Canad. J. Math. Vol. 73 (5), 2021 pp. 1390–1422
http://dx.doi.org/10.4153/S0008414X20000553

# Bounding the Iwasawa invariants of Selmer groups

Sören Kleine

*Abstract.* We study the growth of $p$-primary Selmer groups of abelian varieties with good ordinary reduction at $p$ in $\mathbb{Z}_p$-extensions of a fixed number field $K$. Proving that in many situations the knowledge of the Selmer groups in a sufficiently large number of finite layers of a $\mathbb{Z}_p$-extension over $K$ suffices for bounding the over-all growth, we relate the Iwasawa invariants of Selmer groups in different $\mathbb{Z}_p$-extensions of $K$. As applications, we bound the growth of Mordell–Weil ranks and the growth of Tate-Shafarevich groups. Finally, we derive an analogous result on the growth of fine Selmer groups.

## 1 Introduction

Let $K$ be a number field, and let $p$ be a fixed rational prime. Classical Iwasawa theory studies the asymptotic growth of ideal class groups in $\mathbb{Z}_p$-extensions $K_\infty$ of $K$ by using the action of the Galois group $\mathrm{Gal}(K_\infty/K)$ on these ideal class groups, which can be used to turn the projective limit of the ideal class groups into a so-called Iwasawa module. In the 1960's, mathematicians started to study other classes of Iwasawa modules, the most prominent example being Selmer groups of abelian varieties defined over $K$. Many results have been obtained concerning the growth of Selmer groups over the intermediate fields of certain specific $\mathbb{Z}_p$-extensions like the *cyclotomic* $\mathbb{Z}_p$-extension of $K$, *i.e.*, the unique $\mathbb{Z}_p$-extension of $K$ that is contained in the union $\bigcup_n K(\mu_{p^n})$ obtained by adjoining $p$-power roots of unity.

In this article, we will describe an approach for comparing the growth of $p$-primary Selmer groups over distinct $\mathbb{Z}_p$-extensions of $K$ that are close with respect to a certain topology (basic idea: two $\mathbb{Z}_p$-extensions of $K$ are close if they have large intersection; details will be given in Section 4). The main ingredient is a method for bounding the asymptotic growth of Selmer groups by using only information about a suitable finite subextension of the $\mathbb{Z}_p$-extension. This approach will also enable us to bound, in some situations, the growth of Mordell–Weil- and ($p$-primary) Tate–Shafarevich groups in the tower of a $\mathbb{Z}_p$-extension by using only a finite number of layers.

We will now make this more precise. Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension, and let $A$ be an abelian variety defined over $K$. In most of our results, we will assume that $A$ has (potentially) good ordinary reduction at the primes of $K$ dividing $p$. We denote by $X^{(K_\infty)}$ the Pontryagin dual of the $p$-primary subgroup of the Selmer group $\mathrm{Sel}_A(K_\infty)$.

Received by the editors June 14, 2019; revised March 19, 2020.
Published online on Cambridge Core June 29, 2020.
AMS subject classification: 11R23, 11G05, 11G10, 13C12.
Keywords: Fukuda module, Selmer group, Mordell–Weil rank, fine Selmer group.

Then $X^{(K_\infty)}$ is a module over the completed group ring $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$. In Section 4, we will show that the Iwasawa $\mu$- and $\lambda$-invariants of the Iwasawa modules $X^{(\widetilde{K}_\infty)}$ of $\mathbb{Z}_p$-extensions $\widetilde{K}_\infty$ of $K$ can be bounded explicitly in suitable neighbourhoods of $K_\infty$ (with respect to the topology introduced in Section 4). In fact, the Iwasawa invariants attached to Selmer groups of $\mathbb{Z}_p$-extensions $K_\infty$ of $K$ are *locally maximal* in the following sense.

**Theorem 1.1** *Let $A$ be an abelian variety defined over $K$, and suppose that $A$ has potentially good and ordinary reduction at the primes of $K$ dividing $p$. Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension. We assume that $A(K_\infty)[p^\infty]$ is finite and that $X^{(K_\infty)}$ is a torsion $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$-module. Then the following statements hold for each $\mathbb{Z}_p$-extension $\widetilde{K}_\infty$ of $K$ that is sufficiently close to $K_\infty$:*

- *$X^{(\widetilde{K}_\infty)}$ is $\mathbb{Z}_p[\![\mathrm{Gal}(\widetilde{K}_\infty/K)]\!]$-torsion;*
- *$\mu(X^{(\widetilde{K}_\infty)}) \le \mu(X^{(K_\infty)})$;*
- *$\lambda(X^{(\widetilde{K}_\infty)}) \le \lambda(X^{(K_\infty)})$ whenever $\mu(X^{(\widetilde{K}_\infty)}) = \mu(X^{(K_\infty)})$.*

This theorem will be proved in Section 4 (see Theorem 4.11). Similar questions have been studied for classical Iwasawa modules, *i.e.*, projective limits of the ideal class groups of the intermediate number fields in (multiple) $\mathbb{Z}_p$-extensions, in [6, 16, 17, 18]. It seems, however, that the analogous problem for Selmer groups has not yet been discussed.

The approach used in [16, 17, 18] is quite different from the arguments given in [6]. The basic idea is to bound the size of an Iwasawa module of the form $X = \varprojlim X_n$ by studying a sufficiently large number of the layers $X_n$. It is of course usually very difficult to actually quantify what "sufficiently large" means for some concrete example. For this purpose, we use specific algebraic properties of our Iwasawa modules, which were implicitly used for the first time by Fukuda in [5] in the setting of ideal class groups, *i.e.*, classical Iwasawa modules.

In order to adapt this method to Selmer groups, we will considerably generalise the result of Fukuda in Section 3, where we prove some general algebraic facts. In Section 4, we prove Theorem 1.1. The main argument involves an application of a control theorem for the Selmer groups, which holds under the assumption of (potentially) good and ordinary reduction of $A$ at $p$, and a thorough analysis of the finite kernels and cokernels occurring in this situation. At the end of Section 4, we briefly point out a weak generalisation of our results to Selmer groups over multiple $\mathbb{Z}_p$-extensions.

In Section 5, we discuss further applications. Recall that, for each number field $F$, we have an exact sequence

$$0 \longrightarrow A(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_A(F) \longrightarrow Ш_A(F) \longrightarrow 0\,. \tag{1.1}$$

Using these exact sequences, we derive consequences for Tate–Shafarevich and Mordell–Weil groups. Conjecturally, the Tate–Shafarevich groups $Ш_A(F)$ are finite for all number fields $F$. Assuming that this holds true for the finite layers of a $\mathbb{Z}_p$-extension $K_\infty/K$, we can use the results from Section 4 in order to bound the growth of Tate–Shafarevich and Mordell–Weil groups.

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

If $K$ is abelian over $\mathbb{Q}$, $A$ is an elliptic curve defined over $\mathbb{Q}$ and $K_\infty/K$ denotes the cyclotomic $\mathbb{Z}_p$-extension, then results of Kato and Rohrlich (see [14, 26] and *cf.* also [7, Section 1]) imply that the Mordell–Weil ranks $\operatorname{rank}_{\mathbb{Z}}(A(K_n))$ are bounded as $n \to \infty$. On the other hand, it is known that the ranks of the Mordell–Weil groups $A(K_n)$ are unbounded if $K_\infty$ is the *anticyclotomic* $\mathbb{Z}_p$-extension of an imaginary quadratic number field $K$ and if $A = E$ denotes an elliptic curve defined over $\mathbb{Q}$, which has complex multiplication by $K$ and good ordinary reduction at $p$, provided that the Hasse–Weil $L$-series $L(E,s)$ has an odd order zero at $s = 1$ (see [7, Theorem 1.8]).

We will show that in the situation of Theorem 1.1, $\operatorname{rank}_{\mathbb{Z}}(A(\widetilde{K}_\infty)) \le \lambda(X^{(K_\infty)})$ for each $\mathbb{Z}_p$-extension $\widetilde{K}_\infty$ of $K$ that is sufficiently close to $K_\infty$ and satisfies $\mu(X^{(\widetilde{K}_\infty)}) = \mu(X^{(K_\infty)})$ (see Lemma 5.7). In particular, this applies to the situation studied by Kato and Rohrlich: let $K_\infty = K_\infty^{cyc}$ denote the cyclotomic $\mathbb{Z}_p$-extension of an abelian number field $K$, $p$ odd, and suppose that $A = E$ is an elliptic curve defined over $\mathbb{Q} \subseteq K$ such that the extension $K(E[p^\infty])/K$ is pro-$p$. Then [2, Theorem 3.4] implies that $\mu(X^{(K_\infty)}) = 0$ (*cf.* also the end of Section 5.2); in particular, $\mu(X^{(\widetilde{K}_\infty)}) = \mu(X^{(K_\infty)})$ for each sufficiently close $\widetilde{K}_\infty$. Moreover, in this situation $\lambda(X^{(K_\infty)})$ can be estimated via analytical methods (*cf.* Section 5.1). Note that the analytical approach works only for the cyclotomic $\mathbb{Z}_p$-extension of $K$, whereas Theorem 1.1 yields bounds for the Mordell–Weil ranks in $\mathbb{Z}_p$-extensions of $K$ different from the cyclotomic one.

Using the exact sequences (1.1), we can bound the asymptotical growth of Tate–Shafarevich groups $Ш_A(K_n)$ depending on the growth of Mordell–Weil ranks, and vice versa (for details, see Section 5.1). Several authors considered the problem of finding lower bounds for $\operatorname{rank}_{\mathbb{Z}}(A(K_\infty))$, via showing that the Mordell–Weil ranks grow in the first few layers of a $\mathbb{Z}_p$-extension (*cf.*, for example, [22]). We derive from our main theorem a result (*cf.* Corollary 5.10) that says roughly the following: under a strict finiteness assumption on the $Ш_A(K_n)$, if there exist an integer $M$ and sufficiently many consecutive layers $K_n$ whose Mordell–Weil ranks are all equal to $M$, then $\operatorname{rank}_{\mathbb{Z}}(A(K_m)) \le M + C$ for all $m \gg 0$ and some concrete constant $C \in \mathbb{N}$ (this phenomenon is probably well known, but we have not found an explicit statement in the literature). We can establish explicit bounds (depending on the abelian variety $A$ and the $\mathbb{Z}_p$-extension $K_\infty/K$) for the number of consecutive layers that are necessary for stabilisation (see Corollaries 5.10 and 4.7).

Finally, in Section 5.2, we study *fine Selmer groups* (for the definition, we refer the reader to Section 2). Using the results from Sections 3 and 4, we describe two situations in which we can prove an analog of Theorem 1.1 for the Pontryagin dual $Y^{(K_\infty)}$ of the fine Selmer groups in a $\mathbb{Z}_p$-extension $K_\infty$ of $K$ (see Theorem 5.15). This has interesting applications: the fine Selmer groups tend to be much smaller than the usual Selmer groups. There exist several deep conjectures about the growth of fine Selmer groups in (multiple) $\mathbb{Z}_p$-extensions which are analogous to conjectures about the size of classical Iwasawa modules $X = \varprojlim X_n$ arising from ideal class groups in (multiple) $\mathbb{Z}_p$-extensions (*cf.* [2]). Using the growth stabilisation results for the fine Selmer groups, one can hope to be able to check these conjectures numerically by considerating a finite number of layers $Y_n$, $n \in \mathbb{N}$, in the same way as analogous growth stabilisation results have been used extensively for checking numerically the corresponding conjectures for classical Iwasawa modules $X = \varprojlim X_n$ (*cf.*, for example [5] and several subsequent papers).

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

## 2 Notation and Basic Definitions

Throughout the article, we fix a rational prime $p$ and a number field $K$. For each abelian group $G$, we denote by $G_p = G[p^\infty]$ the $p$-primary subgroup of $G$, *i.e.*, the subgroup of elements of $G$ of $p$-power order.

Let $K_\infty/K$ be a $\mathbb{Z}_p^d$-extension, $1 \le d \in \mathbb{N}$; we write $K_\infty = \bigcup_n K_n$, where $\mathrm{Gal}(K_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z})^d$ for each $n \in \mathbb{N}$. The group ring $\mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$ can be identified with the ring $\Lambda_d := \mathbb{Z}_p[\![T_1, \dots, T_d]\!]$ of formal power series, mapping a set $(\gamma_1, \dots, \gamma_d)$ of topological generators of $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p^d$ to $(T_1 + 1, \dots, T_d + 1)$. We call $\Lambda_d$ the Iwasawa algebra of the $\mathbb{Z}_p^d$-extension $K_\infty/K$. In this article, we will focus on the case $d = 1$, *i.e.*, $\mathbb{Z}_p$-extensions of $K$, but multiple $\mathbb{Z}_p$-extensions will show up in a motivating example in Section 3, and also in a short outlook at the end of Section 4. We will write $\Lambda = \Lambda_1 = \mathbb{Z}_p[\![T]\!]$ for brevity.

Note that $\Lambda_d$ is a local ring and a unique factorisation domain. We denote by $\mathfrak{m} = (p, T_1, \dots, T_d)$ its maximal ideal. If $M$ is any finitely generated $\Lambda_d$-module, then [24, Proposition 5.1.7] implies that there exists a *pseudo-isomorphism* (*i.e.*, a $\Lambda_d$-module homomorphism whose kernel and cokernel are annihilated by two relatively prime elements of the unique factorisation domain $\Lambda_d$) $\varphi : M \longrightarrow E_M$, where $E_M$ is a so-called *elementary* $\Lambda_d$-module. This means that it is of the form

$$E_M = TF(M) \oplus \bigoplus_{i=1}^{s} \Lambda_d/(h_i)$$

for some torsion-free $\Lambda_d$-module $TF(M)$ and suitable $h_1, \dots, h_s \in \Lambda_d$. In the special case $d = 1$, the torsion-free module $TF(M)$ can be replaced by a finitely generated free $\Lambda$-module (*cf.* [24, Theorem 5.1.10]). The element $F_M := \prod_{i=1}^{s} h_i \in \Lambda_d$ is called the *characteristic power series* of $M$; it is determined uniquely by $M$ up to multiplication by units of $\Lambda_d$.

Suppose that $M$ is compact with respect to the $\mathfrak{m}$-adic topology on the local ring $\Lambda_d$, and that $M$ is pro-$p$. Then we define the *Pontryagin dual* of $M$ as

$$M^\vee := \mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p),$$

where $\mathrm{Hom}_{\mathrm{cont}}$ means the set of *continuous* $\mathbb{Z}_p$-module homomorphisms.

Let $A$ denote a fixed abelian variety that is defined over $K$. For each $n \in \mathbb{N}$, we have an injective *Kummer map*

$$\kappa_n : A(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(K_n, A[p^\infty]).$$

If $v$ denotes a prime of $K$ and $w$ is a prime of $K_n$ above $v$, then we can also consider the localised map

$$\kappa_{n,w} : A(K_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(K_{n,w}, A[p^\infty]),$$

where we denote by $K_{n,w}$ the completion of $K_n$ at $w$. We define the ($p$-primary subgroup of the) *Selmer group* of $A$ over $K_n$:

$$\mathrm{Sel}_A(K_n) := \ker\Big(H^1(K_n, A[p^\infty]) \longrightarrow \prod_w H^1(K_{n,w}, A[p^\infty])/\mathrm{im}(\kappa_{n,w})\Big),$$

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

where $w$ runs over all primes of $K_n$. As in (1.1), the Selmer group on each level fits into an exact sequence

$$(2.1) \qquad 0 \longrightarrow A(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_A(K_n) \longrightarrow Ш_A(K_n) \longrightarrow 0,$$

where we denote by $Ш_A(K_n)$ the $p$-primary subgroup of the *Tate-Shafarevich group*. The latter group is by definition the kernel of the map

$$H^1(K_n, A) \longrightarrow \prod_w H^1(K_{n,w}, A),$$

where the product runs over all primes $w$ of $K_n$. We define

$$X^{(K_\infty)} := \varprojlim_n \mathrm{Sel}_A(K_n)^\vee;$$

*i.e.*, $X^{(K_\infty)}$ is the Pontryagin dual of $\mathrm{Sel}_A(K_\infty) := \varinjlim_n \mathrm{Sel}_A(K_n)$, where the injective limit is taken with respect to the restriction maps. $X := X^{(K_\infty)}$ is a finitely generated $\Lambda_d$-module (see [2, Theorem 4.5]). Moreover, $X$ is compact; this follows from the fact that $X_n = \mathrm{Sel}_A(K_n)^\vee$ is compact as being the projective limit of finite abelian $p$-groups (*cf.* [21, Lemma 4.4]). Recall that $X$ is pseudo-isomorphic to some elementary $\Lambda_d$-module $E_X$. The structure of the torsion submodule $\bigoplus_{i=1}^s \Lambda_d/(h_i)$ of $E_X$ can be described in terms of the so-called *Iwasawa invariants*.

Suppose that $d = 1$. If $F_X = \prod_{i=1}^s h_i \in \Lambda$ denotes the characteristic power series of $X$, then $F_X$ is associated with a power of $p$ times a so-called *distinguished polynomial* $f_X(T) \in \mathbb{Z}_p[T]$. We define $\mu(X)$ to be the largest power of $p$ dividing $F_X$ in the unique factorisation domain $\Lambda$, and we let $\lambda(X)$ be the degree of $f_X(T)$ (for more details, *cf.* for example [29, Chapter 13]). In this article, we will denote $\mathbb{Z}_p$-extensions of $K$ by $K_\infty = \bigcup_n K_n$ or $\widetilde{K}_\infty = \bigcup_n \widetilde{K}_n$, and we will study the Iwasawa modules $X^{(\widetilde{K}_\infty)}$ for distinct $\mathbb{Z}_p$-extensions of $K$.

