TOKYO J. MATH.
VOL. 40, NO. 2, 2017
DOI: 10.3836/tjm/1502179233

On the Krull-Schmidt Decomposition of Mordell-Weil Groups

Daniel MACIAS CASTILLO

Instituto de Ciencias Mathemáticas

(Communicated by K. Matsuno)

Abstract. Let A be an abelian variety defined over a number field k and p a prime number. Under some natural and not-too-stringent conditions on A and p we show that certain invariants associated to Iwasawa-theoretic p-adic Selmer groups control the Krull-Schmidt decompositions of the p-adic completions of the groups of points of A over finite extensions of k.

Introduction

Let A be an abelian variety defined over a number field k. We also let p denote a fixed prime number.

If k' is a finite extension of k and F/k' is a finite Galois extension with Galois group G, we wish to study the structure of $A(F)_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} A(F)$ as a $\mathbb{Z}_p[G]$-module. We recall that, if p divides the degree of F/k', then describing the explicit Krull-Schmidt decomposition of $\mathbb{Z}_p[G]$-lattices that occur naturally in arithmetic is known to be a very difficult problem (see, for example, the considerable difficulties already encountered by Rzedowski-Calderón et al in [13] when considering the pro-p completion of the ring of algebraic integers of F).

Explicit structure results in this direction can have various kinds of important consequences, as discussed in the introduction of [5]. For example, they play an essential role in attempts to understand and investigate certain equivariant refinements of the Birch and Swinnerton-Dyer conjecture. We refer the reader to [6] and [1], where an understanding of such explicit structures is crucial in obtaining both theoretical and numerical verifications of certain instances of the equivariant Tamagawa number conjecture.

In [5] Burns, Wuthrich and the author give characterisations of certain properties, such as that of being projective or that of being a trivial source module, for a p-primary Selmer group, associated to a fixed extension F/k', that is closely related to $A(F)_p$. Burns then investigates in [4] the multiplicities of indecomposable modules in the Selmer groups of general critical

Received January 5, 2016; revised September 1, 2016

Mathematics Subject Classification: 11G35 (primary), 11R33, 11R34 (secondary)

The author acknowledges financial support from the Spanish Ministry of Economy and Competitiveness, through the "Severo Ochoa Programme for Centres of Excellence in R&D" (SEV-2015-0554) as well as through project MTM2016-79400-P.

motives as F varies in rank one pro-p p-adic analytic families of extensions of k that satisfy a certain additional condition.

In this note we focus on Mordell-Weil groups and also investigate properties of their Krull-Schmidt decompositions that go beyond the type of algebraic questions considered in [5]. Although our results have consequences for more general extensions F/k', we choose for simplicity to only explicitly discuss those for which G is isomorphic to cyclic groups of order p^n for natural numbers n (which we henceforth denote by C_n). We will let F/k' (and n) vary inside rank one pro-p p-adic analytic extensions K_∞ of k without any further restrictions and instead impose certain natural, not-too-stringent conditions on the choice of prime p. In this way, we obtain a number of results that link invariants of the Iwasawa-theoretic Selmer groups associated to intermediate $\mathbb{Z}_p$-extensions of K_∞/k to the multiplicities with which indecomposable lattices can occur in the Krull-Schmidt decompositions of modules of the form $A(F)_p$.

We recall that Heller and Reiner [9, 10] have proved that, if $n > 2$, then there are infinitely many isomorphism classes of indecomposable $\mathbb{Z}_p[C_n]$-lattices. However, a consequence of our general results is a finiteness statement, for the number of isomorphism classes of such lattices that can occur in modules of the form $A(F)_p$, that holds whenever the μ-invariants of the relevant Selmer groups vanish (see Corollary 2.3). We wish to emphasize that, even in such cases, our methods do not depend on the Selmer groups being torsion, and so the rank of $A(F)$ can be unbounded as F varies.

We also illustrate (in Examples 2.6 and 2.8) how, by considering additional restrictions on the Iwasawa-theoretic structures of the relevant Selmer groups that go beyond the vanishing of their μ-invariants, one can also gradually improve the precision of our general statements concerning the Krull-Schmidt decompositions of Mordell-Weil groups. Furthermore, since even these improvements are not necessarily best possible, we also discuss how by increasing the value of n inductively (rather than letting it be arbitrary) one could do even better. We refer the reader to Theorem 2.10 for an instance in which one can give strikingly sharp bounds on the number of isomorphism classes of indecomposable $\mathbb{Z}_p[C_3]$-lattices that can occur as direct summands of modules of the form $A(F)_p$.

Our algebraic methods, based on a result of Yakovlev [14], can be applied to other arithmetic groups and in particular one could use them to improve the precision of [3, Cor. 2.12] and [4, Thm 1.1].

It is a pleasure to thank David Burns for many interesting discussions and correspondence, as well as the anonymous referee for pointing out an error in a previous version.

1. Preliminaries and notation

For any $\mathbb{Z}_p$-module M we write M_{tor} for the torsion submodule of M and $M^\vee$ for the Pontryagin dual $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$. If M is finitely generated we also write $\mathrm{rk}_p(M)$ for the p-rank $\dim_{\mathbb{Z}/p\mathbb{Z}}(M/pM)$.

For any profinite Galois extension of fields F/E we abbreviate $\mathrm{Gal}(F/E)$ to $G_{F/E}$ and write $\mathbb{Z}_p[[G_{F/E}]]$ for the associated p-adic Iwasawa algebra.

1.1. Abelian varieties. We first introduce some basic notation relating to abelian varieties. Let A be an abelian variety defined over a number field k and fix a prime number p.

For a finite extension field F of k we write $X_p(A/F)$ for the Pontryagin dual of the p-adic Selmer group $\mathrm{Sel}_p(A/F)$ of A over F and $Ш(A/F)_p$ for the p-primary Tate-Shafarevich group of A over F. If F/k is Galois we regard $\mathrm{Sel}_p(A/F)$, $X_p(A/F)$ and $Ш(A/F)_p$ as $\mathbb{Z}_p[G_{F/k}]$-modules in the natural way. For a profinite extension F'/k we write $X_p(A/F')$ for the limit $\varprojlim_F X_p(A/F)$ where F runs over all finite extensions of k in F' and the transition morphisms are the natural corestriction maps.

We recall that, following Mazur [11], the reduction of A at a p-adic place v of k is said-to-be 'non-anomalous' if the number of points of A over the residue field of v is prime to p. It is straightforward to describe examples of abelian varieties A for which there are only finitely many such anomalous places (see, for example, the result of Mazur and Rubin in [12, Lemma A.5]).

We also note that, if p does not divide the order of the torsion subgroup of $A(k)$ and E is a finite extension of k that is contained in a pro-p extension of k, then it is straightforward to show that p does not divide the order of the torsion subgroup of $A(E)$, and therefore that $A(E)_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} A(F)$ is torsion-free. We will often use this fact in the sequel without further explicit comment.

For any finite extensions of fields E/k and F/E we set

$$T^F(A/E) := \ker(Ш(A/E)_p \xrightarrow{\pi_E^F} Ш(A/F)_p)$$

where π_E^F denotes the natural restriction map. We sometimes refer to groups of the form $T^F(A/E)$ as the 'kernel of capitulation' (the author is grateful to Christian Wuthrich for pointing out this convenient terminology).

1.2. Integral representations. We next introduce convenient notation concerning integral representations. Given a finite group G, by a '$\mathbb{Z}_p[G]$-lattice' we shall mean a $\mathbb{Z}_p[G]$-module that is both finitely generated and free over $\mathbb{Z}_p$.

For each non-negative integer n we write C_n for the cyclic group $\mathbb{Z}/p^n\mathbb{Z}$. For each non-negative integer m with $m < n$ we regard C_m as a quotient of C_n in the obvious way. We then also follow [4, §1.2] in fixing a set $\mathrm{IM}_{p,n}$ of representatives of all of the isomorphism classes of indecomposable $\mathbb{Z}_p[C_n]$-lattices which do not contain $\mathbb{Z}_p[C_m]$ for any integer m with $0 \leq m \leq n$. Then, by a classical result of Diederichsen [7] one knows that $|\mathrm{IM}_{p,1}| = 1$, whilst the results of Heller and Reiner in [9, 10] imply that $|\mathrm{IM}_{p,2}| = 4p - 2$ and that $\mathrm{IM}_{p,n}$ is infinite for all $n > 2$.

For each extension of fields M/k' with k' a finite extension of k, each natural number n and each lattice I in $\mathrm{IM}_{p,n}$ we write $m_I(A, M/k')$ for the maximal multiplicity with which I occurs in the Krull-Schmidt decomposition of $A(F)_p$ as F ranges over extensions of k' in

M that are cyclic of degree p^n and for which $Ш(A/F)_p$ is finite and, in each case, $A(F)_p$ is regarded as a $\mathbb{Z}_p[C_n]$-module via some choice of isomorphism of $G_{F/k'}$ with C_n.

Similarly, we write $m_I^{\mathrm{triv}}(A, M/k')$ for the maximal multiplicity with which I occurs in the Krull-Schmidt decomposition of $A(F)_p$ as F ranges over extensions of k' in M that are both cyclic of degree p^n with $Ш(A/F)_p$ finite and such that the natural action of $G_{F/k'}$ on the abelian group $T^F(A/E)$ is trivial for all intermediate fields E of F/k'.

Finally, we write $m_I^{\mathrm{cyc}}(A, M/k')$ for the maximal multiplicity with which I occurs in the Krull-Schmidt decomposition of $A(F)_p$ as F ranges over extensions of k' in M that are both cyclic of degree p^n with $Ш(A/F)_p$ finite and such that the module $T^F(A/E)$ is cyclic as an abelian group for all intermediate fields E of F/k'.

1.3. Explicit bounds. Given natural numbers n and d, we first write M_n^d for the finite set of $n \times d$-matrices with integer entries $(m_{i,j})_{1\le i\le n, 1\le j\le d}$ which, for each index i with $1 \le i \le n$, satisfy

$$(\mathrm{AG}(i))\ \ 0 \le m_{i,1} \le m_{i,2} \le \cdots \le m_{i,d} \le i$$

as well as, for each index i with $1 \le i \le n-1$, each of the properties (RK($i+1$)), (EX($i+1$)) and (OR($i+1$)) that will be introduced in Definition 4.1 below.

Given a matrix $M = (m_{i,j})$ in M_n^d we then set $a_M := \prod_{i=1}^n a_{M,i}$, where $a_{M,i}$ denotes the number of conjugacy classes in $\mathrm{Aut}(\prod_{j=1}^d C_{m_{i,j}})$ comprising elements of order dividing p^{n-i}. We also set $H_M := p^{2\cdot\sum_{i=1}^{n-1}\sum_{1\le k,l\le d}\min\{m_{i,k}, m_{i+1,l}\}}$.

We finally set $\eta_n^0 := 1$, $\eta_1^d := d+1$ and, for $d > 0$ and $n > 1$, define a non-negative integer

$$\eta_n^d := \sum_{M\in M_n^d} H_M \cdot a_M\,.$$

We also write $T_n^d \subset M_n^d$ for the finite set of $n \times d$-matrices with integer entries which satisfy (AG(i)), for each index i, as well as each of the properties (RK($i+1$)), (EX($i+1$)) and (OR($i+1$)) and each of the obvious analogous conditions (RK($i-1$)), (EX($i-1$)) and (OR($i-1$)).

We then set $\tau_n^0 := 1$, $\tau_1^d := d+1$ and, for $d > 0$ and $n > 1$, define a non-negative integer

$$\tau_n^d := \sum_{T\in T_n^d} H_T\,.$$

We finally write R_n for the finite set of vectors of length n with integer entries $(r_i)_{1\le i\le n}$ which, for every index i, satisfy the following properties:

(a) $0 \le r_i \le i$;

(b) $r_i - 1 \le r_{i+1} \le r_i + 1$.

