Journal of the Inst. of Math. Jussieu (2003) **2**(1), 73–108 © Cambridge University Press
DOI:10.1017/S1474748003000045 Printed in the United Kingdom

MODULES OVER IWASAWA ALGEBRAS

J. COATES[1], P. SCHNEIDER[2] AND R. SUJATHA[3]

[1] *Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Centre for Mathematical Science, Wilberforce Road, Cambridge CB3 0WB, UK* (j.h.coates@dpmms.cam.ac.uk)

[2] *Mathematisches Institut, Westfälische Wilhelms-Universität Münster, Einsteinstr. 62, D-48149 Münster, Germany* (pschnei@math.uni-muenster.de)

[3] *School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Colaba, Mumbai 400005, India* (sujatha@math.tifr.res.in)

(Received 27 April 2002; accepted 7 June 2002)

Abstract Let G be a compact p-valued p-adic Lie group, and let $\Lambda(G)$ be its Iwasawa algebra. The present paper establishes results about the structure theory of finitely generated torsion $\Lambda(G)$-modules, up to pseudo-isomorphism, which are largely parallel to the classical theory when G is abelian (except for basic differences which occur for those torsion modules which do not possess a non-zero global annihilator). We illustrate our general theory by concrete examples of such modules arising from the Iwasawa theory of elliptic curves without complex multiplication over the field generated by all of their p-power torsion points.

Keywords: Iwasawa algebras; elliptic curves

AMS 2000 *Mathematics subject classification:* Primary 11G05; 11R23; 16D70; 16E65; 16W70

1. Introduction

Let p be a prime number, and G a compact p-adic Lie group. We recall that the Iwasawa algebra (or completed group ring) of G is defined by

$$\Lambda(G) = \varprojlim_{H} \mathbb{Z}_p[G/H],$$

where H runs over the set of all open normal subgroups of G. Interesting examples of finitely generated modules over $\Lambda(G)$, in which G is the image of Galois in the automorphism group of a p-adic Galois representation, abound in arithmetic geometry (see § 8 for some examples coming from elliptic curves without complex multiplication). The study of such $\Lambda(G)$-modules arising from arithmetic geometry can be thought of as a natural generalization of Iwasawa theory. One of the cornerstones of classical Iwasawa theory is the fact that, when $G = \mathbb{Z}_p^d$ for some integer $d \geqslant 1$, a good structure theory for finitely generated $\Lambda(G)$-modules is known, up to pseudo-isomorphism. When $d = 1$, this was proven by Iwasawa [**25**] by an ad hoc method, but almost immediately Serre (see [**36**] and an unpublished letter to K. Iwasawa, dated 27 August 1958) pointed out that it was a special case of one of the main results of commutative algebra and could be proved for all $d \geqslant 1$ (see [**5**, Chapter VII, § 4.4, Theorems 4 and 5]).

The aim of the present paper is to extend as much as possible of this commutative structure theory to the non-commutative case. The first important step in this direction was taken by Venjakob [**41**, **42**], who, using ideas of Björk [**4**], discovered an appropriate non-commutative generalization of the notion of a pseudo-null module over $\Lambda(G)$. Inspired by Venjakob's work, we propose in § 2 a definition of pseudo-null modules over an arbitrary ring A; in particular, a finitely generated torsion $\Lambda(G)$-module M is pseudo-null if $\mathrm{Ext}^1_{\Lambda(G)}(M, \Lambda(G)) = 0$ whenever G is pro-p and has no element of order p. Venjakob [**41**, **42**] then went on to establish the first fragment of the structure theory by treating the case of finitely generated $\Lambda(G)$-modules which are annihilated by some power of p (see also [**20**, **21**]). In § 4 of this paper, we exploit a well-known filtration on $\Lambda(G)$ (see § 7) to show that ideas about filtered rings, which have their origin in the algebraic theory of microlocalization and seem to go back to [**27**], do enable one to rather simply and elegantly extend Bourbaki's proof of the structure theory in the commutative case to finitely generated torsion modules over $\Lambda(G)$, for a wide class of p-adic Lie groups G. We must confess that we were greatly surprised at first to find that we could do this, as we had initially expected that the structure theory for non-abelian groups G would be fundamentally different from the case of $G = \mathbb{Z}_p^d$.

We also then realized that this structure theory could be derived from earlier work of Chamarie [**8**–**10**] on modules over maximal orders. We explain in detail the connection with Chamarie's work in § 3 of this paper, but we do not repeat the proof of his version of the structure theory, which he formulates only somewhat less precisely than us in the quotient of the category of all $\Lambda(G)$-modules by the subcategory of pseudo-null submodules.

We assume that our compact p-adic Lie group G is p-valued in the sense of Lazard [**29**] (we recall Lazard's definition in § 7). We are very grateful to B. Totaro for pointing out to us that our arguments are valid in this generality, and that the class of p-valued compact p-adic Lie groups enjoys many nice properties (e.g. that every closed subgroup of such a group is again p-valued). Every compact p-adic Lie group contains an open subgroup which is p-valued. Important examples of p-valued G are given by the subgroup of $GL_n(\mathbb{Z}_p)$ consisting of all matrices which are congruent to 1 modulo p or modulo 4, according as p is odd or even, and by any pro-p closed subgroup of $GL_n(\mathbb{Z}_p)$ provided $p > n + 1$. The precise statement of our structure theorem is as follows.

Structure Theorem. *Let G be a p-valued compact p-adic Lie group, and let M be a finitely generated torsion $\Lambda(G)$-module. Let M_o be the maximal pseudo-null submodule of M. Then there exist non-zero left ideals $L_1, \dots, L_m$, and a $\Lambda(G)$-injection*

$$\phi : \bigoplus_{i=1}^{m} \Lambda(G)/L_i \to M/M_\mathrm{o}$$

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

with Coker(ϕ) *pseudo-null. Moreover, all left ideals $L_1, \dots, L_m$ having this property are reflexive as $\Lambda(G)$-modules.*

We recognize that most of the ideas behind the proof of the structure theorem are fairly familiar to the experts in non-commutative algebra. However, we have felt it very important to give a rather full discussion of both our proofs, to make them accessible to a wider audience, especially number theorists. We also wish to point out that the Iwasawa algebra $\Lambda(G)$, despite its great interest in arithmetic geometry, seems to have been neglected as a concrete example for the application of non-commutative methods.

For modules M such that M/M_o has a non-zero global annihilator, we exploit Chamarie's methods in § 5 to prove some form of uniqueness for the ideals $L_1, \dots, L_m$ appearing in the structure theorem, and to define the notion of the characteristic ideal of M. We also study finitely generated $\Lambda(G)$-modules which are not necessarily torsion in § 6 by Chamarie's methods. We have also thought it instructive to present our proofs throughout in the axiomatic fashion, leaving the verification that $\Lambda(G)$ satisfies these axioms until § 7. A major question left open by our work is whether the left ideals $L_1, \dots, L_m$ which occur in the above structure theorem can be chosen to be principal (when $G = \mathbb{Z}_p^d$, this is true because $\Lambda(G)$ is a unique factorization domain). Finally, we point out that modules with zero global annihilator do occur naturally in number theory (cf. [**24**, **43**]) and that little else than a criterion for their cyclicity is known about them at present.

Notation

We summarize here the most important notation used in the paper. All of our rings will be assumed associative and with unit element, but will not, in general, be commutative. If A is such a ring, we will always consider left A-modules unless the contrary is stated. We write Mod(A) for the category of left A-modules, and $\mathfrak{M}(A)$ for the subcategory of finitely generated left A-modules. A module M in Mod(A) will be said to be A-*torsion* if every element of M has an annihilator in A which is not a divisor of zero. We shall often assume that we are given a filtration on A, written $F.A = \{F_nA : n \in \mathbb{Z}\}$, which we shall always assume is indexed by $\mathbb{Z}$, increasing, and exhaustive. We write $\operatorname{gr}.A = \bigoplus_{n\in\mathbb{Z}} F_nA/F_{n-1}A$ for the associated graded ring. We use a similar notation and convention for filtrations on left A-modules. We say that A is Noetherian if every left ideal and right ideal in A is finitely generated. If K is any field, we write $\bar{K}$ for a separable closure of K. If p is a prime number, $\mathbb{Z}_p$ will denote the ring of p-adic integers, and $\mathbb{Q}_p$ the quotient field of $\mathbb{Z}_p$.

2. Pseudo-null modules

As above, let A be an associative ring with unit and let Mod(A) be the category of left A-modules. For the moment, we impose no further conditions on A. One way to introduce in this great generality a dimension filtration on the category Mod(A) is through the following technique. As usual, $E(M)$ denotes the injective hull (cf. [**40**, Chapter V, § 2]) of the A-module M. Consider the 'minimal' injective resolution

$$0 \to L \xrightarrow{\mu_0} E_0 \xrightarrow{\mu_1} E_1 \xrightarrow{\mu_2} \cdots$$

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

of the A-module L, i.e. such that $E_0 = E(L)$ and $E_{i+1} = E(\mathrm{Coker}(\mu_i))$ for any $i \geqslant 0$. Let

$$\mathcal{C}_L^n := \text{full subcategory of all } M \text{ in } \mathrm{Mod}(A) \text{ such that } \mathrm{Hom}_A(M, E_0 \oplus \cdots \oplus E_n) = 0.$$

This subcategory $\mathcal{C}_L^n$ is 'localizing' in the sense that it satisfies the following conditions.

(i) In any short exact sequence $0 \to M' \to M \to M'' \to 0$ of A-modules, M lies in $\mathcal{C}_L^n$ if and only M' and M'' lie in $\mathcal{C}_L^n$.

(ii) Any A-module has a unique largest submodule contained in $\mathcal{C}_L^n$.

It is called the *hereditary torsion theory* cogenerated by the injective module $E_0 \oplus \cdots \oplus E_n$ (see [**40**, Chapter VI]).