Finally, we recall the definition of *fine Selmer groups*. For any number field $F$, the ($p$-primary subgroup of the) fine Selmer group of $A$ over $F$ is defined as

$$\mathrm{Sel}_{A,0}(F) = \ker\Big(H^1(F, A[p^\infty]) \longrightarrow \bigoplus_v H^1(F_v, A[p^\infty])\Big)$$

(one should compare this with the definition of the Selmer group $\mathrm{Sel}_A(K_n)$, as given above). If $K_\infty/K$ denotes a $\mathbb{Z}_p$-extension, then we let $Y^{(K_\infty)} = \varprojlim \mathrm{Sel}_{A,0}(K_n)^\vee$, analogous to $X^{(K_\infty)}$ (again the projective limit is taken with respect to the corestriction maps).

By definition, the fine and usual Selmer groups can be related via the following exact sequence (*cf.* [2, equation (58), p. 828]): for each number field $F$, we have an exact sequence

$$(2.2) \qquad 0 \longrightarrow \mathrm{Sel}_{A,0}(F) \longrightarrow \mathrm{Sel}_A(F) \longrightarrow \bigoplus_{v \mid p} (A(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p),$$

where the sum runs over all primes of $F$ dividing $p$. Here we note that

$$A(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \{0\}$$

for each $v \nmid p$; see [7, Theorem 2.4].

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

## 3 Fukuda Modules

In the current section, we will consider a special family of Iwasawa modules $X = \varprojlim X_n$ which are designed for tackling the following problem: given a sufficiently large number of layers $X_n$, $n \in \mathbb{N}$, explicitly (*e.g.*, via numerical computations), derive information about the projective limit $X = \varprojlim X_n$. This idea will be made more explicit below (see Theorem 3.5); in particular, it will of course be crucial to explicitly determine the number $N$ of layers of $X$ that have to be known for obtaining any information about $X$.

***Definition 3.1*** Let $1 \le d \in \mathbb{N}$ be arbitrary, and let $R = \Lambda_d$ be the ring of formal power series over $\mathbb{Z}_p$ in $d$ variables, as in Section 2. Recall that we denote by $\mathfrak{m} = (p, T_1, \dots, T_d)$ the maximal ideal of the local ring $R$. Let $X = \varprojlim X_n$ denote the projective limit of $R$-modules $X_n$, $n \in \mathbb{N}$, each of which we assume to be an abelian pro-$p$-group. Suppose that $X$ is compact as an $R$-module (with respect to the $\mathfrak{m}$-adic topology). For each $n \in \mathbb{N}$, let $Y_n \subseteq X$ denote the kernel of the projection map $\mathrm{pr}_n : X \longrightarrow X_n$.

Let $C_1, C_2, C_3 \in \mathbb{N}$ be $p$-powers. Then $X$ is called a *Fukuda -R- module with parameters* $(C_1, C_2, C_3)$ if there exists a family of compact $R$-submodules $(Z_n)_n$ of $X$ such that

$$|\mathrm{coker}(\mathrm{pr}_n)| \le C_1, \quad Z_{n+1} \subseteq \mathfrak{m} \cdot Z_n,$$
$$[Y_n : (Y_n \cap Z_n)] \le C_2 \quad \text{and} \quad [Z_n : (Y_n \cap Z_n)] \le C_3$$

for each $n \in \mathbb{N}$. If $C_3 = 1$ (which will happen in most of our cases), then we will abbreviate the notation by saying that $X$ is a $(C_1, C_2)$-Fukuda module.

***Remark 3.1*** We note that whereas $C_1$ is an intrinsic invariant of $X$, the constants $C_2$ and $C_3$ depend on the chosen family of $R$-modules $(Z_n)_n$. In practise, we usually want to minimise $v_p(C_2 \cdot C_3)$ by a good choice of the $Z_n$ ( *cf.* Theorem 3.5).

***Example 3.2*** A notion of Fukuda- $\Lambda_d$-modules with parameters $(1, 1, 1)$ has been introduced earlier in [16] for $d = 1$, and in [17], for arbitrary $d$ ( *cf.* [17, Definition 3.8]), in order to study the growth of ideal class groups in $\mathbb{Z}_p^d$-extensions of number fields. In order to motivate the above definition, we will now describe this special case in more detail, confining ourselves to the case $d = 1$.

Let $K_\infty$ be a $\mathbb{Z}_p$-extension of a number field $K$, $K_\infty = \bigcup_n K_n$ with $K_n/K$ cyclic of degree $p^n$, $n \in \mathbb{N}$. We consider $R = \Lambda_1 = \mathbb{Z}_p[\![T]\!] \cong \mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$ and $X = \varprojlim X_n$, where $X_n$ denotes the $p$-primary subgroup of the ideal class group of $K_n$, $n \in \mathbb{N}$. Suppose that the following condition is satisfied:

(3.1) Each prime of $K$ that ramifies in $K_\infty$ is totally ramified in $K_\infty/K$.

For each $n \in \mathbb{N}$, we let

$$\nu_{n+1,n}(T) = 1 + (T+1)^{p^n} + (T+1)^{2p^n} + \dots + (T+1)^{(p-1)p^n} \in \mathfrak{m} = (p, T).$$

Then a classical result of Iwasawa (*cf.* [12, Theorem 6]) implies that

$$Y_{n+1} = \nu_{n+1,n}(T) \cdot Y_n \subseteq \mathfrak{m} \cdot Y_n$$

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

for each $n \in \mathbb{N}$, where $Y_n = \ker(\mathrm{pr}_n)$, as in Definition 3.1. Moreover, it follows by an argument from class field theory that $\mathrm{pr}_n : X \longrightarrow X_n$ is surjective for each $n$ (here we use that condition (3.1) is satisfied; in fact, it suffices that at least one prime of $K$ is totally ramified in $K_\infty$; *cf.* [29, Theorem 10.1]). In other words, letting $Z_n = Y_n$, we can conclude that $X = \varprojlim X_n$ is a Fukuda- $\Lambda_1$-module with parameters $(1,1,1)$.

More generally, let $K_\infty/K$ be a $\mathbb{Z}_p^d$-extension, $d \geq 1$, and write $K_\infty = \bigcup_n K_n$ with $\mathrm{Gal}(K_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z})^d$, $n \in \mathbb{N}$. Let $X = \varprojlim X_n$ be defined as above. We have shown in [17, Section 3] that under appropriate assumptions on the ramification of primes in $K_\infty/K$, generalising the condition (3.1) above, $X$ is a Fukuda- $\Lambda_d$-module with parameters $(1,1,1)$.

***Remark 3.3*** In fact, the Fukuda modules defined in [16] and [17] have been treated in more generality than in the above example. In the case $d = 1$, we did not assume the validity of condition (3.1). This made it necessary to weaken the definition of Fukuda modules in the following way: the sequence of $R$-modules $(Z_i)_i$ satisfies the conditions from Definition 3.1 only for all $n \geq e$, where $e = e(X)$ is a suitable integer ( *e.g.*, the minimal number $n$ such that the condition (3.1) from Example 3.2 holds for the $\mathbb{Z}_p$-extension $K_\infty/K_n$). Using such a weakened definition, our results ( *e.g.*, Theorem 3.5 ) have to be adjusted (typically one has to restrict to indices $n \geq e$ instead of $n \in \mathbb{N}$). In this article, we will study a class of Fukuda modules different from the standard Example 3.2. For this class, the definition as given in Definition 3.1 is sufficient; therefore, we will not pursue this issue any further.

We want to explain why the notion of Fukuda modules can be helpful in solving the problem stated at the beginning of the current section. Again, we motivate our general result by considering the special case of the $(1,1)$-Fukuda-modules described in Example 3.2. In this case, we have the following theorem due to Fukuda (see [5, Theorem 1]).

***Theorem 3.4*** (Fukuda) *Using the same notation as in Example 3.2, let $X = \varprojlim X_n$ be attached to a $\mathbb{Z}_p$-extension $K_\infty$ of $K$, which satisfies condition (3.1), and suppose that $|X_{n+1}| = |X_n|$ for some $n \in \mathbb{N}$. Then $|X| = |X_n|$, i.e., $|X_m| = |X_n|$ for each $m \geq n$.*

The proof of this theorem reduces to an application of Nakayama's Lemma. More precisely, if $|X_{n+1}| = |X_n|$, then $Y_n = Y_{n+1} \subseteq \mathfrak{m} \cdot Y_n$. Since $X = \varprojlim X_n$ is compact as a $\Lambda_1$-module, $Y_n = \ker(\mathrm{pr}_n)$ is also compact, and thus $Y_n \subseteq \mathfrak{m} \cdot Y_n$ implies that $Y_n = \{0\}$ by Nakayama's Lemma.

Fukuda proved also the following variant: if $\mathrm{rank}_p(X_{n+1}) = \mathrm{rank}_p(X_n)$ for some $n \in \mathbb{N}$, then $\mathrm{rank}_p(X) = \mathrm{rank}_p(X_n)$ (here, $\mathrm{rank}_p(B) = \dim_{\mathbb{F}_p}(B/pB)$ for any abelian group $B$, whenever this is finite). In [16], we observed that more generally, if $X = \varprojlim X_n$ is attached to a $\mathbb{Z}_p$-extension $K_\infty$ of $K$ satisfying (3.1), and if

$$|X_{n+1}/(\lambda \cdot X_{n+1})| = |X_n/(\lambda \cdot X_n)|$$

for some $\lambda \in \Lambda = \mathbb{Z}_p[\![T]\!]$ and some $n \in \mathbb{N}$, then $X/(\lambda \cdot X) \cong X_n/(\lambda \cdot X_n)$. Note: this is much more powerful than Fukuda's original result, since it enables us to exploit the $\Lambda$-module structure of $X$, instead of using only the group structure.

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

In [17], we generalised the above result to $\mathbb{Z}_p^d$-extensions $\mathbb{K}/K$, $d \geq 1$; in this setting, we studied the stabilisation of quotients of the form $X_n/((f_1, \dots, f_d) \cdot X_n)$, where $f_1, \dots, f_d$ are elements in $\Lambda_d = \mathbb{Z}_p[\![T_1, \dots, T_d]\!] \cong \mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{K}/K)]\!]$. We will prove an analogous stabilisation property for quotients of arbitrary Fukuda modules in the sense of Definition 3.1 in Corollary 3.8.

The generalisation of the notion of Fukuda modules given in Definition 3.1 (notably, the possibility of $(C_1, C_2, C_3) \neq (1, 1, 1)$) aims at considering different classes of Fukuda modules that do not arise from ideal class groups, alluding, in particular, to Selmer groups of abelian varieties over $\mathbb{Z}_p$-extensions (see Section 4). We will now prove a generalisation of Fukuda's result described above for the Fukuda modules introduced in Definition 3.1.

***Theorem 3.5*** *Let $R$ be as in Definition 3.1, and let $X = \varprojlim X_n$ be a Fukuda-$R$-module with parameters $(C_1, C_2, C_3)$, and fix a corresponding sequence $(Z_i)_{i \in \mathbb{N}}$ of $R$-modules.*

*If there exist an integer $M \in \mathbb{N}$ and at least $v_p(C_1 C_2 C_3) + 2$ different indices $n_i \in \mathbb{N}$ such that $|X_{n_i}| = M$ for each $n_i$, then $|X|$ is finite, and, in fact,*

$$M \cdot C_1^{-1} \leq |X| \leq M \cdot C_2.$$

***Remark 3.6*** We do not need to assume that each $X_n$ is finite; indeed, the theorem shows that the finiteness of all $X_n$ is a consequence of the hypotheses of the theorem.

**Proof** The inequality $|X| \geq M \cdot C_1^{-1}$ just follows from the fact that $|\mathrm{coker}(\mathrm{pr}_n)| \leq C_1$ by using some $n \in \mathbb{N}$ such that $X_n$ has order $M$.

For the proof of the finiteness of $X$, we first note that $Y_j \subseteq Y_i$ for each $j \geq i$. Let $r = v_p(C_1 C_2 C_3)$, and let $I$ be a finite set of at least $r + 2$ different indices $n_i$ as in the statement of the theorem. Then $|X/Y_j| \leq |X_j| = |X_i| \leq C_1 \cdot |X/Y_i|$ for each $i, j \in I$. In particular,

$$[Y_i : Y_j] \leq C_1 \tag{3.2}$$

for all $i, j \in I$ with $j \geq i$. Now consider the $R$-modules $(Z_i)_{i \in \mathbb{N}}$; note that $Z_j \subseteq \mathfrak{m}^{j-i} \cdot Z_i \subseteq Z_i$ for each $j \geq i$. Let $n$ and $m$ denote the smallest, respectively, largest index contained in $I$. Using the definition of the Fukuda parameters $C_1$, $C_2$, and $C_3$, we can conclude that

$$\begin{aligned} |Z_n/Z_m| \leq |Z_n/(Z_m \cap Y_m)| &\leq C_3 \cdot |(Z_n \cap Y_n)/(Z_m \cap Y_m)| \\ &\leq C_3 \cdot |Y_n/(Z_m \cap Y_m)| \leq C_2 C_3 \cdot |Y_n/Y_m| \overset{(3.2)}{\leq} C_1 C_2 C_3. \end{aligned}$$

By the definition of $r$, it follows that $Z_j = Z_i$ for some $j > i$, $i, j \in I$.

But $Z_i$ is compact by Definition 3.1. Therefore, Nakayama's Lemma implies that $Z_i = \{0\}$, *i.e.*, $|Y_i| \leq C_2$. In particular, $|X| = |X/Y_i| \cdot |Y_i| \leq C_2 \cdot M$. ■

We will now study quotients and submodules of Fukuda modules. More precisely, let

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\iota"] & B \arrow[r, "\psi"] & C \arrow[r] & 0 \end{tikzcd}$$

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

be an exact sequence of $R$-modules of the form $A = \varprojlim A_n$, $B = \varprojlim B_n$, and $C = \varprojlim C_n$ ($C = \varprojlim C_n$ must not be confused with the Fukuda parameters $C_i(X)$, $1 \leq i \leq 3$, of a Fukuda-$R$-module $X = \varprojlim_n X_n$). We assume that we have exact sequences

$$0 \longrightarrow A_n \xrightarrow{\iota} B_n \xrightarrow{\psi} C_n \longrightarrow 0$$

on each level $n$, and that these sequences commute with the natural projection maps $\mathrm{pr}_n : M \longrightarrow M_n$ and $\mathrm{pr}_{j,i} : M_j \longrightarrow M_i$, $j > i$, for each $M \in \{A, B, C\}$.

***Proposition 3.7*** *Let the notation be as above. We assume that there exists some $C_1(A) \in \mathbb{N}$ such that $|\mathrm{coker}(\mathrm{pr}_n^{(A)})| \leq C_1(A)$ for each $n \in \mathbb{N}$, and that the map $\psi$ is defined on $Z_n^{(B)}$ for every $n$. If $B$ is a Fukuda-$R$-module with parameters $(C_1, C_2, C_3)$, then $C$ is a Fukuda-$R$-module with parameters $(C_1, C_1(A) \cdot C_2, C_3)$.*

**Proof** By our assumptions, we have a commutative diagram

$$\begin{tikzcd}
 & Y_n^{(A)} \arrow[r] \arrow[d] & Y_n^{(B)} \arrow[r] \arrow[d] & Y_n^{(C)} \arrow[d] \arrow[dddll, dashed, rounded corners] & \\
0 \arrow[r] & A \arrow[r] \arrow[d, "\mathrm{pr}_n^{(A)}"] & B \arrow[r] \arrow[d, "\mathrm{pr}_n^{(B)}"] & C \arrow[r] \arrow[d, "\mathrm{pr}_n^{(C)}"] & 0 \\
0 \arrow[r] & A_n \arrow[r] \arrow[d] & B_n \arrow[r] & C_n \arrow[r] & 0 \\
 & \mathrm{coker}(\mathrm{pr}_n^{(A)}). & & &
\end{tikzcd}$$

The snake lemma yields an exact sequence

$$0 \longrightarrow Y_n^{(A)} \xrightarrow{\iota} Y_n^{(B)} \xrightarrow{\psi} Y_n^{(C)} \longrightarrow X_n \tag{3.3}$$

for each $n \in \mathbb{N}$, where $X_n = \mathrm{coker}(\mathrm{pr}_n^{(A)})$ is a finite $R$-module of order at most $C_1(A)$.