Given a vector (r_i) in R_n we then set, for each index i with $1 \le i \le n-1$,

$$h_{r_i,r_{i+1}} := \begin{cases} 3, & \text{if } r_{i+1} = 1 = r_i \\ 2, & \text{if } r_{i+1} = r_i > 1 \\ 1, & \text{if } r_{i+1} = r_i - 1 \text{ or } r_{i+1} = r_i + 1 \text{ or } r_{i+1} = 0 = r_i\,. \end{cases} \tag{1}$$

We then set $\rho_1 := 2$ and, if n is greater than 1, define a non-negative integer

$$\rho_n := \sum_{(r_i)\in R_n} \left(\prod_{i=1}^{n-1} h_{r_i,r_{i+1}}\right) \cdot p^{\sum_{i=1}^{n-1} \max\{0,\min\{r_i-1,n-i\}\}}\,.$$

REMARK 1.1. The non-negative integer η_n^d (and consequently also τ_n^d) is smaller than the upper bound of the form $p^{n(n-1)d^2} \cdot \kappa_n^d$ that occurs in [4, Thm. 1.1]. Indeed, in the definition of κ_n^d given just before the statement of [4, Thm. 1.1], the sum runs over all $n \times d$-matrices with integer entries $M = (m_{i,j})$ on which one only imposes conditions (AG(i)), and each of the summands is larger than or equal to a_M. Furthermore, each one of our terms H_M is smaller than or equal to $p^{n(n-1)d^2}$. For example, even in the smallest non-trivial case (with $d = 1$ and $n = 2$) one computes $p^{n(n-1)d^2} \cdot \kappa_n^d = 2p^3 + 4p^2$, while $\eta_2^1 = p^3 + p^2 + 3$ and $\tau_2^1 = 2p^2 + 3$.

For a given natural number n, the non-negative integer ρ_n is smaller than η_n^1. Each term $p^{\sum_{i=1}^{n-1} \max\{0,\min\{r_i-1,n-i\}\}}$ is in fact equal to a_R for any given $R \in R_n \subseteq M_n^1$. To give an explicit example of its value, we compute the equalities $\rho_2 = 7$, $\rho_3 = 4p + 24$ and $\rho_4 = 12p^2 + 21p + 82$. In fact, it is easy to see that the largest exponent of p occurring in ρ_n is $((n-2)/2)^2 + (n-2)/2$ if n is even and $((n-1)/2)^2$ if n is odd.

2. Statement of the main results

2.1. The general case.

We can now state our main result.

THEOREM 2.1. *Let A be an abelian variety defined over a number field k. Let p be an odd prime that does not divide the order of the torsion subgroup of $A(k)$ or any Tamagawa number of A and is such that at every p-adic place of k the reduction of A is good, ordinary and non-anomalous.*

Let k_∞/k be a $\mathbb{Z}_p$-extension and K/k a finite Galois p-extension unramified at every place of bad reduction for A. For each intermediate field N of K/k, write N_∞ for the compositum of N and k_∞.

Then there exist non-negative integers λ and μ, which depend only upon the structure of the $\mathbb{Z}_p[[G_{N_\infty/N}]]$-module $X_p(A/N_\infty)$ as N varies over intermediate fields of K/k, and are *such that for every finite extension k' of k in K_∞ and every natural number n one has*

$$\sum_{I\in \mathrm{IM}_{p,n}} m_I(A, K_\infty/k') \leq \eta_n^d\,, \tag{2}$$

with $d = \lambda + p^n[k' : k]\mu$.

REMARK 2.2. (i) The conditions imposed on p are mainly motivated by a result of Greenberg in [8] (see also Lemma 3.2 below, as well as [5, Rem. 2.1]). Our approach allows us to work in the context of an arbitrary $\mathbb{Z}_p$-extension k_∞ of k, and in particular avoids the hypothesis concerning decomposition subgroups that occurs in [4, Thm. 1.1, Cor 1.4] when studying similar properties for the Selmer groups of critical motives. The approach of loc. cit. however avoids our restrictions on the choice of prime p.
(ii) It is straightforward, using certain ideas from [2], to obtain a generalised version of Theorem 2.1 in which K_∞ is replaced by any pro-p, p-adic analytic extension of k of arbitrary finite rank that is unramified at every place of bad reduction for A, but we have elected not to state it explicitly for simplicity.

2.2. Vanishing of μ-invariants. The proof of Theorem 2.1 is constructive in that structural invariants of natural Iwasawa modules can be used to give formulas for λ and μ. To illustrate this fact we will explain how it directly leads to the following result. Here and throughout the sequel, by the μ-invariant (or the λ-invariant) of a finitely generated Iwasawa module we will mean the μ-invariant (or the λ-invariant) of its torsion submodule.

COROLLARY 2.3. *We assume the hypotheses and notation of Theorem* 2.1. *Then for every intermediate field N of K/k the $\mathbb{Z}_p[[G_{N_\infty/N}]]$-module $X_p(A/N_\infty)$ is finitely generated, and we assume further that its μ-invariant vanishes. We fix a natural number n. Then all of the following claims hold*:

(i) *The bound on $\sum_{I\in \mathrm{IM}_{p,n}} m_I(A, K_\infty/k')$ given by the right hand side of* (2) *is independent of the choice of field k'.*

(ii) *There exists a non-negative integer δ_n which depends only upon A, K_∞/k and n with the following property*: *for any cyclic extension F/k' of degree p^n with $k \subseteq k' \subseteq F \subset K_\infty$ and both of k'/k and $Ш(A/F)_p$ finite, there is an isomorphism of $\mathbb{Z}_p[G_{F/k'}]$-lattices of the form*

$$A(F)_p \cong \left(\bigoplus_{i=0}^{i=n} \mathbb{Z}_p[C_i]^{s_{F/k',i}}\right) \oplus R_{F/k'} \tag{3}$$

where the $\mathbb{Z}_p$-rank of $R_{F/k'}$ is at most δ_n (for suitable non-negative integers $s_{F/k',i}$).

(iii) *There are only finitely many isomorphism classes of indecomposable $\mathbb{Z}_p[C_n]$-lattices that can occur in the Krull-Schmidt decompositions of the modules $A(F)_p$ which arise as F runs over all cyclic extensions F/k' of degree p^n with $k \subseteq k' \subseteq F \subset K_\infty$*

and both of k'/k and $Ш(A/F)_p$ finite. (Here in each case $A(F)_p$ is regarded as a $\mathbb{Z}_p[C_n]$-module via some choice of isomorphism of $G_{F/k'}$ with C_n).

REMARK 2.4. (i) The finiteness assertions of Corollary 2.3(iii) are of interest since they do not assume $X_p(A/k_\infty)$ is a torsion $\mathbb{Z}_p[[G_{k_\infty/k}]]$-module and so the rank of $A(F)$ can be unbounded as the field F varies. They therefore raise interesting questions of the kind considered explicitly in [4, Rem. 1.5(i)].
(ii) The arguments used in the proof are constructive in that they could be combined with knowledge of the structure of certain Iwasawa-theoretic Selmer groups to give an explicit upper bound on the number of isomorphism classes of indecomposable $\mathbb{Z}_p[C_n]$-lattices occurring as direct summands of $A(F)_p$ as in Corollary 2.3(iii) (see Remark 5.1, as well as the results in §2.5). However, they do not give explicit information about the upper bounds δ_n that occur in Corollary 2.3(ii) (for more details in this regard see [4, Rem. 1.5(ii)]).
(iii) It is possible to extend the finiteness assertions of Corollary 2.3(iii), replacing C_n with any abstract finite group G (and considering Galois extensions contained in K_∞/k that have Galois group isomorphic to G). This could be done, for example, through some of the algebraic methods developed in [2].

2.3. Kernels of capitulation with trivial action. The upper bounds on the values of sums $\sum_{I\in \mathrm{IM}_{p,n}} m_I(A, K_\infty/k')$ given in Theorem 2.1 are in general fairly coarse and, after further specialisation, one can do considerably better.

For example, if in the setting of Theorem 2.1 one only considers extensions F/k' that are both cyclic of degree p^n and such that the kernel of capitulation $T^F(A/E)$ vanishes for each intermediate field E of F/k', then our methods imply that no lattice in $\mathrm{IM}_{p,n}$ occurs in the Krull-Schmidt decomposition of $A(F)_p$.

In the next result we consider a slightly more general case.

THEOREM 2.5. *We assume the hypotheses and notation of Theorem 2.1. Then for every finite extension k' of k in K_∞ and every natural number n one has*

$$\sum_{I\in \mathrm{M}_{p,n}} m_I^{\mathrm{triv}}(A, K_\infty/k') \le \tau_n^d$$

with $d = \lambda + p^n[k' : k]\mu$.

EXAMPLE 2.6. Let A be an abelian variety defined over a number field k. Let p be an odd prime that satisfies the hypotheses of the first paragraph of Theorem 2.1. Let k_∞/k be a $\mathbb{Z}_p$-extension and write $\Lambda := \mathbb{Z}_p[[G_{k_\infty/k}]]$ for the associated p-adic Iwasawa algebra. For any non-negative integer m, we also write k_m for the extension of k in k_∞ of degree p^m.

Then $X_p(A/k_\infty)$ is a finitely generated Λ-module. We write $X_p(A/k_\infty)_{\mathrm{T}}$ for the Λ-torsion submodule of $X_p(A/k_\infty)$ and $X_p(A/k_\infty)_{\mathrm{TF}}$ for the quotient of $X_p(A/k_\infty)$ by $X_p(A/k_\infty)_{\mathrm{T}}$. We assume that the μ-invariant of $X_p(A/k_\infty)$ vanishes and that $X_p(A/k_\infty)_{\mathrm{TF}}$ is a free Λ-module. Then the torsion Λ-module $X_p(A/k_\infty)_{\mathrm{T}}$ is finitely generated over $\mathbb{Z}_p$, and we assume further that G_{k_∞/k_a} acts trivially on $X_p(A/k_\infty)_{\mathrm{T}}$ for a given non-negative integer a.

Then, for any non-negative integer b, the module of co-invariants $H_0(G_{k_\infty/k_b}, X_p(A/k_\infty)_{\mathrm{TF}})$ is $\mathbb{Z}_p$-free and so one has canonical isomorphisms

$$(4)\quad (\text{Ш}(A/k_b)_p^\vee)_{\mathrm{tor}} \cong X_p(A/k_b)_{\mathrm{tor}} \cong H_0(G_{k_\infty/k_b}, X_p(A/k_\infty))_{\mathrm{tor}} \\ \cong H_0(G_{k_\infty/k_b}, X_p(A/k_\infty)_{\mathrm{T}})_{\mathrm{tor}}$$

(where the second isomorphism, induced by the dual of the natural restriction map, is indeed bijective by Lemma 3.2 (ii) below). Each module $(\text{Ш}(A/k_b)_p^\vee)_{\mathrm{tor}}$ is therefore canonically isomorphic to a submodule of a quotient of $X_p(A/k_\infty)_{\mathrm{T}}$, and so has both trivial action of G_{k_∞/k_a} and p-rank bounded by

$$(5)\quad \lambda := \dim_{\mathbb{Z}/p\mathbb{Z}}(X_p(A/k_\infty)_{\mathrm{T}}[p]) + \lambda(X_p(A/k_\infty)) \\ = \dim_{\mathbb{Z}/p\mathbb{Z}}(X_p(A/k_\infty)_{\mathrm{T}}[p]) + \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} X_p(A/k_\infty)_{\mathrm{T}}) = \mathrm{rk}_p(X_p(A/k_\infty)_{\mathrm{T}}),$$

where $\lambda(X_p(A/k_\infty))$ denotes the λ-invariant of $X_p(A/k_\infty)$.

