorphisms  $(\iota_3 \circ \bar{\theta} + \phi \circ \epsilon)_\chi$  and  $\xi_\chi$  are block matrices of the form

$$\left( \begin{array}{c|c} A_\chi & 0 \\ \hline C_\chi & B_\chi \end{array} \right), \text{ resp. } \left( \begin{array}{c|c} A_\chi & 0 \\ \hline 0 & B_\chi \end{array} \right)$$

where  $A_\chi$  is the matrix of  $\iota_{2,\chi} \circ (\epsilon^1)_\chi^{-1} \circ \theta_\chi \circ \epsilon_\chi^0 \in \text{Hom}_{\mathbb{C}_p}(\ker(\phi \circ \epsilon)_\chi, \iota_{2,\chi}(\text{cok}(\phi \circ \epsilon)_\chi))$  with respect to the bases  $\mathfrak{B}_1$  and  $\mathfrak{B}'_1$  and  $B_\chi$  is the matrix of  $(\phi \circ \epsilon)'_\chi \in \text{Hom}_{\mathbb{C}_p}(\text{im}(\phi \circ \epsilon)_\chi, \text{im}(\phi \circ \epsilon)_\chi)$  with respect to the basis  $\mathfrak{B}_2$ . It is therefore clear that, computing with respect to the bases  $\mathfrak{B}$  and  $\mathfrak{B}'$ , the determinants of  $(\iota_3 \circ \bar{\theta} + \phi \circ \epsilon)_\chi$  and  $\xi_\chi$  are both equal to  $\det(A_\chi)\det(B_\chi)$ , and in particular are equal to each other, as required.  $\square$

3.2.6. *The proof of Corollary 3.2.6.* Let  $\varpi$  belong to  $\mathcal{C}(H^2(C))$  and let  $\underline{b}$  be an  $R$ -basis of  $F$  constructed as in Lemma 3.1 (we continue to write  $R$  in place of  $\mathbb{Z}_p[G]$ ). Let  $F^\bullet$  belong to  $\mathcal{C}(C)$ . Let  $\Phi$  belong to  $M(C, \pi)$  and let  $\phi'$  be an  $R$ -endomorphism of  $F$  which is represented by  $\Phi$  with respect to  $\underline{b}$ , and for any  $\theta$  in  $\text{Hom}_R(H^1(C), H^2(C))$  let  $\phi'(\theta)$  be an  $R$ -endomorphism of  $F$  which is represented by  $\Phi(\theta)$  with respect to  $\underline{b}$ . It is clear that  $H^2(C)_{\text{tor}}$  is a submodule of  $\ker(\lambda_\Pi)$  because  $\Pi^{\text{pr}}$  has no  $\mathbb{Z}_p$ -torsion and that  $\ker(\lambda_\Pi)$  surjects onto  $\Pi^{\text{pr}}$  via the restriction of  $\pi$ . By combining [41, Th. 4.2] and Theorem 2.10 (iii), we know that  $aR_t(\theta)\mathcal{L}_t e_{\text{pr}}$  belongs to  $a_G(\text{cok}(\phi'(\theta)))$  for any  $a, t, \mathcal{L}_t$  and  $\theta$ . It will hence be enough to prove that  $\text{cok}(\phi'(\theta))$  surjects onto  $\ker(\lambda_\Pi)$  for any such  $\theta$ .

We have an exact commutative diagram of the form

$$\begin{array}{ccccccc} F & \xrightarrow{\phi'(\theta)} & F & \longrightarrow & \text{cok}(\phi'(\theta)) & \longrightarrow & 0 \\ \parallel & & \alpha \downarrow & & \alpha' \downarrow & & \\ F & \xrightarrow{\phi'} & F & \xrightarrow{\pi} & H^2(C) & \longrightarrow & 0 \\ & & \lambda_{\Pi \circ \varpi} \downarrow & & \lambda_\Pi \downarrow & & \\ & & \Pi^{\text{pr}} & \xlongequal{\quad} & \Pi^{\text{pr}} & & \end{array}$$

In this diagram  $\alpha$  is the endomorphism of  $F$  which satisfies  $\alpha(b_i) = 0$  for  $i \in \langle r \rangle$  and  $\alpha(b_i) = b_i$  for  $i \in \langle d \rangle \setminus \langle r \rangle$ , and the first upper square commutes because  $\Phi(\theta)$  agrees with  $\Phi$  in all but the first  $r$  columns and  $\text{im}(\phi) = \ker(\varpi) \subseteq \bigoplus_{i=r+1}^{i=d} \mathbb{Z}_p[G] \cdot b_i$ . We then define  $\alpha'$  to be the unique homomorphism which makes the second upper square commute. The central column is exact by our choice of  $\varpi$  and  $\underline{b}$ , and the commutativity of the diagram then implies that the final column is exact and hence that there is a surjection from  $\text{cok}(\phi'(\theta))$  to  $\ker(\lambda_\Pi)$ , as required.

**3.3. The proof of Theorem 2.17.** Throughout this section we assume that  $p$  is odd and we set  $R := \mathbb{Z}_p[G]$ . Our construction of the family  $M(C, \delta)$  is a natural generalisation of the construction (in the setting of  $\mathbb{Z}_p$ -power extensions of number fields) of ‘organising matrices’ by Mazur and Rubin in [36] and for this reason we will be rather brief with some arguments.

**3.3.1. Preliminary results.** We start by recording a useful technical result.

**Lemma 3.7.** *For both  $i = 1, 2$  we suppose given a complex  $C_i$  in  $D^{\mathbb{P}}(R)$  of the form  $C_i^1 \xrightarrow{d_1} C_i^2$ , where the first term is placed in degree 1 and the tautological homomorphism  $\pi_i : C_i^2 \rightarrow H^2(C_i)$  is a projective cover of the  $R$ -module  $H^2(C_i)$ . Then any isomorphism  $\tau : C \cong C'$  in  $D^{\mathbb{P}}(R)$  can be realised as a morphism of complexes*

$$\begin{array}{ccc} C_1^1 & \xrightarrow{d_1} & C_1^2 \\ \kappa^1 \downarrow & & \downarrow \kappa^2 \\ C_2^1 & \xrightarrow{d_1} & C_2^2 \end{array}$$

in which both  $\kappa^1$  and  $\kappa^2$  are isomorphisms.

*Proof.* By a general result, any isomorphism  $C \cong C'$  in  $D^{\mathbb{P}}(R)$  can be realised as a morphism of complexes  $\kappa : C \rightarrow C'$  and so it suffices to show that in any such case the homomorphisms  $\kappa^1$  and  $\kappa^2$  are both bijective. To show this we consider the following exact commutative diagram

$$(16) \quad \begin{array}{ccccccccc} 0 & \longrightarrow & H^1(C_1) & \xrightarrow{\subseteq} & C_1^1 & \xrightarrow{d_1} & C_1^2 & \xrightarrow{\pi_1} & H^2(C_1) & \longrightarrow & 0 \\ & & H^1(\kappa) \downarrow & & \kappa^1 \downarrow & & \downarrow \kappa^2 & & \downarrow H^2(\kappa) & & \\ 0 & \longrightarrow & H^1(C_2) & \xrightarrow{\subseteq} & C_2^1 & \xrightarrow{d_2} & C_2^2 & \xrightarrow{\pi_2} & H^2(C_2) & \longrightarrow & 0. \end{array}$$

Since  $H^2(\kappa)$  is bijective, both  $\pi_1$  and  $\pi_2$  are projective covers and the third square commutes, Nakayama’s Lemma implies that  $\kappa^2$  is bijective. Since  $H^1(\kappa)$  is bijective and the diagram commutes an application of the Five Lemma implies that  $\kappa^1$  is also bijective, as required.  $\square$

For the remainder of this subsection we fix a pair  $(C, \delta)$  as in §1.1.3 and set  $\epsilon_\delta := 1$ , resp.  $\epsilon_\delta := -1$ , if  $(C, \delta)$  is symmetric, resp. skew-symmetric.

**Proposition 3.8.** *There exists a finitely generated projective  $R$ -module  $\tilde{P}$  and a homomorphism of  $R$ -modules  $h : \tilde{P} \rightarrow \tilde{P}^*$  which together satisfy all of the following properties.*

*We write  $\eta_{\tilde{P}} : \tilde{P} \rightarrow (\tilde{P}^*)^*$  for the natural identification and  $\tilde{P}^\bullet$  for the complex  $\tilde{P} \xrightarrow{h} \tilde{P}^*$ , where the first term is placed in degree 1.*

- (i) *One has  $\text{im}(h) \subseteq J(R) \cdot \tilde{P}^*$  and the homomorphism  $h^* : \tilde{P} \xrightarrow{\eta} (\tilde{P}^*)^* \rightarrow \tilde{P}^*$  that is induced by the  $\mathbb{Z}_p$ -linear dual of  $h$  is equal to  $\epsilon_\delta \cdot h$ .*

- (ii) *There exists an isomorphism  $\tilde{P}^\bullet \rightarrow C$  in  $D^p(R)$ , with respect to which the diagram (1) corresponds to the obvious diagram*

$$\begin{array}{ccc} \tilde{P} & \xrightarrow{h} & \tilde{P}^* \\ \eta \downarrow & & \parallel \\ (\tilde{P}^*)^* & \xrightarrow{\epsilon_\delta \cdot h^*} & \tilde{P}^* \end{array}$$

- (iii) *Let  $(C', \delta')$  be a symmetric, resp. skew-symmetric, pairing that is isomorphic to  $(C, \delta)$  (in the sense described in §1.1.3). Let  $\tilde{P}'^\bullet$  be a complex  $\tilde{P}' \xrightarrow{h'} \tilde{P}'^*$  that is related to  $(C', \delta')$  in the same way that  $\tilde{P}^\bullet$  is related to  $(C, \delta)$ . Then there exists a commutative diagram of  $R$ -modules*

$$\begin{array}{ccc} \tilde{P} & \xrightarrow{h} & \tilde{P}^* \\ \alpha \downarrow & & \downarrow (\alpha^*)^{-1} \\ \tilde{P}' & \xrightarrow{h'} & \tilde{P}'^* \end{array}$$

*in which  $\alpha$ , and hence also  $(\alpha^*)^{-1}$ , is an isomorphism.*

*Proof.* We first fix a projective cover  $\pi : P \rightarrow H^2(C)$  of the  $R$ -module  $H^2(C)$ . Then the same construction as in the proof of Proposition 3.2(i) shows that there is an exact sequence of  $R$ -modules

$$0 \rightarrow H^1(C) \xrightarrow{\iota} P' \xrightarrow{d} P \xrightarrow{\pi} H^2(C) \rightarrow 0$$

with the following property:  $P'$  is finitely generated and projective and writing  $P^\bullet$  for the complex  $P' \xrightarrow{d} P$ , where the first term is placed in degree 1 and the cohomology is identified with  $H^1(C)$  and  $H^2(C)$  using the maps  $\iota$  and  $\pi$  in the above sequence, there exists an isomorphism  $\vartheta : P^\bullet \rightarrow C$  in  $D(R)$  such that  $H^i(\vartheta)$  is the identity map on  $H^i(C)$  for both  $i = 1, 2$ . The induced isomorphism  $(\vartheta^*)^{-1} : P^{\bullet,*} \cong C^*$  then gives an exact sequence

$$0 \rightarrow H^1(C^*[-3]) \rightarrow P^* \xrightarrow{d^*} P'^* \xrightarrow{\pi'} H^2(C^*[-3]) \rightarrow 0$$

in which  $\text{im}(d^*) \subseteq J(R) \cdot P'^*$  (since  $\text{im}(d) \subseteq J(R) \cdot P$  as  $\pi$  is a projective cover) and so  $\pi'$  is a projective cover of  $H^2(C^*)$ .

Applying Lemma 3.7 with  $C_1 = P^\bullet$ ,  $C_2 = P^{\bullet,*}$  and  $\tau = \vartheta^* \circ \delta \circ \vartheta$  we deduce that  $\tau$  is induced by a commutative diagram

$$\begin{array}{ccc} P' & \xrightarrow{d} & P \\ \alpha \downarrow & & \alpha' \downarrow \\ P^* & \xrightarrow{d^*} & P'^* \end{array}$$

in which both  $\alpha$  and  $\alpha'$  are bijective. This diagram is an appropriate replacement for the first commutative square that occurs in the proof of [36, Prop. 6.5]. Noting that any two morphisms of complexes of  $R$ -modules  $P^\bullet \rightarrow P^{\bullet,*}[-3]$  that induce the same morphism in  $D^p(R)$  are homotopic, and that  $p$  is assumed to be odd, one can then

simply mimic the remainder of the proof of [36, Prop. 6.5] to deduce claims (i) and (ii) (and with  $\tilde{P} = P'$ ).

Regarding claim (iii) we first note that Lemma 3.7 combines with claim (ii) to imply that any isomorphism  $C \cong C'$  can be realised as a morphism of complexes

$$\begin{array}{ccc} \tilde{P} & \xrightarrow{h} & \tilde{P}^* \\ \alpha \downarrow & & \beta \downarrow \\ \tilde{P}' & \xrightarrow{h'} & \tilde{P}'^* \end{array}$$

in which both  $\alpha$  and  $\beta$  are bijective. This diagram is the appropriate generalisation of the first diagram that occurs in the proof of [36, Prop. 6.6]. Claim (iii) can then be shown to be a consequence of this diagram by using the same argument as in loc. cit.  $\square$

**3.3.2. The proof.** Returning to the proof of Theorem 2.17 we fix a representative of  $C$  of the form  $\tilde{P}^\bullet$  described in Proposition 3.8. We then choose a finitely generated projective  $R$ -module  $Q$  that is of minimal  $\mathbb{Z}_p$ -rank and such that  $F := \tilde{P} \oplus Q$ , and hence also  $F^* = \tilde{P}^* \oplus Q^*$ , is a free  $R$ -module, of rank  $d$  say. The Krull-Schmidt implies that these conditions specify  $Q$  up to isomorphism and, since Swan's Theorem implies that the  $R$ -modules  $\tilde{P}$  and  $\tilde{P}^*$  are isomorphic (by the same argument as in Proposition 3.2), also imply that  $Q$  is isomorphic to  $Q^*$ . Further, if  $G$  is a  $p$ -group, then [19, Th. 32.13] implies that  $\tilde{P}$  is itself a free  $R$ -module so one has  $Q = \{0\}$  and  $F = \tilde{P}$ .