We define $Z_n^{(C)} := \psi(Z_n^{(B)})$, $n \in \mathbb{N}$. It is then clear that

$$Z_{n+1}^{(C)} \subseteq \psi(\mathfrak{m} \cdot Z_n^{(B)}) = \mathfrak{m} \cdot Z_n^{(C)}$$

and

$$[Z_n^{(C)} : (Z_n^{(C)} \cap Y_n^{(C)})] \leq [Z_n^{(B)} : (Z_n^{(B)} \cap Y_n^{(B)})]$$

for every $n \in \mathbb{N}$. Moreover, since $|\mathrm{coker}(\psi : Y_n^{(B)} \longrightarrow Y_n^{(C)})| \leq C_1(A)$ for each $n \in \mathbb{N}$ by (3.3), it follows that

$$|Y_n^{(C)}/(Z_n^{(C)} \cap Y_n^{(C)})| \leq C_1(A) \cdot |\psi(Y_n^{(B)})/\psi(Z_n^{(B)} \cap Y_n^{(B)})| \leq C_2 \cdot C_1(A).$$

Finally, using the surjections $\psi : B \twoheadrightarrow C$ and $\psi : B_n \twoheadrightarrow C_n$, $n \in \mathbb{N}$, one can show that $|\mathrm{coker}(\mathrm{pr}_n^{(C)})| \leq |\mathrm{coker}(\mathrm{pr}_n^{(B)})| \leq C_1$ for each $n \in \mathbb{N}$. ■

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

We apply this lemma to the quotients $A/(I\cdot A)$, where $A = \varprojlim_n A_n$ is a Fukuda-$R$-module and $I \subseteq R$ denotes an ideal. Note that the canonical surjection

$$\Phi : A \longrightarrow \varprojlim A_n/(I\cdot A_n)$$

has kernel $I \cdot A$: the sequences $(Y_n)_n$ and $(Z_n)_n$ of submodules define the same topology on $A$, and this topology is a refinement of the $\mathfrak{m}$-adic topology on $A$ since $Z_n \subseteq \mathfrak{m}^n$ for every $n$. But $I \cdot A$ is compact with regard to the $\mathfrak{m}$-adic topology, and therefore,

$$\ker(\Phi) = \bigcap_n (Y_n + I\cdot A) = I \cdot A.$$

***Corollary 3.8*** *Let $A = \varprojlim A_n$ be a Fukuda-R-module with parameters $(C_1, C_2, C_3)$, and let $I \subseteq R$ be an ideal. We consider the R-module $A/(I\cdot A) = \varprojlim A_n/(I\cdot A_n)$. Suppose that I can be generated by s elements of R.*

*If there exist an integer $M \in \mathbb{N}$ and at least*

$$v_p(C_1C_1^sC_2C_3) + 2 = v_p(C_1^{s+1}C_2C_3) + 2$$

*different indices $n_i \in \mathbb{N}$ such that $|A_{n_i}/(I\cdot A_{n_i})| = M$ for each i, then*

$$M \cdot C_1^{-1} \le |A/(I\cdot A)| \le M \cdot C_1^sC_2 .$$

**Proof** First note that the cokernel of $\mathrm{pr}_n : I\cdot A \longrightarrow I\cdot A_n$ can be bounded by $C_1^s$ for each $n$, since $\mathrm{pr}_n(I\cdot A) = I\cdot \mathrm{pr}_n(A)$. Indeed, if $g_1, \dots, g_{C_1}$ is a set of representatives covering all the cosets of the quotient $A_n/(\mathrm{pr}_n(A))$ and if $I = (f_1, \dots, f_s)$, then

$$\{f_i \cdot g_j \mid 1 \le i \le s, 1 \le j \le C_1\}$$

covers all the cosets of $(I\cdot A_n)/(I\cdot \mathrm{pr}_n(A))$.

Moreover, since $\psi(Z_n) := Z_n/(I\cdot Z_n)$ can be defined for every $n \in \mathbb{N}$, Proposition 3.7 implies that $C := A/(I\cdot A)$ is a Fukuda module with parameters $(C_1, C_1^s \cdot C_2, C_3)$. The statement of the corollary then follows from Theorem 3.5. ■

Now we study submodules of Fukuda modules. For simplicity, the following result is formulated with respect to the ring $R = \Lambda = \mathbb{Z}_p[\![T]\!]$ (*cf.* Section 2).

***Proposition 3.9*** *Let $B = \varprojlim B_n$ be a $(C_1, C_2, C_3)$-Fukuda- $\Lambda$-module, and let $A \subseteq B$ be a $\Lambda$-submodule. Suppose that*

(i) *$Z_{n+1}^{(B)} = f_{n+1,n} \cdot Z_n^{(B)}$ for some sequence $(f_{n+1,n})_n$ of non-units of $\Lambda$;*
(ii) *B is finitely generated as a $\Lambda$-module, $B/A$ is $\Lambda$-torsion;*
(iii) *for every $n \in \mathbb{N}$, $f_{n+1,n}$ and the characteristic power series of $B/A$ do not share any non-trivial common factor.*

*Then $A \subseteq B$ is a Fukuda- $\Lambda$-module if and only if*

$$|\mathrm{coker}(\mathrm{pr}_n^{(A)})| \le C_1(A)$$

*for some constant $C_1(A)$ and every $n \in \mathbb{N}$.*

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

**Proof** Suppose that $|\mathrm{coker}(\mathrm{pr}_n^{(A)})|$ is bounded. We define $Z_0^{(A)} := Z_0^{(B)} \cap A$ and

$$Z_n^{(A)} := f_n \cdot Z_0^{(A)}, \quad \text{where } f_n := \prod_{i=0}^{n-1} f_{i+1,i}, \ n \in \mathbb{N}.$$

Then

$$Z_n^{(A)} = f_n \cdot (Z_0^{(B)} \cap A) \subseteq f_n \cdot Z_0^{(B)} \cap A = Z_n^{(B)} \cap A,$$

and $[(Z_n^{(B)} \cap A) : Z_n^{(A)}]$ is bounded as $n \to \infty$. Indeed, since $f_n$ and the characteristic power series $F_{B/A}$ of $B/A$ do not share any non-trivial common factor,

$$\big[(f_n \cdot Z_0^{(B)} \cap A) : f_n \cdot (Z_0^{(B)} \cap A)\big] \leq |\ker(f_n : B/A \longrightarrow B/A)|$$

is bounded by the order of the maximal finite $\Lambda$-submodule of $B/A$, $n \in \mathbb{N}$. Let $D$ denote a bound for $[(Z_n^{(B)} \cap A) : Z_n^{(A)}]$. Then

$$\big[Y_n^{(A)} : (Z_n^{(A)} \cap Y_n^{(A)})\big] \leq D \cdot \big[(Y_n^{(B)} \cap A) : (Z_n^{(B)} \cap Y_n^{(B)} \cap A)\big] \leq D \cdot C_2(B)$$

and

$$\big[Z_n^{(A)} : (Z_n^{(A)} \cap Y_n^{(A)})\big] \leq D \cdot \big[(Z_n^{(B)} \cap A) : (Z_n^{(B)} \cap Y_n^{(B)} \cap A)\big] \leq D \cdot C_3(B)$$

for every $n \in \mathbb{N}$. This proves that $A$ is a Fukuda- $\Lambda$-module. ■

***Remark 3.10***

(i) Condition (ii) from Proposition 3.9 is satisfied if $B_n$ is finite for all $n \in \mathbb{N}$. Indeed, in this case, the exact sequence

$$0 \longrightarrow Y_n^{(B)} \longrightarrow B \longrightarrow \mathrm{pr}_n(B) \longrightarrow 0$$

implies that the characteristic power series satisfy $F_{Y_n^{(B)}} = F_B$, $n \in \mathbb{N}$. In particular, all $F_{Z_n^{(B)}} = F_{Y_n^{(B)}}$ are equal, *i.e.* ,

$$Z_n^{(B)}/Z_{n+1}^{(B)} = Z_n^{(B)}/(f_{n+1,n} \cdot Z_n^{(B)})$$

(using (i)) is finite for every $n \in \mathbb{N}$. But this means that for every $n \in \mathbb{N}$, $f_{n+1,n}$ does not share any non-trivial common factor with

$$F_{Z_n^{(B)}} = F_B = F_A \cdot F_{B/A}.$$

Moreover, $B$ is finitely generated and torsion over $\Lambda$, because $B/(f_{n+1,n} \cdot B)$ is finite for every $n \in \mathbb{N}$.

(ii) The Fukuda parameters of the submodules of a Fukuda-module $B = \varprojlim B_n$ can become arbitrarily large.

## 4 Bounding the Growth of Selmer Groups

Let us first fix some notation. Throughout this section, let $A$ be a fixed abelian variety defined over the number field $K$. We denote by $S_p$ the (finite) set of primes of $K$ dividing the rational prime $p$, and we let $S_{\mathrm{br}}$ be the (finite) set of primes of $K$ where $A$ has bad reduction. In the main results, we will usually assume that $S_p \cap S_{\mathrm{br}} = \emptyset$.

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

If $v$ denotes a prime of $K$ and $M$ denotes an abelian extension of $K$, then we will write $M_v$ for the completion of $M$ with respect to any fixed prime dividing $v$.

If $K_\infty/K$ is a $\mathbb{Z}_p$-extension, $K_\infty = \bigcup_n K_n$, then we will write $\Gamma = \mathrm{Gal}(K_\infty/K)$ and $\Gamma_n = \Gamma^{p^n} = \mathrm{Gal}(K_\infty/K_n)$, $n \in \mathbb{N}$. If $M$ denotes any finitely generated $\mathbb{Z}_p[\![\Gamma]\!]$-module, then we will denote by $M_{\Gamma_n}$ the quotient of $\Gamma_n$-coinvariants of $M$, *i.e.*, the maximal quotient of $M$ on which $\Gamma_n$ acts trivially. We fix an isomorphism $\mathbb{Z}_p[\![\Gamma]\!] \cong \mathbb{Z}_p[\![T]\!]$ by identifying a topological generator $\gamma$ of $\Gamma$ with $T+1$. Then

$$M_{\Gamma_n} = M/(w_{n,0}(T)\cdot M),$$

where $w_{n,0}(T) = (T+1)^{p^n} - 1$.

Let $K_\infty$ be a $\mathbb{Z}_p$-extension of $K$. Recall the definition of $\mathrm{Sel}_A(K_n)$ from Section 2. We consider $\mathrm{Sel}_A(K_\infty) = \varinjlim \mathrm{Sel}_A(K_n)$, where the direct limit is taken with respect to the restriction maps from Galois cohomology. Let $X_n^{(K_\infty)} := \mathrm{Sel}_A(K_n)^\vee$, $n \in \mathbb{N}$, be the Pontryagin duals, and let

$$X^{(K_\infty)} = \mathrm{Sel}_A(K_\infty)^\vee = \varprojlim_n X_n^{(K_\infty)}.$$

We will see below a sufficient condition for $X^{(K_\infty)}$ to be a Fukuda- $\Lambda$-module in the sense of Section 3. This property is deeply connected to the fact that a control theorem holds for $X^{(K_\infty)}$.

***Theorem 4.1*** (Mazur's Control Theorem) *Suppose that $A$ has potentially good and ordinary reduction at each prime $v \in S_p$. Then the natural maps*

$$(X^{(K_\infty)})_{\Gamma_n} \longrightarrow X_n^{(K_\infty)} = \mathrm{Sel}_A(K_n)^\vee$$

*have finite kernels and cokernels. The orders of these kernels and cokernels are bounded as $n \to \infty$.*

**Proof** This theorem was proved in [23]; see also [7, Chapter 4] and [9, Proposition 5.1]. ∎

***Corollary 4.2*** *Under the assumptions of Theorem 4.1, $X^{(K_\infty)} = \varprojlim X_n^{(K_\infty)}$ is a Fukuda- $\Lambda$-module with parameters $(C_1, C_2, 1)$ for suitable p-powers $C_1$ and $C_2$.*

**Proof** We let $Z_n = w_{n,0}(T)\cdot X^{(K_\infty)}$, $n \in \mathbb{N}$. Then $Z_{n+1} = v_{n+1,n}\cdot Z_n$, where

$$v_{n+1,n} = 1 + (T+1)^{p^n} + (T+1)^{2p^n} + \cdots + (T+1)^{(p-1)p^n}$$

is contained in the maximal ideal $\mathfrak{m} = (p, T)$ of $\Lambda$, and $(X^{(K_\infty)})_{\Gamma_n} \cong X^{(K_\infty)}/Z_n$ for each $n \in \mathbb{N}$.

Let $\mathrm{pr}_n : X^{(K_\infty)} \to X_n^{(K_\infty)}$ be the natural map. Since $\Gamma_n$ acts trivially on $X_n^{(K_\infty)}$, $\mathrm{pr}_n$ factors through $(X^{(K_\infty)})_{\Gamma_n}$, and therefore, $|\mathrm{coker}(\mathrm{pr}_n)|$ equals the order of the cokernel of the map from Theorem 4.1, because $X^{(K_\infty)} \to (X^{(K_\infty)})_{\Gamma_n}$ is surjective. Moreover, this also shows that $Z_n$ is contained in $Y_n = \ker(\mathrm{pr}_n)$. Finally, $[Y_n : Z_n]$ corresponds to the order of the kernel of the maps from Theorem 4.1, and thus is also bounded. ∎

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

In [6], Greenberg introduced the following topology on the set $\mathcal{E}(K)$ of $\mathbb{Z}_p$-extensions of $K$. The topology is generated by sets of the form

$$\mathcal{E}(K_\infty, m) = \left\{\widetilde{K}_\infty \in \mathcal{E}(K) : [(\widetilde{K}_\infty \cap K_\infty) : K] \geq p^m\right\},$$

where $K_\infty \in \mathcal{E}(K)$ and $m \in \mathbb{N}$. In other words, two $\mathbb{Z}_p$-extensions $K_\infty$ and $\widetilde{K}_\infty$ of $K$ are "close" with respect to this topology if the intersection $K_\infty \cap \widetilde{K}_\infty$ is large.

In the sequel, we fix the abelian variety $A$, and we compare the Selmer groups $X^{(K_\infty)}$, $X^{(\widetilde{K}_\infty)}$ of different $\mathbb{Z}_p$-extensions $K_\infty$ and $\widetilde{K}_\infty$ of $K$ that are close with respect to Greenberg's topology. For this purpose, it will be important to show that the Selmer groups of sufficiently close $\mathbb{Z}_p$-extensions are Fukuda modules with the same parameters. In order to achieve such a result, we will, however, have to restrict the topology in order to take into account the ramification of primes in the different $\mathbb{Z}_p$-extensions.

***Remark 4.3*** This is already necessary for the investigation of the classical Iwasawa modules from Example 3.2. Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension. Recall that we assumed in Example 3.2 that all the ramified primes are totally ramified in $K_\infty/K$. Suppose that there exists some prime $v$ of $K$ dividing $p$ that does not ramify in $K_\infty$. For arbitrarily large $m \in \mathbb{N}$, there exist $\mathbb{Z}_p$-extensions $\widetilde{K}_\infty \in \mathcal{E}(K_\infty, m)$ of $K$ such that $v$ is ramified in $\widetilde{K}_\infty$, and therefore is not totally ramified in $\widetilde{K}_\infty/K$ (in fact, it does not start ramifying before the layer $\widetilde{K}_{m+1}$). This means that the Iwasawa module attached to $\widetilde{K}_\infty/K$ is not a Fukuda module in the sense of Definition 3.1; actually, Theorem 3.5, and therefore also Theorem 1.1, may fail for $\widetilde{K}_\infty$; see *e.g.* , [17, Remark 4.8].

In [16], we have therefore introduced the following finer topology on $\mathcal{E}(K)$. For each $M \in \mathcal{E}(K)$, we denote by $\mathcal{P}(M)$ the set of primes of $K$ that ramify in $M$. Then $\mathcal{P}(M)$ is a subset of the set $S_p$ of primes dividing $p$, and, in particular, is finite for each $M$. Now suppose that $K_\infty \in \mathcal{E}(K)$ and $m \in \mathbb{N}$. Then we let

$$\mathcal{U}(K_\infty, m) := \left\{\widetilde{K}_\infty \in \mathcal{E}(K_\infty, m) \mid \mathcal{P}(\widetilde{K}_\infty) \subseteq \mathcal{P}(K_\infty)\right\}.$$

It has been shown in [16] that the topology on $\mathcal{E}(K)$ generated by the sets $\mathcal{U}(K_\infty, m)$ is sufficient to handle the classical Iwasawa modules from Example 3.2.

In the following, we want to control the $(C_1, C_2, C_3)$-parameters of Selmer groups $X^{(\widetilde{K}_\infty)}$ of $\mathbb{Z}_p$-extensions $\widetilde{K}_\infty \in \mathcal{U}(K_\infty, m)$ of $K$, $K_\infty/K$ fixed and $m \in \mathbb{N}$ sufficiently large. We will always assume that the abelian variety $A$ has potentially good and ordinary reduction at each prime $v \in S_p$. As we will see in the proof of the following theorem, we are naturally led to consider the following refinement of the topologies described above: for $K_\infty \in \mathcal{E}(K)$ and $m \in \mathbb{N}$, let $\mathcal{U}(A, K_\infty, m) \subseteq \mathcal{U}(K_\infty, m)$ denote the subset of $\mathbb{Z}_p$-extensions $\widetilde{K}_\infty$ of $K$ such that each prime of $S_{\text{br}}$ that is totally split in $K_\infty$ does split completely also in $\widetilde{K}_\infty$. In other words, letting $I_v(K_\infty/K)$ and $D_v(K_\infty/K)$ denote the inertia and decomposition subgroups of the prime $v$ of $K$ in $\text{Gal}(K_\infty/K)$, $\mathcal{U}(A, K_\infty, m)$ equals the set

$$\Big\{\widetilde{K}_\infty \in \mathcal{E}(K_\infty, m) \mid \text{rank}_{\mathbb{Z}_p}(I_v(\widetilde{K}_\infty/K)) \leq \text{rank}_{\mathbb{Z}_p}(I_v(K_\infty/K)) \qquad \forall v \in S_p,$$
$$\text{rank}_{\mathbb{Z}_p}(D_v(\widetilde{K}_\infty/K)) \leq \text{rank}_{\mathbb{Z}_p}(D_v(K_\infty/K)) \qquad \forall v \in S_{\text{br}}\Big\}.$$

Note that $S_p \cup S_{\text{br}}$ is finite.

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

***Remark 4.4*** Let $\mathbb{L}/K$ be a $\mathbb{Z}_p^k$-extension. If there exists $M \in \mathcal{E}(K)$, $M \subseteq \mathbb{L}$, such that $v \in S_p$ is contained in $\mathcal{P}(M)$, then the set of $\widetilde{K}_\infty \in \mathcal{E}(K)$ which are contained in $\mathbb{L}$ and satisfy $v \in \mathcal{P}(\widetilde{K}_\infty)$ is dense with respect to Greenberg's topology. Therefore, if $\mathcal{P}(K_\infty) \neq S_p$, already the sets $\mathcal{U}(K_\infty, m)$ are much smaller than $\mathcal{E}(K_\infty, m)$. The same holds true if some $v \in S_p$ is completely split in $K_\infty$, and inert in some $M \in \mathcal{E}(K)$.