It follows that, for any $m \geq a$, for any natural number n and for any I in $\mathrm{IM}_{p,n}$ one has $m_I(A, k_\infty/k_m) = m_I^{\mathrm{triv}}(A, k_\infty/k_m)$, and furthermore in Theorem 2.5 one can take ($\mu := 0$ and also) λ as defined by (5).

Theorem 2.5 therefore gives, for every natural number n, an inequality

$$\sum_{I \in \mathrm{M}_{p,n}} m_I(A, k_\infty/k_m) \leq \tau_n^\lambda$$

which in particular is an upper bound on $\sum_{I \in \mathrm{M}_{p,n}} m_I(A, k_\infty/k_m)$ that both is independent of the choice of $m \geq a$ and is sharper than the upper bound η_n^λ obtained by simply setting $\mu := 0$ in (2).

2.4. Cyclic kernels of capitulation. In the following result we consider yet another more general condition than the vanishing of the relevant kernels of capitulation.

THEOREM 2.7. *We assume the hypotheses and notation of Theorem* 2.1. *Then for every finite extension k' of k in K_∞ and every natural number n one has*

$$\sum_{I \in \mathrm{M}_{p,n}} m_I^{\mathrm{cyc}}(A, K_\infty/k') \leq \rho_n .$$

EXAMPLE 2.8. We keep the notation of Example 2.6 and also assume that the μ-invariant of $X_p(A/k_\infty)$ vanishes.

We write N_2 for the maximal finite Λ-submodule of $X_p(A/k_\infty)_{\mathrm{T}}$ and also assume that one may choose Λ-modules N_1 and N_3, both of them finitely generated over $\mathbb{Z}_p$ and fitting into short exact sequences $0 \to X_p(A/k_\infty)_{\mathrm{TF}} \to Y \to N_1$ and $0 \to X_p(A/k_\infty)_{\mathrm{T}}/N_2 \to$

$E \to N_3$ with Y a free Λ-module and E an elementary Λ-module, with the property that the non-negative integer

$$\lambda(X_p(A/k_\infty)) + \mathrm{rk}_p(N_1) + \mathrm{rk}_p(N_2) + \mathrm{rk}_p(N_3)$$

is equal to 1. (Finite modules fitting into such short exact sequences always exist).

Then the isomorphism $(\text{Ш}(A/k_b)_p^\vee)_{\mathrm{tor}} \cong H_0(G_{k_\infty/k_b}, X_p(A/k_\infty))_{\mathrm{tor}}$ described in (4) combines with the proof of [4, Lem. 3.6] to imply that $(\text{Ш}(A/k_b)_p^\vee)_{\mathrm{tor}}$ is cyclic as an abelian group for every non-negative integer b.

It follows that, for any non-negative integer m, for any natural number n and for any I in $\mathrm{IM}_{p,n}$ one has $m_I^{\mathrm{cyc}}(A, k_\infty/k_m) = m_I(A, k_\infty/k_m)$. Theorem 2.7 therefore gives, for every natural number n, an inequality

$$\sum_{I \in \mathrm{M}_{p,n}} m_I(A, k_\infty/k_m) \le \rho_n$$

which in particular is an upper bound on $\sum_{I \in \mathrm{M}_{p,n}} m_I(A, k_\infty/k_m)$ that both is independent of the choice of m and is sharper than the upper bound η_n^1 obtained by simply setting $d := 1$ in (2).

2.5. Indecomposable $\mathbb{Z}_p[C_3]$-lattices. In the special case given by $n = 2$, Lemma 3.3 below directly combines with an important representation-theoretic theorem of Heller and Reiner in [9] (see also, for example, Table 2 in [13]) to give the following:

THEOREM 2.9. *We assume the hypotheses and notation of Theorem* 2.1, *and fix a finite extension k' of k in K_∞ and a cyclic extension F of k' in K_∞ of degree p^2. We write F' for the* (*unique*) *non-trivial intermediate field of F/k'.*

Then, *in the notation of Table* 2 *in* [13], *the Krull-Schmidt decomposition of $A(F)_p$ as a $\mathbb{Z}_p[G_{F/k'}]$-module is given by a direct sum of indecomposable $\mathbb{Z}_p[C_2]$-modules of the form*

$$R_2^a \oplus R_1^b \oplus Z^c \oplus E^d \oplus (R_2, Z; 1)^e \oplus \bigoplus_{i=0}^{p-2} (R_2, R_1; \lambda_0^i)^{g_i} \oplus \bigoplus_{i=0}^{p-1} (R_2, E; \lambda_0^i)^{h_i}$$

$$\oplus \bigoplus_{i=0}^{p-2} (R_2, Z \oplus R_1; 1 \oplus \lambda_0^i)^{j_i} \oplus \bigoplus_{i=1}^{p-2} (R_2, Z \oplus E; 1 \oplus \lambda_0^i)^{k_i}$$

for suitable non-negative exponents which satisfy both of the equalities

$$ap + e(p-1) + \sum_{i=0}^{p-2} g_i(i+1) + \sum_{i=1}^{p-1} h_i i + \sum_{i=0}^{p-2} j_i(i+1) + \sum_{i=1}^{p-2} k_i i = \mathrm{rk}_p(T^F(A/F'))$$

and

$$a + b + g_0 + 2\sum_{i=1}^{p-2} g_i + \sum_{i=1}^{p-1} h_i + \sum_{i=0}^{p-2} j_i = \mathrm{rk}_p(T^F(A/k')) .$$

The Iwasawa-theoretic invariants μ and λ in the statement of Theorem 2.1 are defined during the proof as a means of providing explicit upper bounds, of the form $\lambda + p^n[k' : k]\mu$, on the p-ranks of the kernels of capitulation occurring in the above equalities. Theorem 2.9 therefore leads, in the special case $n = 2$, to much sharper bounds on the values of the relevant sums of the form $\sum_{I\in \mathrm{IM}_{p,n}} m_I(A, K_\infty/k')$ than are given by (2), as well as to much more precise statements than the finiteness claim provided by Corollary 2.3(iii).

Furthermore, by increasing inductively the value of n, one can use our methods to obtain similar such improvements for any given, arbitrarily large natural number n. In the following result, in order to illustrate how to obtain statements as sharp as possible, we consider only the simplest (non-trivial) instance of this phenomenom, namely with $n = 3$, $\mu = 0$ and $\lambda = 1$ (so that all the relevant kernels of capitulation are actually cyclic as abelian groups), and leave the computation of any other such examples to an interested reader.

Before proceeding, we define two $\mathbb{Z}_p[C_n]$ lattices to be ‘isomorphic up to permutation module’ if there are isomorphisms of $\mathbb{Z}_p[C_n]$-modules of the form

$$M \cong R \oplus \bigoplus_{i=0}^{i=n} \mathbb{Z}_p[C_i]^{a_i} \quad \text{and} \quad N \cong R \oplus \bigoplus_{i=0}^{i=n} \mathbb{Z}_p[C_i]^{b_i} \tag{6}$$

for a suitable $\mathbb{Z}_p[C_n]$-lattice R and non-negative integers a_i and b_i.

For any extension M of k and each natural number n we define a set of $\mathbb{Z}_p[C_n]$-modules by setting

$$\mathrm{MW}_{M,n} := \{A(F)_p : F/k' \text{ cyclic of degree } p^n, k \subseteq k' \subset F \subseteq M, k'/k \text{ finite }\}$$

(with, in each case, $A(F)_p$ regarded as a $\mathbb{Z}_p[C_n]$-module via some choice of isomorphism of $G_{F/k'}$ with C_n). For each lattice I in $\mathrm{IM}_{p,n}$ we also write $m_I(A, M)$ for the maximal multiplicity with which I occurs in the Krull-Schmidt decompositions of the elements of $\mathrm{MW}_{M,n}$.

THEOREM 2.10. *We assume the hypotheses and notation of Theorem* 2.1. *We assume further that, for every cyclic extension L/E of degree dividing p^3 with $k \subseteq E \subset L \subseteq K_\infty$ and E/k finite, the module $T^{L}(A/E)$ is cyclic as an abelian group.*

Then the set of $\mathbb{Z}_p[C_3]$-lattices $\mathrm{MW}_{K_\infty,3}$ contains only finitely many isomorphism up to permutation module classes, and in fact at most $p + 20$ of them.

Furthermore, $m_I(A, K_\infty) \le 1$ for every $I \in \mathrm{IM}_{p,3}$, and there at most $p + 15$ elements of $\mathrm{IM}_{p,3}$ for which $m_I(A, K_\infty) = 1$. In particular,

$$\sum_{I\in \mathrm{IM}_{p,3}} m_I(A, K_\infty) \le p + 15\,.$$

REMARK 2.11. (i) If one fixes a finite extension k' of k in K_∞ and only assumes that the module $T^{L}(A/E)$ is cyclic as an abelian group for all extensions L/E that are contained in cyclic extensions of k' in K_∞ of degree p^3, then our methods still prove that

$$\sum_{I\in \mathrm{IM}_{p,3}} m_I(A, K_\infty/k') \le p+15\,.$$

(ii) The upper bound $p+15$ improves upon the corresponding bound $\rho_3 = 4p+24$ given in Theorem 2.7. In particular, in the situation of Example 2.8, the hypotheses of Theorem 2.10 are satisfied (with $K_\infty = k_\infty$) and therefore the latter result leads to an improvement upon the upper bound for $\sum_{I\in\mathrm{IM}_{p,3}} m_I(A, k_\infty/k_m)$ given there.
(iii) Let A be an abelian variety defined over a number field k. Let p be an odd prime that does not divide the order of the torsion subgroup of $A(k)$ and let M be a pro-p extension of k. In this greater level of generality, our proof of Theorem 2.10 still leads to the same conclusions (with M in place of K_∞) if one imposes the cyclicity hypothesis on all relevant Tate-cohomology groups of the form $\hat{H}^{-1}(G_{L/E}, A(L)_p)$.

3. The invariants μ and λ

Throughout this section, we assume the notation and hypotheses of Theorem 2.1 and prove the following intermediate result.

PROPOSITION 3.1. *There exist non-negative integers λ and μ, which depend only upon the structure of the $\mathbb{Z}_p[[G_{N_\infty/N}]]$-module $X_p(A/N_\infty)$ as N varies over intermediate fields of K/k, with the following property: for every finite extension k' of k in K_∞, every natural number n, every cyclic extension F of k' in K_∞ of degree p^n with $\text{Ш}(A/F)_p$ finite and every subgroup J of $G_{F/k'}$ one has*

$$\mathrm{rk}_p(\hat{H}^{-1}(J, A(F)_p)) \le \lambda + p^n[k':k]\mu\,.$$

Furthermore, each $\mathbb{Z}_p[[G_{N_\infty/N}]]$-module $X_p(A/N_\infty)$ is finitely generated and, if each of their respective μ-invariants vanishes, then the claim above remains valid if one sets $\mu := 0$.

Let k', n, F and J determine data as in the statement of Proposition 3.1. We write F^J_∞ for the $\mathbb{Z}_p$-extension $F^J k_\infty$ of F^J and also then set $\Lambda_{F^J} := \mathbb{Z}_p[[G_{F^J_\infty/F^J}]]$.

In order to prove Proposition 3.1, we will require the following intermediate results.

LEMMA 3.2. (i) *The natural restriction map* $\mathrm{Sel}_p(A/F^J) \to \mathrm{Sel}_p(A/F)^J$ *is an isomorphism of $\mathbb{Z}_p[G_{F^J/k'}]$-modules.*
(ii) *The* (*dual of*) *the natural restriction map*

$$H_0(G_{F^J_\infty/F^J}, X_p(A/F^J_\infty)) \to X_p(A/F^J)$$

is an isomorphism of $\mathbb{Z}_p$-modules.