Next we note that the diagrams in Proposition 3.8(ii) and (iii) obviously extend to give commutative diagrams

$$(17) \quad \begin{array}{ccc} F & \xrightarrow{h \oplus 0} & F^* \\ \eta_F \downarrow & & \parallel \\ (F^*)^* & \xrightarrow{\epsilon_\delta (h \oplus 0)^*} & F^* \end{array} \quad \begin{array}{ccc} F & \xrightarrow{h \oplus 0} & F^* \\ \alpha \oplus \text{id}_Q \downarrow & & \downarrow (\alpha \oplus \text{id}_Q)^{*, -1} \\ F' & \xrightarrow{h' \oplus 0} & F'^* \end{array}$$

with  $F' := \tilde{P}' \oplus Q$ . Thus if we fix an  $R$ -basis of  $F$  and compute the matrix representative  $\Phi$  of  $h \oplus 0$  with respect to this basis and the corresponding dual basis of  $F^*$ , then the first of these diagrams implies that  $\Phi$  is symmetric, resp. skew-symmetric, whilst the second implies that any other matrix  $\Phi'$  constructed in this way will satisfy  $\Phi' = U\Phi U^{\text{tr}}$  for some  $U$  in  $\text{GL}_d(R)$ . This proves Theorem 2.17(i)(a) and the analogous claim in Theorem 2.17(ii).

The claim in Theorem 2.17(i)(b) and the analogous claim in (ii) is then proved by the same argument used in the proof of Theorem 2.10(i) that is given in §3.2.3.

In order to prove the claim in Theorem 2.17(i)(c) and the analogous claim in (ii), we fix a normal subgroup  $J$  of  $G$  and set  $C^J := \text{RHom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G/J], C)$ . Then, since each term of  $C$  is perfect, there is a natural isomorphism in  $D^{\text{p}}(\mathbb{Z}_p[G/J])$  between  $C_J$ , resp.  $C^J$ , and the complex which in each degree  $i$  is equal to  $(C^i)_J$ , resp.  $(C^i)^J$ , and in which the differentials are induced by those of  $C$ . For this reason, the action of  $\sum_{g \in J} g$  on each module  $C^i$  induces an isomorphism in  $D^{\text{p}}(\mathbb{Z}_p[G/J])$  from  $C_J$  to  $C^J$ . The homomorphism  $H^2(\text{RHom}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G/J], \delta))$  therefore induces an isomorphism of  $\mathbb{Z}_p[G/J]$ -modules

$$\begin{aligned} H^2(C_J)_{\text{tor}} &\cong H^2(C^J)_{\text{tor}} \cong H^2(C^*[-3]^J)_{\text{tor}} \cong H^2((C_J)^*[-3])_{\text{tor}} \\ &\cong \text{Hom}_{\mathbb{Z}_p}(H^2(C_J)_{\text{tor}}, \mathbb{Q}_p/\mathbb{Z}_p) \end{aligned}$$

where the last isomorphism is induced by the universal coefficient spectral sequence (cf. §1.1.2), and hence also a non-degenerate pairing

$$(18) \quad H^2(C_J)_{\text{tor}} \times H^2(C_J)_{\text{tor}} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

We now show that this pairing is also induced by an explicit non-degenerate symmetric, resp. skew-symmetric,  $G/J$ -invariant pairing

$$\rho_J : \text{cok}(\Phi_J)_{\text{tor}} \times \text{cok}(\Phi_J^{\text{tr}})_{\text{tor}} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

To define  $\rho_J$  we fix  $(x, y) \in \text{cok}(\Phi_J)_{\text{tor}} \times \text{cok}(\Phi_J^{\text{tr}})_{\text{tor}} = \text{cok}(h_J)_{\text{tor}} \times \text{cok}(h_J^*)_{\text{tor}}$ . Then there exist elements  $a \in \mathbb{Z}_p$ ,  $\alpha \in F_J^*$  and  $\alpha' \in F_J$  such that  $ax = 0$ , the class of  $\alpha$  in  $\text{cok}(h_J)$  equals  $x$  and  $h_J(\alpha') = a\alpha$ . Analogously, the first commutative diagram in (17) implies that there exist elements  $b \in \mathbb{Z}_p$ ,  $\beta \in F_J^*$  and  $\beta' \in F_J$  such that  $by = 0$ , the class of  $\beta$  in  $\text{cok}(h_J^*)$  equals  $y$  and  $h_J^*((\eta_F)_J(\alpha')) = b\beta$ . We then define

$$\rho_J(x, y) := (ab)^{-1}h_J(\alpha')(\beta') \pmod{\mathbb{Z}_p}.$$

The element  $\rho_J(x, y)$  of  $\mathbb{Q}_p/\mathbb{Z}_p$  is then independent of the choices of  $a, b, \alpha'$  and  $\beta'$  and the first commutative diagram in (17) implies that  $\rho_J$  is symmetric, resp. skew-symmetric. It is also straightforward to check that  $\rho_J$  induces the pairing (18).

#### 4. TATE MOTIVES

In this section we apply the theory of organising matrices in the setting of §1.2.1. For any Galois extension of fields  $F/E$  we set  $G_{F/E} := \text{Gal}(F/E)$ . We also set  $G_k := G_{k^c/k}$  and recall that  $G_{k,\Sigma}$  denotes the Galois group over  $k$  of the maximal extension of  $k$  inside  $k^c$  that is unramified outside  $\Sigma$ .

**4.1. The general set up.** Let  $M$  be a motive over  $k$  and  $F$  a finite Galois extension of  $k$  inside  $k^c$ . We fix an odd prime  $p$  and a full  $G_k$ -stable sublattice  $T$  in the  $p$ -adic realisation  $V$  of  $M$ . We also fix a finite set of places  $\Sigma$  of  $k$  containing all archimedean places, all which ramify in  $F/k$ , all at which  $M$  has bad reduction and all above  $p$ . Then  $T_F$  is an étale sheaf of free  $\mathbb{Z}_p[G]$ -modules on  $\text{Spec}(\mathcal{O}_{k,\Sigma})$  and, as in §1.2.1, we obtain an object of  $D^{\text{wa}}(\mathbb{Z}_p[G])$  by setting  $C(T_F) := R\Gamma_c(\mathcal{O}_{k,\Sigma}, T_F)$ . If we regard  $M_F := h^0(\text{Spec}(F)) \otimes_{h^0(\text{Spec}(k))} M$  as a motive defined over  $k$  and with an action of  $\mathbb{Q}[G]$  via the first factor in the tensor product, then the ‘non-commutative Tamagawa number conjecture’ of Fukaya and Kato [26, Conj. 2.3.2] for  $M_F$  conjectures the existence of a characteristic element  $\mathcal{L}$  for  $C(T_F)$  for which  $e_2(C(T_F))\mathcal{L}$  is equal to the value at  $s = 0$  of the  $\zeta(\mathbb{C}[G])$ -valued complex  $L$ -function of  $M_F$  normalised by a product of suitable regulators and periods. This means that when combined with Corollary 2.3 the relevant case of [26, Conj. 2.3.2] predicts explicit annihilators of the  $\mathbb{Z}_p[G]$ -module  $\text{Sel}(T^*(1)_F)$  in terms of the values of complex  $L$ -functions. In a very similar fashion, one can use Corollary 2.3 to show that the relevant (generalised) main conjecture of Iwasawa theory predicts the existence of explicit annihilators for  $\text{Sel}(T^*(1)_F)$  that are constructed from the values of  $p$ -adic  $L$ -functions. By means of

an explicit example, in this section we consider in detail the latter Iwasawa-theoretic approach to the Tate motives  $M = h^0(\mathrm{Spec} k)(r)$ .

**4.2. Annihilation results.** In this section we shall combine Corollary 2.3 with recent results of Ritter and Weiss, of Kakde and the first author concerning the main conjectures of non-commutative Iwasawa theory to prove an explicit restriction on the Galois structures of certain Galois groups, ideal class groups and wild kernels in higher algebraic  $K$ -theory.

For any CM-field  $E$  we write  $E^+$  for its maximal (totally) real subfield. In this subsection we fix a totally real field  $k$  and a finite CM Galois extension  $F$  of  $k$  inside  $k^c$ , set  $G := G_{F/k}$  and write  $\tau$  for the unique non-trivial element of  $G_{F/F^+}$ . We write  $\mu(F, p)$  for the Iwasawa-theoretic ( $p$ -adic)  $\mu$ -invariant of  $F$  and recall that Iwasawa has conjectured in [27] that  $\mu(F, p) = 0$ . We fix a finite set of places  $\Sigma$  of  $k$  containing all archimedean places, all which ramify in  $F/k$  and all above  $p$ . For each integer  $m$  we regard  $\mathbb{Z}_p(r)_F$  as an étale sheaf of free  $\mathbb{Z}_p[G]$ -modules on  $\mathrm{Spec}(\mathcal{O}_{k, \Sigma})$  in the natural way and thus, following §1.2.1, we obtain an object of  $D^{\mathrm{wa}}(\mathbb{Z}_p[G])$  by setting

$$(19) \quad C_m(F/k) := R\Gamma_c(\mathcal{O}_{k, \Sigma}, \mathbb{Z}_p(m)_F).$$

We write  $e_{F/k, m}$  for the idempotent  $e_2(C_m(F/k))$  that is defined in §1.1.4.

For any torsion abelian group  $A$  we write  $A_p$  for its  $p$ -primary part and, as in §2.1.2, we set  $a_G(M) := \mathrm{Ann}_{\zeta(\mathbb{Z}_p[G])}(M)$  for any  $\mathbb{Z}_p[G]$ -module  $M$ . For each integer  $a$  we write  $\mu_{F, p}^{\otimes a}$  for the  $\mathbb{Z}_p[G]$ -module  $H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(a))$  (so that  $\mu_{F, p}^{\otimes 1}$  identifies with the group  $\mu_{F, p}$  of  $p$ -power order roots of unity in  $F$ ) and if  $a > 0$  we also write  $K_{2a}^w(\mathcal{O}_F)$  for the ‘wild kernel’ of higher algebraic  $K$ -theory that is defined by Banaszak in [2]. We set  $\zeta(I_{G, p}) := \zeta(\mathbb{Z}_p[G]) \cap I_{G, p}$  and write  $x \mapsto x^\#$  for the  $\mathbb{Q}_p$ -linear involution on  $\zeta(\mathbb{Q}_p[G])^\times$  that is induced by inverting each element of  $G$ . Finally we write  $\omega_k$  for the Teichmüller character  $G_k \rightarrow \mathbb{Z}_p^\times$ .

**Theorem 4.1.** *Let  $F/k$  and  $\Sigma$  be as above. For each integer  $m$  write  $\mathrm{Ir}_m(G)$  for the subset of  $\mathrm{Ir}(G)$  comprising representations  $\rho : G \rightarrow \mathrm{GL}_{\rho(1)}(\mathbb{Q}_p^\times)$  for which  $\ker(\tilde{\rho})$  contains  $e_{F/k, m}$ .*

- (i) *If  $\rho$  belongs to  $\mathrm{Ir}_m(G)$ , then  $(-1)^{m+1}\tau \in \ker(\rho)$  and  $L_{p, \Sigma}(m, \omega_k^{1-m}\rho) \neq 0$ , where  $L_{p, \Sigma}(m, \omega_k^{1-m}\rho)$  is the value at  $s = m$  of the  $\Sigma$ -truncated  $p$ -adic  $L$ -function of the character  $\omega_k^{1-m}\rho$ . In particular, for each integer  $m$  we obtain a well-defined element of  $e_m\zeta(\mathbb{Q}_p[G])^\times$  by setting*

$$\mathcal{L}_{F/k, \Sigma, m} := \sum_{\rho \in \mathrm{Ir}_m(G)} e_\rho L_{p, \Sigma}(m, \omega_k^{1-m}\rho).$$

*In the sequel we assume that  $\mu(F, p) = 0$  if  $p$  divides  $|G|$ .*

- (ii) *If  $m = 1$ , resp.  $m \neq 1$ , then for any non-zero element  $\alpha$  which can be expressed as the product of an element of  $\zeta(I_{G, p}) \cap \zeta(\mathbb{Q}_p[G](1 - e_G))^\times$  and an element of  $\zeta(I_{G, p})$ , resp. for any non-zero element  $\alpha$  of  $a_G(\mu_{F, p}^{\otimes(1-m)}) \cap \zeta(\mathbb{Q}_p[G])^\times$ , there exists a weakly-organising matrix  $\Phi$  for the pair  $C_m(F/k)$  and  $\alpha$  which satisfies  $\mathrm{nr}_{\mathbb{Q}_p[G]}(\Phi) = \alpha \mathcal{L}_{F/k, \Sigma, m}$ .*

- (iii) *One has*

$$(20) \quad \mathcal{A}_p(G)\zeta(I_{G, p})^2 \mathcal{L}_{F/k, \Sigma, 1} \subseteq a_G(\mathrm{Gal}(M_\Sigma(k)/F))$$

and

$$(21) \quad \mathcal{A}_p(G)(a_G(\mu_{F,p})^\# \mathcal{L}_{F/k,\Sigma,0}^\# + \zeta(I_{G,p})^2 \mathcal{L}_{F/k,\Sigma,1}) \subseteq a_G(\mathrm{Cl}(\mathcal{O}_F)_p),$$

and for each  $m > 1$  also

$$(22) \quad \mathcal{A}_p(G)(a_G(\mu_{F,p}^{\otimes m})^\# \mathcal{L}_{F/k,\Sigma,1-m}^\# + a_G(\mu_{F,p}^{\otimes(m-1)}) \mathcal{L}_{F/k,\Sigma,m}) \subseteq a_G(K_{2m-2}^w(\mathcal{O}_F)_p).$$

**Remark 4.2.**

(i) In the special case that  $G$  is abelian the inclusion (21) is a natural counterpart to Brumer's Conjecture and hence, if  $F$  is abelian over  $\mathbb{Q}$  (in which case Ferrero and Washington [23] have proved that  $\mu(F,p) = 0$  and so (21) is unconditional), to Stickelberger's Theorem. Indeed, whilst the latter uses values of Dirichlet  $L$ -functions at  $s = 0$  to produce annihilators of  $\mathrm{Cl}(\mathcal{O}_F)_p$  that lie inside  $\mathbb{Z}_p[G](1 - \tau)$ , (21) uses the values of  $p$ -adic  $L$ -functions at  $s = 1$  to produce annihilators of  $\mathrm{Cl}(\mathcal{O}_F)_p$  that lie inside  $\mathbb{Z}_p[G](1 + \tau)$ .