On the other hand, if $\mathcal{U}(A, K_\infty, m)$ is strictly larger than the set $\{K_\infty\}$, then it is in fact infinite. Indeed, if $K_\infty \neq \widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$, then each $\mathbb{Z}_p$-extension of $K$ in $\mathcal{E}(K_\infty, m) \cap (K_\infty \cdot \widetilde{K}_\infty)$ will be contained in $\mathcal{U}(A, K_\infty, m)$.

***Theorem 4.5*** *Suppose that $B := A(K_\infty)[p^\infty]$ is finite. Recall that we assume that $A$ has potentially good and ordinary reduction at the primes of $K$ dividing $p$. Then there exist integers $m, C_1, C_2 \in \mathbb{N}$ such that $X^{(\widetilde{K}_\infty)}$ is a Fukuda- $\Lambda_1$-module with bounded parameters $(C_1, C_2, 1)$ for each $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$.*

**Proof** This follows from a thorough analysis of the proof of Mazur's Control Theorem 4.1. We refer the reader to [7, Chapter 4] and to the article [9] for a very detailed exposition; our proof will rely heavily on these sources.

Let $\mathrm{pr}_n^{(\widetilde{K}_\infty)} : X^{(\widetilde{K}_\infty)} \to X_n^{(\widetilde{K}_\infty)}$ be the natural maps, $n \in \mathbb{N}$. Then $\mathrm{pr}_n^{(\widetilde{K}_\infty)}$ factors through the coinvariant module $(X^{(\widetilde{K}_\infty)})_{\Gamma_n}$. As in the proof of Corollary 4.2, we let $Z_n^{(\widetilde{K}_\infty)} = w_{n,0}(T) \cdot X^{(\widetilde{K}_\infty)}$. Then $Z_n^{(\widetilde{K}_\infty)} \subseteq Y_n^{(\widetilde{K}_\infty)}$, and the orders $[Y_n^{(\widetilde{K}_\infty)} : Z_n^{(\widetilde{K}_\infty)}]$ and $|\mathrm{coker}(\mathrm{pr}_n^{(\widetilde{K}_\infty)})|$ can be bounded via the Control Theorem 4.1.

More precisely, for each $n \in \mathbb{N}$, we start from a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_A(\widetilde{K}_n) \arrow[r] \arrow[d, "i_n^{(\widetilde{K}_\infty)}"] & H^1(\widetilde{K}_n, A[p^\infty]) \arrow[r] \arrow[d, "f_n^{(\widetilde{K}_\infty)}"] & \bigoplus\limits_v H^1(\widetilde{K}_{n,v}, A[p^\infty])/\mathrm{im}(\kappa_{n,v}) \arrow[d, "g_n^{(\widetilde{K}_\infty)}"] \\
0 \arrow[r] & \mathrm{Sel}_A(\widetilde{K}_\infty)^{\Gamma_n} \arrow[r] & H^1(\widetilde{K}_\infty, A[p^\infty])^{\Gamma_n} \arrow[r] & \Big(\prod\limits_v H^1(\widetilde{K}_{\infty,v}, A[p^\infty])/\mathrm{im}(\kappa_{\infty,v})\Big)^{\Gamma_n}.
\end{tikzcd}$$

Here, $\Gamma_n = \mathrm{Gal}(\widetilde{K}_\infty/\widetilde{K}_n)$. The snake lemma yields an exact sequence

$$0 \longrightarrow \ker(i_n^{(\widetilde{K}_\infty)}) \longrightarrow \ker(f_n^{(\widetilde{K}_\infty)}) \longrightarrow G_n^{(\widetilde{K}_\infty)} \longrightarrow \mathrm{coker}(i_n^{(\widetilde{K}_\infty)}) \longrightarrow 0,$$

where $G_n^{(\widetilde{K}_\infty)}$ is a subgroup of $\ker(g_n^{(\widetilde{K}_\infty)})$. Here, we use the fact that $f_n^{(\widetilde{K}_\infty)}$ is surjective by the inflation-restriction exact sequence, because $\mathrm{Gal}(\widetilde{K}_\infty/K) \cong \mathbb{Z}_p$ has $p$-cohomological dimension 1; *cf.* [7, Lemma 4.3] and [9, Section 3.I]. Dualising, we obtain exact sequences

$$0 \longrightarrow Y_n^{(\widetilde{K}_\infty)}/Z_n^{(\widetilde{K}_\infty)} \longrightarrow U_n \longrightarrow V_n \longrightarrow \mathrm{coker}(\overline{\mathrm{pr}}_n^{(\widetilde{K}_\infty)}) \longrightarrow 0,$$

where $\overline{\mathrm{pr}}_n^{(\widetilde{K}_\infty)} : X^{(\widetilde{K}_\infty)}/Z_n^{(\widetilde{K}_\infty)} \longrightarrow X_n^{(\widetilde{K}_\infty)}$ denotes the dualised map $(i_n^{(\widetilde{K}_\infty)})^\vee$, $U_n = (G_n^{(\widetilde{K}_\infty)})^\vee$ and $V_n = \ker(f_n^{(\widetilde{K}_\infty)})^\vee$. Our task is to bound $|U_n|$ and $|V_n|$, $n \in \mathbb{N}$.

First, $|U_n|$ can be bounded prime by prime (*cf.* [7, Lemmas 4.4 and 4.6] and [9, Section 4]). If $v$ is totally split in the $\mathbb{Z}_p$-extension $\widetilde{K}_\infty$, then $\widetilde{K}_{\infty,v} = \widetilde{K}_v$, and therefore

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

$v$ does not contribute to $|U_n|$. The same holds for primes of good reduction that are inert in $\widetilde{K}_\infty$ (see [9, Proposition 4.1] for the primes $v \nmid p$ and [9, Proposition 4.3] for the primes $v \mid p$).

In particular, the archimedean primes do not contribute to $|U_n|$, since $\widetilde{K}_\infty/K$ is a real extension; *cf.* [9, Section 4.(B)]. In the following, we will only consider finite primes. More precisely, it remains to consider the primes of bad reduction that are not totally split in $\widetilde{K}_\infty$, as well as the primes $v \mid p$ that are ramified.

We start with the latter set of primes. Choose a finite extension $F$ of $K$ such that $A$ has good, ordinary reduction at all primes dividing $p$ in $F$. It has been shown in the proof of [7, Lemma 4.6], and more generally in [9, Section 4.(C).I], that the contribution to $|U_n|$ of a prime $v \mid p$ ramifying in $\widetilde{K}_\infty$ is bounded by $|\widetilde{A}(\mathcal{R}_{\widetilde{K}_\infty \cdot F,v})[p^\infty]|^2$, where $\mathcal{R}_{\widetilde{K}_\infty \cdot F,v}$ denotes the residue field of $\widetilde{K}_\infty \cdot F$ at some prime dividing $v$ and where $\widetilde{A}$ denotes the reduction of $A$ at $v$. Note that $\mathcal{R}_{\widetilde{K}_\infty \cdot F,v}$ is finite as the residue fields $\mathcal{R}_{\widetilde{K}_n \cdot F,v}$ stabilise, because $v$ ramifies in $\widetilde{K}_\infty$. Moreover, if $m \in \mathbb{N}$ is large enough such that all primes of $K$ ramifying in $K_\infty$ are totally ramified in $K_\infty/K_m$, then the sets of primes of $K$ that ramify in $K_\infty$, respectively, in $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m+1)$, coincide, and the residue fields $\mathcal{R}_{\widetilde{K}_\infty \cdot F,v}$ and $\mathcal{R}_{K_\infty \cdot F,v}$ are both equal to $\mathcal{R}_{K_m \cdot F,v}$.

Now let $v$ be a prime of bad reduction. Then $v \nmid p$ by assumption. If $v$ is totally split in $K_\infty$, then $v$ also splits completely in $\widetilde{K}_\infty$ for each $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$. We are therefore reduced to considering the inert primes. Let $m_v$ be the smallest integer such that $v$ is inert in $K_{m_v+1}/K_{m_v}$, and consider a neighbourhood $\mathcal{U}(A, K_\infty, m)$, where $m \geq m_v + 1$ for each such $v$ (recall that there exist only finitely many primes where $A$ has bad reduction).

Let $B_v = H^0(K_v, A[p^\infty]) = A(K_{\infty,v})[p^\infty]$, where $K_{\infty,v}$ denotes the unramified $\mathbb{Z}_p$-extension of $K_v$. Since $v \nmid p$, $K_{\infty,v}$ is the unique $\mathbb{Z}_p$-extension of $K_v$, and, in particular, does not depend on $K_\infty$; *i.e.*, $B_v$ is the same abelian group for each $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$. It has been shown in the proof of [7, Lemma 4.4] (*cf.* also [9, Proposition 4.1]) that the contribution of $v$ to $|U_n|$ is bounded by the finite index $[B_v : (B_v)_{\mathrm{div}}]$ of the maximal divisible subgroup of $B_v$. By the above, this upper bound holds for each $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$.

It remains to show that $|V_n|$ can be bounded uniformly on $\mathcal{U}(A, K_\infty, m)$ for sufficiently large $m$. For this task, we apply [7, Lemma 4.2] and [9, Section 3.I]. Using the inflation-restriction exact sequence, we see that the Pontryagin dual of $V_n$ is isomorphic to $H^1(\Gamma_n, B)$, where $B = H^0(K_\infty, A[p^\infty])$ is the $p$-primary subgroup of $A(K_\infty)$, and $\Gamma_n = \Gamma^{p^n} = \mathrm{Gal}(K_\infty/K_n)$. Since $B$ is finite by assumption, it follows that $|V_n| = |B/(w_{n,0}(T) \cdot B)|$ for each $n \in \mathbb{N}$. Choose $m \in \mathbb{N}$ large enough such that $w_{m,0}(T) \cdot B = \{0\}$; such an integer exists, because $B$ is finite. Then $|V_r| = |B|$ for each $r \geq m$.

Now we consider some $\widetilde{K}_\infty \in U := \mathcal{U}(A, K_\infty, v_p(|B|) + 1)$. We have to be careful, because $B^{(\widetilde{K}_\infty)} = A(\widetilde{K}_\infty)[p^\infty]$ might be infinite. We let $B_{\mathrm{div}}^{(\widetilde{K}_\infty)}$ denote the maximal divisible subgroup of $B^{(\widetilde{K}_\infty)}$, and we set $C^{(\widetilde{K}_\infty)} = B^{(\widetilde{K}_\infty)}/B_{\mathrm{div}}^{(\widetilde{K}_\infty)}$. This is a finite $\Lambda$-module. The exact sequence

$$0 \longrightarrow B_{\mathrm{div}}^{(\widetilde{K}_\infty)} \longrightarrow B^{(\widetilde{K}_\infty)} \longrightarrow C^{(\widetilde{K}_\infty)} \longrightarrow 0 \tag{4.1}$$

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

induces an exact sequence

$$(4.2)\qquad H^1(\Gamma_n, B_{\mathrm{div}}^{(\widetilde{K}_\infty)}) \longrightarrow H^1(\Gamma_n, B^{(\widetilde{K}_\infty)}) \longrightarrow H^1(\Gamma_n, C^{(\widetilde{K}_\infty)})$$

for each $n \in \mathbb{N}$. Note that the kernel $A(\widetilde{K}_n)[p^\infty] = (B^{(\widetilde{K}_\infty)})^{\Gamma_n}$ of the homomorphism $w_{n,0}(T)$ is finite for each $n$. This implies that $w_{n,0}(T) : B_{\mathrm{div}}^{(\widetilde{K}_\infty)} \longrightarrow B_{\mathrm{div}}^{(\widetilde{K}_\infty)}$ must be surjective (recall that $B^{(\widetilde{K}_\infty)}$ is cofinitely generated over $\mathbb{Z}_p$; dualising, the kernel and cokernel of the induced map both must be finite). It follows that the first term $H^1(\Gamma_n, B_{\mathrm{div}}^{(\widetilde{K}_\infty)})$ of the exact sequence (4.2) is trivial. This means that

$$|H^1(\Gamma_n, B^{(\widetilde{K}_\infty)})| \le |H^1(\Gamma_n, C^{(\widetilde{K}_\infty)})| = |H^0(\Gamma_n, C^{(\widetilde{K}_\infty)})|$$

for each $n$, since $C^{(\widetilde{K}_\infty)}$ is finite, and thus $|(C^{(\widetilde{K}_\infty)})^{\Gamma_n}| = |C^{(\widetilde{K}_\infty)}/(w_{n,0}(T) \cdot C^{(\widetilde{K}_\infty)})|$. On the other hand,

$$|H^0(\Gamma_n, C^{(\widetilde{K}_\infty)})| \le |H^0(\Gamma_n, B^{(\widetilde{K}_\infty)})| = |H^0(\Gamma_n, B)| \le |B|$$

for each $n \le v_p(|B|) + 1$ and every $\widetilde{K}_\infty \in U$. Therefore,

$$|H^1(\Gamma_n, C^{(\widetilde{K}_\infty)})| = |H^1(\Gamma_{n+1}, C^{(\widetilde{K}_\infty)})|$$

for some $n \le v_p(|B|) + 1$, and Nakayama's Lemma implies that $|C^{(\widetilde{K}_\infty)}| \le |B|$.

This means that

$$|V_n^{(\widetilde{K}_\infty)}| = |H^1(\Gamma_n, B^{(\widetilde{K}_\infty)})| \le |B| = |V_n^{(K_\infty)}|$$

for each $\widetilde{K}_\infty \in U$ and every $n \in \mathbb{N}$. ■

***Remark 4.6*** In the above theorem and also in the following results, we assume that $A(K_\infty)[p^\infty]$ is finite. We list several results concerning this condition, without claiming to give an exhaustive overview (special thanks are due to the anonymous referees for bringing these results to our attention).

- If $K_\infty$ denotes the cyclotomic $\mathbb{Z}_p$-extension of $K$, then $A(K_\infty)[p^\infty]$ is finite by work of Imai (if $A$ has good ordinary reduction at $p$, *cf.* [10]) and Ribet ( *cf.* the appendix of [15]).
- It has been proved by Wingberg (*cf.* [30, Theorem 4.3]) that there exist at most $\dim(A)$ different $\mathbb{Z}_p$-extensions $K_\infty$ of $K$ such that $A(K_\infty)[p^\infty]$ is infinite, provided that the abelian variety $A$ is defined over $K$ and simple.
- Improving on a result of Bogomolov, Zarhin proved in [32] that the group $A(K_\infty)[p^\infty]$ is finite if $K_\infty$ is different from the cyclotomic $\mathbb{Z}_p$-extension of $K$ and $K$ does not contain a CM-field. In particular, together with the result of Ribet mentioned above, this proves that $A(K_\infty)[p^\infty]$ is finite for every $\mathbb{Z}_p$-extension of $K$ if $K$ does not contain any CM-field (*e.g.* if $2 \nmid [K : \mathbb{Q}]$).
- It follows from [9, Proposition 3.2(ii)] that $A(K_\infty)[p^\infty]$ is finite if $A$ has potentially ordinary reduction at every prime $v \in S_p$, and the residue field $K_{\infty,w}$ is finite for any prime $w$ of $K_\infty$ above $p$ (here $K_\infty$ is allowed to be a multiple $\mathbb{Z}_p$-extension of $K$).

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

Going through the proof of Theorem 4.5, we can bound the parameters $C_1$, $C_2$ of the Fukuda- $\Lambda$-module $X^{(K_\infty)}$ explicitly as follows.

***Corollary 4.7*** *Suppose that $A$ has potentially good and ordinary reduction at each $v \in S_p$, and let $K_\infty$ be a $\mathbb{Z}_p$-extension of $K$ such that each $v \in S_p$ ramifies in $K_\infty$. Then $X^{(K_\infty)}$ has parameters $(C_1, C_2, 1)$, where*

$$v_p(C_1) \le v_p\big(|A(K_\infty)[p^\infty]|\big) \quad \textit{and} \quad v_p(C_2) \le \sum_{v\in S_{\mathrm{br}}} v_p(c_v) + 2\sum_{v\in S_p} v_p\big(|\widetilde{A}(\mathcal{R}_{K_n\cdot F,v})|\big).$$

*Here, $c_v$ denotes the local Tamagawa factor, $n \in \mathbb{N}$ is chosen large enough such that each $v \in S_p$ has started ramifying in $K_n$, and $F/K$ is a finite extension such that $A$ has good ordinary reduction over $F$.*

**Proof** First, note that $A(K_\infty)[p^\infty]$ is finite, because each $v \in S_p$ ramifies in $K_\infty$ (*cf.* [9, Proposition 3.2,(ii)]). Moreover, if $B_v = A(K_{\infty,v})[p^\infty]$ as in the proof of Theorem 4.5, then $[B_v : (B_v)_{\mathrm{div}}] = v_p(c_v)$ (*cf.* [7, Exercise 4.6]). In particular, these indices can be computed numerically. ■

***Remark 4.8***

(i) We will use the notation from the proof of Theorem 4.5. Suppose now that $A(K)[p^\infty] = \{0\}$. Then the projections $\mathrm{pr}_n^{(\widetilde{K}_\infty)} : X^{(\widetilde{K}_\infty)} \longrightarrow X_n^{(\widetilde{K}_\infty)}$ are surjective for each $n \in \mathbb{N}$ and every $\mathbb{Z}_p$-extension $\widetilde{K}_\infty$ of $K$. Indeed, since $\widetilde{K}_\infty/K$ is a pro-$p$-extension, it follows that $A(\widetilde{K}_\infty)[p^\infty] = \{0\}$. Therefore, the maps $f_n^{(\widetilde{K}_\infty)}$ from the proof of Theorem 4.5 are in fact isomorphisms.