PROOF. The conditions imposed in the first paragraph of Theorem 2.1, combined with (the proof of) [5, Lem. 3.4], ensure that A satisfies the hypotheses of Greenberg's result [8, Prop. 5.6] with respect to both the field extension F/k' and the field extension F^J_∞/F^J, and so the latter result precisely gives both of the required claims. □

The following result is a natural modification of [5, Prop. 3.1].

LEMMA 3.3. *The Tate cohomology group $\hat{H}^{-1}(J, A(F)_p)$ is isomorphic as a $\mathbb{Z}_p[G_{F^J/k'}]$-module to $T^F(A/F^J)$.*

PROOF. We have a commutative diagram of $\mathbb{Z}_p[G_{F^J/k'}]$-modules

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}} A\big(F^J\big) \arrow[r] \arrow[d, "\iota^F_{F^J}"] & \mathrm{Sel}_p(A/F^J) \arrow[r] \arrow[d, "\mathrm{res}^{F^J}_F"] & Ш(A/F^J)_p \arrow[r] \arrow[d, "\pi^F_{F^J}"] & 0 \\
0 \arrow[r] & \big(\mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}} A(F)\big)^J \arrow[r] & \mathrm{Sel}_p(A/F)^J \arrow[r] & Ш(A/F)_p\,. &
\end{tikzcd}$$

In this diagram the rows are exact and $\iota^F_{F^J}$ denotes the homomorphism that is induced by the inclusion $A(F^J) \subseteq A(F)$. Since the map $\mathrm{res}^{F^J}_F$ is bijective by Lemma 3.2(i), we may apply the snake lemma to the diagram to deduce that $T^F(A/F^J)$ is naturally isomorphic to $\mathrm{cok}(\iota^F_{F^J})$ and so it is enough to show that the latter module is also isomorphic to $\hat{H}^{-1}(J, A(F)_p)$.

Now the fact that p does not divide the order of the torsion subgroup of $A(k)$ ensures that $A(F)$ has no p-torsion and hence that there is a natural short exact sequence

$$0 \longrightarrow A(F)_p \longrightarrow \mathbb{Q}_p \otimes_{\mathbb{Z}} A(F) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}} A(F) \longrightarrow 0\,.$$

Taking cohomology this sequence in turn gives a natural exact sequence of $\mathbb{Z}_p[G_{F^J/k'}]$-modules

$$0 \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}} A\big(F^J\big) \xrightarrow{\iota^F_{F^J}} \Big(\mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}} A(F)\Big)^J \longrightarrow \hat{H}^1\big(J, A(F)_p\big) \longrightarrow 0$$

and hence an isomorphism $\mathrm{cok}(\iota^F_{F^J}) \cong \hat{H}^1(J, A(F)_p)$. But, since $G_{F/k'}$ is cyclic, the latter module is isomorphic to $\hat{H}^{-1}(J, A(F)_p)$. □

LEMMA 3.4. $\mathrm{rk}_p(\hat{H}^{-1}(J, A(F)_p)) \le \mathrm{rk}_p(H_0(G_{F^J_\infty/F^J}, X_p(A/F^J_\infty))_{\mathrm{tor}})$.

PROOF. Lemma 3.3, the definition of $T^F(A/F^J)$, the fact that $\hat{H}^{-1}(J, A(F)_p)$ is a finite group and the assumption that so is $Ш(A/F)_p$ combine to imply that

$$\begin{aligned}
\mathrm{rk}_p(\hat{H}^{-1}(J, A(F)_p)) &= \mathrm{rk}_p(T^F(A/F^J)) \\
&\le \mathrm{rk}_p(Ш(A/F^J)_p) \\
&= \mathrm{rk}_p(Ш(A/F^J)_p^\vee) \\
&= \mathrm{rk}_p(X_p(A/F^J)_{\mathrm{tor}})
\end{aligned}$$

$$= \mathrm{rk}_p(H_0(G_{F^J_\infty/F^J}, X_p(A/F^J_\infty))_{\mathrm{tor}}),$$

where the last equality is a consequence of Lemma 3.2(ii). □

In order to prove Proposition 3.1, we first note that Lemma 3.2(ii) ensures that the Λ_{F^J}-module $X_p(A/F^J_\infty)$ is finitely generated. In particular, if N is any intermediate field of K/k, any choice of data k', n, F, J with $F^J = N$ (such as, for example, taking k' to be N itself and taking the subgroup J to be the group $G_{F/k'} = G_{F/N}$ itself) implies that the Λ_N-module $X_p(A/N_\infty)$ is finitely generated, as was explicitly claimed in Proposition 3.1.

Furthermore, we may now apply the general result of [4, Lem. 3.6] (in the special case of a complex comprising a single non-trivial, finitely generated module $X_p(A/F^J_\infty)$) to obtain a natural analogue

$$\mathrm{rk}_p(H_0(G_{F^J_\infty/F^J}, X_p(A/F^J_\infty))_{\mathrm{tor}}) \leq \mu_{F^J}(X_p(A/F^J_\infty)) + \lambda_{F^J_\infty}$$

of the inequality [4, (15)], where $\mu_{F^J}(X_p(A/F^J_\infty))$ is the μ-invariant of the Λ_{F^J}-module $X_p(A/F^J_\infty)$ and $\lambda_{F^J_\infty}$ is a non-negative integer that depends only upon the field F^J_∞. By arguing exactly as in the two paragraphs that follow [4, (15)], one then finds that the rational number

$$\mu_{F^J_\infty} := \frac{\mu_{F^J}(X_p(A/F^J_\infty))}{[F^J : k]}$$

depends only on the field F^J_∞ rather than on F^J, and therefore also that the maximum values μ and λ of the respective sets of non-negative integers $\{[N : k] \cdot \mu_{N_\infty}\}$ and $\{\lambda_{N_\infty}\}$ as N ranges over the finitely many intermediate fields of K/k satisfy the inequality

$$\begin{aligned}\mathrm{rk}_p(H_0(G_{F^J_\infty/F^J}, X_p(A/F^J_\infty))_{\mathrm{tor}}) &\leq \mu_{F^J}(X_p(A/F^J_\infty)) + \lambda_{F^J_\infty}\\ &= [F^J : k]\mu_{F^J_\infty} + \lambda_{F^J_\infty} \leq [F : k]\mu + \lambda = p^n[k' : k]\mu + \lambda\,.\end{aligned}$$

This inequality now combines with Lemma 3.4 to complete the proof of Proposition 3.1.

4. Yakovlev's theorem and counting diagrams

In this section we recall a crucial representation-theoretic result due to Yakovlev [14] and refine a counting argument due to Burns [4, §3.2].

Before proceeding, we introduce the defining properties (RK($i+1$)), (EX($i+1$)) and (OR($i+1$)) for the set of matrices M^d_n (and T^d_n) that were mentioned in §1.3.

DEFINITION 4.1. Given an $n \times d$-matrix with integer entries $M = (m_{i,j})_{1\leq i\leq n, 1\leq j\leq d}$ which satisfies conditions (AG(1)) as well as (AG($i+1$)), for each index i with $1 \leq i \leq n-1$, we write $\alpha(i)$ for the integer $0 \leq \alpha(i) \leq d$ with $m_{i,\alpha(i)} = 0$ and $m_{i,\alpha(i)+1} \neq 0$. We then define the following conditions on the pair (M, i):

(RK($i+1$)) $m_{i+1,1}, m_{i+1,2}, \dots, m_{i+1,\alpha(i)} \in \{0,1\}$;
(EX($i+1$)) $m_{i+1,\alpha(i)+1}, m_{i+1,\alpha(i)+2}, \dots, m_{i+1,d}$
$\in \{0,1\} \cup \{x \in \mathbb{Z} : m_{i,\alpha(i)+1} - 1 \le x \le m_{i,d}+1\}$;
(OR($i+1$)) $\sum_{j=1}^{d} m_{i+1,j} \le (\sum_{j=1}^{d} m_{i,j}) + d$.

We now fix a cyclic group G of order p^n and for each integer i with $1 \le i \le n$ write G_i for the subgroup of G of order p^i.

Then the results of [14, Th. 2.4 and Lem. 5.2] combine to imply that if M and N are any $\mathbb{Z}_p[G]$-lattices for which, for each i with $1 \le i \le n$, there exists an isomorphism of $\mathbb{Z}_p[G/G_i]$-modules $\theta_i : \hat{H}^{-1}(G_i, M) \to \hat{H}^{-1}(G_i, N)$ that lies in commutative diagrams (of $\mathbb{Z}_p[G]$-modules)

(7)
$$\begin{tikzcd}
\hat{H}^{-1}(G_i,M) \arrow[r, "C_M^i"] \arrow[d, "\theta_i"'] & \hat{H}^{-1}(G_{i+1},M) \arrow[d, "\theta_{i+1}"] & \hat{H}^{-1}(G_i,M) \arrow[d, "\theta_i"'] & \hat{H}^{-1}(G_{i+1},M) \arrow[l, "R_M^i"'] \arrow[d, "\theta_{i+1}"] \\
\hat{H}^{-1}(G_i,N) \arrow[r, "C_N^i"] & \hat{H}^{-1}(G_{i+1},N) & \hat{H}^{-1}(G_i,N) & \hat{H}^{-1}(G_{i+1},N) \arrow[l, "R_N^i"']
\end{tikzcd}$$

where the horizontal arrows are the natural corestriction and restriction homomorphisms, then M and N are isomorphic up to permutation modules (in the sense of (6)).

In the sequel we follow [4, §3.2] in referring to finite 'double chains' of homomorphisms of $\mathbb{Z}_p[G]$-modules

(8)
$$X_1 \overset{\psi_1}{\to} X_2 \overset{\psi_2}{\to} \cdots \overset{\psi_{n-2}}{\to} X_{n-1} \overset{\psi_{n-1}}{\to} X_n\,, \quad X_1 \overset{\phi_1}{\leftarrow} X_2 \overset{\phi_2}{\leftarrow} \cdots \overset{\phi_{n-2}}{\leftarrow} X_{n-1} \overset{\phi_{n-1}}{\leftarrow} X_n$$

and

$$X'_1 \overset{\psi'_1}{\to} X'_2 \overset{\psi'_2}{\to} \cdots \overset{\psi'_{n-2}}{\to} X'_{n-1} \overset{\psi'_{n-1}}{\to} X'_n\,, \quad X'_1 \overset{\phi'_1}{\leftarrow} X'_2 \overset{\phi'_2}{\leftarrow} \cdots \overset{\phi'_{n-2}}{\leftarrow} X'_{n-1} \overset{\phi'_{n-1}}{\leftarrow} X'_n$$

as 'equivalent' if there exist isomorphisms of $\mathbb{Z}_p[G]$-modules $\iota_i : X_i \to X'_i$ for each index i which together give commutative diagrams

$$\begin{tikzcd}
X_1 \arrow[r, "\psi_1"] \arrow[d, "\iota_1"'] & X_2 \arrow[r, "\psi_2"] \arrow[d, "\iota_2"'] & \dots \arrow[r, "\psi_{n-2}"] & X_{n-1} \arrow[r, "\psi_{n-1}"] \arrow[d, "\iota_{n-1}"'] & X_n \arrow[d, "\iota_n"'] \\
X'_1 \arrow[r, "\psi'_1"] & X'_2 \arrow[r, "\psi'_2"] & \dots \arrow[r, "\psi'_{n-2}"] & X'_{n-1} \arrow[r, "\psi'_{n-1}"] & X'_n
\end{tikzcd}$$

and

$$\begin{tikzcd}
X_1 \arrow[d, "\iota_1"'] & X_2 \arrow[l, "\phi_1"'] \arrow[d, "\iota_2"'] & \dots \arrow[l, "\phi_2"'] & X_{n-1} \arrow[l, "\phi_{n-2}"'] \arrow[d, "\iota_{n-1}"'] & X_n \arrow[l, "\phi_{n-1}"'] \arrow[d, "\iota_n"'] \\
X'_1 & X'_2 \arrow[l, "\phi'_1"'] & \dots \arrow[l, "\phi'_2"'] & X'_{n-1} \arrow[l, "\phi'_{n-2}"'] & X'_n . \arrow[l, "\phi'_{n-1}"']
\end{tikzcd}$$

We also fix a natural number d. In the sequel, given a double chain of the form (8), we will consider the following conditions on it, for each index i:

(a$_i$) X_i is finite of exponent less than or equal to p^i.
(b$_i$) $\mathrm{rk}_p(X_i) \le d$.
(b$_i$') $\mathrm{rk}_p(X_i) \le 1$.
(c$_i$) G_i acts trivially on X_i.
(c$_i$') G acts trivially on X_i.
(d$_i$) $\psi_i \circ \phi_i$ is given by multiplication by p on X_{i+1}.
(d$_i$') $\psi_i \circ \phi_i$ is given by multiplication by p on X_{i+1} and $\phi_i \circ \psi_i$ is given by multiplication by p on X_i.