(ii) The inclusions in Theorem 4.1(iii) specialise to give a strict improvement of the annihilation results that are proved in the case that  $G$  is abelian by Barrett and the first author in [3, Cor. 3.4 and Cor. 3.7]. In addition, the observations made in [3, Rem. 3.6(iii)] show that the inclusion (20) constitutes a natural generalisation to non-abelian extensions of the main results of Oriat in [43].

(iii) If the ' $p$ -adic Stark conjecture at  $s = 1$ ' of Serre and Tate (for a precise statement of which see [16, Conj. 5.2, Rem. 5.3]) is valid for all characters of  $G$ , then the element  $\mathcal{L}_{F/k,\Sigma,1}$  can be re-expressed explicitly in terms of the values at  $s = 1$  of  $\Sigma$ -truncated Artin  $L$ -functions. In any such case it would therefore be interesting to compare the inclusions of (20) and (21) with the conjectures and theorems regarding the structure of  $\mathrm{Cl}(\mathcal{O}_F)_p$  that are proved by Castillo and Jones in [18].

**Remark 4.3.**

(i) The argument used in the proof of [3, Cor. 3.7], and hence also in our proof of the inclusion (22), relies on the recent verification of the Quillen-Lichtenbaum Conjecture. For more details see Remark 2.9.

(ii) To properly understanding Theorem 4.1 one needs an explicit description of the set  $\mathrm{Ir}_m(G)$ , and hence also of the idempotent  $e_m$ , and the proofs of [3, Cor. 3.4 and Cor. 3.7] give information in this regard. In particular, if for each integer  $m$  we set  $e_{(m)} := (1 - (-1)^m \tau)/2$ , then the arguments given in [3] show the following:  $e_m = e_{(m)}$  for each  $m < 0$ ; the validity of Leopoldt's Conjecture for  $F$  at  $p$  implies that  $e_1 = e_{(1)} - e_{\chi_0}$  where  $\chi_0$  is the trivial character of  $G$ ; if  $m > 1$  and the group  $H^2(\mathcal{O}_{F,\Sigma}, W(1 - m))$  vanishes (as is conjectured by Schneider in [48, p. 192]), then  $e_m = e_{(m)}$  (and so, in particular, the expression on the left hand side of (22) has finite index in  $a_G(K_{2m-2}^w(\mathcal{O}_F)_p)$ ).

We end this subsection by proving the first assertion of Theorem 4.1(i). To do this it is clearly enough to show that any idempotent of  $\zeta(\mathbb{Q}_p[G])$  which annihilates  $H_c^2(\mathcal{O}_{k,\Sigma}, \mathbb{Q}_p(m)_F)$  must also annihilate the space  $\bigoplus_{v|\infty} H^0(k_v, \mathbb{Q}_p(m)_F) \cong H^0(G_{\mathbb{C}/\mathbb{R}}, \prod_{F \rightarrow \mathbb{C}} \mathbb{Q}_p(m))$ , where on the product term  $G_{\mathbb{C}/\mathbb{R}}$  acts diagonally and  $G$  acts via  $F$ .

If  $m = 0$ , then the required claim follows from the isomorphism of  $\mathbb{Q}_p[G]$ -modules  $\mathrm{Hom}_{\mathbb{Q}_p}(H_c^2(\mathcal{O}_{k,\Sigma}, \mathbb{Q}_p(0)_F), \mathbb{Q}_p) \cong H^1(\mathcal{O}_{k,\Sigma}, \mathbb{Q}_p(1)_F) \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{O}_{F,\Sigma}^\times$  coming from

global duality and Kummer theory and the fact that  $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathcal{O}_{F,\Sigma}^\times$  contains a  $\mathbb{Q}_p[G]$ -submodule isomorphic to  $H^0(G_{C/\mathbb{R}}, \prod_{F \rightarrow C} \mathbb{Q}_p) \cong \prod_w \mathbb{Q}_p$  where  $w$  runs over all archimedean places of  $F$ .

On the other hand, if  $m \neq 0$ , then the cohomology sequence of the exact triangle [3, (7)] with  $\mathcal{F} = \mathbb{Z}_p(m)_F$  combines with the fact that  $H^0(\mathcal{O}_{k,\Sigma}, \mathbb{Q}_p(m)_F)$  vanishes to induce an injective homomorphism from  $\bigoplus_{v|\infty} H^0(k_v, \mathbb{Q}_p(m)_F)$  to  $H_c^1(\mathcal{O}_{k,\Sigma}, \mathbb{Q}_p(m)_F)$  and this implies the required claim since any idempotent which annihilates  $H_c^2(\mathcal{O}_{k,\Sigma}, \mathbb{Q}_p(m)_F)$  must also annihilate  $H_c^1(\mathcal{O}_{k,\Sigma}, \mathbb{Q}_p(m)_F)$  (since  $C$  belongs to  $D^{\text{wa}}(\mathbb{Z}_p[G])$  and  $H^3(C)$  is finite). This completes the proof of the first assertion of Theorem 4.1(i).

**4.3. Characteristic elements.** The following result provides a key step in our proof of Theorem 4.1. We recall the complex  $C_m(F/k)$  defined in (19).

**Theorem 4.4.** *Let  $F/k$  and  $\Sigma$  be as in Theorem 4.1 and assume that  $\mu(F, p) = 0$  if  $p$  divides  $|G|$ . Then there exists a characteristic element  $\mathcal{L}_m$  for  $C_m(F/k)$  which satisfies  $e_{F/k,m} \mathcal{L}_m = \mathcal{L}_{F/k,\Sigma,m}$ .*

The proof of this result will occupy the rest of this section.

For any subfield  $F'$  of  $F$  we write  $F'_\infty$  for the cyclotomic  $\mathbb{Z}_p$ -extension of  $F'$ . For any continuous quotient  $\mathcal{G}$  of the group  $G_{F_\infty/k}$  we write  $\Lambda(\mathcal{G})$  for the completed group ring  $\varprojlim_U \mathbb{Z}_p[\mathcal{G}/U]$  where  $U$  runs over all open subgroups of  $\mathcal{G}$  and  $Q(\mathcal{G})$  for the total quotient ring of  $\Lambda(\mathcal{G})$ . For each integer  $m$  we write  $\Lambda(\mathcal{G})^\#(m)$  for the set  $\Lambda(\mathcal{G})$  upon which  $\Lambda(\mathcal{G})$  acts via multiplication and  $G_{k,\Sigma}$  acts in the following way: each  $\sigma$  in  $G_{k,\Sigma}$  acts as multiplication by the element  $\chi_{\text{cyc}}(\sigma)^m \bar{\sigma}^{-1}$  where  $\chi_{\text{cyc}}$  is the cyclotomic character  $G_{k,\Sigma} \rightarrow \mathbb{Z}_p^\times$  and  $\bar{\sigma}$  denotes the image of  $\sigma$  in  $\mathcal{G}$ . We regard  $\tau$  as an element of  $G_{F_\infty/F_\infty^+}$  and hence also for each integer  $m$  we regard the idempotent  $e_{(m)}$  defined in Remark 4.2(iv) as an element of  $\zeta(\Lambda(G_{F_\infty/k}))$ . If  $E$  is the subfield of  $F_\infty$  with  $G_{E/k} = \mathcal{G}$  then, following Nekovář [40] and Fukaya and Kato [26, §2.1.1], we obtain an object of  $D^{\text{p}}(\Lambda(\mathcal{G}))$  by setting

$$(23) \quad C_{E/k,m} := R\Gamma_c(\mathcal{O}_{k,\Sigma}, e_{(m)} \Lambda(\mathcal{G})^\#(m)).$$

To study this complex we write  $S$  for the Ore set of non-zero divisors in  $\Lambda(\mathcal{G})$  comprising elements  $f$  for which the quotient  $\Lambda(\mathcal{G})/\Lambda(\mathcal{G})f$  is a finitely generated  $\mathbb{Z}_p$ -module and  $\Lambda(\mathcal{G})_S$  for the corresponding localisation of  $S$ . We recall that for each element  $\xi$  of  $K_1(\Lambda(\mathcal{G})_S)$  and each representation  $\rho$  in  $A(\mathcal{G})$  there is a well-defined notion of the ‘value of  $\xi$  at  $\rho$ ’ and that this element  $\xi_{\mathcal{G}}(\rho)$  belongs to  $\mathbb{Q}_p^c \cup \{\infty\}$ . We write  $\partial_{\mathcal{G},S}$  for the natural connecting homomorphism  $K_1(\Lambda(\mathcal{G})_S) \rightarrow K_0(\Lambda(\mathcal{G}), \Lambda(\mathcal{G})_S)$  and  $\chi^{\text{ref}}(C)$  for the canonical element of  $K_0(\Lambda(\mathcal{G}), \Lambda(\mathcal{G})_S)$  that is associated to any object  $C$  of  $D^{\text{p}}(\Lambda(\mathcal{G}))$  such that  $\Lambda(\mathcal{G})_S \otimes_{\Lambda(\mathcal{G})} C$  is acyclic.

The following result verifies the case of the main conjecture of non-commutative Iwasawa theory that is relevant to Theorem 4.4. This result is itself a special case of [11, Cor. 9.4] and is proved in loc. cit. by using the results of Ritter and Weiss in [47].

**Proposition 4.5.** *Let  $k$  be a totally real number field and  $F$  a finite CM Galois extension of  $k$  such that  $\mu(F, p) = 0$  if  $p$  divides  $[F : k]$ . We fix a finite set of places  $\Sigma$  of  $k$  that contains all places which ramify in  $F/k$  (and hence all archimedean places) and all places that divide  $p$ . We also set  $\mathcal{G} := G_{F_\infty/k}$  and fix an integer  $m$ .*

- (i) Then  $\Lambda(\mathcal{G})_S \otimes_{\Lambda(\mathcal{G})} C_{F_\infty/k, \Sigma}^\bullet(m)$  is acyclic.
- (ii) There exists an element  $\tilde{\xi}_m$  of  $K_1(\Lambda(\mathcal{G})_S)$  that satisfies both of the following conditions:
- (a) for all irreducible  $\rho \in A(\mathcal{G})$  one has

$$\tilde{\xi}_{m, \underline{g}}(\rho) = \begin{cases} L_{p, \Sigma}(m, \omega_k^{1-m} \rho), & \text{if } (-1)^{m+1} \tau \in \ker(\rho) \\ 1, & \text{otherwise;} \end{cases}$$

- (b)  $\partial_{\mathcal{G}, S}(\tilde{\xi}_m) = \chi^{\text{ref}}(C_{F_\infty/k, \Sigma}(m))$ .

To deduce Theorem 4.4 from Proposition 4.5 we set  $e_m := e_{F/k, m}$  and  $C_{m, 0} := \mathbb{Z}_p[G]e_m \otimes_{\mathbb{Z}_p[G]}^\mathbb{L} C_m(F/k)$  where the complex  $C_m(F/k)$  is as defined in (19). Then the first assertion of Theorem 4.1(i) (already proved at the end of §4.2) implies  $e_m e_{(m)} = e_m$  and hence that there is a natural isomorphism in  $D^p(\mathbb{Z}_p[G]e_m)$  of the form

$$(24) \quad \mathbb{Z}_p[G]e_m \otimes_{R_m}^\mathbb{L} C_{F_\infty/k, m} \cong \mathbb{Z}_p[G]e_m \otimes_{e_{(m)}\mathbb{Z}_p[G]}^\mathbb{L} C_{F/k, m} \\ \cong \mathbb{Z}_p[G]e_m \otimes_{\mathbb{Z}_p[G]}^\mathbb{L} C_m(F/k) = C_{m, 0}$$

where the first isomorphism is induced by the canonical descent isomorphism  $\mathbb{Z}_p[G]e_{(m)} \otimes_{R_m}^\mathbb{L} C_{F_\infty/k, m} \cong C_{F/k, m}$ .

Now, by the very definition of the idempotent  $e_m$ , the complex  $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} C_{m, 0}$  is acyclic and so the isomorphism (24) makes it clear that  $C_{F_\infty/k, m}$  is semisimple at  $\rho$  (in the terminology of [17]) for all  $\rho \in A(\mathcal{G})$  which factor through the algebra homomorphism  $\Lambda(\mathcal{G}) \rightarrow \mathbb{Z}_p[G]e_m$ . Thus, by combining Proposition 4.5 with the isomorphism (24) and the descent formalism of [17, Th. 2.2 and Rem. 2.3] one deduces that there exists a characteristic element  $\xi_{m, F/k}$  for  $C_{m, 0}$  which satisfies  $L_{p, \Sigma}(m, \omega_k^{1-m} \rho) = e_\rho \xi_{m, F/k} \neq 0$  for all  $\rho$  in  $\text{Ir}_m(G)$ . The result of Theorem 4.4 is now an immediate consequence of Lemma 1.4 (with  $\mathfrak{A} = \mathbb{Z}_p[G]$  and  $C = C_{F/k, m}$  so  $e_2 = e_m$ ).

**4.4. The proof of Theorem 4.1.** To prove Theorem 4.1 we combine Theorem 4.4 with Theorem 2.1 and Corollary 2.3. We shall also need the following result.