Lemma 2.1. *An A-module M lies in $\mathcal{C}_L^n$ if and only if $\mathrm{Ext}_A^i(M', L) = 0$ for any $i \leqslant n$ and any submodule $M' \subseteq M$.*

Proof. See [**40**, Chapter VI, Proposition 6.9]. □

Suppose that A is Noetherian, and has no divisors of zero. Then the classical (left and right) ring of quotients D of A exists and is a skew-field [**40**, Chapter II, Proposition 1.7]. Since D is injective as a left and right A-module [**40**, Chapter II, Proposition 3.8], we have $E(A) = D$. Further, as

$$\mathrm{Hom}_A(M, D) = \mathrm{Hom}_D(D \otimes_A M, D) = 0 \quad \text{if and only if } D \otimes_A M = 0,$$

it follows that

$$\mathcal{C}_A^0 = \text{full subcategory of all torsion modules } M \text{ (i.e. such that } D \otimes_A M = 0).$$

Lemma 2.2. *Suppose that A is Noetherian without zero divisors and that $A \neq D$. We then have*

$$\begin{aligned} \mathcal{C}_A^1 = {} & \textit{full subcategory of all } M \textit{ such that} \\ & \mathrm{Hom}_A(M', D/A) = 0 \textit{ for any submodule } M' \subseteq M. \end{aligned}$$

Proof. Since D/A is an essential submodule of $E_1 = E(D/A)$, the asserted condition on M is equivalent to $\mathrm{Hom}_A(M, E_1) = 0$. It therefore remains to show that this condition implies that $\mathrm{Hom}_A(M, D) = 0$. It certainly implies that

$$\mathrm{Hom}_A(M, A) = \mathrm{Hom}_A(M, D).$$

Consider now any $f \in \mathrm{Hom}_A(M, A)$. For any non-zero $b \in A$, we have the A-linear map $f_b : M \to D$ defined by $f_b(x) := f(x)b^{-1}$. This shows that

$$f(M) \subseteq \bigcap_{0 \neq b \in A} Ab.$$

Suppose that the right-hand side contains an $a \neq 0$. Choose a non-zero and non-invertible $c \in A$ ($A \neq D$!) and set $b := ca \neq 0$. There must exist a $d \in A$ such that $a = db = dca$ and hence $1 = dc$, which is a contradiction. □

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Example 2.3 (cf. Chapter VII, Proposition 6.10 of [40]). Suppose that A is an integrally closed Noetherian commutative integral domain. Then an A-module M lies in $\mathcal{C}_A^1$ if and only if $M_{\mathfrak{p}} = 0$ for any prime ideal $\mathfrak{p} \subseteq A$ of height greater than or equal to 1. Hence a finitely generated A-module lies in $\mathcal{C}_A^1$ if and only if it is pseudo-zero in the sense of [**5**, Chapter VII, § 4.4].

Another very interesting class of rings (which includes Iwasawa algebras, see [**41**, **42**]) consists of the Auslander regular rings, and we now recall their definition. The *grade* of a left or right A-module M is defined to be the smallest non-negative integer $j(M) = j_A(M)$ such that $\mathrm{Ext}_A^{j(M)}(M, A) \neq 0$ (we let $j(\{0\}) = \infty$). For any finitely generated $M \neq 0$, the grade $j(M)$ is bounded above by the projective dimension of M. We say that M satisfies the *Auslander condition* if, for each $k \geqslant 0$ and any submodule N of $\mathrm{Ext}_A^k(M, A)$, we have $j_A(N) \geqslant k$ (note that if M is a left (right) A-module, then the right (left) multiplication on A makes $\mathrm{Ext}_A^k(M, A)$ into a right (left) A-module). A Noetherian ring A is defined to be *Auslander regular* if every finitely generated left or right A-module has finite projective dimension and satisfies the Auslander condition (this is slightly more general than that given in [**23**, Chapter III, Definition 2.1.7], in that we do not necessarily assume that A has finite global dimension). We mention that a commutative Noetherian ring is Auslander regular if and only if it is regular (see [**3**, Corollary 4.6, Proposition 4.21] or [**7**, Corollary 3.5.11]). Returning to a general Auslander regular ring A, we note that any finitely generated A-module M lies in the subcategory $\mathcal{C}_A^{j(M)-1}$. We say that a module M is *pure* if $\mathrm{Ext}_A^i(\mathrm{Ext}_A^i(M, A), A) = 0$ for any $i \neq j(M)$. Suppose that the A-module M is finitely generated and let d denote its projective dimension. Then M (see [**4**] or [**23**, Chapter III]) carries a natural filtration, called the *dimension filtration*, by submodules

$$M = \Delta^0(M) \supseteq \Delta^1(M) \supseteq \cdots \supseteq \Delta^{d+1}(M) = 0$$

(note that we have changed the numbering of this filtration compared to [**4**] and [**23**], because we believe that the above, in which the numbering corresponds to codimension, is more natural). This filtration is characterized by the property that a submodule $L \subseteq M$ has grade $j(L) \geqslant p$ if and only if $L \subseteq \Delta^p(M)$. In addition, one has

(i) $j(M) = \max\{p \geqslant 0 : \Delta^p(M) = M\}$;

(ii) if M is pure, then $M = \Delta^{j(M)}(M) \supset \Delta^{j(M)+1}(M) = 0$;

(iii) $\Delta^p(M)/\Delta^{p+1}(M)$ is zero or pure of grade p.

Lemma 2.4. *If A is Auslander regular, then a finitely generated A-module M lies in $\mathcal{C}_A^n$ if and only if $j_A(M) > n$.*

Proof. Suppose that $j(M) > n$. We know that $j(M') \geqslant j(M) > n$ for any submodule $M' \subseteq M$, which, by Lemma 2.1, implies that M lies in $\mathcal{C}_A^n$. The converse is immediate from Lemma 2.1. □

This result shows in particular that over an Auslander regular ring A a finitely generated module M lies in $\mathcal{C}_A^1$ if and only it is pseudo-null in the sense of [**41**, Definition 1.5.1]. In light of these two examples, we suggest the following definition.

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Definition 2.5. A module M over an arbitrary ring A is called *pseudo-null* if it lies in $\mathcal{C}_A^1$.

3. Review of Chamarie's work

We assume throughout this section that A is Noetherian and has no zero divisors, and we write D for the skew-field of fractions of A. If A is commutative and integrally closed, then one of the basic results of commutative algebra is the structure theory of finitely generated torsion A-modules up to pseudo-isomorphism [**5**, Chapter VII, § 4.4 Theorem 5]. In this section, we discuss one generalization of this theory to non-commutative rings due to Chamarie in [**10**], and in the next section we shall present in detail a second generalization based on ideas from the algebraic theory of microlocalization.

We recall that A is called a *maximal order* if, for any intermediate ring B with $A \subseteq B \subseteq D$ such that there exist elements $u, v \in D^\times$ with $uBv \subseteq A$, we always have $A = B$.

Examples 3.1 (cf. Chapter 5, §§ 1 and 3 of [30]).

(1) If A is commutative, then it is a maximal order if and only if it is integrally closed.

(2) Any Weyl algebra over a field k and any universal enveloping algebra of a finite-dimensional Lie algebra over k is a maximal order.

(3) Let R be a commutative Noetherian integral domain with quotient field k. Any R-order in a central simple algebra over k which is maximal with respect to inclusion is a maximal order (possibly with zero divisors).

For later use, we quote the following criterion.

Lemma 3.2. *The ring A is a maximal order if and only if for any non-zero two-sided ideal $I \subseteq A$ and any $u \in D \setminus A$ we have $uI \not\subseteq I$ and $Iu \not\subseteq I$.*

Proof. See [**30**, Proposition 5.1.4]. □

We write $\mathrm{Mod}(A)/\mathcal{C}_A^1$ for the quotient category of $\mathrm{Mod}(A)$ by the subcategory $\mathcal{C}_A^1$ of pseudo-null A-modules, and put

$$Q : \mathrm{Mod}(A) \to \mathrm{Mod}(A)/\mathcal{C}_A^1$$

for the quotient functor (see [**16**] for the construction of quotient categories). We call an A-module M *pseudo-cyclic* if it contains a cyclic submodule N such that the quotient M/N lies in $\mathcal{C}_A^1$. It turns out to be rather involved to define the notion of a cyclic object in the quotient category $\mathrm{Mod}(A)/\mathcal{C}_A^1$. We define an object $Q(M)$ in $\mathrm{Mod}(A)/\mathcal{C}_A^1$ to be *cyclic* if every A-module N such that $Q(N) \cong Q(M)$ is pseudo-cyclic. According to [**35**, Lemma 1.6], the object $Q(M)$ is cyclic if and only if any submodule $N \subseteq M$ such that M/N lies in $\mathcal{C}_A^1$ contains a cyclic submodule L such that M/L lies in $\mathcal{C}_A^1$. In general, it need not even be true that $Q(A)$ is cyclic, but, for the rings which interest us, we shall show later (Lemma 3.7) that the notion of $Q(M)$ being cyclic for an A-torsion

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

module M coincides with what we intuitively hope to be true. In the quotient category $\mathrm{Mod}(A)/\mathcal{C}_A^1$, Chamarie establishes the following important structure theorem when A is a maximal order.

Proposition 3.3. *If A is a maximal order, then any object of finite length in* $\mathrm{Mod}(A)/\mathcal{C}_A^1$ *is a direct sum of cyclic objects.*

Proof. See [**10**, Theorem 4.2.7]. □

We next explain how one can describe the subobjects of $Q(A)$ in terms of a certain class of left ideals of A. For an arbitrary hereditary torsion theory $\mathcal{C}$ in $\mathrm{Mod}(A)$, one has the notion of a $\mathcal{C}$-closed left ideal in A [**40**, Chapter IX, § 1]. We do not recall the definition here, since we can work with the following characterization (cf. [**40**, Chapter IX, Proposition 4.2]), because the torsion theory $\mathcal{C}_A^1$ has the property that the ring A itself is $\mathcal{C}_A^1$-closed [**40**, Chapter IX, Proposition 2.15]. A left ideal $L \subseteq A$ is $\mathcal{C}_A^1$-*closed* if and only if the quotient module A/L is $\mathcal{C}_A^1$-torsion free, i.e. does not contain any non-zero submodule lying in $\mathcal{C}_A^1$. Granted this characterization, we see immediately that, for the torsion theory $\mathcal{C}_A^1$, the definitions of a $\mathcal{C}_A^1$-closed left ideal given in [**40**] and in [**8**–**10**] coincide.

If A is Auslander regular, the properties of the dimension filtration show that a finitely generated A-module is $\mathcal{C}_A^1$-torsion free if and only if $\Delta^2(M) = 0$. In particular, a left ideal $L \subseteq A$ is $\mathcal{C}_A^1$-closed if and only if $\Delta^2(A/L) = 0$. Since for non-zero L the quotient A/L is A-torsion, it follows that a proper left ideal $0 \subset L \subset A$ is $\mathcal{C}_A^1$-closed if and only if the quotient module A/L is pure of grade 1.