(ii) In the special case $A(K_\infty)[p^\infty] = \{0\}$, the estimates from Corollary 4.7 also simplify. More precisely, we can take $C_1 = 1$, and the upper bound for $C_2$ is sharp: the proof of Theorem 4.5 then shows that

$$|\ker(\overline{\mathrm{pr}}_n^{(K_\infty)})| = |Y_n^{(K_\infty)}/Z_n^{(K_\infty)}| = |U_n|.$$

In view of [9, Remark after Proposition 4.1, and Proposition 4.2], this number is equal to

$$\sum_{v\in S_{\mathrm{br}}} v_p(c_v) + 2\sum_{v\in S_p} v_p\big(|\widetilde{A}(\mathcal{R}_{K_n\cdot F,v})|\big) \tag{4.3}$$

for all sufficiently large $n$.

***Example 4.9*** We consider the elliptic curve

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

defined over $\mathbb{Q}$, and $p = 3$. Then $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $E$ has good ordinary reduction at $p$, and the discriminant of $E$ equals $65 = 5 \cdot 13$. The local Tamagawa factors (*cf.* Corollary 4.7) are all 1; the prime $v = 3$ is totally ramified in the cyclotomic $\mathbb{Z}_3$-extension $K_\infty$ of $\mathbb{Q}$, and $|\widetilde{E}(\mathbb{F}_p)[p^\infty]| = 3$. Therefore, $X^{(K_\infty)}$ is a Fukuda- $\Lambda$-module with parameters $(1, 9)$ by Corollary 4.7 and the above remark.

Exploiting the Fukuda module structure of $X^{(K_\infty)} = \varprojlim X_n^{(K_\infty)}$, we can derive information about $X^{(K_\infty)}$ by studying sufficiently many layers $X_n^{(K_\infty)}$, by an appli-

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

cation of Theorem 3.5. Recall from Section 2 that any finitely generated torsion $\Lambda$-module $X$ has Iwasawa invariants $\mu(X)$ and $\lambda(X)$.

***Corollary 4.10*** *Let $A$ be as in Theorem 4.5, and let $(C_1, C_2)$ be a pair of Fukuda parameters of $X^{(K_\infty)}$. Suppose that there exist at least $v_p(C_1^2 C_2) + 2$ different layers $X_n^{(K_\infty)}$ such that $\operatorname{rank}_p(X_n^{(K_\infty)}) := v_p(|X_n^{(K_\infty)}/(p \cdot X_n^{(K_\infty)})|) = M$ for some $M \in \mathbb{N}$. Then $X^{(K_\infty)}$ is $\Lambda$-torsion, $\mu(X^{(K_\infty)}) = 0$, and $\lambda(X^{(K_\infty)}) \leq MC_1C_2$.*

**Proof** It follows from Corollary 3.8 that $\operatorname{rank}_p(X^{(K_\infty)}) \leq MC_1C_2$ (let $I := (p)$ be the principal ideal generated by $p$ in this corollary). In particular, Nakayama's Lemma implies that $X^{(K_\infty)}$ is a $\mathbb{Z}_p$-module of rank at most $MC_1C_2$, and in particular is $\Lambda$-torsion. ■

Using more general quotients $X/(\lambda \cdot X)$, with arbitrary $\lambda \in \Lambda$, we can now prove an application of Theorem 4.5 that transfers information about the Selmer module $X^{(K_\infty)}$ from some $\mathbb{Z}_p$-extension $K_\infty/K$ to $\mathbb{Z}_p$-extensions $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$, for sufficiently large $m$. The following theorem restates and concretises Theorem 1.1 from the Introduction.

***Theorem 4.11*** *Let $A$ be an abelian variety defined over $K$, and suppose that $A$ has potentially good and ordinary reduction at the primes of $K$ dividing $p$. Let $K_\infty$ be a $\mathbb{Z}_p$-extension of $K$. We assume that $A(K_\infty)[p^\infty]$ is finite and that $X^{(K_\infty)}$ is a torsion $\Lambda$-module. Then there exists a neighbourhood $U = \mathcal{U}(A, K_\infty, m)$ of $K_\infty$ such that*

- *$X^{(\widetilde{K}_\infty)}$ is a torsion $\Lambda$-module for each $\widetilde{K}_\infty \in U$;*
- *$\mu(X^{(\widetilde{K}_\infty)}) \leq \mu(X^{(K_\infty)})$ for each $\widetilde{K}_\infty \in U$;*
- *$\lambda(X^{(\widetilde{K}_\infty)}) \leq \lambda(X^{(K_\infty)})$ for each $\widetilde{K}_\infty \in U$ such that $\mu(X^{(\widetilde{K}_\infty)}) = \mu(X^{(K_\infty)})$.*

**Proof** Let $U = \mathcal{U}(A, K_\infty, m)$ be a neighbourhood of $K_\infty$ as in Theorem 4.5, and suppose that $C_1, C_2 \in \mathbb{N}$ denote integers as in that theorem, bounding the parameters of the Fukuda modules $X^{(\widetilde{K}_\infty)}$ for $\widetilde{K}_\infty \in U$. We let $X = X^{(K_\infty)}$, $C_1 = C_1(X)$, and $C_2 = C_2(X)$, and we choose a polynomial

$$\nu = \nu_{2k,k}(T) := \frac{(T+1)^{p^{2k}} - 1}{(T+1)^{p^k} - 1} \in \Lambda$$

such that

(a) $X/(\nu \cdot X)$ is finite (just choose $\nu$ such that it does not share any non-trivial common factor with the characteristic polynomial $F_X(T)$ of $X$ in $\Lambda$; this is possible because $\nu_{2k,k}(T)$ and $\nu_{2l,l}(T)$ have no common factors as soon as $k \geq 2l$, respectively);
(b) $\lambda(X) < p^{k-1}(p-1)$;
(c) $p^k > k \cdot \lambda(X) + C$, where $C = v_p(|F^{(X)}|) + v_p(C_1^2 \cdot C_2)$, $F^{(X)}$ denoting the maximal finite $\Lambda$-submodule of $X$, and
(d) $k > C$.

For any $\Lambda$-module $M$, we define $\operatorname{rank}_\nu(M) = v_p(|M/(\nu \cdot M)|)$, provided that this is finite. Since $\operatorname{rank}_\nu(X) < \infty$, we have $\operatorname{rank}_\nu(X_i) \leq \operatorname{rank}_\nu(X) + v_p(C_1)$ for each $i \in \mathbb{N}$. This means that there exists an integer $M \leq \operatorname{rank}_\nu(X) + v_p(C_1)$ such that

$$\operatorname{rank}_\nu(X_i) = M$$

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

for infinitely many $i$; choose $m$ large enough such that $\mathrm{rank}_\nu(X_i) = M$ for at least $\nu_p(C_1^2 \cdot C_2) + 2$ different indices $i \le m$. Then Corollary 3.8, applied with the principal ideal $I = (\nu)$, implies that

$$\mathrm{rank}_\nu(X^{(\widetilde{K}_\infty)}) \le M + \nu_p(C_1 \cdot C_2) \le \mathrm{rank}_\nu(X) + \nu_p(C_1^2 C_2)$$

for every $\widetilde{K}_\infty \in U$, because each $X^{(\widetilde{K}_\infty)}$ is a Fukuda- $\Lambda$-module with parameters at most $C_1$, $C_2$ by Theorem 4.5. If $E_{X^{(\widetilde{K}_\infty)}}$ denotes the elementary $\Lambda$-module attached to $X^{(\widetilde{K}_\infty)}$, then

$$\mathrm{rank}_\nu(E_{X^{(\widetilde{K}_\infty)}}) \le \mathrm{rank}_\nu(X^{(\widetilde{K}_\infty)})$$

for each $\widetilde{K}_\infty \in \mathcal{E}(K)$ (and for each $\nu \in \Lambda$); *cf.* [16, Proposition 3.4 and the proof of Theorem 3.10]. Therefore, $X^{(\widetilde{K}_\infty)}$ is a torsion $\Lambda$-module for each $\widetilde{K}_\infty \in U$. On the other hand, since $\frac{\lambda(X)}{p^{k-1}(p-1)} < 1$, we have

$$\text{(4.4)}\quad \mathrm{rank}_\nu(E_X) = (p^{2k} - p^k)\mu(X) + (2k-k)\lambda(X) = p^k(p^k-1)\mu(X) + k\lambda(X).$$

The first equality can be seen as follows. The quotient $Z := \Lambda/(\nu)$ is a free $\mathbb{Z}_p$-module, and multiplication by $T$ is a $\mathbb{Z}_p$-linear map on $Z$ with eigenvalues equal to the roots of the polynomial $\nu$ in some fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, *i.e.* given by $\zeta - 1$, where $\zeta$ runs over the primitive $p^l$-th roots of unity in $\overline{\mathbb{Q}}_p$, $k < l \le 2k$. For every divisor $h_i$ of $F_X(T)$, the quotient $\Lambda/(h_i, \nu)$ is the cokernel of the endomorphism on $Z$ given by multiplication by $h_i$. This map has eigenvalues $h_i(\zeta - 1)$, $\zeta$ as above, and the order of the cokernel is associated in $\mathbb{Z}_p$ with the determinant, *i.e.*, the product of the eigenvalues.

Since $F_X(T) = \prod_i h_i$, we can conclude that

$$\mathrm{rank}_\nu(E_X) = \sum_{\substack{k<l\le 2k \\ \zeta^{p^l}=1}} \nu_p\big(F_X(\zeta-1)\big).$$

Now $F_X(T)$ is associated with $p^{\mu(X)}$ times a distinguished polynomial of degree $\lambda(X)$. If $\frac{\lambda(X)}{p^{k-1}(p-1)} < 1$, then $\nu_p(F_X(\zeta - 1)) = \mu(X) + \frac{\lambda(X)}{p^{l-1}(p-1)}$ for each $\zeta$ of exact order $p^l$, $k < l$. This proves the first equality in (4.4).

Furthermore, $\mathrm{rank}_\nu(X) \le \mathrm{rank}_\nu(E_X) + \nu_p(|F^{(X)}|)$ by [16, Proposition 3.4]. Summarising,

$$\text{(4.5)}\quad \mathrm{rank}_\nu(E_{X^{(\widetilde{K}_\infty)}}) \le p^k(p^k-1)\mu(X) + k\lambda(X) + C$$

for each $\widetilde{K}_\infty \in U$, where $C$ is as in condition (c) above.

The statement of the theorem now follows by imitating the proof of [16, Theorem 3.10]. First, $\mathrm{rank}_\nu(E_{X^{(\widetilde{K}_\infty)}}) \ge p^k(p^k-1)\mu(X^{(\widetilde{K}_\infty)})$, and therefore $\mu(X^{(\widetilde{K}_\infty)}) \le \mu(X)$ because of assumption (c) above. Now we restrict to the subset of $\mathbb{Z}_p$-extensions $\widetilde{K}_\infty$ of $K$ that satisfy $\mu(X^{(\widetilde{K}_\infty)}) = \mu(X)$; from now on we will assume that $\mu(X) = \mu(X^{(\widetilde{K}_\infty)}) = 0$. This means that

$$\mathrm{rank}_\nu(E_{X^{(\widetilde{K}_\infty)}}) \le k \cdot \lambda(X) + C$$

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

for each $\widetilde{K}_\infty \in U$. Similarly as above,

$$\operatorname{rank}_\nu(E_{X(\widetilde{K}_\infty)}) = \sum_{\substack{k<l\le 2k \\ \zeta^{p^l}=1}} v_p\big(F_{X(\widetilde{K}_\infty)}(\zeta-1)\big).$$

If $\lambda(X^{(\widetilde{K}_\infty)}) = \deg(F_{X(\widetilde{K}_\infty)})$ is greater than or equal to $p^k(p-1)$, then

$$v_p\big(F_{X(\widetilde{K}_\infty)}(\zeta-1)\big) \ge 1$$

for each primitive $p^{k+1}$-th root of unity, and therefore, $\operatorname{rank}_\nu(E_{X(\widetilde{K}_\infty)}) \ge p^k(p-1)$, yielding a contradiction to assumption (c). Therefore,

$$\operatorname{rank}_\nu(E_{X(\widetilde{K}_\infty)}) = k\cdot\lambda(X^{(\widetilde{K}_\infty)}) \le k\cdot\lambda(X) + C,$$

and thus $\lambda(X^{(\widetilde{K}_\infty)}) \le \lambda(X)$, because $k > C$ by assumption (d). ■

Let us state an important special case.

***Corollary 4.12*** *Let $A$ be an elliptic curve defined over $\mathbb{Q}$, and suppose that $K/\mathbb{Q}$ is abelian, and that $A$ has potentially good and ordinary reduction at the primes of $K$ dividing $p$. Let $K_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension. Then there exists a neighbourhood $U = \mathcal{E}(K_\infty, m)$, $m \in \mathbb{N}$, in the sense of Greenberg's original topology from [6], such that the conclusions of Theorem 4.11 hold for each $\widetilde{K}_\infty \in U$.*

**Proof** Since each prime of $K$ dividing $p$ ramifies in $K_\infty$, it follows from [9, Proposition 3.2,(ii)] that $A(K_\infty)[p^\infty]$ is finite. The main result of [14] implies that $X^{(K_\infty)}$ is $\Lambda$-torsion, because $K$ is abelian. Moreover, as each prime of $K$ is finitely decomposed in $K_\infty$, $\mathcal{U}(A, K_\infty, m) = \mathcal{E}(K, m)$ as long as $m$ has been chosen large enough to ensure that each prime of $K$ dividing $p$ has already started ramifying in $K_m$. ■

If $X^{(K_\infty)}$ is not known to be $\Lambda$-torsion, then we can at least bound the $\Lambda$-rank of (the maximal torsion-free quotient of) $X^{(\widetilde{K}_\infty)}$ in some neighbourhood $U$.

***Lemma 4.13*** *Let $A$ be an abelian variety defined over $K$, and suppose that $A$ has potentially good and ordinary reduction at the primes of $K$ dividing $p$. We assume that $K_\infty$ denotes a $\mathbb{Z}_p$-extension of $K$ such that $B = A(K_\infty)[p^\infty]$ is finite. Then there exists a constant $r \in \mathbb{N}$ such that*

$$\operatorname{rank}_\Lambda(X^{(\widetilde{K}_\infty)}) \le \operatorname{rank}_\Lambda(X^{(K_\infty)}) + r$$

*for each $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$, $m \in \mathbb{N}$ sufficiently large.*

**Proof** We consider $\operatorname{rank}_{(p,T)}(X^{(\widetilde{K}_\infty)}) = v_p(|X^{(\widetilde{K}_\infty)}/((p,T)\cdot X^{(\widetilde{K}_\infty)})|)$. First, note that

$$\operatorname{rank}_{(p,T)}(X^{(K_\infty)}) \le \operatorname{rank}_\Lambda(X^{(K_\infty)}) + v_p(|F^{(X^{(K_\infty)})}|) + s,$$

where $F^{(X^{(K_\infty)})}$ denotes the maximal finite submodule of $X^{(K_\infty)}$, as in the proof of Theorem 4.11, and where $s$ denotes the number of summands $\Lambda/(h)$ of an elementary $\Lambda$-module $E$ corresponding to $X^{(K_\infty)}$.

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

Let $(C_1^{(K_\infty)}, C_2^{(K_\infty)})$ be the parameters of the Fukuda- $\Lambda$-module $X^{(K_\infty)}$. Then

$$\operatorname{rank}_{(p,T)}(X_i^{(K_\infty)}) \le \operatorname{rank}_{(p,T)}(X^{(K_\infty)}) + v_p(C_1^{(K_\infty)})$$

for each $i \in \mathbb{N}$, and Theorem 4.5 and Corollary 3.8 (applied with the ideal $I = (p, T)$) imply that

$$\operatorname{rank}_{(p,T)}(X^{(\widetilde{K}_\infty)}) \le \operatorname{rank}_{(p,T)}(X^{(K_\infty)}) + v_p(C)$$

for each $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$ and some fixed $C \in \mathbb{N}$, provided that $m$ is sufficiently large. Since

$$\operatorname{rank}_\Lambda(X^{(\widetilde{K}_\infty)}) \le \operatorname{rank}_{(p,T)}(X^{(\widetilde{K}_\infty)}),$$

the statement of the lemma follows. ∎

Let us conclude the current section by pointing out briefly that the above approach can also be used for the consideration of Selmer groups in multiple $\mathbb{Z}_p$-extensions. In order to be able to directly adapt the proof of Theorem 4.5 to $\mathbb{Z}_p^d$-extensions, $d > 1$, we will restrict to a special situation.

(a) Since $\operatorname{Gal}(K_\infty/K) \cong \mathbb{Z}_p^d$, $d > 1$ is not longer pro-cyclic, our argument for bounding $|C^{(\widetilde{K}_\infty)}| \le |B^{(K_\infty)}|$ used in the proof of Theorem 4.5 does not apply; we therefore assume the boundedness of $|B^{(\widetilde{K}_\infty)}|$ in a suitable neighbourhood of $K_\infty$. A sufficient condition for $|B^{(\widetilde{K}_\infty)}|$ to being finite is that each $v \in S_p$ is almost totally ramified in $\widetilde{K}_\infty$, *i.e.*, that the corresponding inertia subgroups in $\operatorname{Gal}(\widetilde{K}_\infty/K) \cong \mathbb{Z}_p^d$ have $\mathbb{Z}_p$-rank $d$ (*cf.* [9, Proposition 3.2,(ii)]; the main point is that the residue field of $\widetilde{K}_{\infty,v}$ is then finite for each $v \in S_p$).

(b) If $d > 1$, then each prime $v \nmid p$ splits into infinitely many primes in $K_\infty$. In order to nevertheless bound the contribution to $|U_n|$, we do not know how to do better than assuming that $A(K_v)[p^\infty] = \{0\}$ for each $v \in S_{\mathrm{br}}$ (which ensures that in fact $A(\widetilde{K}_{\infty,v})[p^\infty] = \{0\}$ for each $\mathbb{Z}_p^d$-extension $\widetilde{K}_\infty$ of $K$).