**Lemma 4.6.** *There are canonical identifications*

$$(25) \quad \text{Sel}(\mathbb{Z}_p(m)_F)e_{(m)} \cong \begin{cases} K_{2m-2}^w(\mathcal{O}_F)_p e_{(m)}, & \text{if } m > 1, \\ \text{Cl}(\mathcal{O}_F)_p e_{(m)}, & \text{if } m = 1, \\ \text{Cl}(\mathcal{O}_F)_p^\vee e_{(m)}, & \text{if } m = 0, \\ K_{-2m}^w(\mathcal{O}_F)_p^\vee e_{(m)}, & \text{if } m < 0, \end{cases}$$

and

$$(26) \quad H^3(C_m(F/k)e_{(m)}) \cong \begin{cases} \mathbb{Z}_p, & \text{if } m = 1, \\ (\mu_{F, p}^{\otimes(1-m)})^\vee \cong \mu_{F, p}^{\otimes(m-1)}, & \text{if } m \neq 1. \end{cases}$$

*Proof.* From any representation  $T$  as in §1.2.1 the explicit definition of the Bloch-Kato Tate-Shafarevich group  $\text{III}(T_F)$  of  $T_F$  gives rise to a canonical exact sequence of  $\mathbb{Z}_p[G]$ -modules

$$(27) \quad 0 \rightarrow \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}_p} H_f^1(k, T_F) \rightarrow \text{Sel}(T_F) \rightarrow \text{III}(T_F) \rightarrow 0.$$

One also knows that the module  $H_f^1(k, \mathbb{Z}_p(m)_F)$  vanishes if  $m \leq 0$  and identifies with  $K_{2m-1}(\mathcal{O}_k) \otimes \mathbb{Z}_p$  if  $m > 0$ . For each integer  $m$  it follows that the module  $H_f^1(k, \mathbb{Z}_p(m)_F)e_{(m)}$  vanishes and hence that  $\text{Sel}(\mathbb{Z}_p(m)_F)e_{(m)} = \text{III}(\mathbb{Z}_p(m)_F)e_{(m)}$ . In [24] Flach shows that  $\text{III}(\mathbb{Z}_p(1)_F)$  is canonically isomorphic to  $\text{Cl}(\mathcal{O}_F) \otimes \mathbb{Z}_p$  and if  $m > 1$ , then it is known that  $\text{III}(\mathbb{Z}_p(m)_F)$  is canonically isomorphic to  $K_{2m-2}^w(\mathcal{O}_F) \otimes \mathbb{Z}_p$  (see the proof of [3, Cor. 3.7]). The isomorphisms in (25) for  $m < 0$  then follow because the  $G_k$ -module  $\mathbb{Z}_p(m)_F^*(1)$  identifies with  $\mathbb{Z}_p(1-m)_F$  and because Flach's generalisation of the Cassels-Tate pairing induces a canonical isomorphism  $\text{III}(T_F) \cong \text{III}(T_F^*(1))^\vee$  for every representation  $T$ .

The isomorphisms in (26) result from the isomorphisms

$$\begin{aligned} H^3(C_m(F/k)e_{(m)}) &= H^3(C_m(F/k))e_{(m)} \cong H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(1-m))^\vee e_{(m)} \\ &= (\mu_{F,p}^{\otimes(1-m)})^\vee e_{(m)} \cong \mu_{F,p}^{\otimes(m-1)} e_{(m)} = \mu_{F,p}^{\otimes(m-1)} \end{aligned}$$

where the first indicated isomorphism is induced by global duality and the second is obvious.  $\square$

We first recall that Theorem 4.1(i) was proved at the end of §4.2. To prove Theorem 4.1(ii) and (iii) we apply Theorem 2.1 and Corollary 2.3(i) respectively, with the complex  $C$  equal to  $C_m := C_m(F/k)$  for each integer  $m$  and with the characteristic element  $\mathcal{L}_m$  as described in Theorem 4.4.

If  $m = 1$ , resp.  $m \neq 1$ , then the isomorphism (26) shows that in this setting we may apply Theorem 2.1 by taking  $\alpha$  to be the product of any element of  $\zeta(I_{G,p}) \cap \zeta(\mathbb{Q}_p[G](1-e_G))^\times$  and any element of  $\zeta(I_{G,p})$ , resp. by taking  $\alpha$  to be any element of  $a_G(\mu_{F,p}^{\otimes(1-m)}) \cap \zeta(\mathbb{Q}_p[G])^\times$ , and in either case with  $g_3(C_m) = 1$ . Then for any  $m$  one has by Theorem 2.1(iv) that  $\alpha \mathcal{L}_{F/k, \Sigma, m} = \alpha e_{F/k, m} \mathcal{L}_m = \alpha e_1 e_3 \mathcal{L}_m = \alpha e_1 \mathcal{L}_m = \text{nr}_{\mathbb{Q}_p[G]}(\Phi_{C_m, \alpha}) u_{\mathcal{L}_m} = \text{nr}_{\mathbb{Q}_p[G]}(\Phi_{C_m, \alpha}) \text{nr}_{\mathbb{Q}_p[G]}(U_{\mathcal{L}_m}) = \text{nr}_{\mathbb{Q}_p[G]}(\Phi_{C_m, \alpha} \cdot U_{\mathcal{L}_m})$  for some weakly-organising matrix  $\Phi_{C_m, \alpha} \in \text{M}_d(\mathbb{Z}_p[G])$  for  $C_m$  and  $\alpha$  and some  $U_{\mathcal{L}_m} \in \text{GL}_d(\mathbb{Z}_p[G])$ . Noting that  $\Phi := \Phi_{C_m, \alpha} \cdot U_{\mathcal{L}_m} \in \text{M}_d(\mathbb{Z}_p[G])$  is also a weakly-organising matrix for  $C_m$  and  $\alpha$  completes the proof of Theorem 4.1(ii).

If  $m = 1$ , resp.  $m \neq 1$ , then the isomorphism (26) shows that in this setting we may apply Corollary 2.3(i) by taking  $\beta$  and  $\gamma$  to be any elements of  $\zeta(I_{G,p})$ , resp. by taking  $\beta$  to be any element of  $a_G(\mu_{F,p}^{\otimes(1-m)})$  and  $\gamma = 1$ , and in either case with  $g_3(C_m) = 1$ , and in this way one deduces that

$$(28) \quad \begin{cases} \mathcal{A}_p(G) a_G(\mu_{F,p}^{\otimes(m-1)}) \mathcal{L}_{F/k, \Sigma, m} \subseteq a_G(H^2(C_m)), & \text{if } m > 1, \\ \mathcal{A}_p(G) \zeta(I_{G,p})^2 \mathcal{L}_{F/k, \Sigma, m} \subseteq a_G(H^2(C_m)), & \text{if } m = 1, \\ \mathcal{A}_p(G) a_G(\mu_{F,p}^\vee) \mathcal{L}_{F/k, \Sigma, m} \subseteq a_G(H^2(C_m)), & \text{if } m = 0, \\ \mathcal{A}_p(G) a_G((\mu_{F,p}^{\otimes(1-m)})^\vee) \mathcal{L}_{F/k, \Sigma, m} \subseteq a_G(H^2(C_m)), & \text{if } m < 0. \end{cases}$$

The inclusions of Theorem 4.1 are then a direct consequence of (28) because for every integer  $m$  the module  $\text{Sel}(\mathbb{Z}_p(1-m)_F)^\vee e_{(m)}$  is isomorphic to a quotient of  $H^2(C_m)$  (as already observed in §1.2.1) and so the isomorphism (25) implies that

$$a_G(H^2(C_m)) \subseteq \begin{cases} a_G(K_{2m-2}^w(\mathcal{O}_F)_p)e_{(m)}, & \text{if } m > 1, \\ a_G(\text{Cl}(\mathcal{O}_F)_p)e_{(m)}, & \text{if } m = 1, \\ a_G(\text{Cl}(\mathcal{O}_F)_p)^\#e_{(m)}, & \text{if } m = 0, \\ a_G(K_{-2m}^w(\mathcal{O}_F)_p)^\#e_{(m)}, & \text{if } m < 0, \end{cases}$$

where (for each  $m \leq 0$ ) we use the fact that  $a_G(M^\vee) = a_G(M)^\#$  for any finite  $\mathbb{Z}_p[G]$ -module  $M$ .

## 5. CRITICAL MOTIVES

In this section we fix notation and hypotheses as in §1.2.2 and also set  $e_1 := e_1(C(T_F, T_F^0))$ . We recall that in [26, Th. 4.1.12] Fukaya and Kato have proved that the (local and global) non-commutative Tamagawa number conjectures for the pair  $(M_F, \mathbb{Z}_p[G])$  combine to predict the existence of a characteristic element  $\mathcal{L}$  for  $C(T_F, T_F^0)$  such that  $e_1\mathcal{L}$  is equal to the value at  $s = 0$  of the  $\zeta(\mathbb{C}[G_{F/\mathbb{Q}}])$ -valued complex  $L$ -function of  $M_F$  multiplied by a suitable combination of natural regulators, periods and Euler factors. When combined with Corollary 2.3 this observation predicts the existence of explicit restrictions on the values at  $s = 0$  of the complex  $L$ -functions  $L(M, \chi, s)$  for  $\chi \in \text{Ir}(G)$  and also predicts that these values should influence the explicit structure of the  $\mathbb{Z}_p[G]$ -module  $\text{Sel}(T_F^*(1))$ . By means of an explicit example, in the next subsection we shall consider in greater detail the case of abelian varieties.

**5.1. Abelian varieties.** In this subsection we fix an abelian variety  $A$  that is defined over  $\mathbb{Q}$  and has good ordinary reduction at  $p$  and write  $A^t$  for the dual abelian variety. We write  $T$  for the  $p$ -adic Tate module of  $A^t$  (so that  $V^0$  can be identified with the  $\mathbb{Q}_p$ -space spanned by the  $p$ -adic Tate module of the formal group of  $A^t$  [16, Exam. 6.3]). We regard the motive  $M_F := h^1(A/F)(1)$  as defined over  $\mathbb{Q}$  and with coefficients  $\mathbb{Q}[G_{F/\mathbb{Q}}]$ .

We fix an isomorphism of fields  $\mathbb{C} \cong \mathbb{C}_p$  and henceforth use this to identify the sets of irreducible  $\mathbb{C}$ -valued and  $\mathbb{C}_p$ -valued characters of  $G$ . We also fix an isomorphism  $\beta$  as in [26, §4.2.24] and then define  $L_{\Sigma, \beta}(A/F, 1)$  to be the unique element of  $\zeta(\mathbb{C}_p[G])$  such that for every  $\rho \in \text{Ir}(G)$  one has

$$(29) \quad e_\rho L_{\Sigma, \beta}(A/F, 1) = e_\rho \frac{L_\Sigma(A, \check{\rho}, 1)}{\Omega_\infty(M(\check{\rho}))} \Omega_{p, \beta}(M(\check{\rho})) \Gamma_{\mathbb{Q}_p}(V_F^0)^{-1} \frac{P_{L, p}((V_\check{\rho}^0)^*(1), 1)}{P_{L, p}(V_\check{\rho}^0, 1)}.$$

Here  $L_\Sigma(A, \check{\rho}, 1)$  denotes the value at  $s = 1$  of the  $\Sigma$ -truncated Hasse-Weil  $L$ -function of  $A$  twisted by the contragredient representation  $\check{\rho}$ ,  $M(\check{\rho})$  is the tensor product of  $h^1(A)(1)$  with the Artin motive associated to  $\check{\rho}$ ,  $V_\check{\rho}^0$  is the representation  $V^0 \otimes V_\check{\rho}$  where  $V_\check{\rho}$  is a representation of character  $\check{\rho}$  and the archimedean and  $p$ -adic periods  $\Omega_\infty(M(\check{\rho}))$  and  $\Omega_{p, \beta}(M(\check{\rho}))$ , non-zero rational number  $\Gamma_{\mathbb{Q}_p}(V_F^0)$  and Euler factors  $P_{L, p}(-, s)$  are all as defined by Fukaya and Kato in [26, §4.1.11, §3.3.6, Lem. 4.1.7]. (For a more explicit description of the formula (29) in the case that  $A$  is an elliptic curve see §5.2.) If  $B$  denotes either  $A$  or  $A^t$ , then we write  $\text{III}(B/F)$  and  $\text{Sel}_p(B/F)$  for the (classical) Tate-Shafarevich and  $p$ -primary Selmer groups of  $B$  over  $F$  respectively. We also write  $B(F)[p^\infty]$  for the Sylow  $p$ -subgroup of  $B(F)_{\text{tor}}$ .

**Theorem 5.1.** *Let  $A, p, F/\mathbb{Q}$  and  $\Sigma$  be as above. We assume that  $A^t(F)[p^\infty]$  vanishes, that  $\text{III}(A_{/F}^t)$  is finite and that the relevant cases of all of the conjectures discussed by Fukaya and Kato in [26, §2 and §3] are valid (see Remark 5.2(i) for more details about these conjectures).*

- (i) *For each multiple  $h$  of  $|A(F)[p^\infty]|$ , there exists a weakly-organising matrix  $\Phi$  for  $C(T_F, T_F^0)$  and  $h$  for which one has  $h^g L_{\Sigma, \beta}(A_{/F}, 1) = \text{nr}_{\mathbb{Q}_p[G]}(\Phi) \in I_{G, p}^{[\text{rk}(A(\mathbb{Q}))]}$ , where  $g$  denotes the minimal number of generators of the  $\mathbb{Z}_p[G]$ -module  $A(F)[p^\infty]^\vee$ .*
- (ii) *One has  $\mathcal{A}_p(G)(a_G(A(F)[p^\infty])^\# L_{\Sigma, \beta}(A_{/F}, 1) \subseteq a_G(\text{Sel}_p(A_{/F})^\vee)$ .*
- (iii) *If  $A(F)[p^\infty]$  vanishes, then  $L_{\Sigma, \beta}(A_{/F}, 1)$  generates  $\text{Fit}_{\mathbb{Z}_p[G]}(H^2(C(T_F, T_F^0)))$ .*

*Proof.* In this argument we set  $C := C(T_F, T_F^0)$  and  $L_{\Sigma, \beta} = L_{\Sigma, \beta}(A_{/F}, 1)$ .