The crucial observation in describing the subobjects of $Q(A)$ is the following [**40**, Chapter IX, Corollary 4.4], in which we have once more dropped the assumption that A is Auslander regular. The quotient functor Q induces a bijection between the set of $\mathcal{C}_A^1$-closed left ideals in A and the set of subobjects of $Q(A)$. We denote by $\mathrm{K}_1\mathrm{dim}(A)$ the Krull dimension of the object $Q(A)$ in the quotient category $\mathrm{Mod}(A)/\mathcal{C}_A^1$. Equivalently, $\mathrm{K}_1\mathrm{dim}(A)$ is the deviation [**30**, Chapter 6, § 1] of the partially ordered (with respect to inclusion) set of $\mathcal{C}_A^1$-closed left ideals in A.

We shall be mainly interested in rings A with the property that $\mathrm{K}_1\mathrm{dim}(A) \leqslant 1$. By definition, this means that for any descending chain $L_1 \supseteq L_2 \supseteq \cdots$ of $\mathcal{C}_A^1$-closed left ideals $L_i \subseteq A$ all but finitely many of the sets

$$\{L' \subseteq A : L' \text{ a } \mathcal{C}_A^1\text{-closed left ideal with } L_{i+1} \subseteq L' \subseteq L_i\}$$

satisfy the descending chain condition. But actually a more precise statement holds true. Let $L \subseteq A$ be a non-zero $\mathcal{C}_A^1$-closed left ideal. Suppose that

$$A \supset L_1 \supset L_2 \supset \cdots \supset L$$

is a strictly descending infinite chain of $\mathcal{C}_A^1$-closed left ideals. We fix a non-zero element $b \in L$ and consider the descending chain

$$Q(A) \supseteq Q(Ab) \supseteq Q(Ab^2) \supseteq \cdots$$

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

of subobjects of $Q(A)$ (recall that the quotient functor Q is exact). For each $j \geqslant 0$, we have the intermediate chain

$$Q(Ab^j) \supset Q(L_1 b^j) \supset Q(L_2 b^j) \supset \cdots \supseteq Q(Lb^j) \supseteq Q(Ab^{j+1}).$$

Since

$$Q(L_i b^j)/Q(L_{i+1} b^j) = Q(L_i b^j/L_{i+1} b^j) \cong Q(L_i/L_{i+1}) \neq 0,$$

all inclusions in these latter chains labelled '$\supset$' are strict. This shows that $\mathrm{K}_1\mathrm{dim}(A) > 1$. The condition $\mathrm{K}_1\mathrm{dim}(A) \leqslant 1$ therefore ensures that the object $Q(A/L)$, for any non-zero $\mathcal{C}^1_A$-closed left ideal $L \subseteq A$, has finite length. By a simple induction on the number of generators, we derive the following fact.

Remark 3.4. Suppose that $\mathrm{K}_1\mathrm{dim}(A) \leqslant 1$. For any finitely generated torsion A-module M the object $Q(M)$ has finite length in $\mathcal{C}^0_A/\mathcal{C}^1_A$.

Corollary 3.5. *Suppose that A is a maximal order satisfying $\mathrm{K}_1\mathrm{dim}(A) \leqslant 1$ and let M be any finitely generated torsion A-module. We then have*

(i) *$Q(M)$ is a direct sum of cyclic objects;*

(ii) *there are non-zero $\mathcal{C}^1_A$-closed left ideals $L_1, \dots, L_m \subseteq A$ together with an injective homomorphism of A-modules with pseudo-null cokernel*

$$\bigoplus_{i=1}^{m} A/L_i \to M/M_{\mathrm{o}},$$

where M_{o} denotes the largest pseudo-null submodule of M.

Proof. (i) This is immediate from Proposition 3.3 and the above Remark 3.4.

(ii) By (i), we have an isomorphism

$$\bigoplus_{i=1}^{m} Q(N_i) \xrightarrow{\cong} Q(M)$$

in the quotient category $\mathrm{Mod}(A)/\mathcal{C}^1_A$ where the $Q(N_i)$ are cyclic objects. Consider the restriction of this morphism to a fixed summand on the left-hand side

$$Q(N_i) \to Q(M).$$

By the construction of the quotient category, it is represented by an actual homomorphism of A-modules

$$N_i' \to M/M_i',$$

where $N_i' \subseteq N_i$ and $M_i' \subseteq M$ are submodules such that N_i/N_i' and M_i' are pseudo-null. In particular, we have $M_i' \subseteq M_{\mathrm{o}}$. Since N_i is pseudo-cyclic, we may assume that N_i' is a cyclic A-module, i.e. is of the form $N_i' = A/L_i'$ for some non-zero left ideal $L_i' \subseteq A$. Let

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

$L_i \subseteq A$ be the left ideal such that L_i/L_i' is the largest pseudo-null submodule of A/L_i'. Then L_i is $\mathcal{C}_A^1$-closed and the above map induces a homomorphism

$$A/L_i \to M/M_{\mathrm{o}}.$$

The corresponding sum

$$\bigoplus_{i=1}^{m} A/L_i \to M/M_{\mathrm{o}}$$

represents in the quotient category the original isomorphism and therefore has pseudo-null kernel and cokernel. Since the left-hand side, by construction, has no non-zero pseudo-null submodule, this last map actually is injective. □

According to [**10**, Corollary 4.1.2], the condition $\mathrm{K}_1\mathrm{dim}(A) \leqslant 1$ is satisfied if A is bounded (i.e. every non-zero left or right ideal contains a non-zero two-sided ideal), and hence in particular if A is commutative.

To provide further examples of maximal orders including the concrete examples of Iwasawa algebras, and which satisfy $\mathrm{K}_1\mathrm{dim}(A) \leqslant 1$, we now consider a class of filtered rings A. Thus we now assume that A is endowed with an exhaustive and complete filtration $F.A$ (we observe the conventions on filtrations as explained in § 1.1) such that the associated graded ring $\mathrm{gr}\,.A$ is Noetherian without zero divisors. The reader should compare this assumption with the axioms (C1) and (C2) imposed on A in § 3, noting in particular that we do not impose here that $\mathrm{gr}\,.A$ is commutative. As is explained in § 3 (see also § 3 for an explanation of a good filtration on an A-module), the above assumption guarantees that A is a Zariski ring in the sense of [**23**]. In particular, A has the following properties.

(i) A is Noetherian without zero divisors [**23**, Chapter II, Proposition 1.2.3].

(ii) Any left ideal $L \subseteq A$ is closed in the filtration topology [**23**, Chapter I, Corollary 5.5].

(iii) The filtration induced by $F.A$ on any subquotient module of A is good [**23**, Chapter II, Proposition 1.2.3].

(iv) If $\mathrm{gr}\,.A$ is Auslander regular, then so is the ring A itself [**23**, Chapter III, Theorem 2.2.5].

(v) If M is any finitely generated A-module endowed with a good filtration, we then have [**23**, Chapter III, Theorem 2.5.2]

$$j_A(M) = j_{\mathrm{gr}\,.A}(\mathrm{gr}\,.M).$$

Lemma 3.6. *Assume that A is endowed with an exhaustive and complete filtration such that $\mathrm{gr}\,.A$ is Noetherian without zero divisors. Then*

(i) *if $\mathrm{gr}\,.A$ is a maximal order, so is A;*

(ii) *if $\mathrm{gr}\,.A$ is Auslander regular, then $\mathrm{K}_1\mathrm{dim}(A) \leqslant \mathrm{K}_1\mathrm{dim}(\mathrm{gr}\,.A)$.*

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Proof. (i) This is [**8**, Proposition 2.3.1]. For the convenience of the reader we recall the argument. We will use the criterion of Lemma 3.2. Let $I \subseteq A$ be a non-zero two-sided ideal and let $u \in D$ be such that $uI \subseteq I$. If $u = b^{-1}a$ with $a, b \in A$, then the latter is equivalent to $aI \subseteq bI$. We have to show that $u \in A$, i.e. that $a \in bA$. That the ideal bA is closed in the filtration topology means that

$$bA = \bigcap_{n \in \mathbb{Z}} (bA + F_nA).$$

Hence it suffices to show that $a \in bA + F_nA$ for all sufficiently small $n \in \mathbb{Z}$. The filtration being exhaustive, we find an $m \in \mathbb{Z}$ such that $a \in F_mA \subseteq bA + F_mA$. So it furthermore suffices to prove that $a \in bA + F_{n-1}A$ provided $a \in bA + F_nA$. Let us assume that $a = by + z$ with $y \in A$ and $z \in F_nA$. Obviously, we only need to treat the case where $z \neq 0$. Suppose that $z \in F_mA \setminus F_{m-1}A$ and $b \in F_pA \setminus F_{p-1}A$ and put $\bar{z} := z + F_{m-1}A \in \mathrm{gr}_{\cdot} A$ and $\bar{b} := b + F_{p-1}A \in \mathrm{gr}_{\cdot} A$. We have

$$zI \subseteq aI + byI \subseteq bI.$$

Forming $\mathrm{gr}_{\cdot} I$ with respect to the induced filtration gives a non-zero two-sided ideal in $\mathrm{gr}_{\cdot} A$. We claim that

$$\bar{z} \cdot \mathrm{gr}_{\cdot} I \subseteq \bar{b} \cdot \mathrm{gr}_{\cdot} I.$$

Consider any $0 \neq \bar{c} = c + F_{r-1}A \in \mathrm{gr}_r I$. Then $zc = bd$ for some $0 \neq d \in I$. Suppose that $d \in F_sI \setminus F_{s-1}I$ and put $\bar{d} := d + F_{s-1}I \in \mathrm{gr}_s I$. Since $\mathrm{gr}_{\cdot} A$ has no zero divisors, we must have $m + r = p + s$ and

$$\bar{z} \cdot \bar{c} = zc + F_{m+r-1}A = bd + F_{p+s-1}A = \bar{b} \cdot \bar{d}.$$

This proves our claim. Since $\mathrm{gr}_{\cdot} A$ is a maximal order, it follows that

$$\bar{z} \in \bar{b} \cdot \mathrm{gr}_{\cdot} A.$$

Hence there is a $\bar{x} = x + F_{s-r-1}A \in \mathrm{gr}_{s-r-1} A$ such that $\bar{z} = \bar{b} \cdot \bar{x} = bx + F_{m-1}A$. We obtain $z - bx \in F_{m-1}A \subseteq F_{n-1}A$ and consequently

$$a = by + z = b(y + x) + z - bx \in bA + F_{n-1}A.$$

The argument for $Iu \subseteq I$ implying that $u \in A$ is analogous.