We then write Θ_n^d, resp. $\Theta_n^{d,\mathrm{triv}}$, resp. Θ_n^{cyc} for the number of non-equivalent double chains of homomorphisms of $\mathbb{Z}_p[G]$-modules of the form (8) which satisfy all of the conditions (a$_i$), (b$_i$), (c$_i$) and (d$_i$), resp. (a$_i$), (b$_i$), (c$_i$') and (d$_i$'), resp. (a$_i$), (b$_i$'), (c$_i$) and (d$_i$').

The following result refines [4, Lem. 3.1].

LEMMA 4.2. *$\Theta_n^d \le \eta_n^d$, $\Theta_n^{d,\mathrm{triv}} \le \tau_n^d$ and $\Theta_n^{\mathrm{cyc}} \le \rho_n$.*

PROOF. We write $e(X)$ for the exponent of a finite abelian p-group.

Given any index i, the category of $\mathbb{Z}_p[G]$-modules X that are finite with $e(X) \le p^i$, $\mathrm{rk}_p(X) \le d$ and trivial action of G_i is equivalent to the category of pairs $(\tilde{X}, \alpha)$ where $\tilde{X}$ is an abelian p-group satisfying $e(\tilde{X}) \le p^i$ and $\mathrm{rk}_p(\tilde{X}) \le d$ and α is an element of $\mathrm{Aut}_{\mathbb{Z}_p}(\tilde{X})$ of order dividing p^{n-i}.

If one fixes a generator g of G, then this equivalence is induced by the assignment $X \mapsto ([X], g_X)$ where $[X]$ is the abelian p-group underlying X and g_X corresponds to the action of g on $\tilde{X}$ and $\mathbb{Z}_p[G]$-homomorphisms $\theta : X \to Y$ correspond to group homomorphisms $[\theta] : [X] \to [Y]$ which satisfy $[\theta] \circ g_X \circ [\theta]^{-1} = g_Y$.

This implies, in particular, that the isomorphism classes of $\mathbb{Z}_p[G]$-modules X that are finite with $e(X) \le p^i$, $\mathrm{rk}_p(X) \le d$ and trivial action of G_i are represented by pairs $(\prod_{j=1}^d C_{m_{i,j}}, \beta_i)$ as $(m_{i,j})_{1\le j\le d}$ runs over all vectors of length d with integer entries satisfying $0 \le m_{i,1} \le m_{i,2} \le \cdots \le m_{i,d} \le i$ and β_i over the set $A((m_{i,j})_{1\le j\le d})_{n-i}$ of conjugacy classes of $\mathrm{Aut}_{\mathbb{Z}_p}(\prod_{j=1}^d C_{m_{i,j}})$ comprising elements of order dividing p^{n-i}.

A trivial version of this same argument implies that the isomorphism classes of $\mathbb{Z}_p[G]$-

modules X that are finite with $e(X) \leq p^i$, $\mathrm{rk}_p(X) \leq d$ and trivial action of G are represented by the modules $\prod_{j=1}^{d} C_{t_{i,j}}$ as $(t_{i,j})_{1\leq j\leq d}$ runs over all vectors of length d with integer entries satisfying $0 \leq t_{i,1} \leq t_{i,2} \leq \cdots \leq t_{i,d} \leq i$.

Via Lemma 4.3 below, it is then clear that any double chain of the form (8) which satisfies all of the conditions (a$_i$), (b$_i$), (c$_i$) and (d$_i$) is equivalent to a double chain of the form

$$\Big[\prod_{j=1}^{d} C_{m_{1,j}}, \beta_1\Big] \overset{\psi_1}{\to} \Big[\prod_{j=1}^{d} C_{m_{2,j}}, \beta_2\Big] \overset{\psi_2}{\to} \dots \overset{\psi_{n-2}}{\to} \Big[\prod_{j=1}^{d} C_{m_{n-1,j}}, \beta_{n-1}\Big] \overset{\psi_{n-1}}{\to} \Big[\prod_{j=1}^{d} C_{m_{n,j}}, \beta_n\Big],$$

$$\Big[\prod_{j=1}^{d} C_{m_{1,j}}, \beta_1\Big] \overset{\phi_1}{\leftarrow} \Big[\prod_{j=1}^{d} C_{m_{2,j}}, \beta_2\Big] \overset{\phi_2}{\leftarrow} \dots \overset{\phi_{n-2}}{\leftarrow} \Big[\prod_{j=1}^{d} C_{m_{n-1,j}}, \beta_{n-1}\Big] \overset{\phi_{n-1}}{\leftarrow} \Big[\prod_{j=1}^{d} C_{m_{n,j}}, \beta_n\Big]$$

where each $[\prod_{j=1}^{d} C_{m_{i,j}}, \beta_i]$ is the $\mathbb{Z}_p[G]$-module which corresponds to some choice of matrix $M := (m_{i,j})_{1\leq i\leq n, 1\leq j\leq d}$ that belongs to M_n^d and of β_i in $A((m_{i,j})_{1\leq j\leq d})_{n-i}$.

Similarly, via double applications of Lemma 4.3 below, any double chain of the form (8) which satisfies all of the conditions (a$_i$), (b$_i$), (c$_i$') and (d$_i$') is equivalent to a double chain of the form

$$\Big[\prod_{j=1}^{d} C_{t_{1,j}}\Big] \overset{\psi_1}{\to} \Big[\prod_{j=1}^{d} C_{t_{2,j}}\Big] \overset{\psi_2}{\to} \dots \overset{\psi_{n-2}}{\to} \Big[\prod_{j=1}^{d} C_{t_{n-1,j}}\Big] \overset{\psi_{n-1}}{\to} \Big[\prod_{j=1}^{d} C_{t_{n,j}},\Big],$$

$$\Big[\prod_{j=1}^{d} C_{t_{1,j}}\Big] \overset{\phi_1}{\leftarrow} \Big[\prod_{j=1}^{d} C_{t_{2,j}}\Big] \overset{\phi_2}{\leftarrow} \dots \overset{\phi_{n-2}}{\leftarrow} \Big[\prod_{j=1}^{d} C_{t_{n-1,j}}\Big] \overset{\phi_{n-1}}{\leftarrow} \Big[\prod_{j=1}^{d} C_{t_{n,j}}\Big]$$

where each $[\prod_{j=1}^{d} C_{t_{i,j}}]$ is the $\mathbb{Z}_p[G]$-module which corresponds to some choice of matrix $T := (t_{i,j})_{1\leq i\leq n, 1\leq j\leq d}$ that belongs to T_n^d.

It is therefore clear that Θ_n^d is at most

$$\begin{aligned}
&\sum_{(M,\beta_1,\dots,\beta_n)} \prod_{i=1}^{n-1} \Big|\mathrm{Hom}_{\mathbb{Z}_p[G]}\Big(\Big[\prod_{k=1}^{d} C_{m_{i,k}}, \beta_i\Big], \\
&\qquad\qquad \Big[\prod_{l=1}^{d} C_{m_{i+1,l}}, \beta_{i+1}\Big]\Big)\Big| \cdot \Big|\mathrm{Hom}_{\mathbb{Z}_p[G]}\Big(\Big[\prod_{l=1}^{d} C_{m_{i+1,l}}, \beta_{i+1}\Big], \Big[\prod_{k=1}^{d} C_{m_{i,k}}, \beta_i\Big]\Big)\Big| \\
\leq &\sum_{(M,\beta_1,\dots,\beta_n)} \prod_{i=1}^{n-1} \Big|\mathrm{Hom}_{\mathbb{Z}}\Big(\prod_{k=1}^{d} C_{m_{i,k}}, \prod_{l=1}^{d} C_{m_{i+1,l}}\Big)\Big| \cdot \Big|\mathrm{Hom}_{\mathbb{Z}}\Big(\prod_{l=1}^{d} C_{m_{i+1,l}}, \prod_{k=1}^{d} C_{m_{i,k}}\Big)\Big| \\
= &\sum_{M\in M_n^d} \Big(\prod_{i=1}^{n} a_{M,i}\Big) \prod_{i=1}^{n-1} \Big|\mathrm{Hom}_{\mathbb{Z}}\Big(\prod_{k=1}^{d} C_{m_{i,k}}, \prod_{l=1}^{d} C_{m_{i+1,l}}\Big)\Big| \cdot \Big|\mathrm{Hom}_{\mathbb{Z}}\Big(\prod_{l=1}^{d} C_{m_{i+1,l}}, \prod_{k=1}^{d} C_{m_{i,k}}\Big)\Big|
\end{aligned}$$

$$= \sum_{M\in M_n^d} a_M \prod_{i=1}^{n-1} \prod_{1\le k,l\le d} \left|\mathrm{Hom}_{\mathbb{Z}}\Big(C_{m_{i,k}}, C_{m_{i+1,l}}\Big)\right| \cdot \left|\mathrm{Hom}_{\mathbb{Z}}\Big(C_{m_{i+1,l}}, C_{m_{i,k}}\Big)\right|$$

$$= \sum_{M\in M_n^d} a_M \prod_{i=1}^{n-1} \prod_{1\le k,l\le d} (p^{\min\{m_{i,k},m_{i+1,l}\}})^2$$

$$= \sum_{M\in M_n^d} a_M \cdot p^{2\cdot\sum_{i=1}^{n-1}\sum_{1\le k,l\le d}\min\{m_{i,k},m_{i+1,l}\}},$$

which is precisely the definition of η_n^d.

Similarly, $\Theta_n^{d,\mathrm{triv}}$ is at most

$$\sum_{T\in T_n^d} \prod_{i=1}^{n-1} \left|\mathrm{Hom}_{\mathbb{Z}_p[G]}\Big(\Big[\prod_{k=1}^{d} C_{t_{i,k}}\Big], \Big[\prod_{l=1}^{d} C_{t_{i+1,l}}\Big]\Big)\right| \cdot \left|\mathrm{Hom}_{\mathbb{Z}_p[G]}\Big(\Big[\prod_{l=1}^{d} C_{t_{i+1,l}}\Big], \Big[\prod_{k=1}^{d} C_{t_{i,k}}\Big]\Big)\right|$$

$$= \sum_{T\in T_n^d} \prod_{i=1}^{n-1} \left|\mathrm{Hom}_{\mathbb{Z}}\Big(\prod_{k=1}^{d} C_{t_{i,k}}, \prod_{l=1}^{d} C_{t_{i+1,l}}\Big)\right| \cdot \left|\mathrm{Hom}_{\mathbb{Z}}\Big(\prod_{l=1}^{d} C_{t_{i+1,l}}, \prod_{k=1}^{d} C_{t_{i,k}}\Big)\right|$$

$$= \sum_{T\in T_n^d} p^{2\cdot\sum_{i=1}^{n-1}\sum_{1\le k,l\le d}\min\{t_{i,k},t_{i+1,l}\}},$$

which is precisely the definition of τ_n^d.