At the outset we recall that if  $\text{III}(A_{/F})$  is finite, then [6, Prop. 5.4] implies that  $\text{Sel}(T_F^*(1))$  is canonically isomorphic to  $\text{Sel}_p(A_{/F})$  and that the space  $H_f^1(\mathbb{Q}, V_F) \cong H_f^1(F, V)$  identifies with  $\mathbb{Q}_p \otimes_{\mathbb{Z}} A^t(F) = \mathbb{Q}_p \otimes_{\mathbb{Q}} H_f^1(M_F)$ . We also recall that in this case the spaces  $H^0(\mathbb{Q}_p, V_F/V_F^0)$ ,  $H^0(\mathbb{Q}_p, (V_F^0)^*(1))$  and  $H^0(\mathbb{Q}_\ell, V_F)$  for each prime  $\ell \notin \Sigma$  all vanish (cf. [16, Exam. 6.3]) as required by the discussion in §1.2.2. In addition, the group  $H^0(\mathbb{Z}_\Sigma, W_F)$  identifies with  $A^t(F)[p^\infty]$  and so [3, (26)] implies  $a_G(A^t(F)_{\text{tor}}) \subseteq a_G(H^1(C)_{\text{tor}})$ . Our assumption  $p \nmid |A^t(F)_{\text{tor}}|$  therefore implies that  $C$  is an object of  $D^{\text{wa}}(\mathbb{Z}_p[G])$ . The key point now is that if the conjectures discussed in [26, §2 and §3] are valid in the relevant cases, then there exists a characteristic element  $\mathcal{L}$  of  $C$  for which

$$(30) \quad e_1 \mathcal{L} = e_1 L_{\Sigma, \beta} = L_{\Sigma, \beta}$$

where  $L_{\Sigma, \beta}$  is as defined above. Indeed, the existence of a characteristic element  $\mathcal{L}$  that satisfies the first equality follows directly from [26, Th. 4.1.12] and the second equality follows from the validity of the Deligne-Beilinson Conjecture (in the form of [26, §2.2.8, (1)]) with  $M = M_F$  and  $K = \mathbb{Q}[G]$ . To explain the latter point note that a character  $\rho$  in  $\text{Ir}(G)$  belongs to  $\text{Ir}_0(G) := \{\rho \in \text{Ir}(G) : L_\Sigma(A, \rho, 1) \neq 0\}$  if and only if  $e_\rho(\mathbb{Q}_p^c \otimes_{\mathbb{Q}_p} H_f^1(\mathbb{Q}, V_F)) = 0$ , or equivalently  $e_1 e_\rho = e_\rho$ . One therefore has

$$L_{\Sigma, \beta} = \sum_{\rho \in \text{Ir}(G)} e_\rho L_{\Sigma, \beta} = \sum_{\rho \in \text{Ir}_0(G)} e_\rho L_{\Sigma, \beta} = \sum_{\rho \in \text{Ir}_0(G)} e_1 e_\rho L_{\Sigma, \beta} = e_1 L_{\Sigma, \beta},$$

as claimed.

Next we note that  $H^0(\mathbb{Z}_\Sigma, W_F^*(1))$  identifies with  $A(F)[p^\infty]$  and so [3, (26)] implies the existence of a surjective homomorphism

$$(31) \quad A(F)[p^\infty]^\vee \twoheadrightarrow H^3(C).$$

This surjection implies that  $H^3(C)$  is finite, that the integer  $g$  in claims (i) and (ii) satisfies  $g \geq g_3(C)$  and that  $|A(F)[p^\infty]|$  is a multiple of  $|H^3(C)|$ . To prove claim (i) we note that the complex  $C_G$  identifies with  $C(T, T^0)$  and that  $\mathbb{Q}_p \otimes_{\mathbb{Z}} A(\mathbb{Q})$  is isomorphic to a subspace of  $H^2(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} C(T, T^0))$  and so  $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2(C_G)) \geq \text{rk}(A(\mathbb{Q}))$ . Claim (i) therefore results directly from applying Corollary 2.3(ii) to the complex  $C$  and using the equality (30).

We may also apply Corollary 2.3(i) to the complex  $C$  with  $\beta$  any element of  $a_G(A(F)[p^\infty]^\vee) = a_G(A(F)[p^\infty])^\#$  and with  $e_1 \mathcal{L} = L_{\Sigma, \beta}$ . This implies claim (ii).

Regarding claim (iii) we note that if  $A(F)[p^\infty]$  vanishes, then the surjection (31) implies that  $H^3(C)$  vanishes. Claim (iii) thus follows directly by applying Corollary 2.3(iii) to the complex  $C$  and using the equality (30).  $\square$

**Remark 5.2.**

(i) The conjectures from [26, §2 and §3] that are being assumed in Theorem 5.1 are as follows: [26, §2.2.8] (the Deligne-Beilinson conjecture) for the motive  $M_F$  and algebra  $K = \mathbb{Q}[G]$ ; [26, Conj. 2.3.2] (the non-commutative Tamagawa number conjecture), [26, Conj. 3.4.3] (the local non-commutative Tamagawa number conjecture) and [26, Conj. 3.5.5] (compatibility of the above conjectures with the relevant functional equation), in each case for the ring  $\Lambda = \mathbb{Z}_p[G]$  and sheaf  $T = T_F$ .

(ii) If  $G$  is abelian, then the techniques of [9, §9] combine with the properties of  $\Phi$  described in Theorem 2.10(ii) and (iii) to show Theorem 5.1(i) implies an explicit congruence for the residue class of  $L_{\Sigma, \beta}(A/F, 1)$  modulo  $I_{G, p}^{\text{rk}(A(\mathbb{Q})) + 1}$  in terms of the discriminant of a natural algebraic height pairing  $H^1(C(T, T^0)) \otimes H^2(C(T, T^0)) \rightarrow I_{G, p}/I_{G, p}^2$ . Such conjectural formulas constitute a natural generalisation of the congruences for modular symbols that are conjectured by Mazur and Tate in [38]. In addition, Theorem 5.1(iii) constitutes a (non-abelian) ‘strong main conjecture’ of the kind that Mazur and Tate explicitly ask for in [38, Remark after Conj. 3] (see also Remark 5.4 below). In particular, it would also be interesting to know if there are any connections between this (conjectural) equality and the explicit conjectural formulas for the Fitting ideals of Selmer groups that are formulated (in certain special cases) by Kurihara in [29].

**5.2. Elliptic curves: the rank zero component.** The predictions of Theorem 5.1 can be made even more explicit if  $A$  is equal to an elliptic curve  $E$ . To do this we let  $u$  in  $\mathbb{Z}_p^\times$  be the unit root of the polynomial  $1 - a_p X + pX^2$  where  $a_p := p + 1 - |\tilde{E}_p(\mathbb{F}_p)|$  with  $\tilde{E}_p$  the reduction of  $E$  modulo  $p$ . We set  $G := G_{F/\mathbb{Q}}$  and for each  $\rho \in \text{Ir}(G)$  we fix a  $\mathbb{Q}_p^c[G]$ -module  $V_\rho$  of character  $\rho$ , regarded as a module over  $G_\mathbb{Q}$  via the natural projection  $G_\mathbb{Q} \rightarrow G$ , and then define a polynomial

$$P_p(\rho, X) := \det_{\mathbb{Q}_p^c}(1 - \varphi_p X \mid H^0(I_p, V_\rho)) \in \mathbb{Q}_p^c[X]$$

where  $I_p$  is the inertia subgroup of  $p$  in  $G$  and  $\varphi_p$  the geometric frobenius of  $p$  in  $G/I_p$ . We also write  $p^{f_\rho}$  for the  $p$ -part of the conductor of  $\rho$  and  $\epsilon_p(\rho)$  for the local  $\epsilon$ -factor of  $\rho$  at the prime  $p$ . We note in passing that if both  $\rho(1) = 1$  and  $f_\rho \neq 0$ , then ( $\rho$  is non-trivial, irreducible and of degree 1 and  $I_p$  acts non-trivially on  $V_\rho$  so) the space  $H^0(I_p, V_\rho)$  vanishes and hence  $P_p(\rho, X)$  is identically 1.

We also use the period  $\Omega_E := \int_\gamma \omega$  where  $\omega$  is the Néron differential of  $E$  and  $\gamma$  is a generating element for the (free rank one  $\mathbb{Z}$ -) module  $H^0(G_{\mathbb{C}/\mathbb{R}}, H_1(E(\mathbb{C}), \mathbb{Z}))$ .

**Corollary 5.3.** *Let  $L_\Sigma(E, 1)$  denote the unique element of  $\zeta(\mathbb{C}_p[G])$  which at each  $\rho$  in  $\text{Ir}(G)$  satisfies*

$$(32) \quad e_\rho L_\Sigma(E, 1) = e_\rho \frac{L_\Sigma(E, \check{\rho}, 1)}{\Omega_E^{\rho(1)}} \epsilon_p(\rho) u^{-f_\rho} \frac{P_p(\rho, u^{-1})}{P_p(\check{\rho}, up^{-1})}.$$

*Then if the conjectures discussed in §5.1 are valid with  $A = E$  all of the following claims are also valid.*

- (i)  $L_\Sigma(E/F, 1)$  belongs to  $I_{G, p}^{\text{rk}(E(\mathbb{Q}))}$  and generates  $\text{Fit}_{\mathbb{Z}_p[G]}(H^2(C(T_F, T_F^0)))$ .

- (ii)  $\mathcal{A}_p(G)L_\Sigma(E/F, 1) \subseteq \text{Ann}_{\zeta(\mathbb{Z}_p[G])}(\text{Sel}_p(E/F)^\vee)$ .
- (iii) For every  $\rho$  in  $\text{Ir}(G)$  one has  $\rho(1)^{-1}|G|e_\rho L_\Sigma(E, 1) \in \mathbb{Z}_p[\rho][G]$ , where  $\mathbb{Z}_p[\rho]$  is the extension of  $\mathbb{Z}_p$  that is generated by the values of  $\rho$ .

*Proof.* Since  $F$  is assumed to be totally real, the same argument as used in the proof of [17, Prop. 7.8] shows that the expressions on the right hand sides of (29) and (32) coincide (when  $A = E$ ). (It is important to note here that the argument of [17, Prop. 7.8] uses the explicit computation of [26, Th. 4.2.26] and hence relies upon choosing the isomorphism  $\beta$  which arises in the definition of the  $p$ -adic period  $\Omega_{p,\beta}(M(\check{\rho}))$  as in [26, §4.2.24].) In addition, in this case one has  $E^t(F) = E(F)$  and so our assumptions imply that the group  $E(F)[p^\infty]$  vanishes.

Given these facts, claim (i) follows directly from Theorem 5.1(i) and (iii) and claim (ii) follows from Theorem 5.1(ii). Finally we note that claim (iii) follows by combining claim (ii) with the observation in Remark 2.4(ii).  $\square$

**Remark 5.4.** Let  $E, p$  and  $F/k$  be as in §1.2.3. If also  $F$  is totally real and  $k = \mathbb{Q}$ , then [9, Prop. 4.3.2] shows that the equivariant Tamagawa number conjecture of [14, Conj. 4.1] implies that the approach of §5.1 can also be used after replacing  $C(T_F, T_F^0)$  by  $C_f(T_F)$  and  $L_\Sigma(E, 1)$  by the (unique) element  $L_\Sigma(E, 1)'$  of  $\zeta(\mathbb{C}_p[G])$  which at each  $\rho$  in  $\text{Ir}(G)$  satisfies

$$e_\rho L_\Sigma(E, 1)' = e_\rho \Omega_E^{-\rho(1)} \tau^*(\rho) L_{S_r}(E, \check{\rho}, 1),$$

where  $\tau^*(\rho)$  is the adjusted Galois-Gauss sum defined in [9, §4.3] and  $S_r$  the set of rational primes that ramify in  $F/\mathbb{Q}$ . In particular, under these conditions the predictions in Corollary 5.3(i) and (ii) should also be valid after replacing  $L_\Sigma(E/F, 1)$  and  $H^2(C(T_F, T_F^0))$  by  $L_\Sigma(E, 1)'$  and  $\text{Sel}_p(E/F)^\vee$  respectively.

**5.3. Elliptic curves: dihedral extensions.** Corollary 2.2.1 can be combined with Theorem 2.10 to give analogues of the predictions in Corollary 5.3 in which twisted Hasse-Weil  $L$ -functions are replaced by their higher order derivatives. In [33] the second author has investigated this approach in the setting of cyclic  $p$ -power degree extensions of  $\mathbb{Q}$  and, in particular, has shown that it gives strong refinements of the conjectures formulated by Fearnley and Kisilevsky in [21, 22]. In this subsection we therefore focus on the case of dihedral extensions. The results of Mazur and Rubin in [37] play a key role in this subsection.

**5.3.1. Explicit structures.** If  $E$  is an elliptic curve defined over  $K$ , then for any extension  $K'$  of  $K$  we write  $\text{Sel}_p(E/K')$  and  $\text{III}_p(E/K')$  for the  $p$ -primary Selmer module and the maximal  $p$ -torsion subgroup of the Tate-Shafarevich group  $\text{III}(E/K')$  of  $E$  over  $K'$  respectively. In the following result we also use the notation introduced in §1.2.3.

**Theorem 5.5.** *Let  $p$  be an odd prime, let  $F/k$  be a dihedral extension of number fields of degree  $2p^n$  and let  $E$  an elliptic curve defined over  $k$ . For each integer  $i$  with  $0 \leq i \leq n$  write  $K_i$  for the (unique) intermediate field in  $F/k$  with  $[K_i : k] = 2p^i$  and set  $K := K_0$ . Write  $S_r^K$  and  $S_b^K$  for the finite sets of places of  $K$  which ramify in  $F/k$  and at which  $E/K$  has bad reduction respectively.*

*Assume that all of the following conditions are satisfied:*

- (a)  $p \nmid \text{cond}(E)|E(K)_{\text{tor}}| \prod_{v \in S_r^K} |\tilde{E}_v(\mathbb{F}_v)| \prod_{v \in S_b^K} [E(K_v) : E_0(K_v)]$ .

- (b) Every place in  $S_b^K$  is unramified in  $F/K$ .
- (c) Either
  - (1)  $p \nmid \text{disc}(F/\mathbb{Q})$ , or
  - (2)  $E$  has ordinary reduction at all places above  $p$ ; for  $v$  in  $S_b^K$  either  $E(K_v)$  has no point of order  $p$  or  $E(K_v^{\text{un}})[p^\infty]$  is divisible;  $F$  is contained in a  $\mathbb{Z}_p^d$ -extension  $K'$  of  $K$  which is Galois over  $k$  and such that  $\text{Sel}_p(E/K')^\vee$  is a torsion  $\Lambda(G_{K'/K})$ -module.
- (d) For each  $i$  with  $0 \leq i \leq n$  the group  $\text{III}(E/K_i)$  is finite.