(ii) Let $0 \subset L \subset A$ be a proper $\mathcal{C}^1_A$-closed left ideal. Equipping L and A/L with the induced filtrations, we obtain the proper left ideal $\mathrm{gr}_{\cdot} L \subset \mathrm{gr}_{\cdot} A$ such that $j(\mathrm{gr}_{\cdot} A / \mathrm{gr}_{\cdot} L) = j(\mathrm{gr}_{\cdot} A/L) = j(A/L) = 1$. Let $\mathrm{gr}_{\cdot} L \subset \widetilde{\mathrm{gr}}\, L \subset \mathrm{gr}_{\cdot} A$ denote the proper left ideal such that $\widetilde{\mathrm{gr}}\, L / \mathrm{gr}_{\cdot} L = \Delta^2(\mathrm{gr}_{\cdot} A / \mathrm{gr}_{\cdot} L)$. Then $\mathrm{gr}_{\cdot} A / \widetilde{\mathrm{gr}}\, L$ is pure of grade 1 so that $\widetilde{\mathrm{gr}}\, L$ is $\mathcal{C}^1_{\mathrm{gr}_{\cdot} A}$-closed. Hence $L \mapsto \widetilde{\mathrm{gr}}\, L$ is an inclusion-preserving map from the set of proper $\mathcal{C}^1_A$-closed left ideals in A to the set of proper $\mathcal{C}^1_{\mathrm{gr}_{\cdot} A}$-closed left ideals in $\mathrm{gr}_{\cdot} A$. To establish our assertion, it suffices to show that this map preserves strict inclusions. Consider therefore two proper $\mathcal{C}^1_A$-closed left ideals $L \subset L'$ strictly contained in each other. By the purity of A/L, we have $j(\mathrm{gr}_{\cdot} L' / \mathrm{gr}_{\cdot} L) = j(\mathrm{gr}_{\cdot} L'/L) = j(L'/L) = 1$. Hence $\mathrm{gr}_{\cdot} L' \not\subseteq \widetilde{\mathrm{gr}}\, L$ and *a fortiori* $\widetilde{\mathrm{gr}}\, L' \neq \widetilde{\mathrm{gr}}\, L$. □

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

This lemma applies, for example, if $\operatorname{gr}.A$ is a commutative Noetherian regular integral domain. Then $\operatorname{gr}.A$ is integrally closed and hence a maximal order and is Auslander regular [**23**, Chapter III, 2.4.3] with $\mathrm{K}_1\dim(\operatorname{gr}.A) \leqslant 1$. Hence A is an Auslander regular maximal order with $\mathrm{K}_1\dim(A) \leqslant 1$.

Finally, we note the following simple criterion for cyclicity in the quotient category $\mathrm{Mod}(A)/\mathcal{C}_A^1$.

Lemma 3.7. *Suppose that A is a maximal order satisfying $\mathrm{K}_1\dim(A) \leqslant 1$ and let M be a torsion A-module. Then $Q(M)$ is cyclic in $\mathrm{Mod}(A)/\mathcal{C}_A^1$ if and only if there is a non-zero left ideal $L \subseteq A$ such that $Q(M) \cong Q(A/L)$.*

Proof. If $Q(M)$ is cyclic, then, by definition, we find a cyclic torsion A-module N such that $Q(M) \cong Q(N)$. But any such N is isomorphic to A/L for some non-zero left ideal $L \subseteq A$. For the reverse implication we use that, according to [**10**, Theorem 4.2.4], any quotient of $Q(A)$ which is of finite length is cyclic. Under our assumptions, $Q(A/L)$ is such a quotient by Remark 3.4. □

4. The approach via filtered rings

The aim of this section is to show that the classical proof of the structure theory of finitely generated torsion modules over commutative Noetherian integrally closed domains (see [**5**]) has a natural extension to a wide class of non-commutative filtered rings A. Thus, throughout this section, A will denote a ring, which is endowed with a separated and exhaustive filtration $F.A$, and which satisfies the following axioms, where, as usual, $\operatorname{gr}.A$ denotes the associated graded ring:

(C1) A is complete with respect to the filtration $F.A$;

(C2) $\operatorname{gr}.A$ is a polynomial ring in finitely many variables over a field such that the variables are all of strictly negative (possibly different) degree.

We note that the axioms imply that A is Auslander regular. We thank H. Qin for pointing out that the axioms needed to be strengthened to this present version. Our proof will make extensive use of techniques which grew out of the algebraic theory of microlocalization, and are, for example, studied systematically in [**23**].

Let R be any filtered ring, with increasing filtration $F.R$. We recall (see [**23**, Chapter II, Theorem 2.2]) that one of the equivalent definitions of R being a *Zariski ring* is that $\operatorname{gr}.R$ is left and right Noetherian, and that the completion $\hat{R} = \varprojlim_n R/F_nR$ is a faithful and flat left and right R-module. Applying this definition to our ring A, the next lemma is plain from axioms (C1) and (C2).

Lemma 4.1. *A is a Zariski ring.*

Throughout this section we fix a torsion module M in $\mathfrak{M}(A)$. We shall always use a *good* filtration on M, whose definition we now recall. Pick any finite set $w_1, \dots, w_s$ of

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

generators of M as an A-module, and fixed integers $k_1, \dots, k_s$. For each n in $\mathbb{Z}$, we then define

$$F_n M = \sum_{i=1}^{s} F_{n-k_i} A \cdot w_i.$$

It is clear that the $F_n M$ are an increasing sequence of additive subgroups of M, whose union is M. Any filtration of M obtained in this manner is defined to be a good filtration. Let $F.M$ be a good filtration on M. As the ring A is Zariski, it follows from the basic properties of these rings [**23**, Chapter I, Corollary 5.5 and Chapter II, Theorem 2.2] that not only is $F.M$ separated, but more generally that it satisfies the closure property, i.e. any submodule N is closed in the filtration topology. Since M is A-torsion, it is plain that $\operatorname{gr}.M$ is $\operatorname{gr}.A$-torsion. Also, $\operatorname{gr}.M$ is a finitely generated $\operatorname{gr}.A$-submodule because the filtration $F.M$ is good [**23**, Chapter I, Lemma 5.4].

By axiom (C2), $\operatorname{gr}.A$ is a commutative ring, and our starting point for the proof of the structure theorem is to apply the classical commutative theory to the finitely generated torsion $\operatorname{gr}.A$-module $\operatorname{gr}.M$. For this commutative theory, we follow, wherever possible, the notation and terminology of [**5**]. Hence we write $\operatorname{Ass}(\operatorname{gr}.M)$ for the set of prime ideals $\mathfrak{p}$ of $\operatorname{gr}.A$ which are associated to $\operatorname{gr}.M$; recall that this set consists of prime ideals in $\operatorname{gr}.A$ which are of the form $\operatorname{ann}(x)$ for a non-zero element $x \in \operatorname{gr}.M$. Note that the zero ideal is not in $\operatorname{Ass}(\operatorname{gr}.M)$ as $\operatorname{gr}.M$ is a finitely generated torsion module. We define

$$W(M) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$$

to be the set of prime ideals of height one in $\operatorname{Ass}(\operatorname{gr}.M)$.

Remark 4.2. While $\operatorname{Ass}(\operatorname{gr}.M)$ in general depends on the choice of the good filtration $F.M$, it is true, as our notation suggests, that $W(M)$ is independent of this choice. Indeed, the set of minimal elements of $\operatorname{Ass}(\operatorname{gr}.M)$ coincides with the set of minimal elements of the support of $\operatorname{gr}.M$ [**5**, Chapter IV, § 1.4], denoted by $\operatorname{Supp}(\operatorname{gr}.M)$. But $\operatorname{Supp}(\operatorname{gr}.M)$ is precisely the set of all prime ideals containing the radical $J(M)$ of $\operatorname{ann}_{\operatorname{gr}.A}(\operatorname{gr}.M)$, and $J(M)$ is well defined and independent of the filtration [**4**, Proposition 5.1].

Definition 4.3. The multiplicatively closed set S is defined to be the set of all homogeneous elements in $\operatorname{gr}.A$ which do not belong to $\mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_r$.

If $W(M)$ is empty, then S is defined to be the set of all non-zero homogeneous elements of $\operatorname{gr}.A$. As S is a homogeneous multiplicatively closed set, we can clearly localize graded modules with respect to S. We also have the graded domain [**5**, Chapter II, § 2.9]

$$(\operatorname{gr}.A)_S := S^{-1} \operatorname{gr}.A.$$

Since $\operatorname{gr}.M$ is a graded $\operatorname{gr}.A$-module, every ideal in $\operatorname{Ass}(\operatorname{gr}.M)$ is graded [**5**, Chapter IV, § 3.1, Proposition 1]. In particular, the ideals in $W(M)$ are all graded.

Proposition 4.4.

(i) *The ideals $S^{-1}\mathfrak{p}_i$, $1 \leqslant i \leqslant r$, are graded prime ideals of height* 1 *in* $(\operatorname{gr}.A)_S$.

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

(ii) *Every proper graded ideal of* $(\mathrm{gr}\,.A)_S$ *is contained in one of the* $S^{-1}\mathfrak{p}_i$, $1 \leqslant i \leqslant r$.

(iii) *Every non-zero graded prime ideal of* $(\mathrm{gr}\,.A)_S$ *is of the form* $S^{-1}\mathfrak{p}_i$ *for some* i, $1 \leqslant i \leqslant r$.

Proof. (i) To establish (i), we use [**5**, Chapter II, § 2.5, Proposition 11]. Now, for each $i = 1, \dots, r$, $\mathfrak{p}_i$ is a prime ideal of $\mathrm{gr}\,.A$, which does not intersect S. Hence $S^{-1}\mathfrak{p}_i$ is a prime ideal of $(\mathrm{gr}\,.A)_S$. Moreover, if $\mathfrak{q}$ were any non-zero prime ideal of $(\mathrm{gr}\,.A)_S$ with $\mathfrak{q} \subseteq S^{-1}\mathfrak{p}_i$, we would necessarily have $\mathfrak{q} = S^{-1}\mathfrak{p}$ with $\mathfrak{p} \subseteq \mathfrak{p}_i$, and thus $\mathfrak{p} = \mathfrak{p}_i$ because $\mathfrak{p}_i$ has height one.