In order to prove that $\Theta_n^{\mathrm{cyc}} \le \rho_n$, we first note that $R_n = T_n^1 \subseteq M_n^1$ and that an explicit computation proves that, for any $R = (r_i) \in R_n$, one has

$$a_{R,i} = p^{\max\{0,\min\{r_i-1,n-i\}\}}. \tag{9}$$

Now, using once again Lemma 4.3 below, it is elementary to show that any double chain of the form (8) which satisfies all of the conditions (a$_i$), (b$_i$'), (c$_i$) and (d$_i$') is equivalent to a double chain of the form

$$[C_{r_1},\beta_1] \overset{\psi_1}{\to} [C_{r_2},\beta_2] \overset{\psi_2}{\to} \cdots \overset{\psi_{n-2}}{\to} [C_{r_{n-1}},\beta_{n-1}] \overset{\psi_{n-1}}{\to} [C_{r_n},\beta_n],$$
$$[C_{r_1},\beta_1] \overset{\phi_1}{\leftarrow} [C_{r_2},\beta_2] \overset{\phi_2}{\leftarrow} \cdots \overset{\phi_{n-2}}{\leftarrow} [C_{r_{n-1}},\beta_{n-1}] \overset{\phi_{n-1}}{\leftarrow} [C_{r_n},\beta_n]$$

where each $[C_{r_i},\beta_i]$ is the $\mathbb{Z}_p[G]$-module which corresponds to some choice of vector $R := (r_i)_{1\le i\le n}$ that belongs to R_n and of β_i in $A((r_i))_{n-i}$, and furthermore in which each of the arrows can be taken to be as follows:

- If $r_{i+1} = 1 = r_i$, then (ψ_i,ϕ_i) is either $(0,0)$ or $(0,1)$ or $(1,0)$.
- If $r_{i+1} = r_i > 1$, then (ψ_i,ϕ_i) is either $(1,p)$ or $(p,1)$.
- If $r_{i+1} = r_i - 1$, then (ψ_i,ϕ_i) is $(1,p)$.
- If $r_{i+1} = r_i + 1$, then (ψ_i,ϕ_i) is $(p,1)$.

- If $r_{i+1} = 0 = r_i$, then (ψ_i, ϕ_i) is $(0, 0)$.

Recalling the explicit definition (1) of $h_{r_i,r_{i+1}}$ and using (9), it is therefore clear that Θ_n^{cyc} is at most

$$\sum_{(R,\beta_1,\dots,\beta_n)} \prod_{i=1}^{n-1} h_{r_i,r_{i+1}} = \sum_{R\in R_n} a_R \prod_{i=1}^{n-1} h_{r_i,r_{i+1}} = \sum_{R\in R_n} \left(\prod_{i=1}^{n-1} h_{r_i,r_{i+1}}\right) p^{\sum_{i=1}^{n-1} \max\{0,\min\{r_i-1,n-i\}\}},$$

which is precisely the definition of ρ_n. □

LEMMA 4.3. *Let $M = (m_{k,j})_{k\in\{i,i+1\},1\le j\le d}$ be a $2 \times d$ matrix with integer entries which satisfy $0 \le m_{k,j} \le m_{k,j+1}$ for every k and j. If there exist $\psi \in \mathrm{Hom}_{\mathbb{Z}}(\prod_{j=1}^d C_{m_{i,j}}, \prod_{j=1}^d C_{m_{i+1,j}})$ and $\phi \in \mathrm{Hom}_{\mathbb{Z}}(\prod_{j=1}^d C_{m_{i+1,j}}, \prod_{j=1}^d C_{m_{i,j}})$ with the property that $\psi \circ \phi$ is given by multiplication by p on $\prod_{j=1}^d C_{m_{i+1,j}}$, then M satisfies conditions* (RK($i + 1$)), (EX($i + 1$)) *and* (OR($i + 1$)).

PROOF. Condition (RK($i + 1$)) holds because $\mathrm{rk}_p(p \cdot \prod_{j=1}^d C_{m_{i+1,j}}) \le \mathrm{rk}_p(\mathrm{im}(\psi)) \le \mathrm{rk}_p(\prod_{j=1}^d C_{m_{i,j}})$.

To prove that condition (EX($i + 1$)) holds, we first note that if there exists an index j with $2 \le m_{i+1,j} \le m_{i,\alpha(i)+1} - 2$, then there exists an element x of $\prod_{j=1}^d C_{m_{i+1,j}}$ that is not divisible by p and has order larger than p with the property that $\phi(x)$ is divisible by p^2. But then $p \cdot x = \psi(\phi(x))$ would be divisible by p^2, which would contradict the choice of x.

Similarly, if $m_{i+1,d} \ge m_{i,d} + 2$, then the projection to $C_{m_{i+1,d}}$ of any element of $\mathrm{im}(\psi) \supseteq \mathrm{im}(\psi \circ \phi)$ is divisible by p^2, contradicting our hypothesis. We have thus proved that condition (EX($i + 1$)) holds.

Condition (OR($i + 1$)) holds because

$$\begin{aligned} p^{(\sum_{j=1}^d m_{i,j})+d} &= \left|\prod_{j=1}^d C_{m_{i,j}}\right| p^d \ge \left|\mathrm{im}(\psi)\right| p^d \ge \left|p \cdot \prod_{j=1}^d C_{m_{i+1,j}}\right| p^d \\ &\ge \left|p \cdot \prod_{j=1}^d C_{m_{i+1,j}}\right| \left|\left(\prod_{j=1}^d C_{m_{i+1,j}}\right)[p]\right| = \left|\prod_{j=1}^d C_{m_{i+1,j}}\right| = p^{\sum_{j=1}^d m_{i+1,j}}. \end{aligned}$$

□

For any natural number d we now write Lat_G^d for the set of $\mathbb{Z}_p[G]$-lattices N for which one has $\mathrm{rk}_p(\hat{H}^{-1}(G_i, N)) \le d$ for all i with $1 \le i \le n$. Similarly, we write $\mathrm{Lat}_G^{d,\mathrm{triv}}$ for the set of $\mathbb{Z}_p[G]$-lattices N for which, for all $1 \le i \le n$, one has both that $\mathrm{rk}_p(\hat{H}^{-1}(G_i, N)) \le d$ and that G acts trivially on $\hat{H}^{-1}(G_i, N)$.

For each I in $\mathrm{IM}_{p,n}$ we also write m_I^d, resp. $m_I^{d,\mathrm{triv}}$, for the maximal multiplicity with which I occurs as a direct summand of any lattice in Lat_G^d, resp. in $\mathrm{Lat}_G^{d,\mathrm{triv}}$.

The following result refines [4, Lem. 3.2].

LEMMA 4.4. *For any natural number d, one has $\sum_{I\in \mathrm{IM}_{p,n}} m_I^d \leq \eta_n^d$ and also $\sum_{I\in \mathrm{IM}_{p,n}} m_I^{d,\mathrm{triv}} \leq \tau_n^d$. Furthermore, we also have $\sum_{I\in \mathrm{IM}_{p,n}} m_I^1 \leq \rho_n$.*

PROOF. The key point is that, for any N in Lat_G^d, the double chain of homomorphisms of $\mathbb{Z}_p[G]$-modules determined by the modules $\hat{H}^{-1}(G_i, N)$ together with the homomorphisms C_N^i and R_N^i satisfies all of the conditions (a$_i$), (b$_i$), (c$_i$) and (d$_i$). Indeed, all of them are well-known facts in the Tate-cohomology theory of finite groups.

It is also well-known that $R_N^i \circ C_N^i$ is given by the action of the norm element N_{G_{i+1}/G_i} on $\hat{H}^{-1}(G_i, N)$ and, if either G acts trivially on $\hat{H}^{-1}(G_i, N)$ or $\mathrm{rk}_p(\hat{H}^{-1}(G_i, N)) \leq 1$, then it is straightforward to verify that the action of N_{G_{i+1}/G_i} also coincides with multiplication by p on $\hat{H}^{-1}(G_i, N)$. It is therefore also true that for any N in $\mathrm{Lat}_G^{d\mathrm{triv}}$, resp. in Lat_G^1, the double chain of homomorphisms of $\mathbb{Z}_p[G]$-modules determined by the modules $\hat{H}^{-1}(G_i, N)$ together with the homomorphisms C_N^i and R_N^i satisfies all of the conditions (a$_i$), (b$_i$), (c$_i$') and (d$_i$'), resp. (a$_i$), (b$_i$'), (c$_i$) and (d$_i$').

Now, for each I in $\mathrm{IM}_{p,n}$, the lattice $I^{m_I^d}$ belongs to Lat_G^d. In addition, for each I and J in $\mathrm{IM}_{p,n}$ and each pair of natural numbers a and b, the $\mathbb{Z}_p[G]$-lattices I^a and J^b are isomorphic, or equivalently (by Yakovlev's Theorem) the respective double chains that they determine are equivalent, if and only if $I = J$ and $a = b$.

These observations imply that the modules $N = I^a$, for I in $\mathrm{IM}_{p,n}$ and $1 \leq a \leq m_I^d$, account for at least $\sum_{I\in \mathrm{IM}_{p,n}} m_I^d$ of the at most Θ_n^d non-equivalent double chains satisfying all of the conditions (a$_i$), (b$_i$), (c$_i$) and (d$_i$) and so Lemma 4.2 in turn implies that $\sum_{I\in \mathrm{IM}_{p,n}} m_I^d \leq \eta_n^d$.

The exact same considerations also lead one to conclude, via Lemma 4.2, that $\sum_{I\in \mathrm{IM}_{p,n}} m_I^{d,\mathrm{triv}} \leq \tau_n^d$and that $\sum_{I\in \mathrm{IM}_{p,n}} m_I^1 \leq \rho_n$. □

5. The proofs of the main results

5.1. The proofs of Theorem 2.1, Theorem 2.5 and Theorem 2.7.

Proposition 3.1 implies the existence of non-negative integers λ and μ of the kind specified in Theorem 2.1. It furthermore implies that, for every finite extension k' of k in K_∞, every natural number n and every cyclic extension F of k' of degree p^n with $\text{Ш}(A/F)_p$ finite, the $\mathbb{Z}_p[G_{F/k'}]$-lattice $A(F)_p$ belongs to the set $\mathrm{Lat}_{C_n}^d$ (as defined in §4) for $d := \lambda + p^n[k' : k]\mu$. For any I in $\mathrm{IM}_{p,n}$ we therefore have that $m_I(A, K_\infty/k') \leq m_I^d$ and so by Lemma 4.4 we conclude that

$$\sum_{I\in \mathrm{IM}_{p,n}} m_I(A, K_\infty/k') \leq \eta_n^d\,.$$

This completes the proof of Theorem 2.1.

Similarly, if F is chosen so that, for every intermediate field E of F/k', the module $T^F(A/E)$ has trivial (natural) action of $G_{F/k'}$, resp. is cyclic as an abelian group, then Lemma 3.3 combines with Proposition 3.1 to ensure that the $\mathbb{Z}_p[G_{F/k'}]$-lattice $A(F)_p$ belongs to the set $\mathrm{Lat}_{C_n}^{d,\mathrm{triv}}$ for $d := \lambda + p^n[k' : k]\mu$, resp. directly implies that the $\mathbb{Z}_p[G_{F/k'}]$-lattice $A(F)_p$ belongs to the set $\mathrm{Lat}_{C_n}^1$. For any I in $\mathrm{IM}_{p,n}$ we therefore have that $m_I^{\mathrm{triv}}(A, K_\infty/k') \leq m_I^{d,\mathrm{triv}}$, resp. that $m_I^{\mathrm{cyc}}(A, K_\infty/k') \leq m_I^1$, and so by Lemma 4.4 we conclude that

$$\sum_{I\in\mathrm{IM}_{p,n}} m_I^{\mathrm{triv}}(A, K_\infty/k') \leq \tau_n^d\,,$$

resp. that

$$\sum_{I\in\mathrm{IM}_{p,n}} m_I^{\mathrm{cyc}}(A, K_\infty/k') \leq \rho_n\,.$$

We have therefore proved both Theorem 2.5 and Theorem 2.7.