We fix an element  $\tau$  of  $G$  that has order 2. Then all of the following claims are valid.

- (i) If for each  $i < n$  one has  $p \nmid |\text{III}(E/K_i)|$ , then  $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F)$  is a permutation module.
- (ii) If all places of  $k$  above  $p$  are split in  $K/k$ , the group  $E(K)$  has odd rank and for each  $i < n$  one has  $p \nmid |\text{III}(E/K_i)|$ , then the  $\mathbb{Z}_p[G]$ -module  $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F)$  has a direct summand that is isomorphic to  $\mathbb{Z}_p[G]e_{E,F/k}$  with

$$e_{E,F/k} := \begin{cases} \frac{1}{2}(1 - \tau), & \text{if } E(k) \text{ is finite} \\ \frac{1}{2}(1 + \tau), & \text{otherwise.} \end{cases}$$

- (iii) If all places of  $k$  above  $p$  are split in  $K/k$ , the group  $E(K)$  has rank one and  $p \nmid |\text{III}(E/K)|$ , then  $p \nmid |\text{III}(E/F)|$  and the  $\mathbb{Z}_p[G]$ -module  $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F)$  is isomorphic to  $\mathbb{Z}_p[G](1 - (-1)^{\text{rk}(E(k))}\tau)$ .

*Proof.* For each integer  $i$  we write  $P_i$  for the normal subgroup  $G_{F/K_i}$  of  $G$  and set  $G_i := G_{K_i/k}$ . We note that  $P := P_n$  is the unique Sylow  $p$ -subgroup of  $G$  (and is normal). We also note that, since  $F/K$  is a  $p$ -extension, the assumption  $p \nmid |E(K)_{\text{tor}}|$  (in (a)) combines with Nakayama's Lemma to imply that  $p \nmid |E(F)_{\text{tor}}|$ .

We write  $T_p$  for the  $p$ -adic Tate module of  $E$ . Then the hypotheses of (a), (b) and (c)(1) combine to imply that the assumptions in §1.2.3 are satisfied and hence that each complex  $C_{f,i} := C_f(T_{p,K_i})$  belongs to  $D^a(\mathbb{Z}_p[G_i])$  and is such that  $H^1(C_{f,i}) = \mathbb{Z}_p \otimes_{\mathbb{Z}} E(K_i)$  and  $H^2(C_{f,i}) = \text{Sel}_p(E/K_i)^\vee$ . Thus, under these hypotheses, Corollary 2.5 implies that  $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F)$  is a permutation module if any weakly-organising matrix  $\Phi$  for  $C_f(T_{p,F})$  is such that  $\Phi^{P_i}$  is saturated for each integer  $i < n$ . But the construction of  $C_f(T_{p,F})$  in [12] implies that  $\mathbb{Z}_p[G_i] \otimes_{\mathbb{Z}_p[G]}^{\mathbb{L}} C_f(T_{p,F})$  is isomorphic in  $D^p(\mathbb{Z}_p[G_i])$  to  $C_{f,i}$  and hence that  $\Phi^{P_i}$  is a weakly-organising matrix for  $C_{f,i}$ . Thus, since (d) implies  $H^2(C_{f,i})_{\text{tor}} = \mathbb{Z}_p \otimes_{\mathbb{Z}} \text{III}(E/K_i)^\vee$ , the assumption that  $p \nmid |\text{III}(E/K_i)|$  implies  $\Phi^{P_i}$  is saturated, as required. This proves claim (i) under the condition (c)(1).

We now assume that the conditions (c)(2) is satisfied. In this case all of the hypotheses listed by Mazur and Rubin in [36, (7.1)-(7.4)] are satisfied and so the observations made in loc. cit. (which rely on constructions of Nekovář in [40, §9.7]) imply that  $C_{K'/k} := \text{Sel}_p(E/K')^\vee[-2]$  belongs to  $D^p(\Lambda(G_{K'/k}))$ . Further, the 'Perfect Control assumption' of [36, (7.5)] is satisfied (as a consequence of [36, Cor. A.3] and our assumptions (a) and (c)(2)) and so the finiteness of  $\text{III}(E/K_i)$  combines with [36, Th. 7.7] to imply that each complex  $C_i := \mathbb{Z}_p[G_i] \otimes_{\Lambda(G_{K'/k})}^{\mathbb{L}} C_{K'/k}$  belongs to  $D^a(\mathbb{Z}_p[G_i])$  and that  $H^1(C_i) = \mathbb{Z}_p \otimes_{\mathbb{Z}} E(K_i)$  and  $H^2(C_i) = \text{Sel}_p(E/K_i)^\vee$ . Since the definition of  $C_n$  makes it clear that  $\mathbb{Z}_p[G_i] \otimes_{\mathbb{Z}_p[G]}^{\mathbb{L}} C_n$  identifies with  $C_i$  one can now prove that  $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F)$  is a permutation module by copying the argument in the preceding

paragraph (with the role of  $C_f(T_{p,F})$  in that paragraph now played by  $C_n$ ). This completes the proof of claim (i).

To prove claim (ii) we use the main result of Mazur and Rubin in [37]. To be precise, the assumptions that are made in claim (ii) imply that the hypotheses of [37, Th. B] are valid and so the latter result implies the  $\mathbb{Q}[P]$ -module  $\mathbb{Q} \otimes_{\mathbb{Z}} E(F)$  has a summand that is isomorphic to  $\mathbb{Q}[P]$ . We set  $e := e_{E,F/k}$ . Then, since the  $\mathbb{Z}_p[P]$ -module  $\mathbb{Z}_p[G/P_i] = \mathbb{Z}_p[G/P_i]e \oplus \mathbb{Z}_p[G/P_i](1-e) = \mathbb{Z}_p[P/P_i]e \oplus \mathbb{Z}_p[P/P_i](1-e)$  has a summand that is isomorphic to  $\mathbb{Z}_p[P]$  if and only if  $i = 0$ , it follows that the permutation module  $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(K)$  has at least one summand that is isomorphic to either  $\mathbb{Z}_p[G]e$  or  $\mathbb{Z}_p[G](1-e)$ . The result of claim (ii) then follows because  $(\mathbb{Z}_p[G](1+\tau))^G \cong \mathbb{Z}_p$  and  $(\mathbb{Z}_p[G](1-\tau))^G$  vanishes, whilst  $(\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F))^G = \mathbb{Z}_p \otimes_{\mathbb{Z}} E(k)$  vanishes if and only if  $E(k)$  is finite.

We prove claim (iii) by induction on  $n$ . The case  $n = 0$  is obvious and so we assume  $n > 0$  and (by induction) that  $p \nmid |\text{III}(E/K_i)|$  for all  $i < n$ . Then claim (ii) applies to imply that  $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F)$  has a summand isomorphic to  $\mathbb{Z}_p[G]e$ . As  $(\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F))^P = \mathbb{Z}_p \otimes_{\mathbb{Z}} E(K)$  and  $(\mathbb{Z}_p[G]e)^P$  are both of rank one, the  $\mathbb{Z}_p[G]$ -module  $\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F)$ , and hence also  $(\text{Sel}_p(E/F)^\vee)_{\text{tf}} \cong \text{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes_{\mathbb{Z}} E(F), \mathbb{Z}_p)$ , is thus itself isomorphic to  $\mathbb{Z}_p[G]e$ . Since  $\mathbb{Z}_p[G]e$  is a free  $\mathbb{Z}_p[P]$ -module the exact sequence  $0 \rightarrow \text{III}_p(E/F)^\vee \rightarrow \text{Sel}_p(E/F)^\vee \rightarrow \mathbb{Z}_p[G]e \rightarrow 0$  therefore splits. In addition, our assumptions imply that  $(\text{Sel}_p(E/F)^\vee)_P$  is isomorphic to  $\text{Sel}_p(E/K)^\vee$  and so, since  $(\mathbb{Z}_p[G]e)_P$  is torsion-free, we obtain an identification of  $(\text{III}_p(E/F)^\vee)_P$  with  $(\text{Sel}_p(E/K)^\vee)_{\text{tor}} = \text{III}_p(E/K)^\vee$ . Since the latter group vanishes, Nakayama's lemma implies that  $\text{III}_p(E/F)^\vee$ , and hence also  $\text{III}_p(E/F)$ , vanishes, as claimed. To complete the proof of claim (iii) we now need only note that since, under the present hypotheses,  $\text{rk}(E(k))$  is either 0 or 1 the definition of  $e$  ensures that  $2e = 1 - (-1)^{\text{rk}(E(k))}\tau$ .  $\square$

**5.3.2. Explicit congruences.** There are considerable technical difficulties involved in obtaining numerical evidence in support of the finer predictions for the leading terms of Hasse-Weil  $L$ -functions that are made by the conjectures of Fukaya and Kato discussed in Remark 5.2(i) and by the equivariant Tamagawa number conjecture of [14, Conj. 4] (in this regard see, for example, the impressive work of Bley in [4, 5]). However, our next result shows that in certain cases the structural results of Theorem 5.5 allow an interpretation of these predictions that is much more amenable to numerical computations. We thereby obtain the first examples in which the predictions of [14, Conj. 4] have been made completely explicit for a class of extensions of arbitrary degree and a class of elliptic curves of arbitrarily large Mordell-Weil rank.

We fix an odd prime  $p$ , a totally real dihedral extension  $F$  of  $\mathbb{Q}$  of degree  $2p^n$  and an elliptic curve  $E$  over  $\mathbb{Q}$ . We write  $S_r$  for the set of primes that ramify in  $F/\mathbb{Q}$ , set  $n_r := |S_r|$  and let  $n'_r$  denote the number of primes in  $S_r$  that split in the unique quadratic extension  $K$  of  $\mathbb{Q}$  in  $F$ . For each  $\ell$  in  $S_r$  we fix a place  $w$  of  $F$  above  $\ell$  and write  $I_w$  for its inertia subgroup in  $G$ . We write  $d_K$  for the discriminant of  $K/\mathbb{Q}$ ,  $P$  for the subgroup of  $G$  of order  $p^n$  and  $Nf(\phi)$  for the absolute norm of the conductor of each  $\phi$  in  $\text{Ir}(P)$ . For each  $\rho$  in  $\text{Ir}(G)$  we fix a representation space  $V_\rho$  of character  $\rho$  and set  $T_\rho := \sum_{g \in G} \rho(g^{-1})g \in \zeta(\mathbb{C}[G])$ . We also fix elements  $\tau$  and  $\sigma$  of  $G$  that have orders 2 and  $p^n$  respectively and write  $\mathbf{1}$  for the trivial character of  $G$  and  $\epsilon$  for the unique non-trivial linear character of  $G$ .

We assume that all Hasse-Weil  $L$ -functions that arise in the following have an analytic continuation to  $s = 1$  (as predicted by [14, Conj. 4(i)]). We also assume that  $\text{III}(E/F)$ , and hence also  $\text{III}(E/K)$ , is finite and recall that in this case [14, Conj. 4(iv)] for the pair  $(h^1(E/F)(1), \mathbb{Z}[G])$  asserts the validity of an equality in the group  $K_0(\mathbb{Z}[G], \mathbb{R}[G])$ . We shall therefore say that the ‘ $p$ -part’ of [14, Conj. 4] is valid for  $(h^1(E/F)(1), \mathbb{Z}[G])$  if in this case [14, Conj. 4(ii)] is valid and the equality of [14, Conj. 4(iv)] is valid modulo the kernel of the natural homomorphism  $K_0(\mathbb{Z}[G], \mathbb{R}[G]) \rightarrow K_0(\mathbb{Z}_{(p)}[G], \mathbb{R}[G])$ , where we write  $\mathbb{Z}_{(p)}$  for the  $p$ -localisation of  $\mathbb{Z}$ . We write  $\Omega_E$  for the period of  $E$ .

**Theorem 5.6.** *Fix an odd prime  $p$ , a totally real dihedral field  $F$  of degree  $2p^n$  and an elliptic curve  $E$  as above. Assume that this data satisfies the hypotheses of Theorem 5.5(a), (b), (c)(1) and (d), that  $p$  splits in  $K/\mathbb{Q}$ , that  $E(K)$  has rank one and that  $p \nmid |\text{III}(E/K)|$ .*

*Then there exists a point  $Q$  in  $E(F)$  which satisfies  $\tau(Q) = -(-1)^{\text{rk}(E(\mathbb{Q}))}Q$  and generates a  $\mathbb{Z}[\frac{1}{2}][G]$ -module that is both isomorphic to  $\mathbb{Z}[\frac{1}{2}][G](1 - (-1)^{\text{rk}(E(\mathbb{Q}))}\tau)$  and has finite, prime-to- $p$ , index in  $\mathbb{Z}[\frac{1}{2}] \otimes_{\mathbb{Z}} E(F)$ . In the sequel we fix such a point  $Q$ .*

*We write  $\rho'_E$  for the character of the action of  $G$  on  $\mathbb{C} \otimes_{\mathbb{Z}} E(K)$  and  $\rho_E$  for the only other linear character of  $G$  and for each  $\rho$  in  $\text{Ir}(G) \setminus \{\rho_E\}$  we define a non-zero complex number  $h_{F,\rho}(Q) := |G|^{-1} \langle T_\rho(Q), T_{\check{\rho}}(Q) \rangle_F$  where  $\langle \cdot, \cdot \rangle_F$  is the  $\mathbb{C}$ -bilinear extension of the Néron-Tate height pairing on  $E$ , defined relative to the field  $F$ .*

*Then the  $p$ -part of [14, Conj. 4] is valid for the pair  $(h^1(E/F)(1), \mathbb{Z}[G])$  if and only if all of the following conditions are satisfied by any (and therefore every) point  $Q$  as above.*