(ii) By [**5**, Chapter III, § 1.3, Proposition 8] and axiom (C2), it follows that given a graded ideal $\mathfrak{a} \subseteq \mathrm{gr}\,.A$ with the property that $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ for $1 \leqslant i \leqslant r$ there exists a homogeneous element in $\mathfrak{a} \cap S$. Hence the proper graded ideals of $(\mathrm{gr}\,.A)_S$ are precisely those of the form $S^{-1}\mathfrak{a}$ with $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

(iii) To prove (iii), let $\mathfrak{q}$ be a non-zero graded prime ideal of $(\mathrm{gr}\,.A)_S$. Then, by (ii), $\mathfrak{q} \subseteq S^{-1}\mathfrak{p}_i$ for some i. But, by (i), $S^{-1}\mathfrak{p}_i$ is a prime ideal of height one in $(\mathrm{gr}\,.A)_S$, and so we must have $\mathfrak{q} = S^{-1}\mathfrak{p}_i$. This completes the proof of the proposition. □

Proposition 4.5. *Every graded ideal in* $(\mathrm{gr}\,.A)_S$ *is principal.*

Proof. By axiom (C2), the ring $\mathrm{gr}\,.A$ is factorial and so the localization $(\mathrm{gr}\,.A)_S$ is also factorial by [**5**, Chapter VII, § 3.4, Proposition 3]. Now take $\mathfrak{b}$ to be any non-zero graded ideal of $(\mathrm{gr}\,.A)_S$. Thus the module $(\mathrm{gr}\,.A)_S/\mathfrak{b}$ is graded, and so every element of $\mathrm{Ass}((\mathrm{gr}\,.A)_S/\mathfrak{b})$ must be a graded prime ideal of $(\mathrm{gr}\,.A)_S$ [**5**, Chapter IV, § 3.1, Proposition 1]. But Proposition 4.4 shows that every non-zero prime ideal of $(\mathrm{gr}\,.A)_S$ which is graded has height one. It follows from [**5**, Chapter VII, § 1.6, Proposition 10] therefore that the ideal $\mathfrak{b}$ is divisorial, whence $\mathfrak{b}$ is principal by the definition of a factorial ring. This completes the proof of the proposition. □

While it is technically very convenient that we shall not need to pass to the algebraic microlocalizations of our modules, we shall nevertheless now make essential use of the beginnings of that theory. We recall the definition of the *principal symbol* map. If x is any non-zero element of M, we define $\bar{x}$ to be the class of x modulo $F_{n-1}M$, where n is the unique integer such that x belongs to F_nM but not to $F_{n-1}M$. Similarly, we can define by sending a to $\bar{a}$ the map $A \setminus \{0\} \to \mathrm{gr}\,.A$. Now let S be the multiplicative set of non-zero homogeneous elements of $\mathrm{gr}\,.A$ defined above in Definition 4.3.

Definition 4.6. The set T is defined as $T = \{t \in A : \bar{t} \in S\}$.

As S is a multiplicatively closed set of non-zero elements of $\mathrm{gr}\,.A$, it is plain that T is a multiplicatively closed set of non-zero elements of A. What is not at all obvious, and lies at the heart of our proof, is the following well-known and basic result. We recall that a multiplicatively closed subset R of non-zero elements of A is a *left and right Ore set* in A if, for each r in R and a in A, we have $aR \cap rA$ and $Ra \cap Ar$ are both non-empty sets.

Proposition 4.7. *T is a left and right Ore set in A.*

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Proof. We understand that results of this kind go back to Kashiwara [**27**]. For purely algebraic proofs, we refer the reader to [**22**], or to the last part of [**44**] for a proof due to Björk. □

In view of Proposition 4.7, an entirely parallel construction to that in the commutative case (see [**40**] for instance) proves the existence of the localized domains $T^{-1}A$ and AT^{-1}. The left and right localizations are in fact isomorphic, and from now on, we shall denote either of these two by A_T. Moreover, as is explained in [**22**], A_T is naturally endowed with a separated and exhaustive filtration $F.A_T$. Now, it is also shown in [**22**, Proposition 2.3], that this filtration has the property that

$$\mathrm{gr}\,.(A_T) = (\mathrm{gr}\,.A)_S.$$

If N is any finitely generated (left) module over A with a good filtration $F.N$, then we define the localization $N_T = A_T \otimes_A N$. This is a finitely generated left module over A_T, and comes equipped with a natural good filtration which we denote by $F.N_T$. Further (cf. [**22**, Corollary 2.5 and Proposition 2.6]), we have

$$\mathrm{gr}\,.N_T \simeq (\mathrm{gr}\,.N)_S.$$

Even though we have imposed the axiom that A is complete with respect to its filtration, it will not in general be true that A_T is complete with respect to the filtration $F.A_T$. However, for our purposes, the following weaker result suffices.

Proposition 4.8. *The ring A_T with its natural filtration $F.A_T$ is a Zariski ring.*

Proof. See [**22**, Proposition 2.8]. □

We can now prove the first main result of this section.

Proposition 4.9. *Every left and right ideal of A_T is principal.*

Proof. By symmetry, it suffices to prove that any left ideal L of A_T is generated by one element. Endow L with the filtration induced from A_T. By a basic property of Zariski rings (see [**23**, Chapter I, § 5, Corollary 5.5]), this induced filtration on L is good. Plainly, $\mathrm{gr}\,.L$ is a graded ideal in $\mathrm{gr}\,.A_T = (\mathrm{gr}\,.A)_S$. By Proposition 4.5, $\mathrm{gr}\,.L$ is therefore principal, and thus we can find a homogeneous z in $\mathrm{gr}\,.L$ such that $\mathrm{gr}\,.L = (\mathrm{gr}\,.A)_S \cdot z$. Now pick w to be any element of L such that $\bar{w} = z$. But now, by another basic property of Zariski rings [**23**, Chapter I, § 5, Corollary 5.5], we conclude that $L = A_T w$. We stress that, thanks to the remarkable properties of Zariski rings, we are able to carry out this last step without passing to the microlocalization of A_T. □

We now consider the left A_T-module M_T which is finitely generated and torsion over A_T, because M is assumed to be finitely generated and torsion over A. Since A_T is a principal ideal domain by Proposition 4.9, the classical theory of finitely generated modules over principal ideal domains (see [**26**, Chapter 3, Theorem 19] or [**30**, Corollary 5.7.19]), which are not necessarily commutative, immediately gives the following result.

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Proposition 4.10. *There exist elements $w_1, \dots, w_m$ in M_T such that*

$$M_T = A_T w_1 \oplus \cdots \oplus A_T w_m.$$

Under the present assumptions on the ring A we now are able, using Proposition 4.10, to give the following alternative proof for Corollary 3.5.

Proposition 4.11. *Let M be any A-torsion module in $\mathfrak{M}(A)$, and let $M_\circ$ denote the maximal pseudo-null submodule of M. Then there exist non-zero reflexive left ideals $L_1, \dots, L_m$ of A, along with an injective A-homomorphism*

$$\phi : \bigoplus_{i=1}^{m} A/L_i \to M/M_\circ,$$

such that $\operatorname{Coker}(\phi)$ *is pseudo-null.*

The reflexivity of the ideals follows from the following general lemma. We thank O. Venjakob for pointing this out to us.

Lemma 4.12. *Let R be any Noetherian Auslander regular ring without zero divisors and let $0 \subset L \subset R$ be a proper left ideal of R. Then L is reflexive if and only if R/L is pure of grade 1.*

Proof. For any left R-module M, let $E^i(M) := \operatorname{Ext}^i_R(M, R)$. Clearly, $E^0(M) = M^* = 0$ if M is torsion. Consider the exact sequence

$$0 \to L \to R \to R/L \to 0.$$

Taking the long exact Ext sequence associated to it twice, we get a commutative diagram as follows with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d] & R \arrow[r] \arrow[d] & R/L \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L^{**} \arrow[r] & R^{**} \arrow[r] & E^1E^1(R/L) &
\end{tikzcd}$$

Here, the first two vertical arrows are the natural maps, hence the middle map is an isomorphism, and the last vertical arrow is induced by exactness. By the snake lemma, we see that L is reflexive if and only if the map $R/L \to E^1E^1(R/L)$ is injective. But the injectivity of this map is in turn equivalent to R/L being pure of grade 1 (cf. [**23**, Chapter III, § 4.2]) and the lemma is proved. □

A crucial step in the proof of Proposition 4.11 is given by the following proposition, whose proof will be given at the end of this section. We write $\psi : M \to M_T$ for the canonical A-homomorphism, and define $M' := \operatorname{Im}(\psi)$.

Proposition 4.13. *Let N be any subquotient module of the torsion module M. Then $N_T = 0$ if and only if N is pseudo-null.*

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Proof of Proposition 4.11. Assuming Proposition 4.13, we now deduce Proposition 4.11 from Proposition 4.10. Put $N := \operatorname{Ker}(\psi)$. Since $\operatorname{Ker}(\psi)$ is precisely the set of T-torsion elements in M, we have $N_T = 0$ and so N is pseudo-null by Proposition 4.13. Now M' is an A-submodule of M_T with $M'_T = M_T$. Let $w_1, \dots, w_m$ be the elements of M_T given by Proposition 4.10. Since we are clearly free to multiply these elements by any element of T, the fact that $M'_T = M_T$ allows us to assume that each of $w_1, \dots, w_m$ belongs to M'. We now define the A-submodule M'' of M' by

$$M'' := Aw_1 \oplus \cdots \oplus Aw_m,$$

where the sum is clearly direct because $w_1, \dots, w_m$ are even linearly independent over A_T. But $N := M'/M''$ is a quotient of M with $N_T = 0$. Hence N is pseudo-null by Proposition 4.13. Moreover, the map $a \mapsto aw_i$ induces an isomorphism of A-modules from A/L'_i to Aw_i, where L'_i is the annihilator of w_i in A. The composed map

$$\bigoplus_{i=1}^{m} A/L'_i \xrightarrow{\cong} \bigoplus_{i=1}^{m} Aw_i = M'' \subseteq M' \cong M/\operatorname{Ker}(\psi)$$

is an injective A-homomorphism with pseudo-null cokernel. It induces the map ϕ in the assertion once we replace each L'_i by the unique left ideal L_i such that L_i/L'_i is the maximal pseudo-null submodule of A/L'_i. As $M/M_\circ$ is pure of grade 1, so are the modules A/L_i and the reflexivity follows from Lemma 4.12. This completes the proof of Proposition 4.11. □

Proof of Proposition 4.13. Take N to be any A-subquotient of M. Our filtration $F.M$ being fixed, we always endow N with the natural filtration which makes $\operatorname{gr}.N$ a subquotient of $\operatorname{gr}.M$, namely, if we write $N = V/V'$, where $V' \subset V$ are submodules of M, then we take the filtration on V induced from that on M, and then the quotient filtration on N. By a fundamental property of Zariski rings (see [**23**, Chapter II, § 2.1, Theorem 2]), this filtration on N is good because we start with a good filtration on M. We next observe that since $\operatorname{gr}.N$ is a subquotient of $\operatorname{gr}.M$, the support of $\operatorname{gr}.N$ must be a subset of the support of $\operatorname{gr}.M$, whence (see Remark 4.2)

$$W(N) \subseteq W(M).$$

Finally, it will be important for us to distinguish between homogeneous localization and ordinary localization of a $\operatorname{gr}.A$-module at a prime ideal of $\operatorname{gr}.A$. Let R denote a $\operatorname{gr}.A$-module, and $\mathfrak{p}$ a prime ideal of $\operatorname{gr}.A$. As usual, we write $R_{\mathfrak{p}}$ for the localization of R with respect to the multiplicative set $S_{\mathfrak{p}} = \operatorname{gr}.A \setminus \mathfrak{p}$. If, in addition, R is a graded $\operatorname{gr}.A$-module and $\mathfrak{p}$ is a graded prime ideal, we shall write $R_{\mathfrak{p}^*}$ for the localization of R with respect to the multiplicative set $S_{\mathfrak{p}^*}$ of all homogeneous elements of $\operatorname{gr}.A \setminus \mathfrak{p}$.