For a $\mathbb{Z}_p^d$-extension $K_\infty$ of $K$ and any $m \in \mathbb{N}$, we denote by $\mathcal{E}(K_\infty, m)$ the set of $\mathbb{Z}_p^d$-extensions $\widetilde{K}_\infty$ of $K$ such that $(\widetilde{K}_\infty \cap K_\infty) \supseteq K_n$, where $K_n$ denotes the intermediate field of $K_\infty/K$ that is fixed by $\operatorname{Gal}(K_\infty/K)^{p^n}$ (i.e., $\operatorname{Gal}(K_n/K)$ is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^d$).

Using this notation, we can formulate a generalisation of Theorem 4.5.

**Theorem 4.14** *Suppose that $A$ has potentially good and ordinary reduction at each prime of $K$ dividing $p$, and that these primes are almost totally ramified in the $\mathbb{Z}_p^d$-extension $K_\infty/K$. We assume that $A(K_v)[p^\infty] = \{0\}$ for each prime $v$ of bad reduction, and that $|A(\mathbb{K})[p^\infty]|$ is finite, where $\mathbb{K}$ denotes the composite of all $\mathbb{Z}_p$-extensions of $K$. Then there exists an integer $m \in \mathbb{N}$ such that $X^{(\widetilde{K}_\infty)}$ is a Fukuda- $\Lambda_d$-module with bounded parameters $(C_1, C_2, 1)$ for each $\widetilde{K}_\infty \in \mathcal{E}(K_\infty, m)$.*

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

Note: if $S_{\mathrm{br}} \neq \emptyset$, then the fact that $A(K_v)[p^\infty] = \{0\}$ for $v \in S_{\mathrm{br}}$ also implies that automatically

$$A(K)[p^\infty] = A(\mathbb{K})[p^\infty] = \{0\}.$$

**Proof** We start from an exact sequence

$$W_n \longrightarrow Y_n^{(\widetilde{K}_\infty)}/Z_n^{(\widetilde{K}_\infty)} \longrightarrow U_n \longrightarrow V_n \longrightarrow \operatorname{coker}(\mathrm{pr}_n^{(\widetilde{K}_\infty)}) \longrightarrow 0,$$

and we have to bound $|U_n|$, $|V_n|$, and $|W_n|$ uniformly in $n$.

For $|U_n|$, we proceed as in the proof of Theorem 4.5. The primes $v \in S_{\mathrm{br}}$ do not contribute to $|U_n|$, since $B_v = A(K_v)[p^\infty] = \{0\}$, and therefore $A(\widetilde{K}_{\infty,v})[p^\infty] = \{0\}$ for each such prime $v$ and every $\mathbb{Z}_p^d$-extension $\widetilde{K}_\infty$ of $K$. For a ramified prime $v \in S_p$, we can use [9, Proposition 4.2] in order to conclude that the contribution to $|U_n|$ is bounded by $|\widetilde{A}(\mathcal{R}_v)[p^\infty]|^2$ for some fixed finite extension $\mathcal{R}_v$ of $\mathbb{F}_p$ that arises as residue field of the completion at $v$ of a finite extension $F$ of $K$ such that $A$ has good ordinary reduction over $F$ and such that the residue fields of the primes in $S_p$ have stabilised in $K_\infty \cap F$. If $m$ has been chosen large enough such that $K_\infty \cap F$ is contained in the $m$-th layer $K_m := K_\infty^{\mathrm{Gal}(K_\infty/K)^{p^m}}$, and such that each prime $v \in S_p$ is totally ramified in $K_\infty/K_{m-1}$, then this extension $F$ can be used for each $\widetilde{K}_\infty \in \mathcal{E}(K_\infty, m)$. Finally, if $v \nmid p$ is a prime of good reduction, then it does not contribute to $|U_n|$ by [9, Proposition 4.1].

Using the results of [9, Section 3], we can bound $|V_n|$ and $|W_n|$ (recall from the proof of Theorem 4.5 that, in fact, $|W_n| = 1$ for $\mathbb{Z}_p^1$-extensions of $K$). Indeed, the proof of [9, Proposition 3.1] implies that letting $B := B^{(K_\infty)}$, we have

$$|V_n^{(K_\infty)}| = |H^1(\Gamma_n, B)| \leq |B|^d \quad \text{and} \quad |W_n^{(K_\infty)}| \leq |H^2(\Gamma_n, B)| \leq |B|^{d^2}$$

for each $n \in \mathbb{N}$, where $\Gamma_n = \mathrm{Gal}(K_\infty/K)^{p^n}$ (here we see that $|W_n^{(K_\infty)}| = 1$ for a $\mathbb{Z}_p^1$-extension, since in this case $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ has $p$-cohomological dimension 1). By assumption, $A(\mathbb{K})[p^\infty] \supseteq B$ is finite; this shows that $|V_n^{(\widetilde{K}_\infty)}|$ and $|W_n^{(\widetilde{K}_\infty)}|$ are bounded on $\mathcal{E}(K_\infty, m)$.

In particular, if $S_{\mathrm{br}} \neq \emptyset$, then $B^{(\mathbb{K})} = \{0\}$, and therefore $|V_n^{(\widetilde{K}_\infty)}| = |W_n^{(\widetilde{K}_\infty)}| = 1$ for each $n$ and every $\widetilde{K}_\infty$. ∎

***Remark 4.15*** Restrictions on the number of rational $p$-torsion points seem necessary in order to bound the Fukuda parameters: starting from *any* abelian variety $A$ over any number field $K$, Greenberg constructed in [9, end of Section 3] an example of a $\mathbb{Z}_p^d$-extension $L_\infty$ of $L := K(A[p^\infty])$ such that $L_\infty/K$ is normal and $|V_n|$ is unbounded in $L_\infty/L$ as $n \to \infty$ (of course $L$ is not longer a number field, but the unboundedness of $|A(L)[p^\infty]|$, and thus of $|A(L_\infty)[p^\infty]|$, seems to play a role here).

We have seen in the proof of Theorem 4.14 that

$$|V_n^{(\widetilde{K}_\infty)}| = |H^1(\Gamma_n, B^{(\widetilde{K}_\infty)})|.$$

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

On the other hand, as Greenberg notes on [9, p. 262], for $p \neq 2$ and an arbitrary $\mathbb{Z}_p^d$-extension $K_\infty/K$, we have an isomorphism

$$W_n^{(K_\infty)} \cong H^2(\Gamma_n, B^{(K_\infty)}).$$

It seems plausible that the orders of these cohomology groups can be unbounded if $B^{(\mathbb{K})} = A(\mathbb{K})[p^\infty]$ is infinite.

Using Theorem 4.14, one can prove an analogue of Theorem 4.11 for bounding the so-called *generalised Iwasawa invariants* of Selmer groups $X^{(K_\infty)}$ for multiple $\mathbb{Z}_p$-extensions (using arguments from [17, 18]). Finally, one can also generalise Lemma 4.13. For any finitely generated $\Lambda_d$-module $X$, we denote by $\operatorname{rank}_{\Lambda_d}(X)$ the rank of the maximal torsion-free quotient of the elementary $\Lambda_d$-module $E_X$, and we let $\dim(X)$ denote the Krull dimension of $\Lambda_d/\operatorname{Ann}(X)$, where $\operatorname{Ann}(X) \subseteq \Lambda_d$ denotes the annihilator ideal of $X$ (which is $(0)$ if $X$ is not $\Lambda_d$-torsion). Then $\dim(X)$ is smaller than or equal to the Krull dimension $d+1$ of $\Lambda_d$, it is at most $d$ if $X$ is $\Lambda_d$-torsion, and typically can be even smaller. One should also compare this with the dimension of the classical Fukuda module $X^{(K_\infty)} = \varprojlim X_n$ attached to the $\mathbb{Z}_p^d$-extension $K_\infty/K$, as defined in Example 3.2. This $\Lambda_d$-module often happens to be *pseudo-null*, which means that $\dim(X^{(K_\infty)}) \leq d-1 = \dim(\Lambda_d) - 2$. For instance, if $K_\infty = \mathbb{K}$ denotes the composite of all $\mathbb{Z}_p$-extensions of $K$, then by Greenberg's Generalised Conjecture (*cf.* [8, Conjecture 3.5]) $X^{(K_\infty)}$ should be pseudo-null as a $\Lambda_d$-module. We also mention the following special case: over $\Lambda_1 = \Lambda$, a Noetherian module $X$ is pseudo-null if and only if $X$ is finite.

Recall that $\mathcal{E}(K_\infty, m)$ denotes a neighbourhood with respect to Greenberg's topology, *i.e.*, it contains every $\mathbb{Z}_p^d$-extension $\widetilde{K}_\infty$ of $K$ that coincides with $K_\infty$ up to the $m$-th layer; we defined these sets in the paragraph before Theorem 4.14.

***Lemma 4.16*** *In the situation of Theorem 4.14, there exists a neighbourhood $U = \mathcal{E}(K_\infty, m)$, $m \in \mathbb{N}$, of $K_\infty$ such that*

(i) $\operatorname{rank}_{\Lambda_d}(X^{(\widetilde{K}_\infty)}) \leq \operatorname{rank}_{\Lambda_d}(X^{(K_\infty)}) + r$ *for each* $\widetilde{K}_\infty \in U$, *where* $r \in \mathbb{N}$ *denotes a fixed constant, and*

(ii) $\dim(X^{(\widetilde{K}_\infty)}) \leq \dim(X^{(K_\infty)})$ *for each* $\widetilde{K}_\infty \in U$.

**Proof** We start with the proof of (ii). Letting $s = \dim(X^{(K_\infty)})$, there exist elements $f_1, \ldots, f_s$ contained in the maximal ideal $(p, T_1, \ldots, T_d)$ of $\Lambda_d$ such that $X^{(K_\infty)}/((f_1, \ldots, f_s) \cdot X^{(K_\infty)})$ is finite. We let

$$\operatorname{rank}_{(f_1,\ldots,f_s)}(X^{(K_\infty)}) = v_p\big(|X^{(K_\infty)}/((f_1, \ldots, f_s) \cdot X^{(K_\infty)})|\big).$$

As in the proof of Lemma 4.13, Corollary 3.8 implies that for sufficiently large $m \in \mathbb{N}$, we have

$$\operatorname{rank}_{(f_1,\ldots,f_s)}(X^{(\widetilde{K}_\infty)}) \leq \operatorname{rank}_{(f_1,\ldots,f_s)}(X^{(K_\infty)}) + v_p(C)$$

for some constant $C \in \mathbb{N}$. In other words, $X^{(\widetilde{K}_\infty)}/((f_1, \ldots, f_s) \cdot X^{(\widetilde{K}_\infty)})$ is finite for each $\widetilde{K}_\infty \in U$, and therefore $\dim(X^{(\widetilde{K}_\infty)}) \leq s$.

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

Statement (i) can be proved analogously by working with $(p, T_1, \dots, T_d)$-ranks. As in the proof of Lemma 4.13, we cannot avoid the occurrence of some fixed constant $r$ in our estimate. ∎

# 5 Further Applications

In this section, we will study several topics that are related to the theory of Selmer groups. We will still use the general notation from Sections 2 and 4.

## 5.1 Mordell-Weil Groups and Tate–Shafarevich Groups

Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension. In this subsection, we will apply the Fukuda module structure of the Selmer group $X^{(K_\infty)}$ to modules related to $X^{(K_\infty)}$ via the exact sequences (1.1) from the Introduction. Dualising (1.1), we obtain the following commutative diagram:

$$\begin{tikzcd}
 & (\text{Ш}_A(K_\infty)^\vee)_{\Gamma_n} \arrow[r] \arrow[d, "s_n^{\text{Ш}}"] & (X^{(K_\infty)})_{\Gamma_n} \arrow[r] \arrow[d, "\mathrm{pr}_n"] & (\widehat{A}^{(K_\infty)})_{\Gamma_n} \arrow[r] \arrow[d, "s_n^A"] & 0 \\
0 \arrow[r] & \text{Ш}_A(K_n)^\vee \arrow[r] & X_n^{(K_\infty)} \arrow[r] & \widehat{A}^{(K_n)} \arrow[r] & 0.
\end{tikzcd}$$

Here, $\text{Ш}_A(K_n)^\vee$, $n \in \mathbb{N}$, denotes the Pontryagin dual of the $p$-primary subgroup of the Tate-Shafarevich group, as defined in Section 2, and $\widehat{A}^{(K_n)}$ denotes the Pontryagin dual of $A(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, *i.e.*,

$$\widehat{A}^{(K_n)} \cong \mathrm{Hom}_{\mathrm{cont}}(A(K_n), \mathbb{Z}_p) \cong \mathbb{Z}_p^{\mathrm{rank}_{\mathbb{Z}}(A(K_n))}.$$

$\widehat{A}^{(K_\infty)}$ and $\text{Ш}_A(K_\infty)^\vee$ are defined analogously. The maps $s_n^A$ and $s_n^{\text{Ш}}$ are chosen such that the diagram is commutative (note that $\mathrm{pr}_n$ is induced by the cohomological corestriction map, and therefore, $s_n^A$ is induced by the norm map, *cf.* [21, Appendix 2]). The snake lemma yields an exact sequence

$$\ker(\mathrm{pr}_n) \longrightarrow \ker(s_n^A) \longrightarrow \mathrm{coker}(s_n^{\text{Ш}}) \longrightarrow \mathrm{coker}(\mathrm{pr}_n) \longrightarrow \mathrm{coker}(s_n^A) \longrightarrow 0\,.$$

If $A$ has potentially good ordinary reduction at each prime $v \in S_p$, then $X^{(K_\infty)}$ is a Fukuda module by Corollary 4.2; in the following, we will write $(C_1, C_2)$ for the Fukuda parameters of $X^{(K_\infty)}$. In particular, $|\mathrm{coker}(s_n^A)|$ is then bounded as $n \to \infty$, and the order of $\ker(s_n^A)$ is bounded if and only if the order of $\mathrm{coker}(s_n^{\text{Ш}})$ is bounded.

We now make the following assumption.

***Assumption 5.1*** There exists an integer $l$ such that

$$\mathrm{rank}_{\mathbb{Z}}(A(K_m)) = \mathrm{rank}_{\mathbb{Z}}(A(K_l))$$

for every $m \geq l$, and $\mathrm{coker}(s_n^{\text{Ш}})$ is finite for each $n < l$.

***Lemma 5.2*** *Let $A$ be an abelian variety defined over $K$, and suppose that $A$ has potentially good ordinary reduction at each prime $v \in S_p$. Under Assumption 5.1, $\widehat{A}^{(K_\infty)} = \varprojlim \widehat{A}^{(K_n)}$ is a Fukuda- $\Lambda$-module with parameters $(C_1, C \cdot C_2, 1)$, for a suitable $C \in \mathbb{N}$.*

**Proof** First, note that $|\mathrm{coker}(s_n^{\text{Ш}})|$ is bounded. Indeed, the maps $s_n^A$ from the above commutative diagram have finite cokernels; since $\widehat{A}^{(K_n)}$ and $\widehat{A}^{(K_\infty)}$ are free $\mathbb{Z}_p$-modules of the same rank for every $n \geq l$ by Assumption 5.1, it follows that $\widehat{A}^{(K_\infty)} \cong (\widehat{A}^{(K_\infty)})_{\Gamma_n} \cong \widehat{A}^{(K_n)}$ and that the $s_n^A$ are actually injective for all $n \geq l$, and therefore

$$|\mathrm{coker}(s_n^{\text{Ш}})| \leq |\mathrm{coker}(\mathrm{pr}_n)| \leq C_1$$

for every $n \geq l$. This means that

$$|\mathrm{coker}(s_n^{\text{Ш}})| \leq C := \max\left(C_1, |\mathrm{coker}(s_1^{\text{Ш}})|, \ldots, |\mathrm{coker}(s_{l-1}^{\text{Ш}})|\right)$$

for every $n \in \mathbb{N}$.