- (i) *If  $\rho'_E$  is equal to  $\epsilon$ , resp.  $\mathbf{1}$ , then the order of vanishing at  $s = 1$  of  $L_{S_r}(E, s)$  is equal to zero, resp. one. For each  $\phi$  in  $\text{Ir}(P)$  the order of vanishing at  $s = 1$  of  $L_{S_r}(E/K, \check{\phi}, s)$  is equal to one. For each  $\rho$  in  $\text{Ir}(G)$  we may therefore define a non-zero complex number*

$$\mathcal{Q}_\rho := \begin{cases} (-1)^{n_r} \Omega_E^{-1} L_{S_r}(E, 1), & \text{if } \rho = \mathbf{1} = \rho_E \\ (-1)^{n_r} (\Omega_E h_{F,\mathbf{1}}(Q))^{-1} L'_{S_r}(E, 1), & \text{if } \rho = \mathbf{1} = \rho'_E \\ (-1)^{n'_r} (\Omega_E L'_{S_r}(E, 1))^{-1} \sqrt{d_K} L'_{S_r}(E/K, 1), & \text{if } \rho = \epsilon = \rho_E \\ (-1)^{n'_r} (\Omega_E h_{F,\epsilon}(Q))^{-1} L_{S_r}(E, 1)^{-1} \sqrt{d_K} L'_{S_r}(E/K, 1), & \text{if } \rho = \epsilon = \rho'_E \\ u_\rho (\Omega_E^2 h_{F,\rho}(Q))^{-1} \sqrt{d_K} Nf(\phi) L'_{S_r}(E/K, \check{\phi}, 1), & \text{if } \rho = \text{Ind}_P^G(\phi) \\ & \text{with } \phi \in \text{Ir}(P), \end{cases}$$

*where for each  $\rho$  in  $\text{Ir}(G)$  we write  $u_\rho$  for the ‘non-ramified characteristic’  $\prod_{\ell \in S_r} \det(-\text{Fr}_w | V_\rho^{I_w})^{-1}$ .*

- (ii) *For each  $\rho$  in  $\text{Ir}(G)$  the number  $\mathcal{Q}_\rho$  defined above belongs to  $\mathbb{Z}[\rho]$ , is a unit above  $p$  and satisfies  $(\mathcal{Q}_\rho)^\alpha = \mathcal{Q}_{\rho^\alpha}$  for all  $\alpha$  in  $\text{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$ .*
- (iii) *For all integers  $i$  in the range  $0 \leq i < p^n$  one has*

$$(33) \quad \mathcal{Q}_{\rho_E} \mathcal{Q}_{\rho'_E} \equiv - \sum_{\rho} \phi(\sigma)^i \mathcal{Q}_\rho \pmod{p^n \mathbb{Z}_{(p)}},$$

*or equivalently*

$$(-1)^{n_r + n'_r + 1} \frac{\sqrt{d_K} L'_{S_r}(E/K, 1)}{\Omega_E^2 h_{F,\rho'_E}(Q)} \equiv \sum_{\rho} \phi(\sigma)^i u_\rho \frac{\sqrt{d_K} Nf(\phi) L'_{S_r}(E/K, \check{\phi}, 1)}{\Omega_E^2 h_{F,\rho}(Q)} \pmod{p^n \mathbb{Z}_{(p)}},$$

where in both sums  $\rho = \text{Ind}_P^G(\phi)$  runs over the  $(p^n - 1)/2$  irreducible degree two characters of  $G$ .

*Proof.* Throughout this argument we fix an identification of fields  $\mathbb{C} \cong \mathbb{C}_p$  and so freely interchange between modules over  $\mathbb{C}$  and  $\mathbb{C}_p$ . We also set  $\mathbb{Z}' := \mathbb{Z}[\frac{1}{2}]$  and  $M' := \mathbb{Z}' \otimes_{\mathbb{Z}} M$  for any  $G$ -module  $M$ . For any subgroup  $H$  of  $G$  we identify  $\zeta(\mathbb{C}_p[H])^\times$  with  $\prod_{\rho \in \text{Ir}_p(H)} \mathbb{C}_p$  in the natural way and write  $(\xi_\rho)_\rho$  for the corresponding decomposition of each element  $\xi$  of  $\zeta(\mathbb{C}_p[H])^\times$ .

Theorem 5.5(iii) combines with Roiter's Lemma ([19, (31.6)]) to imply the existence of an exact sequence of  $\mathbb{Z}'[G]$ -modules  $0 \rightarrow \mathbb{Z}'[G](1 - (-1)^{\text{rk}(E(\mathbb{Q}))}\tau) \rightarrow E(F)' \rightarrow X \rightarrow 0$  where  $X$  is finite and of order prime to  $p$ . It follows that the image in  $E(F)'$  of  $(1 - (-1)^{\text{rk}(E(\mathbb{Q}))}\tau)$  multiplied by a large enough power of 2 is a point  $Q$  of  $E(F)$  that has the properties described above. We fix such a point  $Q$  in what follows.

The above exact sequence also implies that the  $\mathbb{C}[G]$ -module  $\mathbb{C} \otimes_{\mathbb{Z}} E(F)$  is isomorphic to  $\mathbb{C}[G](1 - (-1)^{\text{rk}(E(\mathbb{Q}))}\tau)$  and, by an explicit computation, one then finds that

$$\dim_{\mathbb{C}}(\text{Hom}_{\mathbb{C}[G]}(V_{\check{\rho}}, \mathbb{C} \otimes_{\mathbb{Z}} E(F))) = \begin{cases} 0, & \text{if } \rho = \rho_E \\ 1, & \text{otherwise.} \end{cases}$$

Taken in conjunction with the inductivity property of Hasse-Weil  $L$ -functions this formula shows that [14, Conj. 4(ii)] is equivalent to the order of vanishing assertions given in (i).

We next note that the final congruences in (iii) are obtained from those in (33) by direct substitution of the definition of each term  $\mathcal{Q}_\rho$  and hence that it suffices to prove that the  $p$ -part of [14, Conj. 4(iv)] is valid for the pair  $(h^1(E/F)(1), \mathbb{Z}[G])$  if and only if both the conditions in (ii) and the congruences in (33) are valid. To do this we write  $C_f$  for the 1-shift of the complex  $C_f(T_F)$  in  $D^a(\mathbb{Z}_p[G])$  that is defined in §1.2.3. Then  $H^0(C_f)$  identifies with  $E(F)_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} E(F)$  and, since Theorem 5.5(iii) combines with our present hypotheses on  $p, E(K)$  and  $\text{III}(E/K)$  to imply that  $p \nmid |\text{III}(E/F)|$ , the group  $H^1(C_f)$  also identifies with  $E(F)_p^* := \text{Hom}_{\mathbb{Z}_p}(E(F)_p, \mathbb{Z}_p)$ . We write  $t_{\text{NT}}$  for the element of  $\text{Is}_{\mathbb{C}_p[G]}(H^0(C_f)_{\mathbb{C}_p}, H^1(C_f)_{\mathbb{C}_p})$  that is induced by the Néron-Tate height pairing for  $E$  relative to  $F$  and  $\mathcal{L}$  for the element of  $\zeta(\mathbb{C}_p[G])^\times$  with  $\mathcal{L}_\rho := \Omega_E^{-\rho(1)} \tau^*(\rho) L_{S_r}^*(E, \check{\rho}, 1)$  for all  $\rho$  in  $\text{Ir}(G)$ , where  $\tau^*(\rho)$  is the modified Galois-Gauss sum that occurs in Remark 5.4 and  $L_{S_r}^*(E, \check{\rho}, 1)$  the leading term at  $s = 1$  of  $L_{S_r}(E, \check{\rho}, s)$ .

Now the argument of [9, Prop. 4.3.1] shows that if the assertions in (i) are valid, then the  $p$ -part of [14, Conj. 4] is valid for the pair  $(h^1(E/F)(1), \mathbb{Z}[G])$  if and only if  $\mathcal{L}$  is a characteristic element for the pair  $(C_f, t_{\text{NT}})$ . Lemma 5.7 below then implies that this condition on  $\mathcal{L}$  is satisfied if and only if both the assertions in (ii) and the congruences in (33) are valid with each term  $\mathcal{Q}_\rho$  replaced by  $\mathcal{L}_\rho h_{F,\rho}(Q)^{-1}$ . The claimed result will therefore follow if we can show that  $\mathcal{L}_\rho h_{F,\rho}(Q)^{-1} = \mathcal{Q}_\rho$  for all  $\rho$  in  $\text{Ir}_p(G)$  and, given the inductivity properties of Hasse-Weil  $L$ -functions, this is quickly reduced to proving

$$\tau^*(\rho) := \begin{cases} (-1)^{n_r}, & \text{if } \rho = \mathbf{1} \\ (-1)^{n_r'} \sqrt{d_K}, & \text{if } \rho = \epsilon \\ u_\rho \sqrt{d_K N f(\phi)}, & \text{if } \rho = \text{Ind}_P^G(\phi) \text{ with } \phi \in \text{Ir}(P). \end{cases}$$

To do this we first recall  $\tau^*(\rho)$  is by definition equal to  $\tau(\mathbb{Q}, \rho)u_\rho$  where  $\tau(\mathbb{Q}, \rho)$  is the Galois-Gauss sum defined in [25, Chap. I, §5]. If firstly  $\rho = \mathbf{1}$ , then  $\tau(\mathbb{Q}, \rho) = 1$  and  $V_\rho^{I_w} = \mathbb{C}_p$  for each  $\ell$  in  $S_r$  so  $\tau^*(\rho) = u_\rho = (-1)^{n_r}$ , as claimed. If now  $\rho = \epsilon$ , then  $u_\rho = (-1)^{n_r}$  since  $\det(-\text{Fr}_w | V_\rho^{I_w})$  is equal to  $-1$ , resp.  $1$ , if  $\ell$  splits in  $K/\mathbb{Q}$ , resp. otherwise. Since  $\rho = \text{Ind}_P^G(\mathbf{1}_P) - \epsilon$  with  $\mathbf{1}_P$  the trivial character of  $P$ , one also has  $\tau(\mathbb{Q}, \rho) = \tau(\mathbb{Q}, \text{Ind}_P^G(\mathbf{1}_P))\tau(\mathbb{Q}, \mathbf{1})^{-1} = \tau(\mathbb{Q}, \text{Ind}_P^G(\mathbf{1}_P)) = \sqrt{d_K}$ , where the last equality is true because  $K$  is totally real, and so the claimed formula for  $\tau^*(\rho)$  is also clear in this case. In a similar way, if  $\rho = \text{Ind}_P^G(\phi)$  with  $\phi$  a non-trivial element of  $\text{Ir}(P)$ , then the behaviour of Galois-Gauss sums under induction implies  $\tau(\mathbb{Q}, \rho) = \tau(K, \phi)\tau(\mathbb{Q}, \text{Ind}_P^G(\mathbf{1}_P)) = \tau(K, \phi)\sqrt{d_K}$ . This implies the claimed formula in this case as  $\tau(K, \phi) = \sqrt{Nf(\phi)}$  by [7, Lem. 4.4(2)].  $\square$

**Lemma 5.7.** *An element  $\mathcal{L}$  of  $\zeta(\mathbb{C}_p[G])^\times$  is a characteristic element for the pair  $(C_f, t_{\text{NT}})$  if and only if both the conditions of Theorem 5.6(ii) and the congruences in (33) are valid with each term  $\mathcal{Q}_\rho$  replaced by  $\mathcal{L}_\rho h_{F, \rho}(Q)^{-1}$ , where we set  $h_{F, \rho_E}(Q) := 1$  and  $h_{F, \rho}(Q) := |G|^{-1}\langle T_\rho(Q), T_{\bar{\rho}}(Q) \rangle_F$  for all  $\rho$  in  $\text{Ir}(G) \setminus \{\rho_E\}$ .*

*Proof.* We write  $C$  for the complex  $E(F)_p \xrightarrow{0} E(F)_p^*$ , where the first term is placed in degree zero, and note Theorem 5.5(iii) implies  $C$  belongs to  $D^p(\mathbb{Z}_p[G])$ . We also write  $\theta_Q$  for the (unique) generator of the  $\mathbb{Z}_p[G]$ -module  $E(F)_p^*$  that sends  $Q$  to 1 and  $g(Q)$  to zero for each non-trivial element  $g$  of  $P$  and define a resolvent  $R_Q := \sum_{g \in P} \langle Q, g(Q) \rangle_F g \in \mathbb{C}_p[G]$ . Then  $t_{\text{NT}}(Q) = R_Q(\theta_Q)$  and, using this fact, an easy explicit computation shows  $\text{nr}_{\mathbb{C}[G]}(\lambda_Q)$  is a characteristic element for  $(C, t_{\text{NT}})$  where  $\lambda_Q$  is the element of  $\text{Aut}_{\mathbb{C}[G]}(\mathbb{C} \otimes_{\mathbb{Z}} E(F))$  that sends  $Q$  to  $R_Q(Q)$ . Now if  $\rho = \rho_E$ , then  $\text{Hom}_{\mathbb{C}_p[G]}(V_{\bar{\rho}}, \mathbb{C} \otimes_{\mathbb{Z}} E(F))$  vanishes and so  $\text{nr}_{\mathbb{C}[G]}(\lambda_Q)_\rho = 1 = h_{F, \rho_E}(Q)$ . If  $\rho \in \text{Ir}(G) \setminus \{\rho_E\}$ , then  $E(F)_\rho := \text{Hom}_{\mathbb{C}_p[G]}(V_{\bar{\rho}}, \mathbb{C} \otimes_{\mathbb{Z}} E(F)) = \mathbb{C}[G] \cdot T_\rho(Q)$  has dimension one as a complex vector space and so one has  $\text{nr}_{\mathbb{C}[G]}(\lambda_Q)_\rho \cdot T_\rho(Q) = \lambda_Q(T_\rho(Q)) = T_\rho(\lambda_Q(Q)) = R_Q \cdot T_\rho(Q)$ . Noting that the element  $|G|^{-1}T_{\bar{\rho}}(\theta_Q)$  of  $\text{Hom}_{\mathbb{C}}(E(F)_\rho, \mathbb{C})$  sends  $T_\rho(Q)$  to 1 one finds that the last equation implies that

$$\begin{aligned} \text{nr}_{\mathbb{C}[G]}(\lambda_Q)_\rho &= |G|^{-1}T_{\bar{\rho}}(\theta_Q)(R_Q \cdot T_\rho(Q)) \\ &= |G|^{-1}T_{\bar{\rho}}(R_Q(\theta_Q))(T_\rho(Q)) \\ &= |G|^{-1}T_{\bar{\rho}}(t_{\text{NT}}(Q))(T_\rho(Q)) \\ &= |G|^{-1}t_{\text{NT}}(T_{\bar{\rho}}(Q))(T_\rho(Q)) \\ &= |G|^{-1}\langle T_\rho(Q), T_{\bar{\rho}}(Q) \rangle_F \\ &=: h_{F, \rho}(Q) \end{aligned}$$

where the second equality follows from the fact that  $R_Q$  is invariant under the  $\mathbb{C}$ -linear involution of  $\mathbb{C}[P]$  that inverts elements of  $P$  and the third from the equality  $t_{\text{NT}}(Q) = R_Q(\theta_Q)$ .