Suppose now that N is a subquotient of M with $N_T = 0$. We must show that N is pseudo-null. Since A is Zariski, it is well known that (see [**23**, Chapter III, § 2.2])

$$j_A(N) \geqslant j_{\operatorname{gr}.A}(\operatorname{gr}.N),$$

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

where j denotes the grade of the relevant module as defined in § 1. Thus, by Lemma 2.1, to prove that N is pseudo-null, it suffices to prove that $\operatorname{gr}.N$ is pseudo-null as a $\operatorname{gr}.A$-module. Hence, by Example 2.3, we must prove that $(\operatorname{gr}.N)_{\mathfrak{p}} = 0$ for every prime ideal $\mathfrak{p}$ in $W(N)$. But, as remarked in the previous paragraph, $W(N) \subseteq W(M)$ because N is a subquotient of M, and so it suffices to show that $(\operatorname{gr}.N)_{\mathfrak{p}_i} = 0$ for $1 \leqslant i \leqslant r$. Now our good filtration on N gives rise (see [**22**, Corollary 2.5]) to a good filtration on the A_T-module N_T, with the property that

$$\operatorname{gr}.N_T = (\operatorname{gr}.N)_S.$$

Hence we must have $(\operatorname{gr}.N)_S = 0$. But this automatically implies that, for $1 \leqslant i \leqslant r$, we have $(\operatorname{gr}.N)_{\mathfrak{p}_i} = 0$, because $S \subseteq S_{\mathfrak{p}_i{}^*} \subseteq S_{\mathfrak{p}_i}$.

Conversely, assume that N is pseudo-null. Since A is Auslander regular, we have $j_A(N) = j_{\operatorname{gr}.A}(\operatorname{gr}.N)$ (see [**23**, Chapter III, § 2.2, Theorem 5]). Hence, by Lemma 2.4, $\operatorname{gr}.N$ is a pseudo-null $\operatorname{gr}.A$-module, since N is pseudo-null. Let $\mathfrak{p}$ denote any graded prime ideal of height 1 of $\operatorname{gr}.A$. As $\operatorname{gr}.N$ is pseudo-null, we have $(\operatorname{gr}.N)_{\mathfrak{p}} = 0$. In fact, we claim that we have the stronger assertion that $(\operatorname{gr}.N)_{\mathfrak{p}^*} = 0$. Let $w_1, \dots, w_k$ denote a set of homogeneous generators for $\operatorname{gr}.N$ as a $\operatorname{gr}.A$-module. For each $j = 1, \dots, k$, we can find $s_j \in S_{\mathfrak{p}}$ such that $s_j w_j = 0$. Writing s_j as a sum of its homogeneous components $s_{j,h}$, we must always have $s_{j,h} w_j = 0$. But at least one of the $s_{j,h}$ does not belong to $\mathfrak{p}$. Hence we must have $s_{j,h} \in S_{\mathfrak{p}^*}$ for some h, which proves that $(\operatorname{gr}.N)_{\mathfrak{p}^*} = 0$. We claim that this, in turn, implies that $(\operatorname{gr}.N)_S = 0$. Indeed, the prime ideals in $W(M) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ are all graded, and the previous argument has shown that there exists a homogeneous element t_i in $\operatorname{ann}_{\operatorname{gr}.A}(\operatorname{gr}.N)$ such that t_i does not belong to $\mathfrak{p}_i$. Let $\mathfrak{a}$ be the graded ideal of $\operatorname{gr}.A$ generated by $t_1, \dots, t_r$. Picking a homogeneous element t of $\mathfrak{a}$ which does not belong to $\mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_r$ (see [**5**, Chapter III, § 1.3, Proposition 8]), we have $t \cdot \operatorname{gr}.N = 0$ and $t \in S$, so that $(\operatorname{gr}.N)_S = 0$, as asserted. Recall that our goal is to show that $N_T = 0$. Now, as always, our good filtration on N gives rise to a good filtration on the A_T-module N_T with the property that $\operatorname{gr}.N_T = (\operatorname{gr}.N)_S$. Hence we have $\operatorname{gr}.N_T = 0$. But A_T is a Zariski ring, and thus every good filtration is separated [**23**, Chapter II, § 2.1, Theorem 2], and so $\operatorname{gr}.N_T = 0$ implies that $N_T = 0$. This completes the proof of Proposition 4.13. □

Finally, we record the following corollary that emerges from our methods, and which is of independent interest.

Corollary 4.14. *Let A be a Zariski ring such that $\operatorname{gr}.A$ is a polynomial ring in finitely many variables over a field k. Suppose $M \in \mathfrak{M}(A)$ is a torsion module and T is defined as before. Assume further that M has no T-torsion. Then there exists a good filtration on M such that $\operatorname{gr}.M$ is S-torsion free.*

Proof. Indeed, A is then Auslander regular, and if M has no T-torsion then, by Proposition 4.13, M is pure [**23**, Chapter III, § 4.2, Theorem 6]. It is well known that in this case there is a good filtration [**23**, Chapter III, § 4.2, Theorem 13 (4)] on M such that $\operatorname{gr}.M$ is a pure module over $\operatorname{gr}.A$. But this means in particular [**23**, Chapter III, § 4.3, Proposition 5] that $\operatorname{Ass}(\operatorname{gr}.M) = W(M)$. Recall that the set of zero divisors on $\operatorname{gr}.M$ is equal

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

to the union of the prime ideals in $\mathrm{Ass}(\mathrm{gr}\,.M)$. By definition, S has trivial intersection therefore with the set of zero divisors and hence $\mathrm{gr}\,.M$ has no S-torsion. □

5. The characteristic ideal

Let us return to the general situation when A is a Noetherian maximal order without zero divisors and with skew-field of fractions D. We always assume that $A \neq D$. There are certain additional features of the structural result Proposition 3.3 which at least partly generalize [**5**, Chapter VII, § 4.5] to the non-commutative situation. As before, the annihilator ideal of an A-module M is denoted by $\mathrm{ann}_A(M)$. If $\mathrm{ann}_A(M) \neq 0$, then the module M is called *bounded*. The annihilator ideal of an object $\mathcal{M}$ in the quotient category $\mathrm{Mod}(A)/\mathcal{C}_A^1$ is defined by

$$\mathrm{ann}(\mathcal{M}) := \sum \{\mathrm{ann}_A(M) : Q(M) \cong \mathcal{M}\}.$$

The object $\mathcal{M}$ is called *completely faithful* if $\mathrm{ann}(\mathcal{N}) = 0$ for any non-zero subquotient object $\mathcal{N}$ of $\mathcal{M}$. It is called *(locally) bounded* if $\mathrm{ann}(\mathcal{N}) \neq 0$ for any subobject $\mathcal{N} \subseteq \mathcal{M}$ (of finite type). Since A is Noetherian, it follows from [**40**, Chapter XIII, Proposition 1.1] that $\mathcal{N}$ is of finite type if and only if it is of the form $\mathcal{N} \cong Q(N)$ for some finitely generated module N.

Under the condition that $\mathrm{K}_1\mathrm{dim}(A) \leqslant 1$, there is an alternative description of $\mathrm{ann}(Q(M))$ for any finitely generated A-torsion module M in terms of the left ideals $L_1, \dots, L_m$ occurring in Corollary 3.5. For $i = 1, \dots, m$, let J_i be the maximal two-sided ideal of A contained in L_i, and let $J := \bigcap_{i=1}^m J_i$. Then we have

$$\mathrm{ann}(Q(M)) = J.$$

This follows easily on combining Corollary 3.5 with the observation $\mathrm{ann}_A(A/L_i) = J_i$, and using the fact [**35**, Lemma 2.5] that $\mathrm{ann}(Q(M)) = \mathrm{ann}_A(M/M_{\mathrm{o}})$, where again M_{o} denotes the maximal pseudo-null submodule of M. Note also that M is bounded, or equivalently $J \neq 0$ if and only if all of $J_1, \dots, J_m$ are non-zero.

Proposition 5.1.

(i) *Any object $\mathcal{M}$ in $\mathcal{C}_A^0/\mathcal{C}_A^1$ decomposes uniquely into a direct sum $\mathcal{M} = \mathcal{M}_0 \oplus \mathcal{M}_1$, where $\mathcal{M}_0$ is completely faithful and $\mathcal{M}_1$ is locally bounded.*

(ii) *Any completely faithful object of finite length in $\mathrm{Mod}(A)/\mathcal{C}_A^1$ is cyclic.*

Proof. See [**10**, Proposition 4.2.2 and Corollary 4.2.3]. □

Let $(\mathcal{C}_A^0/\mathcal{C}_A^1)^b$ denote the full subcategory of all bounded objects in $\mathcal{C}_A^0/\mathcal{C}_A^1$. As a consequence of [**35**, Lemma 2.4], this category is an abelian subcategory. We want to investigate the Grothendieck group $G((\mathcal{C}_A^0/\mathcal{C}_A^1)^b)$ of objects of finite length in the category $(\mathcal{C}_A^0/\mathcal{C}_A^1)^b$ modulo short exact sequences. By the Jordan–Hölder theorem, $G((\mathcal{C}_A^0/\mathcal{C}_A^1)^b)$ is the free abelian group on the set of isomorphism classes of simple objects in the category

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

$(\mathcal{C}_A^0/\mathcal{C}_A^1)^b$. The tool we will use is a certain group $G(A)$ of fractional ideals of the maximal order A whose construction we now briefly review, after first introducing more notation.