5.2. The proof of Corollary 2.3. The choice of non-negative integers λ and μ as specified by Theorem 2.1 is made via Proposition 3.1, and therefore the final claim of the latter result leads, under the hypotheses of Corollary 2.3, to an inequality

$$\sum_{I\in\mathrm{IM}_{p,n}} m_I(A, K_\infty/k') \leq \eta_n^\lambda \tag{10}$$

by setting $\mu := 0$ in (2). This last inequality gives a bound on $\sum_{I\in\mathrm{IM}_{p,n}} m_I(A, K_\infty/k')$ that does not depend on the choice of field k', precisely as required by claim (i) of Corollary 2.3.

We next keep n fixed but allow k' to vary over finite extensions of k in K_∞ and F over cyclic extension of k' of degree p^n in K_∞ with $Ш(A/F)_p$ finite. The Krull-Schmidt theorem then gives isomorphisms of $\mathbb{Z}_p[C_n]$-modules of the form

$$A(F)_p \cong \left(\bigoplus_{i=0}^{i=n} \mathbb{Z}_p[C_i]^{s_{F/k',i}}\right) \oplus \bigoplus_{I\in\mathrm{IM}_{p,n}} I^{s_{F/k',I}} \tag{11}$$

where each integer $s_{F/k',i}$ is non-negative and each integer $s_{F/k',I}$ is both non-negative and at most $m_I(A, K_\infty/k')$. In addition, since the inequality (10) implies that for each I in $\mathrm{IM}_{p,n}$ the maximal multiplicity $m_I(A, K_\infty/k')$ is finite and is non-zero for only finitely many I, and also that the sum $\sum_{I\in\mathrm{IM}_{p,n}} m_I(A, K_\infty/k')$ is bounded independently of k', the $\mathbb{Z}_p$-rank of the modules $R_{F/k'} := \bigoplus_{I\in\mathrm{IM}_{p,n}} I^{s_{F/k',I}}$ is bounded as k' and F range over all possible choices. The isomorphism (11) is therefore a direct sum decomposition of the required form (3), and this observation completes the proof of claim (ii) of Corollary 2.3.

Claim (iii) of Corollary 2.3 is now a direct consequence of the fact there are only finitely many $\mathbb{Z}_p[C_n]$-lattices of any given rank up to isomorphism.

REMARK 5.1. If, under the hypotheses of Corollary 2.3, for each intermediate field N of K/k one knows $X_p(A/N_\infty)$ explicitly (as a $\mathbb{Z}_p[[G_{N_\infty/N}]]$-module), then one can compute explicitly the upper bounds $\mathrm{rk}_p(\hat{H}^{-1}(J, A(F)_p)) \leq \lambda = \max_N\{\lambda_{N_\infty}\}$ given by Proposition 3.1. This is because, via the proof of [4, Lem. 3.6], each term λ_{N_∞} depends only upon the λ-invariant of $X_p(A/N_\infty)$ and upon the p-ranks of the finite modules N_1, N_2 and N_3 that occur in loc. cit. (with the relevant complex comprising a single non-trivial module $X_p(A/N_\infty)$ placed in degree i). We also note in passing that, under the additional hypotheses of Example 2.6, one can equivalently obtain the upper bounds $\mathrm{rk}_p(\hat{H}^{-1}(J, A(F)_p)) \leq \lambda$ by simply taking λ to be as defined in (5).

The explicit computation of these bounds in turn gives an explicit bound on the sizes of each of the groups that occurs in the diagrams (7). One can therefore also compute an explicit upper bound for the total number of possible diagrams (7) and, via the isomorphisms (6), this leads to an explicit upper bound for the number of isomorphism classes of indecomposable $\mathbb{Z}_p[C_n]$-lattices which can arise as direct summands of $A(F)_p$ as F varies as in Corollary 2.3(iii).

6. Indecomposable $\mathbb{Z}_p[C_3]$-lattices

6.1. The proof of Theorem 2.10. The validity of Theorem 2.10 will follow readily from that of the following auxiliary result.

PROPOSITION 6.1. *Assume the notation and hypotheses of Theorem* 2.10*. Let k' be a finite extension of k in K_∞ and F be a cyclic extension of degree p^3 of k' in K. For $i \in \{1, 2, 3\}$ we write G_i for the subgroup of $G_{F/k'}$ of order p^i. Then the double chain of homomorphisms of* $\mathbb{Z}_p[G_3]$*-modules*

$$\begin{tikzcd} \hat{H}^{-1}(G_3, A(F)_p) \arrow[r, "R^2_{A(F)p}"] & \hat{H}^{-1}(G_2, A(F)_p) \arrow[r, "R^1_{A(F)p}"] & \hat{H}^{-1}(G_1, A(F)_p)\,, \\ \hat{H}^{-1}(G_1, A(F)_p) \arrow[r, "C^1_{A(F)p}"] & \hat{H}^{-1}(G_2, A(F)_p) \arrow[r, "C^2_{A(F)p}"] & \hat{H}^{-1}(G_3, A(F)_p) \end{tikzcd} \tag{12}$$

is equivalent (*in the sense of* §4) *to one of the following*:

(i) $0 \to 0 \to 0\,, \qquad 0 \to 0 \to 0.$

(ii) $C_1 \to 0 \to 0\,, \qquad 0 \to 0 \to C_1\,.$

(iii) $0 \to C_1 \to 0\,, \qquad 0 \to C_1 \to 0.$

(iv) $0 \to 0 \to C_1\,, \qquad C_1 \to 0 \to 0.$

(v) $C_1 \to 0 \to C_1\,, \qquad C_1 \to 0 \to C_1.$

(vi) $0 \to C_1 \xrightarrow{0} C_1\,, \qquad C_1 \xrightarrow{0} C_1 \to 0.$

(vii) $0 \to C_1 \xrightarrow{1} C_1\,, \qquad C_1 \xrightarrow{0} C_1 \to 0.$

(viii) $C_1 \xrightarrow{0} C_1 \to 0\,, \qquad 0 \to C_1 \xrightarrow{0} C_1\,.$

(ix) $C_1 \xrightarrow{1} C_1 \to 0\,, \qquad 0 \to C_1 \xrightarrow{0} C_1\,.$

(x) $C_1 \xrightarrow{0} C_1 \xrightarrow{0} C_1\,, \quad C_1 \xrightarrow{0} C_1 \xrightarrow{0} C_1\,.$

(xi) $C_1 \xrightarrow{1} C_1 \xrightarrow{0} C_1\,, \quad C_1 \xrightarrow{0} C_1 \xrightarrow{0} C_1\,.$

(xii) $C_1 \xrightarrow{0} C_1 \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{0} C_1 \xrightarrow{0} C_1\,.$

(xiii) $C_1 \xrightarrow{0} C_1 \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{0} C_1 \xrightarrow{1} C_1\,.$

(xiv) $C_1 \xrightarrow{1} C_1 \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{0} C_1 \xrightarrow{0} C_1\,.$

(xv) $C_2 \xrightarrow{1} C_1 \to 0\,, \quad 0 \to C_1 \xrightarrow{p} C_2\,.$

(xvi) $C_2 \xrightarrow{1} C_1 \xrightarrow{0} C_1\,, \quad C_1 \xrightarrow{0} C_1 \xrightarrow{p} C_2\,.$

(xvii) $C_2 \xrightarrow{1} C_1 \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{0} C_1 \xrightarrow{p} C_2\,.$

(xviii) $C_2 \xrightarrow{1} C_2 \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{p} C_2 \xrightarrow{p} C_2\,.$

(xix) $C_2 \xrightarrow{p} C_2 \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{p} C_2 \xrightarrow{1} C_2\,.$

(xx) $C_3 \xrightarrow{1} C_2 \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{p} C_2 \xrightarrow{p} C_3\,.$

(r) $C_1 \xrightarrow{p} C_2(\sigma, r) \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{p} C_2(\sigma, r) \xrightarrow{1} C_1\,.$

Here C_i always denotes the $\mathbb{Z}_p[G_3]$-module given by the abelian group C_i with trivial action of G_3. We have also fixed a choice of generator σ of G_3/G_2 and, for any r with $0 \leq r \leq p-1$, written $C_2(\sigma, r)$ for the $\mathbb{Z}_p[G_3]$-module given by the abelian group C_2 with trivial action of G_2 and $\sigma \cdot 1 = rp + 1$.

Before proceeding to prove Proposition 6.1, we explain how the claims given in Theorem 2.10 follow from its validity. In fact, Yakovlev's result discussed in §4 directly implies that the set of $\mathbb{Z}_p[C_3]$-lattices $\mathrm{MW}_{K_\infty,3}$ contains at most $p + 20$ isomorphism up to permutation module classes. Furthermore, since none of the $p+20$ double chains listed above is the direct sum, in the obvious sense, of two or more copies of any possible single double chain, one finds that $m_I(A/K_\infty) \leq 1$ for every $I \in \mathrm{IM}_{p,3}$. Finally, since some of the double chains listed can be decomposed as direct sums of pairs (or triples) of some of the other double chains, it is clear (using once again Yakovlev's theorem) that not all of the $p + 19$ non-trivial double chains can both occur as equivalent to a double chain (12) and be the analogous double chain that would correspond to an indecomposable module. In fact, a closer analysis of the list easily shows that at most $p+15$ of them could possibly do so, and hence there at most $p+15$ elements of $\mathrm{IM}_{p,3}$ for which $m_I(A/K) = 1$, as required.

6.2. The proof of Proposition 6.1. We will require of all the following facts, which are well known.

LEMMA 6.2. *Let M be a $\mathbb{Z}_p[G_3]$-lattice.*

(i) *Via an appropriate choice of generators of each group $H^2(G_i, \mathbb{Z})$, cup products induce isomorphisms of $\mathbb{Z}_p[G_3/G_i]$-modules $\hat{H}^{-1}(G_i, M) \to H^1(G_i, M)$ which commute with restriction and corestriction maps.*

(ii) *For $i \leq j$*, $\mathrm{Cor}_i^j \circ \mathrm{Res}_i^j$ *coincides with multiplication by* p^{j-i} *on* $H^1(G_j, M)$ *and* $\mathrm{Res}_i^j \circ \mathrm{Cor}_i^j$ *coincides with the action of the norm element* N_{G_j/G_i} *on* $H^1(G_i, M)$.
(iii) *The diagrams of* $\mathbb{Z}_p[G_3]$*-modules*

$$\begin{tikzcd}
0 \arrow[r] & H^1(G_3/G_1, M^{G_1}) \arrow[r, "\mathrm{Inf}_1^3"] \arrow[d, "\mathrm{Res}_{2,1}^{3,1}"'] & H^1(G_3, M) \arrow[r, "\mathrm{Res}_1^3"] \arrow[d, "\mathrm{Res}_2^3"'] & H^1(G_1, M)^{G_3/G_1} \arrow[d, "\mathrm{id}"'] \\
0 \arrow[r] & H^1(G_2/G_1, M^{G_1}) \arrow[r, "\mathrm{Inf}_1^2"] & H^1(G_2, M) \arrow[r, "\mathrm{Res}_1^2"] & H^1(G_1, M)^{G_2/G_1}
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & H^1(G_2/G_1, M^{G_1}) \arrow[r, "\mathrm{Inf}_1^2"] \arrow[d, "\mathrm{Cor}_{2,1}^{3,1}"'] & H^1(G_2, M) \arrow[r, "\mathrm{Res}_1^2"] \arrow[d, "\mathrm{Cor}_2^3"'] & H^1(G_1, M)^{G_2/G_1} \arrow[d, "N_{G_3/G_2}"'] \\
0 \arrow[r] & H^1(G_3/G_1, M^{G_1}) \arrow[r, "\mathrm{Inf}_1^3"] & H^1(G_3, M) \arrow[r, "\mathrm{Res}_1^3"] & H^1(G_1, M)^{G_3/G_1}
\end{tikzcd}$$

are commutative and have exact rows.