Using the exact sequence

$$0 \longrightarrow \text{Ш}_A(K_\infty)^\vee \longrightarrow X^{(K_\infty)} \longrightarrow \widehat{A}^{(K_\infty)} \longrightarrow 0\,,$$

Proposition 3.7 implies that $\widehat{A}^{(K_\infty)}$ is a $(C_1, C \cdot C_2, 1)$-Fukuda- $\Lambda$-module. ■

***Lemma 5.3*** *Let $A$ be an abelian variety defined over $K$ that has potentially good ordinary reduction at each prime $v \in S_p$. Suppose that*

$$\mathrm{rank}_{\mathbb{Z}}(A(K_m)) = \mathrm{rank}_{\mathbb{Z}}(A(K))$$

*for all $m \in \mathbb{N}$, that $\text{Ш}_A(K)$ is finite, and let $C := \max(C_1, |\text{Ш}_A(K)|)$ (cf. also the constant defined in the proof of Lemma 5.2).*

*Then $\text{Ш}_A(K_\infty)^\vee = \varprojlim \text{Ш}_A(K_n)^\vee$ is a $(C, C_2, 1)$-Fukuda- $\Lambda$-module.*

**Proof** Since $\mathrm{rank}_{\mathbb{Z}}(A(K_\infty)) = \mathrm{rank}_{\mathbb{Z}}(A(K))$, the polynomials

$$v_{n+1,n}(T) = \frac{(T+1)^{p^{n+1}} - 1}{(T+1)^{p^n} - 1} = \frac{w_{n+1,0}(T)}{w_{n,0}(T)}$$

do not share any non-trivial common factor with the characteristic power series of $\widehat{A}^{(K_\infty)}$, because the quotient $(T \cdot \widehat{A}^{(K_\infty)})/(w_{n,0}(T) \cdot \widehat{A}^{(K_\infty)})$ is finite for all $n$. Therefore, Proposition 3.9 can be applied with the choices $Z_n^{(B)} := w_{n,0}(T) \cdot X^{(K_\infty)}$ and $f_{n+1,n} := v_{n+1,n}(T)$; note that $X^{(K_\infty)}/\text{Ш}_A(K_\infty)^\vee \cong \widehat{A}^{(K_\infty)}$ is $\Lambda$-torsion as finitely generated $\mathbb{Z}_p$-module. Moreover, $\widehat{A}^{(K_\infty)} \cong \mathbb{Z}_p^{\mathrm{rank}_{\mathbb{Z}}(A(K_\infty))}$ does not contain any non-trivial finite $\Lambda$-submodules. Therefore, (the proof of) Proposition 3.9 implies that $\text{Ш}_A(K_\infty)^\vee$ is a Fukuda-submodule of $X^{(K_\infty)}$ with parameters $(C, C_2, 1)$. ■

***Remark 5.4*** In the situation of Lemma 5.3, if the $\text{Ш}_A(K_n)$ are finite for all $n \in \mathbb{N}$, then $v_p(|\text{Ш}_A(K_n)|)$ grows asymptotically as in Iwasawa's famous class number formula, *i.e.*,

$$v_p\left(|\text{Ш}_A(K_n)|\right) = \mu\left(\text{Ш}_A(K_\infty)^\vee\right) \cdot p^n + \lambda\left(\text{Ш}_A(K_\infty)^\vee\right) \cdot n + O(1).$$

***Lemma 5.5*** *If $X^{(K_\infty)}$ is $\Lambda$-torsion, then the first part of Assumption 5.1 holds.*

**Proof** It is well known that $\mathrm{rank}_{\mathbb{Z}}(A(K_n)) \leq \lambda(X^{(K_\infty)})$ for all $n \in \mathbb{N}$ (see, *e.g.*, the proof of [7, Corollary 4.9]): this follows from the exact sequences (1.1) by using that $\widehat{X^{(K_\infty)}}_{\mathrm{div}} = \mathrm{Sel}_A(K_\infty)_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$, via application of the Control Theorem 4.1. In particular, there exists some $l \in \mathbb{N}$ such that $\mathrm{rank}_{\mathbb{Z}}(A(K_n)) = \mathrm{rank}_{\mathbb{Z}}(A(K_l))$ for all $n \geq l$. ■

***Remark 5.6***

(i) $X^{(K_\infty)}$ is conjectured to be $\Lambda$-torsion (which implies the first part of Assumption 5.1 by Lemma 5.5) if $K_\infty/K$ is the cyclotomic $\mathbb{Z}_p$-extension and $A = E$ is an elliptic curve with potentially good and ordinary reduction at each $v \in S_p$; this conjecture is a theorem when $A$ is defined over $\mathbb{Q}$ and $K$ is abelian ([14, 26]). On the other hand, it is known that there exist (non-cyclotomic) $\mathbb{Z}_p$-extensions $\widetilde{K}_\infty/K$ such that $X^{(\widetilde{K}_\infty)}$ has $\Lambda$-rank greater than zero, *e.g.*, if $A = E$ is an elliptic curve over $\mathbb{Q}$ and $\widetilde{K}_\infty$ is the *anticyclotomic* $\mathbb{Z}_p$-extension of an imaginary quadratic number field $K$ such that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$, $E$ has good ordinary reduction at $p$, and the Hasse-Weil $L$-series $L(E, s)$ has an odd order zero at $s = 1$ (*cf.* [7, Theorem 1.8]).

(ii) Turning towards the second part of Assumption 5.1: it is conjectured that the Tate–Shafarevich group attached to any abelian variety over any number field is finite. Note that we are not assuming that $|\text{Ш}_A(K_n)|$ is bounded as $n \to \infty$.

On the other hand, if we know that Assumption 5.1 holds, and if

$$|\text{Ш}_A(K_m)| = |\text{Ш}_A(K_{m+1})| = \ldots = |\text{Ш}_A(K_{m+k})|$$

for some $m \in \mathbb{N}$ and some sufficiently large $k \in \mathbb{N}$ (the necessary magnitude of $k$ depends on a bound $C$ as in (the proof of) Lemma 5.2), then we can deduce that the $|\text{Ш}_A(K_n)|$ are actually bounded, and therefore, that $\text{Ш}_A(K_\infty)$ is finite.

Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension. Then Theorem 4.11 can be used to bound the growth of $\mathrm{rank}_{\mathbb{Z}}(A(\widetilde{K}_i))$, $i \in \mathbb{N}$, for all $\mathbb{Z}_p$-extensions $\widetilde{K}_\infty$ of $K$ that are close to $K_\infty$.

***Lemma 5.7*** *Let $A$, $K_\infty$, and $X^{(K_\infty)}$ be as in Theorem 4.11, and let $\lambda = \lambda(X^{(K_\infty)})$. If $U = \mathcal{U}(K_\infty, m)$ denotes a neighbourhood as in Theorem 4.11, then*

$$\mathrm{rank}_{\mathbb{Z}}(A(\widetilde{K}_n)) \leq \lambda$$

*for each $\widetilde{K}_\infty \in U$ satisfying $\mu(X^{(\widetilde{K}_\infty)}) = \mu(X^{(K_\infty)})$ and for every $n \in \mathbb{N}$.*

**Proof** By the choice of $U$, we have $\lambda(X^{(\widetilde{K}_\infty)}) \leq \lambda$ for each $\widetilde{K}_\infty \in U$ satisfying $\mu(X^{(\widetilde{K}_\infty)}) = \mu(X^{(K_\infty)})$. As in the proof of Lemma 5.5, this bounds the Mordell-Weil ranks: $\mathrm{rank}_{\mathbb{Z}}(A(\widetilde{K}_n)) \leq \lambda$ for each such $\widetilde{K}_\infty \in U$ and every $n \in \mathbb{N}$. ■

***Remark 5.8*** More generally, if $X^{(K_\infty)}$ is not necessarily $\Lambda$-torsion, then Lemma 4.13 together with [7, Corollary 4.12] implies that there exists a neighbourhood $U = \mathcal{U}(K_\infty, m)$ of $K_\infty$ such that

$$\mathrm{rank}_{\mathbb{Z}}(A(\widetilde{K}_n)) \leq (\mathrm{rank}_\Lambda(X^{(K_\infty)}) + r_1) \cdot p^n + r_2$$

for suitable constants $r_1, r_2 \in \mathbb{N}$ that do not depend on $n$; $r_1$, moreover, is independent from $\widetilde{K}_\infty$.

We now briefly describe why these results might prove useful for numerical computations. In the following, we will always assume that $A = E$ is an elliptic curve

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

defined over $\mathbb{Q}$, which will be considered over a number field $K$, and that $E$ has good ordinary reduction at the primes of $K$ dividing $p$. Mordell–Weil ranks in a cyclotomic tower are often bounded via analytical tools. More precisely, let $K_\infty = K_\infty^{cyc}$ be the cyclotomic $\mathbb{Z}_p$-extension of $K$. Under the main conjecture, the Iwasawa invariants of $X^{(K_\infty)}$ are equal to the analytical Iwasawa invariants $\mu^{an}(K)$ and $\lambda^{an}(K)$ of the $p$-adic $L$-function $L_p(E,s) \in \Lambda = \mathbb{Z}_p[\![T]\!]$. Therefore, the corresponding analytical $\lambda$-invariant (which is by definition the degree of the distinguished polynomial associated with $L_p(E,s)$ via the Weierstraß Preparation Theorem) bounds the Mordell–Weil ranks of the $A(K_n)$, $n \in \mathbb{N}$. Note: for this bound, one part of the main conjecture suffices, namely, the inequality $\lambda(X^{(K_\infty)}) \leq \lambda^{an}(K)$; this direction has been proved in [14] for abelian $K$ under the above ordinaryness assumption—the reverse inequality is also known in many cases due to the work of Skinner and Urban (*cf.* [28]).

However, this approach only works for the cyclotomic $\mathbb{Z}_p$-extension, and only if (one part of) the main conjecture is known over $K$; to the best of the author's knowledge, there does not exist any family of fields $K$ which are not abelian over $\mathbb{Q}$ or over an imaginary quadratic number field, and for which the main conjecture is known.

If $K$ is imaginary quadratic, then there exist further special $\mathbb{Z}_p$-extensions of $K$, like the anticyclotomic $\mathbb{Z}_p$-extension $K_\infty^{anti}$, for which main conjectures have been proved in some cases. If $E$ is a non-CM elliptic curve defined over $\mathbb{Q}$, then inequalities of the form $\lambda(X^{(K_\infty^{anti})}) \leq \lambda^{an}(K)$ (for a suitable analytic $\lambda$-invariant) have been obtained first by Bertolini–Darmon and Darmon–Iovita (*cf.* [1, 4]). Suppose now that $E$ is an elliptic curve which has CM by the ring of integers $\mathcal{O}_K$ of $K$, and that $E$ has good ordinary reduction at a prime $p > 3$. If $p$ splits in $K$, $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, then Rubin (*cf.* [27]) has proved a main conjecture for the unique $\mathbb{Z}_p$-extension $K_\infty^{\mathfrak{p}}$ of $K$ that is unramified outside of $\mathfrak{p}$.

By application of Theorem 4.11 to $X^{(K_\infty)}$ for a given $\mathbb{Z}_p$-extension $K_\infty/K$, we obtain bounds for the growth of the Mordell–Weil ranks in infinitely many $\mathbb{Z}_p$-extensions $\widetilde{K}_\infty \neq K_\infty$. Moreover, as pointed out in Corollary 4.10, we can in principle use Fukuda theory for obtaining upper bounds for the Iwasawa invariants of $X^{(K_\infty)}$ via computation of the first layers $X_n$, without using any analytical information about $p$-adic $L$-functions.

***Example 5.9*** Let $A = E$ be the elliptic curve of discriminant 11 defined over $\mathbb{Q}$ by

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

We consider the prime $p = 5$ and the cyclotomic $\mathbb{Z}_5$-extension of the 5-th cyclotomic field $K = \mathbb{Q}(\mu_5)$ *(i.e.* $K_\infty$ is generated over $\mathbb{Q}$ by adjoining all 5-power roots of unity). $E$ has good ordinary reduction at $p = 5$, and in view of Corollary 4.12, we can apply Theorem 4.11 to the Selmer group $X^{(K_\infty)}$. In fact, it has been shown in [3, Theorem 5.4] that $X^{(K_\infty)} = \{0\}$; therefore, $\mu(X^{(\widetilde{K}_\infty)}) = \lambda(X^{(\widetilde{K}_\infty)}) = 0$ for all $\mathbb{Z}_p$-extensions $\widetilde{K}_\infty$ of $K$ that are contained in a suitable Grenberg open neighbourhood of $K_\infty$. In particular, the Mordell–Weil ranks of number fields contained in infinitely many different $\mathbb{Z}_p$-extensions of $K$ are all zero (see Lemma 5.7). Moreover, we note that Assumption 5.1 holds in this example.

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

Using the Fukuda module structure of $\widehat{A}^{(K_\infty)} = \varprojlim \widehat{A}^{(K_n)}$, we can bound the growth of Mordell–Weil ranks without referring to $\lambda(X^{(K_\infty)})$.

**Corollary 5.10** *In the situation of Lemma 5.2, let $C_1, C_2 \in \mathbb{N}$ be the parameters of the Fukuda- $\Lambda$-module $X^{(K_\infty)}$. We assume that there exist at least*

$$v_p(C_1^2 \cdot C_2 \cdot C) + 2$$

*different indices $n_i \le m$, $m \in \mathbb{N}$, such that $\operatorname{rank}_{\mathbb{Z}}(A(K_{n_i})) = M$ for each $n_i$ and some fixed $M \in \mathbb{N}$, where $C$ is a constant as in the proof of Lemma 5.2. Then*

$$\operatorname{rank}_{\mathbb{Z}}(A(K_n)) \le M + v_p(C_1 C_2 C)$$

*for each $n \in \mathbb{N}$.*

**Proof** Lemma 5.2 implies that $\widehat{A}^{(K_\infty)}$ is a $(C_1, C \cdot C_2)$-Fukuda- $\Lambda$-module. Therefore,

$$\operatorname{rank}_{\mathbb{Z}}(A(K_\infty)) \le M + v_p(C_1 C_2 C)$$

by application of Corollary 3.8 to the $\Lambda$-module $\widehat{A}^{(K_\infty)}/(p \cdot \widehat{A}^{(K_\infty)})$, noting that

$$\widehat{A}^{(K_n)}/(p \cdot \widehat{A}^{(K_n)}) \cong (\mathbb{Z}/p\mathbb{Z})^{\operatorname{rank}_{\mathbb{Z}}(A(K_n))}$$

for each $n$, because $\widehat{A}^{(K_n)}$ is $\mathbb{Z}_p$-free of rank $\operatorname{rank}_{\mathbb{Z}}(A(K_n))$. The corollary follows, since $\operatorname{rank}_{\mathbb{Z}}(A(K_n)) \le \operatorname{rank}_{\mathbb{Z}}(A(K_\infty))$ for each $n \in \mathbb{N}$. ∎

This corollary can be used, for example, if $|Ш_A(K_n)| \le C$ for all $n \in \mathbb{N}$ (this is of course a strong assumption).

## 5.2 Fine Selmer Groups

In [20], Lei and Ponsinet proved a control theorem for *fine Selmer groups* (the definitions are recalled in Section 2) for the cyclotomic $\mathbb{Z}_p$-extension $K_\infty/K$, provided that the rational prime $p$ is unramified in $K/\mathbb{Q}$ and that $A$ has good *supersingular* reduction at each prime $v \in S_p$. We will use a modification of this result in order to prove that the fine Selmer groups of abelian varieties over an arbitrary $\mathbb{Z}_p$-extension yield a Fukuda module under suitable assumptions. Note: in the case of supersingular reduction, there does not exist a control theorem for usual Selmer groups, since the cokernels of the maps

$$\operatorname{pr}_n : (X^{(K_\infty)})_{\Gamma_n} \longrightarrow X_n^{(K_\infty)}$$

do not have bounded orders (see [25, Section 2]). The task of finding an appropriate control theorem for fine Selmer groups of elliptic curves in the supersingular case has been considered also by Kurihara (*cf.* [19]) and Wuthrich (*cf.* [31]) for the cyclotomic $\mathbb{Z}_p$-extension, and by Iovita and Pollack (*cf.* [11]) for arbitrary $\mathbb{Z}_p$-extensions. The growth of fine Selmer groups in more general, non-necessarily commutative, extensions, has been studied by Coates and Sujatha, *cf.* [2].

For any $\mathbb{Z}_p$-extension $K_\infty$ of $K$, we let $Y^{(K_\infty)} = \varprojlim Y_n$ denote the projective limit of the duals $Y_n = \operatorname{Sel}_{A,0}(K_n)^\vee$ of the fine Selmer groups.

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

***Theorem 5.11*** *Let $A$ be an abelian variety defined over $K$, and suppose that $A$ has good reduction at each prime $v \in S_p$. Moreover, we assume that $A(K_v)[p^\infty] = \{0\}$ for each $v \in S_p$. Let $K_\infty$ be a $\mathbb{Z}_p$-extension of $K$. Then there exist $m, C_2 \in \mathbb{N}$ such that the fine Selmer group $Y^{(\widetilde{K}_\infty)}$ is a Fukuda- $\Lambda$-module with parameters $(1, C_2, 1)$ for each $\widetilde{K}_\infty \in \mathcal{E}(K_\infty, m)$ (this is a neighbourhood in the sense of Greenberg's topology, as defined in Section 3).*

**Proof** We modify the proof of [20, Lemma 2.3], using also arguments from [9]. For any $\mathbb{Z}_p$-extension $\widetilde{K}_\infty$ of $K$ and each $n \in \mathbb{N}$, we let

$$r_n^{(\widetilde{K}_\infty)} : H^1(\widetilde{K}_n, A[p^\infty]) \longrightarrow \prod_v H^1((\widetilde{K}_n)_v, A[p^\infty])$$

be the localisation map. Then $Y_n = \ker(r_n^{(\widetilde{K}_\infty)})^\vee$, $n \in \mathbb{N}$ (*cf.* Section 2). We obtain a commutative diagram

$$\begin{tikzcd}
 & \prod_v (H^1(\widetilde{K}_v, A[p^\infty])^\vee)_{\Gamma_n} \arrow[r] \arrow[d, "g_n^{(\widetilde{K}_\infty)}"] & (H^1(\widetilde{K}_\infty, A[p^\infty])^\vee)_{\Gamma_n} \arrow[r] \arrow[d, "f_n^{(\widetilde{K}_\infty)}"] & Y_{\Gamma_n} \arrow[r] \arrow[d, "\mathrm{pr}_n^{(\widetilde{K}_\infty)}"] & 0 \\
0 \arrow[r] & \mathrm{im}(r_n^{(\widetilde{K}_\infty)})^\vee \arrow[r] & H^1(\widetilde{K}_n, A[p^\infty])^\vee \arrow[r] & Y_n \arrow[r] & 0.
\end{tikzcd}$$

Since $S_p \neq \emptyset$, the assumed triviality of $A(K_v)[p^\infty]$ for each $v \in S_p$ implies that $A(K)[p^\infty] = \{0\}$ and therefore also $B^{(\widetilde{K}_\infty)} := A(\widetilde{K}_\infty)[p^\infty] = \{0\}$. Therefore, the inflation-restriction exact sequence implies that $f_n^{(\widetilde{K}_\infty)}$ is an isomorphism for each $n \in \mathbb{N}$ and every $\mathbb{Z}_p$-extension $\widetilde{K}_\infty$ of $K$.