For any left or right A-module M, let $M^* := \mathrm{Hom}_A(M, A)$ denote the dual right or left A-module.

A non-zero left (right) A-submodule $L \subseteq D$ is called a fractional left (right) ideal if there is a $v \in D^\times$ such that $L \subseteq Av$ ($L \subseteq vA$). If $I \subseteq D$ is a fractional left as well as right ideal, we call it a fractional ideal. For any fractional left ideal L, the map

$$\begin{aligned} \{x \in D : Lx \subseteq A\} &\xrightarrow{\cong} L^*, \\ x &\mapsto [b \mapsto bx], \end{aligned}$$

is an isomorphism of right A-modules. Moreover, in a maximal order, one has

$$\{x \in D : Lx \subseteq A\} = \{x \in D : LxL \subseteq L\} =: L^{-1}.$$

Defining

$$\bar{L} := (L^{-1})^{-1},$$

we have an isomorphism $\bar{L} \cong L^{**}$. It follows from the left–right symmetry of the definition of L^{-1} that a fractional ideal $I \subseteq D$ is reflexive as a left A-module if and only if it is reflexive as a right A-module. A reflexive fractional ideal (respectively, a non-zero reflexive two-sided ideal in A) is called a fractional c-ideal (respectively, a c-ideal). According to Asano [**2**] (see also [**8**, **31**] or [**1**, Lemma 1.1]), one has the following.

(i) If I is a fractional ideal, then $\bar{I}$ is a fractional c-ideal.

(ii) The set of all fractional c-ideals is an abelian group $G(A)$ with respect to the product

$$I \cdot J := \overline{IJ}$$

and the inverse $I \mapsto I^{-1}$.

(iii) Every maximal element in the set of all c-ideals is a prime ideal of height one (i.e. a minimal non-zero prime ideal). The group $G(A)$ is the free abelian group on the set $\mathcal{P} = \mathcal{P}(A)$ of all prime c-ideals.

(iv) For any pairwise distinct $P_1, \dots, P_r \in \mathcal{P}$ and any $n_1, \dots, n_r \in \mathbb{N}$, one has

$$P_1^{n_1} \cdot \cdots \cdot P_r^{n_r} = P_1^{n_1} \cap \cdots \cap P_r^{n_r}.$$

If $C(P)$, for any $P \in \mathcal{P}$, denotes the multiplicative set of elements in A which are regular modulo P, then it is proved in [**9**, Propositions 1.8 (b), 1.9 and 2.5] or [**8**, Proposition 3.3.4 and Lemma 3.3.5] that the following hold.

(v) $C(P)$ satisfies the left and right Ore condition.

(vi) The localization $A_{C(P)} = {}_{C(P)}A$ is a bounded left and right principal maximal order with Jacobson radical $\mathrm{Jac}(A_{C(P)}) = PA_{C(P)}$ such that $A_{C(P)}/PA_{C(P)}$ is simple artinian and such that the non-zero two-sided ideals in $A_{C(P)}$ are precisely the powers of $\mathrm{Jac}(A_{C(P)})$.

(vii) For any non-zero $a \in A$, there are at most finitely many $P \in \mathcal{P}$ such that $a \notin C(P)$.

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Lemma 5.2. *For any A-module M in $\mathcal{C}_A^0$ the following assertions are equivalent.*

(i) *$Q(M)$ is completely faithful.*

(ii) *$A_{C(P)} \otimes_A M = 0$ for any $P \in \mathcal{P}$.*

Proof. See [**10**, Lemma 4.2.1]. □

In particular, this lemma implies that $A_{C(P)} \otimes_A N = 0$ for every pseudo-null A-module N. Since localization is exact, we therefore obtain, for each $P \in \mathcal{P}$, a well-defined exact functor

$$\begin{gathered}\mathcal{C}_A^0/\mathcal{C}_A^1 \to \operatorname{Mod}(A_{C(P)}),\\ \mathcal{M} = Q(M) \mapsto A_{C(P)} \otimes_A \mathcal{M} := A_{C(P)} \otimes_A M\end{gathered}$$

Suppose now that $\mathcal{M}$ is an object of finite length in $(\mathcal{C}_A^0/\mathcal{C}_A^1)^b$. As remarked earlier, we then have $\mathcal{M} \cong Q(M)$ for some finitely generated torsion A-module M. Hence $A_{C(P)} \otimes_A \mathcal{M} \cong A_{C(P)} \otimes_A M$ is a finitely generated torsion $A_{C(P)}$-module. Since $A_{C(P)}$ is principal, this latter module is of finite length $\ell_P(\mathcal{M})$. The last fact which we recalled before Lemma 5.2 implies that $\ell_P(\mathcal{M}) \neq 0$ for at most finitely many P. Hence

$$\chi(\mathcal{M}) := \prod_{P \in \mathcal{P}} P^{\ell_P(\mathcal{M})}$$

is a well-defined c-ideal. We call it the *characteristic ideal* of the object $\mathcal{M}$. It follows from Lemma 5.2 that $\chi(\mathcal{M}) = A$ implies $\mathcal{M} = 0$.

Lemma 5.3. *Let M be a finitely generated bounded torsion A-module, and let M_{o} be the maximal pseudo-null submodule of M. We then have*

(i) $\operatorname{ann}_A(M/M_{\mathrm{o}}) = \operatorname{ann}(Q(M))$ *is a c-ideal;*

(ii) $\chi(Q(M)) \subseteq \operatorname{ann}(Q(M))$*;*

(iii) $\chi(Q(M))$ *and* $\operatorname{ann}(Q(M))$ *have the same prime factors.*

Proof. Replacing M by M/M_{o}, we may assume that M has no non-zero pseudo-null submodules.

(i) According to [**10**, corollary of Theorem 2.5], we may apply [**35**, Lemma 2.5] and obtain $I := \operatorname{ann}_A(M) = \operatorname{ann}(Q(M))$. Hence $I \neq 0$, by assumption, and it remains to show that $\bar{I} \subseteq I$. But

$$I \cdot I^{-1} \cdot \bar{I} = I \cdot I^{-1} \cdot (I^{-1})^{-1} \subseteq \operatorname{ann}_A(M).$$

Since the ideal $J := I \cdot I^{-1}$, by [**10**, Lemma 2.2], is such that the quotient A/J is pseudo-null, the submodule $\bar{I} \cdot M$, being annihilated by J, is pseudo-null as well. It follows that $\bar{I} \cdot M = 0$ which means that $\bar{I} \subseteq \operatorname{ann}_A(M) = I$.

(ii) Any $A_{C(P)}$-module of length m is annihilated by $\operatorname{Jac}(A_{C(P)})^m$. Hence, for any $P \in \mathcal{P}$, we have

$$\begin{aligned}A_{C(P)} \otimes_A \chi(Q(M))M &\subseteq A_{C(P)} \otimes_A P^{\ell_P(Q(M))}M\\ &\subseteq \operatorname{Jac}(A_{C(P)})^{\ell_P(Q(M))}(A_{C(P)} \otimes_A M) = 0.\end{aligned}$$

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Lemma 5.2 then implies that $\chi(Q(M))M$ is a pseudo-null submodule of M and hence is zero by our assumption on M.

(iii) The prime factors of $\operatorname{ann}_A(M)$ are precisely the prime c-ideals which contain $\operatorname{ann}_A(M)$. Because of (ii), it therefore suffices to show that any $P \in \mathcal{P}$ such that $A_{C(P)} \otimes_A M \neq 0$ contains $\operatorname{ann}_A(M)$. Since $\operatorname{ann}_A(M)$ is reflexive by (i), it follows from [**10**, Lemma 3.3] that $\operatorname{ann}_A(M) \subseteq P$ if and only if $\operatorname{ann}_A(M) \cap C(P) = \emptyset$. The latter condition certainly is satisfied if $A_{C(P)} \otimes_A M \neq 0$. □

Thanks to the exactness of localization and the additivity of the length function, the formation of the characteristic ideal induces a homomorphism of abelian groups

$$\chi : G((\mathcal{C}_A^0/\mathcal{C}_A^1)^b) \to G(A).$$

To understand this homomorphism, consider any simple object $\mathcal{M}$ in $(\mathcal{C}_A^0/\mathcal{C}_A^1)^b$. By Proposition 3.3, it is cyclic and therefore a quotient object of $Q(A)$. Since the subobjects of $Q(A)$ are in bijection with the $\mathcal{C}_A^1$-closed left ideals, we see that $\mathcal{M}$, up to isomorphism, is of the form

$$\mathcal{M} = Q(A/L),$$

where the left ideal L is maximal among all $\mathcal{C}_A^1$-closed left ideals. In addition, since $\operatorname{ann}_A(A/L) = \operatorname{ann}(\mathcal{M})$, by [**10**, corollary of Theorem 2.5] and [**35**, Lemma 2.5], and the latter is non-zero by assumption, the left ideal L is bounded. Applying [**9**, Lemma 2.7], we obtain that L is reflexive. By Lemma 5.2, there exists a $P \in \mathcal{P}$ such that $A_{C(P)} \otimes_A \mathcal{M} = A_{C(P)} \otimes_A A/L \neq 0$ and hence that $\operatorname{ann}_A(A/L) \cap C(P) = \emptyset$. Since both $\operatorname{ann}_A(A/L)$ (see Lemma 5.3 (i)) and L are reflexive and bounded, we can apply [**10**, Lemma 3.3] twice (observing that $\operatorname{ann}_A(A/L)$ is the largest two-sided ideal contained in L) and conclude that $\operatorname{ann}_A(A/L) \subseteq P$ and $L \cap C(P) = \emptyset$. Suppose that $L \subseteq L' \subsetneq A$ is another left ideal such that $L' \cap C(P) = \emptyset$. Then $A_{C(P)} \otimes_A A/L' = A_{C(P)}/A_{C(P)}L'$ is non-zero. Hence, by Lemma 5.2 again, $Q(A/L')$ is a non-zero quotient of $\mathcal{M}$ and therefore must be equal to $\mathcal{M}$. This implies that L'/L is pseudo-null. But since L is $\mathcal{C}_A^1$-closed, the quotient A/L contains no non-zero pseudo-null submodules. This shows that $L' = L$ and establishes that L is maximal with respect to the property $L \cap C(P) = \emptyset$. Such left ideals are called *P-critical* and are studied in [**28**]. In particular, it is shown in [**28**, Theorem 3.5] that any P-critical left ideal contains P. In our case, this means that

$$\operatorname{ann}(\mathcal{M}) = P.$$

Moreover, as explained in the proof of [**8**, Proposition 3.4.6], if L is P-critical, then $L_{C(P)} = A_{C(P)}L$ is a maximal left ideal in $A_{C(P)}$ and $L_{C(Q)} = A_{C(Q)}L = A_{C(Q)}$ for any $Q \in \mathcal{P}$ different from P. On the one hand, this implies that

$$\chi(\mathcal{M}) = P.$$

On the other hand, it also follows that if we give ourselves a $P' \in \mathcal{P}$ and choose a P'-critical left ideal L', then $\chi(Q(A/L')) = P'$. By Lemma 5.2, the object $Q(A/L')$ in $(\mathcal{C}_A^0/\mathcal{C}_A^1)^b$ necessarily is simple.