Now, as  $H^1(C_f) \cong E(F)_p^*$  is a projective  $\mathbb{Z}_p[G]$ -module, there exists an isomorphism  $C_f \cong C$  in  $D^p(\mathbb{Z}_p[G])$  which induces the identity map on  $H^i(C_f)$  for  $i \in \{0, 1\}$ . It follows that an element  $\mathcal{L}$  is a characteristic element for  $(C_f, t_{\text{NT}})$  if and only if it is a characteristic element for  $(C, t_{\text{NT}})$ , or equivalently that  $\mathcal{E} := \mathcal{L} \cdot \text{nr}_{\mathbb{C}[G]}(\lambda_Q)^{-1}$  belongs to the kernel of the homomorphism  $\delta_p := \delta_{\mathbb{Z}_p[G], \mathbb{C}_p[G]}$ . Since the computation

above implies  $\mathcal{E}_\rho = \mathcal{L}_\rho h_{F,\rho}(Q)^{-1}$  for all  $\rho$  in  $\text{Ir}(G)$  it is thus enough to show that  $\delta_p(\mathcal{E})$  vanishes if and only if both the conditions of Theorem 5.6(ii) and the congruences in (33) are valid with each term  $\mathcal{Q}_\rho$  replaced by  $\mathcal{E}_\rho$ .

To investigate  $\delta_p(\mathcal{E})$  we fix a maximal  $\mathbb{Z}_p$ -order  $\mathfrak{M}_p$  in  $\mathbb{Q}_p[G]$  that contains  $\mathbb{Z}_p[G]$ . Then  $\delta_p(\mathcal{E})$  belongs to the subgroup  $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G])_{\text{tor}}$  of  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$  if and only if  $\mathcal{E}$  belongs to  $\text{nr}_{\mathbb{Q}_p[G]}(\mathfrak{M}_p^\times)$  and this condition is satisfied if and only if the conditions of Theorem 5.6(ii) are valid with each term  $\mathcal{Q}_\rho$  replaced by  $\mathcal{E}_\rho$  (for more details of these equivalences see, for example, the proof of [14, Lem. 11]). Given this, it suffices to show that an element  $\mathcal{E}'$  of  $\text{nr}_{\mathbb{Q}_p[G]}(\mathfrak{M}_p^\times)$  belongs to  $\ker(\delta_p)$  if and only if the congruences in (33) are valid with each term  $\mathcal{Q}_\rho$  replaced by  $\mathcal{E}'_\rho$ . To prove this we use the diagram

$$\begin{array}{ccc} \text{nr}_{\mathbb{Q}_p[G]}(\mathfrak{M}_p^\times) & \xrightarrow{\text{res}'} & \mathfrak{M}'_p{}^\times \\ \delta_p \downarrow & & \delta'_p \downarrow \\ K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G])_{\text{tor}} & \xrightarrow{\text{res}} & K_0(\mathbb{Z}_p[P], \mathbb{Q}_p[P])_{\text{tor}}, \end{array}$$

where we write  $\mathfrak{M}'_p$  for the integral closure of  $\mathbb{Z}_p$  in  $\mathbb{Q}_p[P]$ ,  $\delta'_p$  for  $\delta_{\mathbb{Z}_p[P], \mathbb{C}_p[G]}$ , ‘res’ for the natural restriction homomorphism and ‘res’ for the homomorphism that sends each element  $(\xi_\rho)_{\rho \in \text{Ir}(G)}$  of  $\text{nr}_{\mathbb{Q}_p[G]}(\mathfrak{M}_p^\times) \subset \zeta(\mathbb{C}_p[G])^\times$  to  $(\xi_\phi)_{\phi \in \text{Ir}(P)}$  with  $\xi_{\mathbf{1}_P} := \xi_{\mathbf{1}} \xi_\epsilon$  and  $\xi_\phi := \xi_{\text{Ind}_G^E(\phi)}$  for each  $\phi$  in  $\text{Ir}(P) \setminus \{\mathbf{1}_P\}$ . Breuning has shown that this diagram commutes (by [7, Lem. 3.9]) and that res is injective (by [7, Prop. 3.2(2)]) and so  $\delta_p(\mathcal{E}') = 0$  if and only if  $\text{res}'(\mathcal{E}') \in \ker(\delta'_p) = \mathbb{Z}_p[P]^\times$ . We now need only note that [7, Lem. 3.5] implies that  $\text{res}'(\mathcal{E}')$  belongs to  $\mathbb{Z}_p[P]^\times$  if and only if the congruences in (33) are valid with each term  $\mathcal{Q}_\rho$  replaced by  $\mathcal{E}'_\rho$ .  $\square$

**Example 5.8.** We are very grateful to Christian Wuthrich for pointing out that, despite the long list of conditions that are imposed on the curve  $E$  and field  $F$  in the first paragraph of Theorem 5.6, it is not difficult to find suitable examples. For instance, if one takes  $p = 3$  then with  $E$  equal to  $40a1$  (with equation  $y^2 = x^3 - 7x - 6$ ) and  $F$  the splitting field of  $x^3 - 4x + 1$  all conditions are satisfied and  $\rho'_E = \epsilon$ , whilst with  $E$  equal to  $43a1$  (with equation  $y^2 + xy = x^3 + x^2$ ) and  $F$  the splitting field of  $x^3 - 4x + 2$  all conditions are satisfied and  $\rho'_E = \mathbf{1}$ . In both of these examples Wuthrich has also numerically verified all of the assertions in Theorem 5.6(i), (ii) and (iii) and hence also numerically verified the 3-part of [14, Conj. 4] for the pair  $(h^1(E/F)(1), \mathbb{Z}[G])$  (for more details see [52]). It should be noted that his examples are the first in which this conjecture has been (numerically) verified in the technically most difficult case of a prime  $p$  that divides  $|G|$  and an elliptic curve  $E$  for which  $E(F)$  has strictly positive rank.

#### REFERENCES

- [1] M. F. Atiyah, C. T. C. Wall, Cohomology of Groups In: ‘Algebraic Number Theory’ (Ed. J. W. S. Cassels and A. Fröhlich), Academic Press, London, (1967) 94-115.
- [2] G. Banaszak, Generalisation of the Moore exact sequence and the wild kernel for higher  $K$ -groups, *Compositio Math.* **86** (1993) 281-305.
- [3] J. Barrett, D. Burns, Annihilating Selmer Modules, to appear in *J. Reine Angew. Math.*
- [4] W. Bley, Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture, to appear in *Exp. Math.*

- [5] W. Bley, Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture (Part II), to appear in *Math. Comp.*
- [6] 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.
- [7] M. Breuning, On equivariant global epsilon constants for certain dihedral extensions, *Math. Comp.* **73** (2004), 881-898.
- [8] M. Breuning, D. Burns, Additivity of Euler characteristics in relative algebraic  $K$ -groups, *Homology, Homotopy Appl.* **7** (2005), No. 3, 11–36.
- [9] D. Burns, Leading terms and values of equivariant motivic  $L$ -functions, *Pure App. Math. Q.* **6** (2010) 83-172.
- [10] D. Burns, On derivatives of Artin  $L$ -series, to appear in *Invent. Math.*
- [11] D. Burns, On main conjectures in non-commutative Iwasawa theory and related conjectures, submitted for publication.
- [12] D. Burns, M. Flach, Motivic  $L$ -functions and Galois module structure, *Math. Ann.* **305** (1996) 65-102.
- [13] D. Burns, M. Flach, On Galois structure invariants associated to Tate motives, *Amer. J. Math.* **120** (1998) 1343-1397.
- [14] D. Burns, M. Flach, Equivariant Tamagawa numbers for motives with (non-commutative) coefficients, *Doc. Math.* **6** (2001) 501-570.
- [15] D. Burns, C. Greither, Equivariant Weierstrass Preparation and values of  $L$ -functions at negative integers, *Doc. Math.*, Extra volume (2003) 157-185.
- [16] D. Burns, O. Venjakob, Leading terms of Zeta isomorphisms and  $p$ -adic  $L$ -functions in non-commutative Iwasawa theory, *Doc. Math.*, Extra Volume (2006) 165-209.
- [17] D. Burns, O. Venjakob, On descent theory and main conjectures in non-commutative Iwasawa theory, *J. Inst. Math. Jussieu* **10** (2011) 59-118.
- [18] H. Castillo, A. Jones, Values of Dedekind Zeta functions at  $s = 1$  and the structure of Galois groups, preprint, 2011.
- [19] C. W. Curtis, I. Reiner, *Methods of Representation Theory*, Vol. I, John Wiley and Sons, New York, 1987.
- [20] P. Deligne, *Seminaire de géométrie algébrique du Bois-Marie, SGA4 $\frac{1}{2}$* , *Lecture Note Math.* **569**, Springer, New York, 1977.
- [21] J. Fearnley, H. Kisilevsky, Critical values of derivatives of twisted elliptic  $L$ -functions, *Exp. Math.* **19** (2010) 149-160.
- [22] J. Fearnley, H. Kisilevsky, Critical values of higher derivatives of twisted elliptic  $L$ -functions, to appear in *Exp. Math.*
- [23] B. Ferrero, L. Washington, The Iwasawa invariant  $\mu_p$  vanishes for abelian number fields, *Ann. Math.* **109** (1979), 377-395.
- [24] M. Flach, A generalisation of the Cassels-Tate pairing, *J. Reine u. Angew. Math.* **412** (1990) 113-127.
- [25] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, *Ergebnisse Math.* **1**, Springer Verlag, New York, 1983.
- [26] T. Fukaya, K. Kato, A formulation of conjectures on  $p$ -adic zeta functions in non-commutative Iwasawa theory, *Proc. St. Petersburg Math. Soc. Vol. XII*, 1–85, *Amer. Math. Soc. Transl. Ser. 2*, **219**, Amer. Math. Soc., Providence, RI, 2006.
- [27] K. Iwasawa, On the  $\mu$ -invariants of  $\mathbb{Z}_l$ -extensions, In: *Number Theory, Algebraic Geometry and Commutative Algebra*, in honor of Y. Akizuki, Kinokuniya, Tokyo 1973, 1-11.
- [28] H. Jacobinski, On extensions of lattices, *Michigan Math. J.* **13** (1966) 471-475.
- [29] M. Kurihara, Iwasawa theory and Fitting ideals, *J. Reine u. Angew. Math.* **561** (2003) 39-86.
- [30] T. Y. Lam, *A First Course in Noncommutative Rings (Second Edn.)*, *Grad. Text Math.* **131**, Springer-Verlag 2001.
- [31] S. Lichtenbaum, Values of zeta functions, étale cohomology and algebraic  $K$ -theory, *Lecture Notes in Math.* **342**, 489-501, Springer Verlag, 1973.
- [32] D. Macias Castillo, On higher order Stickelberger-type theorems, submitted for publication.
- [33] D. Macias Castillo, Congruences for critical values of higher derivatives of twisted elliptic  $L$ -functions, preprint 2011.

- [34] 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.
- [35] 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.
- [36] B. Mazur, K. Rubin, Organizing the arithmetic of elliptic curves, Adv. Math. **198** (2005) 504-546.
- [37] B. Mazur, K. Rubin, Finding large Selmer rank via an arithmetic theory of local constants, Ann. Math. **166** (2007) 579-612.
- [38] B. Mazur, J. Tate, Refined Conjectures of the Birch and Swinnerton-Dyer Type, Duke Math. J. **54** (1987) 711-750.
- [39] J. S. Milne, Arithmetic Duality Theorems, Academic Press, Boston, 1986.
- [40] J. Nekovář, Selmer complexes, Astérisque **310**, S.M.F., Paris, 2006.
- [41] A. Nickel, Non-commutative Fitting invariants and annihilation of class groups, J. Algebra **323** (2010) 2756-2778.
- [42] 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.
- [43] B. Oriat, Annulation de groupes de classes réelles, Nagoya Math. J. **81** (1981) 45-56.
- [44] A. Parker, Non-commutative Fitting invariants and equivariant Tamagawa numbers, Ph.D. Thesis, King's College London, 2007.
- [45] I. B. S. Passi, The associated graded ring of a group ring, Bull. London Math. Soc. **10** (1978) 241-255.
- [46] B. Perrin-Riou, Représentations  $p$ -adiques ordinaires, Astérisque **223** (1994), 185-220.
- [47] J. Ritter, A. Weiss, On the 'main conjecture' of equivariant Iwasawa theory, to appear in J. Amer. Math. Soc.
- [48] P. Schneider, Über gewisse Galoiscohomologiegruppen, Math. Zeit. **168** (1979) 181-205.
- [49] V. P. Snaith, Relative  $K_0$ , annihilators, Fitting ideals and Stickelberger phenomena, Proc. London Math. Soc. **90** (2005) 545-590.
- [50] J. Tate, The cohomology groups of tori in finite Galois extensions of number fields, Nagoya Math. J., **27** (1966) 709-719.
- [51] C. Weibel, The norm residue isomorphism theorem, J. Topology **2** (2009) 346-372.
- [52] C. Wuthrich, Numerical examples for the article 'Organising Matrices for Arithmetic Complexes' by Burns and Castillo, preprint 2011.
- [53] A. V. Yakovlev, Homological definability of  $p$ -adic representations of groups with cyclic Sylow  $p$ -subgroup, An. St. Univ. Ovidius Constantza **4** (1996) 206-221.

King's College London,  
 Dept. of Mathematics,  
 London WC2R 2LS,  
 United Kingdom  
 david.burns@kcl.ac.uk

Math. Inst. Univ. München  
 Theresienstr. 39  
 D-80333 München  
 Germany  
 daniel.macias-castillo  
 @kcl.ac.uk