Following [20], the order of the cokernel of $g_n^{(\widetilde{K}_\infty)}$ can be bounded prime by prime, and the local contribution of a prime $v$ is $|H^1(\Gamma_n, B_v^{(\widetilde{K}_\infty)})|$, where

$$B_v^{(\widetilde{K}_\infty)} = A(\widetilde{K}_{\infty,v})[p^\infty].$$

Consider first the primes $v \nmid p$. If $A$ has good reduction at $v$, then $v$ does not contribute at all to $|\mathrm{coker}(g_n^{(\widetilde{K}_\infty)})|$, as shown in [20]. If $A$ has bad reduction at $v$, then the contribution to $|\mathrm{coker}(g_n^{(\widetilde{K}_\infty)})|$ is smaller than or equal to the index $[B_v : (B_v)_{\mathrm{div}}]$, which is bounded (again, this is essentially the same argument as in the proof of Theorem 4.5). Note that $B_v$ is the same for each $\widetilde{K}_\infty \in \mathcal{E}(K_\infty, m)$, since the unramified $\mathbb{Z}_p$-extension of $K_v$ is unique. If $v$ is totally decomposed in $\widetilde{K}_\infty$, then $\widetilde{K}_{\infty,v} = (\widetilde{K}_m)_v = K_v$, and $H^1(\Gamma_m, B^{(\widetilde{K}_\infty)}) = \{0\}$. We are therefore reduced to considering the primes of bad reduction that are finitely decomposed in $K_\infty$. We can choose $m \in \mathbb{N}$ large enough such that the number of primes of $\widetilde{K}_\infty$ dividing these $v$ is constant on $\mathcal{E}(K_\infty, m)$. Therefore, the corresponding contribution to $|\mathrm{coker}(g_n^{(\widetilde{K}_\infty)})|$ is bounded independently of $n$ and $\widetilde{K}_\infty \in \mathcal{E}(K_\infty, m)$.

Now consider the primes $v \in S_p$. Since $A(K_v)[p^\infty] = \{0\}$ by assumption, it follows that also $A(\widetilde{K}_{\infty,v})[p^\infty] = \{0\}$, and therefore $v$ does not contribute to $|\mathrm{coker}(g_n^{(\widetilde{K}_\infty)})|$.

The theorem follows by applying the snake lemma to the above commutative diagram. ■

***Remark 5.12*** Let $v \in S_p$. In [20], the authors give the following sufficient criterion for $A(K_v)[p^\infty]$ to be trivial (recall that this condition is needed in Theorem 5.11): $A$ has good supersingular reduction at $v$, and the rational prime $p$ is unramified in $K/\mathbb{Q}$. Indeed, if $p$ is unramified in $K$, then [23, Lemma 5.11] implies that the canonical reduction map induces an isomorphism $A(K_v)[p^\infty] \cong \widetilde{A}(\mathcal{R}_v)[p^\infty]$, where $\mathcal{R}_v$ denotes the finite residue field of $K_v$. If $A$ has supersingular reduction at $v$, the latter group is trivial.

Using Proposition 3.7, we can derive another set of conditions that are sufficient for $Y^{(K_\infty)}$ to be a Fukuda module. This approach is based on the exact sequences (2.2) (see Section 2) that relate the fine and usual Selmer groups. Dualising, we obtain

$$\bigoplus_{v|p} \widehat{A}^{(F_v)} \longrightarrow X_A(F) \longrightarrow Y_A(F) \longrightarrow 0\,,$$

where $\widehat{A}^{(F_v)} \cong \mathbb{Z}_p^{\mathrm{rank}_{\mathbb{Z}}(A(F_v))}$ denotes the Pontryagin dual of $A(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, as in Section 5.1.

**Theorem 5.13** *Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension. We assume that $A$ has potentially good ordinary reduction at each prime $v \in S_p$, and that each $v \in S_p$ is ramified in $K_\infty/K$. Then there exist integers $m, C_1, C_2 \in \mathbb{N}$ such that $Y^{(\widetilde{K}_\infty)}$ is a Fukuda- $\Lambda$-module with parameters $(C_1, C_2, 1)$ for each $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$, where the neighbourhood is defined as in Section 3.*

**Proof** In view of Proposition 3.7, it is sufficient to show that the orders of the cokernels of the projection maps

$$\mathrm{pr}_n : \prod_{v|p} (\widehat{A}^{(\widetilde{K}_{\infty,v})})_{\Gamma_n} \longrightarrow \bigoplus_{v|p} \widehat{A}^{(\widetilde{K}_{n,v})}$$

are bounded as $n \to \infty$. Dualising, we study the kernels of the natural maps

$$i_n : \bigoplus_{v|p} (A(\widetilde{K}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \prod_{v|p} (A(\widetilde{K}_{\infty,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(\widetilde{K}_{\infty,v}/\widetilde{K}_{n,v})},$$

$n \in \mathbb{N}$.

First, it follows from [9, Proposition 3.2] that each $A(\widetilde{K}_{\infty,v})[p^\infty]$ is finite, provided that $m \in \mathbb{N}$ has been chosen large enough to ensure that the primes $v \in S_p$ are ramified in each $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$. More precisely, it follows from the proof of Theorem 4.5 that $|A(\widetilde{K}_{\infty,v})[p^\infty]| \le |A(K_{\infty,v})[p^\infty]|$ for every $v \in S_p$ and $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, m)$, provided that $m$ has been chosen large enough. In the following, we write $B_v := A(K_{\infty,v})[p^\infty]$ and $b_v := |B_v|$, $v \in S_p$.

We will now bound the exponent of $\ker(i_n)$ in terms of $\prod_{v|p} b_v$. Suppose that $e$ denotes the exponent of the group $\ker(i_n)$ for some $n$. Let

$$P \otimes p^{-e} \in A(\widetilde{K}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

be an element of order $p^e$ such that $i_n(P \otimes p^{-e}) = 0$. Then $P = p^e \cdot Q$ for some $Q \in A(\widetilde{K}_{\infty,v})$. Since the extension $\widetilde{K}_{\infty,v}/\widetilde{K}_{n,v}$ is normal, $\gamma(Q) \in A(\widetilde{K}_{\infty,v})$ for each $\gamma \in \mathrm{Gal}(\widetilde{K}_{\infty,v}/\widetilde{K}_{n,v})$. Therefore, $p^e \cdot (Q - \gamma(Q)) = 0$, since $\gamma(P) = P$. But this shows

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

that $e \leq \max_v(\exp(A(\widetilde{K}_{\infty,v})[p^\infty]))$. Since $\operatorname{rank}_p(\ker(i_n))$ is finite for every $n \in \mathbb{N}$, this also shows that each individual kernel $\ker(i_n)$ is finite.

Now let $n_0 \geq m$ be large enough such that

$$A(K_{n_0,v})[p^\infty] = A(K_{\infty,v})[p^\infty]$$

for each $v \in S_p$ (the analogous equality then holds for every $\widetilde{K}_\infty \in \mathcal{U}(A, K_\infty, n_0)$, by cardinality reasons).

We fix $n \geq n_0$, $v \in S_p$, and we choose a topological generator $\gamma \in \operatorname{Gal}(\widetilde{K}_{\infty,v}/K_v)$. Then we define

$$\varphi : \ker(i_n|_{(A(\widetilde{K}_{n,v})\otimes\mathbb{Q}_p/\mathbb{Z}_p)}) \longrightarrow A(\widetilde{K}_{\infty,v})[p^\infty]$$

by mapping $P \otimes p^{-e} \in \ker(i_n)$ to $Q - \gamma^{p^n}(Q)$, where $Q \in A(\widetilde{K}_{\infty,v})$ satisfies $P = p^e \cdot Q$, as above. The map $\varphi$ is a well-defined group homomorphism, and it is actually injective. This shows that

$$|\ker(i_n)| \leq B := \max\Big(\prod_{v\in S_p} b_v, |\ker(i_0)|, \dots, |\ker(i_{n_0})|\Big). \qquad \blacksquare$$

***Example 5.14*** Let $p = 3$, and consider the elliptic curve

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

over $K = \mathbb{Q}$. Then $E$ has good, supersingular reduction at $p$, $S_{\mathrm{br}} = \{43\}$, all local Tamagawa factors $c_v$ (*cf.* Corollary 4.7) are 1, and $|\widetilde{E}(\mathbb{F}_3)| = 5$. Therefore, $E(\mathbb{Q}_3)[3^\infty] = \{0\}$ by Remark 5.12, and it follows from (the proof of) Theorem 5.11 that $Y^{(K_\infty)}$ is a Fukuda- $\Lambda$-module with parameters $(1,1)$, where $\mathbb{Q}_\infty$ denotes the cyclotomic $\mathbb{Z}_3$-extension of $K = \mathbb{Q}$.

In particular, if one could compute the first layers of $Y^{(K_\infty)}$, then a result similar to Corollary 4.10 could be used in order to obtain information about the $\Lambda$-module structure of $Y^{(K_\infty)}$ (it would be sufficient to find two consecutive layers with the same rank, as $C_1 = C_2 = 1$ in this example).

If, on the other hand, $E$ denotes the elliptic curve

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

from Example 4.9, which has good ordinary reduction at $p = 3$, then $Y^{(K_\infty)}$ is a Fukuda module with parameters $(1, 9B, 1)$, where $B = |E(\mathbb{Q}_{\infty,3})[3^\infty]|$ (this is an upper bound for $|\ker(i_n)|$, *cf.* the proof of Theorem 5.13). Since the 3-division polynomial $\psi_3(x) = 3x^4 + x^3 - 6x^2 - 1$ has no root modulo 9, it follows that actually $B = 1$.

It is a straightforward task to prove an analogue of Theorem 4.11 for fine Selmer groups.

***Theorem 5.15*** *Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension, and suppose that the assumptions of either Theorem 5.11 or Theorem 5.13 are satisfied. If $Y^{(K_\infty)}$ is $\Lambda$-torsion, then there exists a neighbourhood $U = \mathcal{U}(A, K_\infty, m)$ of $K_\infty$ such that*

- *$Y^{(\widetilde{K}_\infty)}$ is a torsion $\Lambda$-module for each $\widetilde{K}_\infty \in U$;*
- *$\mu(Y^{(\widetilde{K}_\infty)}) \leq \mu(Y^{(K_\infty)})$ for each $\widetilde{K}_\infty \in U$;*
- *$\lambda(Y^{(\widetilde{K}_\infty)}) \leq \lambda(Y^{(K_\infty)})$ for each $\widetilde{K}_\infty \in U$ such that $\mu(Y^{(\widetilde{K}_\infty)}) = \mu(Y^{(K_\infty)})$.*

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

We finally point out an interesting analogy between the fine Selmer group $Y^{(K_\infty)}$ of a $\mathbb{Z}_p$-extension $K_\infty$ of $K$ and the classical Iwasawa module $X^{(K_\infty)} = \varprojlim X_n$ (*cf.* Example 3.2; the module $X^{(K_\infty)}$ should not be confused with the usual Selmer group here). In [2], Coates and Sujatha raised the following conjecture.

**Conjecture 5.16** *If $K_\infty$ denotes the cyclotomic $\mathbb{Z}_p$-extension of the number field $K$, then $Y^{(K_\infty)}$ is a torsion $\mathbb{Z}_p[\![T]\!]$-module such that*

$$\mu(Y^{(K_\infty)}) = 0$$

*(i.e. , $Y^{(K_\infty)}$ is finitely generated over $\mathbb{Z}_p$).*

For comparison, we state the analogous conjecture for $X = \varprojlim X_n$.

**Conjecture 5.17** *If $K_\infty/K$ denotes the cyclotomic $\mathbb{Z}_p$-extension, then*

$$\mu(X^{(K_\infty)}) = 0.$$

Conjecture 5.17 is due to Iwasawa (see [13]). Coates and Sujatha proved in [2, Theorem 3.4] that Conjectures 5.16 and 5.17 are equivalent if $E$ is an elliptic curve, $p \neq 2$ and $K(E[p^\infty])/K$ is a pro-$p$-extension. Note that the finite layers $X_n$ of the classical Iwasawa modules can be computed more easily than the (fine) Selmer groups, and therefore (at least currently), our method remains primarily of theoretical interest.

**Acknowledgment** I would like to thank Cornelius Greither for carefully reading a preliminary version of this article. Moreover, I am very grateful to the anonymous referees for their numerous suggestions for improvements.

## References

[1] M. Bertolini and H. Darmon, *Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions.* Ann. of Math. (2) **162**(2005), 1–64. http://dx.doi.org/10.4007/annals.2005.162.1

[2] J. Coates and R. Sujatha, *Fine Selmer groups of elliptic curves over $p$-adic Lie extensions.* Math. Ann. **331**(2005), 809–839. http://dx.doi.org/10.1007/s00208-004-0609-z

[3] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves.* 2nd ed., Narosa Publishing House/Published for the Tata Institute of Fundamental Research, Mumbai, 2010.

[4] H. Darmon and A. Iovita, *The anticyclotomic main conjecture for elliptic curves at supersingular primes.* J. Inst. Math. Jussieu 7(2008), 291–325. http://dx.doi.org/10.1017/S1474748008000042

[5] T. Fukuda, *Remarks on $\mathbb{Z}_p$-extensions of number fields.* Proc. Jpn. Acad. Ser. A Math. Sci. **70**(1994), 264–266.

[6] R. Greenberg, *The Iwasawa invariants of $\Gamma$-extensions of a fixed number field.* Amer. J. Math. **95**(1973), 204–214. http://dx.doi.org/10.2307/2373652

[7] R. Greenberg, *Introduction to Iwasawa theory for elliptic curves.* In: Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., 9, Amer. Math. Soc., Providence, RI, 2001. http://dx.doi.org/10.1090/pcms/009/06

[8] R. Greenberg, *Iwasawa theory—past and present.* In: Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001. http://dx.doi.org/10.2969/aspm/03010335

[9] R. Greenberg, *Galois theory for the Selmer group of an abelian variety.* Compos. Math. **136**(2003), 255–297. https://doi.org/10.1023/A:1023251032273

[10] H. Imai, *A remark on the rational points of Abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions.* Proc. Jpn. Acad. **51**(1975), 12–16.

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press

[11] A. Iovita and R. Pollack, *Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields.* J. Reine Angew. Math. **598**(2006), 71–103. http://dx.doi.org/10.1515/CRELLE.2006.069

[12] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields.* Ann. Math. (2) **98**(1973), 246–326.

[13] K. Iwasawa, *On the $\mu$-invariants of $\mathbb{Z}_\ell$-extensions.* In: Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo, 1973, pp. 1–11.

[14] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et applications arithmétiques (III).* Astérisque **295**(2004), 117–290.

[15] N. M. Katz and S. Lang, *Finiteness theorems in geometric classfield theory (with an appendix by K. A. Ribet).* Enseign. Math. (2) **27**(1981), 285–319.

[16] S. Kleine, *Local behavior of Iwasawa's invariants.* Int. J. Number Theory **13**(2017), 1013–1036. https://doi.org/10.1142/S1793042117500543

[17] S. Kleine, *Local behaviour of generalised Iwasawa invariants.* Ann. Math. Qué. **43**(2019), 305–339. http://dx.doi.org/10.1007/s40316-018-0106-5

[18] S. Kleine, *Generalised Iwasawa invariants and the growth of class numbers*. Forum Math., 2020. https://doi.org/10.1515/forum-2019-0119

[19] M. Kurihara, *On the Tate-Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I.* Invent. Math. **149**(2002), 195–224. http://dx.doi.org/10.1007/s002220100206

[20] A. Lei and G. Ponsinet, *On the Mordell-Weil ranks of supersingular abelian varieties in cyclotomic extensions.* Proc. Am. Math. Soc. Ser. B **7**(2020), 1–16. http://dx.doi.org/10.1090/bproc/43

[21] Y. I. Manin, *Cyclotomic fields and modular curves.* Russ. Math. Surv. **26**(1971), 7–71.

[22] K. Matsuno, *Mordell-Weil ranks of elliptic curves in the cyclotomic $\mathbb{Z}_2$-extension of the rationals.* Int. J. Number Theory **13**(2017), 429–438. http://dx.doi.org/10.1142/S1793042117500257

[23] B. Mazur, *Rational points of Abelian varieties with values in towers of number fields.* Invent. Math. **18**(1972), 183–266. http://dx.doi.org/10.1007/BF01389815

[24] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields.* 2nd ed., Grundlehren der Mathematischen Wissenschaften, 323, Springer-Verlag, Berlin, 2008. http://dx.doi.org/10.1007/978-3-540-37889-1

[25] R. Pollack, *An algebraic version of a theorem of Kurihara.* J. Number Theory **110**(2005), 164–177. http://dx.doi.org/10.1016/j.jnt.2003.10.008

[26] D. E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers.* Invent. Math. **75**(1984), 409–423. http://dx.doi.org/10.1007/BF01388636

[27] K. Rubin, *The one-variable main conjecture for elliptic curves with complex multiplication.* In: *L*-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, UK, 1991, pp. 353–371. http://dx.doi.org/10.1017/CBO9780511526053.015

[28] C. Skinner and E. Urban, *The Iwasawa main conjectures for* $\mathrm{GL}_2$. Invent. Math. **195**(2014), 1–277. http://dx.doi.org/10.1007/s00222-013-0448-1

[29] L. C. Washington, *Introduction to cyclotomic fields.* 2nd ed., Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997. http://dx.doi.org/10.1007/978-1-4612-1934-7

[30] K. Wingberg, *On the rational points of abelian varieties over $\mathbb{Z}_p$-extensions of number fields.* Math. Ann. **279**(1987), 9–24. http://dx.doi.org/10.1007/BF01456190

[31] C. Wuthrich, *Iwasawa theory of the fine Selmer group.* J. Algebr. Geom. **16**(2007), 83–108. http://dx.doi.org/10.1090/S1056-3911-06-00436-X

[32] Y. G. Zarhin, *Torsion of abelian varieties, Weil classes and cyclotomic extensions*. Math. Proc. Cambridge Philos. Soc. **126**(1999), 1–15. http://dx.doi.org/10.1017/S0305004198003235

*Institut für Theoretische Informatik, Mathematik und Operations Research, Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, D-85577 Neubiberg, Germany*

https://doi.org/10.4153/S0008414X20000553 Published online by Cambridge University Press