We next note that the hypotheses of Theorem 2.10 combine with repeated applications of Lemma 3.3 to imply that all of the Tate cohomology groups $\hat{H}^{-1}(G_2, A(F)_p)$, $\hat{H}^{-1}(G_1, A(F)_p)$, $\hat{H}^{-1}(G_3/G_1, A(F^{G_1})_p)$ and $\hat{H}^{-1}(G_2/G_1, A(F^{G_1})_p)$ have p-rank at most 1. Theorem 2.9 therefore implies that $A(F^{G_1})_p$ is isomorphic as a $\mathbb{Z}_p[G_3/G_1]$-module to

$$R_1^b \oplus Z^c \oplus E^d \oplus (R_2, R_1; \lambda_0^0)^{g_0} \oplus (R_2, E; \lambda_0^0)^{h_0} \oplus (R_2, E; \lambda_0^1)^{h_1}$$
$$\oplus (R_2, Z \oplus R_1; 1 \oplus \lambda_0^0)^{j_0} \oplus (R_2, Z \oplus E; 1 \oplus \lambda_0^1)^{k_1}$$

and that $A(F)_p$ is isomorphic as a $\mathbb{Z}_p[G_2]$-module to

$$R_1^{b'} \oplus Z^{c'} \oplus E^{d'} \oplus (R_2, R_1; \lambda_0^0)^{g'_0} \oplus (R_2, E; \lambda_0^0)^{h'_0} \oplus (R_2, E; \lambda_0^1)^{h'_1}$$
$$\oplus (R_2, Z \oplus R_1; 1 \oplus \lambda_0^0)^{j'_0} \oplus (R_2, Z \oplus E; 1 \oplus \lambda_0^1)^{k'_1},$$

in each case for suitable non-negative exponents which satisfy $b + g_0 + h_1 + j_0 + k_1 \leq 1$ and $b' + g'_0 + h'_1 + j'_0 + k'_1 \leq 1$ respectively.

Furthermore, by considering the structure of $A(F^{G_1})_p$ as a $\mathbb{Z}_p[G_2/G_1]$-module, one finds that the only compatible choices for the exponents b, g_0, h_1, j_0, k_1 and $b', g'_0, h'_1, j'_0, k'_1$ are included in the following list of 18 cases: $b+g_0+h_1+j_0+k_1 = 0 = b'+g'_0+h'_1+j'_0+k'_1$; $b + g_0 + h_1 + j_0 + k_1 = 0$ and $h'_1 = 1$; $b + g_0 + h_1 + j_0 + k_1 = 0$ and $k'_1 = 1$; $b = 1$ and $b' + g'_0 + h'_1 + j'_0 + k'_1 = 0$; $b = 1 = h'_1$; $b = 1 = k'_1$; $g_0 = 1 = b'$; $h_1 = 1 = b'$; $j_0 = 1 = b'$; $k_1 = 1 = b'$; $g_0 = 1 = g'_0$; $h_1 = 1 = g'_0$; $j_0 = 1 = g'_0$; $k_1 = 1 = g'_0$; $g_0 = 1 = j'_0$; $h_1 = 1 = j'_0$; $j_0 = 1 = j'_0$; $k_1 = 1 = j'_0$.

The proof of Proposition 6.1 now proceeds as a case by case analysis, through repeated applications of Lemma 6.2 for $M = A(F)_p$. In the process one further finds that the case $j_0 = 1 = g_0'$ and the case $k_1 = 1 = g_0'$ can not actually occur. We will not give all of the details, but rather just describe which of the $p + 20$ double chains listed in Proposition 6.1 can correspond to each of the remaining 16 cases.

If $b + g_0 + h_1 + j_0 + k_1 = 0 = b' + g_0' + h_1' + j_0' + k_1'$ then the double chain of homomorphisms of $\mathbb{Z}_p[G_3]$-modules (12) is equivalent to

$$(i)\ \ 0 \to 0 \to 0\,, \qquad 0 \to 0 \to 0\,.$$

If $b + g_0 + h_1 + j_0 + k_1 = 0$ and $h_1' = 1$ then (12) is equivalent to

$$(vii)\ \ 0 \to C_1 \xrightarrow{1} C_1\,, \qquad C_1 \xrightarrow{0} C_1 \to 0$$

or to

$$(xiv)\ \ C_1 \xrightarrow{1} C_1 \xrightarrow{1} C_1\,, \qquad C_1 \xrightarrow{0} C_1 \xrightarrow{0} C_1\,.$$

If $b + g_0 + h_1 + j_0 + k_1 = 0$ and $k_1' = 1$ then (12) is equivalent to

$$(iv)\ \ 0 \to 0 \to C_1\,, \qquad C_1 \to 0 \to 0\,.$$

If $b = 1$ and $b' + g_0' + h_1' + j_0' + k_1' = 0$ then (12) is equivalent to

$$(ii)\ \ C_1 \to 0 \to 0\,, \qquad 0 \to 0 \to C_1\,.$$

If $b = 1 = h_1'$ then (12) is equivalent to

$$(xii)\ \ C_1 \xrightarrow{0} C_1 \xrightarrow{1} C_1\,, \qquad C_1 \xrightarrow{0} C_1 \xrightarrow{0} C_1$$

or to

$$(xiii)\ \ C_1 \xrightarrow{0} C_1 \xrightarrow{1} C_1\,, \qquad C_1 \xrightarrow{0} C_1 \xrightarrow{1} C_1$$

or to

$$(xvii)\ \ C_2 \xrightarrow{1} C_1 \xrightarrow{1} C_1\,, \qquad C_1 \xrightarrow{0} C_1 \xrightarrow{p} C_2\,.$$

If $b = 1 = k_1'$ then (12) is equivalent to

$$(v)\ \ C_1 \to 0 \to C_1\,, \qquad C_1 \to 0 \to C_1\,.$$

If $g_0 = 1 = b'$ then (12) is equivalent to

$$(xv)\ \ C_2 \xrightarrow{1} C_1 \to 0\,, \qquad 0 \to C_1 \xrightarrow{p} C_2\,.$$

If $h_1 = 1 = b'$ then (12) is equivalent to

$$(ix)\ \ C_1 \xrightarrow{1} C_1 \to 0\,, \qquad 0 \to C_1 \xrightarrow{0} C_1\,.$$

If $j_0 = 1 = b'$ then (12) is equivalent to

$$(viii)\ C_1 \xrightarrow{0} C_1 \to 0\,, \qquad 0 \to C_1 \xrightarrow{0} C_1\,.$$

If $k_1 = 1 = b'$ then (12) is equivalent to

$$(iii)\ 0 \to C_1 \to 0\,, \qquad 0 \to C_1 \to 0\,.$$

If $g_0 = 1 = g_0'$ then (12) is equivalent to

$$(xix)\ C_2 \xrightarrow{p} C_2 \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{p} C_2 \xrightarrow{1} C_2$$

or to

$$(xx)\ C_3 \xrightarrow{1} C_2 \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{p} C_2 \xrightarrow{p} C_3\,.$$

If $h_1 = 1 = g_0'$ then (12) is equivalent to one of the diagrams

$$(r)\ C_1 \xrightarrow{p} C_2(\sigma, r) \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{p} C_2(\sigma, r) \xrightarrow{1} C_1$$

or to

$$(xviii)\ C_2 \xrightarrow{1} C_2 \xrightarrow{1} C_1\,, \quad C_1 \xrightarrow{p} C_2 \xrightarrow{p} C_2\,.$$

If $g_0 = 1 = j_0'$ then (12) is equivalent to

$$(xvi)\ C_2 \xrightarrow{1} C_1 \xrightarrow{0} C_1\,, \quad C_1 \xrightarrow{0} C_1 \xrightarrow{p} C_2\,.$$

If $h_1 = 1 = j_0'$ then (12) is equivalent to

$$(xi)\ C_1 \xrightarrow{1} C_1 \xrightarrow{0} C_1\,, \quad C_1 \xrightarrow{0} C_1 \xrightarrow{0} C_1.$$

If $j_0 = 1 = j_0'$ then (12) is equivalent to

$$(x)\ C_1 \xrightarrow{0} C_1 \xrightarrow{0} C_1\,, \quad C_1 \xrightarrow{0} C_1 \xrightarrow{0} C_1\,.$$

If $k_1 = 1 = j_0'$ then (12) is equivalent to

$$(vi)\ 0 \to C_1 \xrightarrow{0} C_1\,, \qquad C_1 \xrightarrow{0} C_1 \to 0\,.$$

References

[1] W. BLEY and D. MACIAS CASTILLO, Congruences for critical values of higher derivatives of twisted Hasse-Weil L-functions, J. Reine U. Angew. Math. **722** (2017), 105–136.

[2] D. BURNS, On the Galois structure of arithmetic cohomology I: compactly supported p-adic cohomology, to appear in Nagoya Math. J.

[3] D. BURNS and A. KUMON, On the Galois structure of arithmetic cohomology II: ray class groups, to appear in J. Math. Soc. Japan.

[4] D. BURNS, On the Galois structure of arithmetic cohomology III: Selmer groups of critical motives, to appear in Kyoto J. Math.

[5] D. BURNS, D. MACIAS CASTILLO and C. WUTHRICH, On the Galois structure of Selmer groups, Int. Math. Res. Notices **2015** (2015), 11909–11933.

[6] D. BURNS, D. MACIAS CASTILLO and C. WUTHRICH, On Mordell-Weil groups and congruences between derivatives of twisted Hasse-Weil L-functions, to appear in J. Reine U. Angew. Math.

[7] F. E. DIEDERICHSEN, Über die Ausreduktion ganzahliger Gruppendarstellungen bei arithmetischer Aquivalenz, Abh. Math. Sem. Univ. Hamburg **14** (1940), 357–412.

[8] R. GREENBERG, Galois Theory for the Selmer Group of an Abelian Variety, Compos. Math. **136** (2003), 255–297.

[9] A. HELLER and I. REINER, Representations of cyclic groups in rings of integers. I, Ann. Math. **76** (1962), 73–92.

[10] A. HELLER and I. REINER, Representations of cyclic groups in rings of integers. II, Ann. Math. **77** (1963), 318–328.

[11] B. MAZUR, Rational points of abelian varieties with values in towers of number fields, Invent. Math. **18** (1972), 183–266.

[12] B. MAZUR and K. RUBIN, Organizing the arithmetic of elliptic curves, Adv. Math. **198** (2005), 504–546.

[13] M. RZEDOWSKI-CALDERÓN, G. D. VILLA SALVADOR and M. L. MADAN, Galois module structure of rings of integers, Math. Z. **204** (1990), 401–424.

[14] A. V. YAKOVLEV, Homological definability of p-adic representations of groups with cyclic Sylow p-subgroup, An. St. Univ. Ovidius Constanţa **4** (1996), 206–221.

Present Address:
INSTITUTO DE CIENCIAS MATEMÁTICAS (ICMAT),
28049 MADRID, SPAIN.
e-mail: daniel.macias@icmat.es

UNIVERSIDAD AUTÓNOMA DE MADRID (UAM),
28049 MADRID, SPAIN.
e-mail: daniel.macias@uam.es