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Suppose now that $\mathcal{N}$ is a second simple object in $(\mathcal{C}_A^0/\mathcal{C}_A^1)^b$ such that $\operatorname{ann}(\mathcal{N}) = \operatorname{ann}(\mathcal{M}) = P$. Let $\mathcal{N}$ be of the form $\mathcal{N} = Q(A/L')$ with L' maximal among the $\mathcal{C}_A^1$-closed left ideals. Then L' also is P-critical and [**28**, Lemma 3.7] says that there are elements $a \in A \setminus L$ and $b \in A \setminus L'$ such that

$$a^{-1}L := \{x \in A : xa \in L\} = \{y \in A : yb \in L'\} =: b^{-1}L'.$$

Consider the injective map

$$A/a^{-1}L \xrightarrow{\cdot a} A/L.$$

Since A/L has no non-zero pseudo-null submodules, $Q(A/a^{-1}L)$ is a non-zero subobject of $\mathcal{M}$ and therefore is isomorphic to $\mathcal{M}$. We obtain

$$\mathcal{M} \cong Q(A/a^{-1}L) = Q(A/b^{-1}L') \cong \mathcal{N}.$$

Altogether, this proves the following result.

Proposition 5.4. *The homomorphism $\chi : G((\mathcal{C}_A^0/\mathcal{C}_A^1)^b) \xrightarrow{\cong} G(A)$ is an isomorphism. More precisely, χ induces a bijection between the set of isomorphism classes of simple objects in $(\mathcal{C}_A^0/\mathcal{C}_A^1)^b$ and the set $\mathcal{P}(A)$ of prime c-ideals.*

Suppose that A is a maximal order satisfying $\mathrm{K}_1\mathrm{dim}(A) \leqslant 1$. We then can reformulate the above result as follows. Let $\mathcal{C}_A$ denote the abelian category of all finitely generated torsion A-modules with non-zero annihilator ideal and let $\mathcal{Z}_A \subseteq \mathcal{C}_A$ denote the subcategory of pseudo-null modules. The isomorphism classes of simple objects in the quotient category $\mathcal{C}_A/\mathcal{Z}_A$ are, via the characteristic ideal, in bijection with the set $\mathcal{P}$.

Following [**1**], we call A a *unique factorization ring* if any prime c-ideal in A is principal. Here, a two-sided ideal $I \subseteq A$ is called principal if $I = Ab$ (and then necessarily also $I = bA$ by [**8**, Lemma 2.2.9]) for some $b \in A$. It is clear then that all fractional c-ideals of A are principal. In this case, the characteristic ideal $\chi(\mathcal{M})$ determines, through its generator, a *characteristic element* for the object $\mathcal{M}$ in A which is well defined up to a unit in A.

6. Finitely generated but not necessarily torsion modules

Under the same assumptions as in the previous section we now want to look at the structure of an arbitrary finitely generated A-module M modulo pseudo-null modules. Our aim is to at least partly generalize [**5**, Chapter VII, § 4.4, Example (3) and Theorem 4] which says that, if A is commutative, then the torsion submodule of M always splits off in the quotient category $\mathrm{Mod}(A)/\mathcal{C}_A^1$.

Lemma 6.1. *Let $P \in \mathcal{P}(A)$ and let M be an A-module such that $Q(M) \cong Q(A/L)$ for some P-critical left ideal $L \subseteq A$. The natural map $M \to A_{C(P)} \otimes_A M$ viewed as a homomorphism of A-modules induces an isomorphism $Q(M) \xrightarrow{\cong} Q(A_{C(P)} \otimes_A M)$.*

Proof. We may assume that $M = A/L$. From the proof of Proposition 5.4, we know the following facts.

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

(a) L contains P.

(b) $A_{C(Q)} \otimes_A M = A_{C(Q)}/A_{C(Q)}L = 0$ for any $Q \in \mathcal{P}$ different from P.

Consider now the natural map

$$M = A/L \to A_{C(P)} \otimes_A M = A_{C(P)}/A_{C(P)}L.$$

Because of (a), the A-modules on both sides are bounded. For our claim that this map induces an isomorphism in the quotient category, it therefore suffices, by Lemma 5.2, to show that the localized maps

$$A_{C(Q)} \otimes_A M \to A_{C(Q)} \otimes_A A_{C(P)} \otimes_A M$$

are isomorphisms for any $Q \in \mathcal{P}$. For $Q = P$ this is obvious. Suppose therefore that $Q \neq P$. Then the left-hand side is zero by (b). Since $A_{C(Q)} \otimes_A A_{C(P)} = D$, by [**8**, Lemma 3.5.2], the right-hand side is zero as well, because M is A-torsion. □

Proposition 6.2. *Let N be a finitely generated A-torsion free A-module, and let $\mathcal{M}$ be a bounded object of finite length in the quotient category $\mathfrak{U} := \mathrm{Mod}(A)/\mathcal{C}_A^1$. Then*

$$\mathrm{Ext}^1_{\mathfrak{U}}(Q(N), \mathcal{M}) = 0.$$

Proof. First of all, we note that $\mathcal{M}$ being bounded lies in the subcategory $\mathcal{C}_A^0/\mathcal{C}_A^1$. By induction with respect to the length of $\mathcal{M}$, we may assume that $\mathcal{M}$ is simple. In the proof of Proposition 5.4, we have seen that there is then a prime c-ideal $P \in \mathcal{P}$ such that $\mathcal{M} \cong Q(A/L)$ for some P-critical left ideal $L \subseteq A$. We therefore have to show that any given extension

$$0 \to Q(A/L) \to \mathcal{E} \to Q(N) \to 0 \tag{6.1}$$

in $\mathfrak{U}$ splits. We choose an exact sequence of A-modules

$$0 \to M \to E \to N' \to 0 \tag{6.2}$$

such that (6.1) is isomorphic to the exact sequence arising from (6.2) by applying the functor Q (see [**35**, Lemma 1.1]). Consider now the exact sequence

$$0 \to A_{C(P)} \otimes_A M \to A_{C(P)} \otimes_A E \to A_{C(P)} \otimes_A N' \to 0. \tag{6.3}$$

The $A_{C(P)}$-module $A_{C(P)} \otimes_A M \cong A_{C(P)} \otimes_A A/L$ is finitely generated and torsion whereas the $A_{C(P)}$-module $A_{C(P)} \otimes_A N' \cong A_{C(P)} \otimes_A N$ is finitely generated and torsion free. Since $A_{C(P)}$ is a (non-commutative) principal ideal domain, it follows [**30**, Lemma 5.7.4] that the sequence (6.3) splits. Let $\sigma : A_{C(P)} \otimes_A E \to A_{C(P)} \otimes_A M$ be a splitting of (6.3). If σ_{o} denotes the restriction of σ to E, then we deduce from Lemma 6.1 that $Q(\sigma_{\mathrm{o}})$ induces a splitting of (6.1). □

Remark 6.3. Any bounded object $\mathcal{M}$ in the quotient category $\mathrm{Mod}(A)/\mathcal{C}_A^1$ has injective dimension less than or equal to 1.

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Proof. Let $\mathcal{M} = Q(M)$ and let

$$0 \to M \to E_0 \to E_1 \to \cdots$$

be the 'minimal' injective resolution of the A-module M as in § 1. With M, all the injective A-modules E_i are A-torsion [**40**, Chapter VI, Corollary 6.8, Proposition 7.3]. Hence the exact sequence

$$0 \to \mathcal{M} \to Q(E_0) \to Q(E_1) \to \cdots$$

lies in $\mathcal{C}_A^0/\mathcal{C}_A^1$. According to Proposition 5.1 (i), each

$$Q(E_i) = Q(E_i)_0 \oplus Q(E_i)_1$$

decomposes uniquely into a completely faithful object $Q(E_i)_0$ and a locally bounded object $Q(E_i)_1$. Since $\mathcal{M}$ is bounded, the sequence

$$0 \to \mathcal{M} \to Q(E_0)_1 \to Q(E_1)_1 \to \cdots$$

is still exact. We claim that $Q(E_i)_1$ is injective in $\mathrm{Mod}(A)/\mathcal{C}_A^1$ for any $i \geqslant 0$ and is equal to zero for $i \geqslant 2$. By [**16**, Chapter III, § 3, Corollary 2], we have, for any $i \geqslant 0$, another decomposition

$$Q(E_i) = Q(E_i') \oplus \mathcal{E}_i,$$

where E_i' is the injective hull of some pseudo-null A-module and $\mathcal{E}_i$ is an injective object in $\mathrm{Mod}(A)/\mathcal{C}_A^1$. At this point, we have to introduce the intermediate ring $A \subseteq A_0 \subseteq D$ defined by

$$A_0 := \{u \in D : uI \subseteq A \text{ for some non-zero two sided ideal } I \subseteq A\}.$$

Let $\mathcal{C}_A^{1/2}$ denote the hereditary torsion theory cogenerated by the injective A-module $D \oplus E(A_0/A)$ (cf. § 1). Since $E(A_0/A)$ embeds into $E(D/A)$, we have

$$\mathcal{C}_A^1 \subseteq \mathcal{C}_A^{1/2} \subseteq \mathcal{C}_A^0.$$

According to [**6**, Remark 4.4 (i)], an A-module N lies in $\mathcal{C}_A^{1/2}$ if and only if $A_{C(P)} \otimes_A N = 0$ for any $P \in \mathcal{P}(A)$. It therefore follows from Lemma 5.2 that an A-torsion module N lies in $\mathcal{C}_A^{1/2}$ if and only if $Q(N)$ is completely faithful. The subcategory $\mathcal{C}_A^{1/2}$ of $\mathrm{Mod}(A)$ has the important additional property [**6**, Theorem 4.2] that it is stable with respect to the formation of injective hulls. In our situation, this shows that

$$Q(E_i') \subseteq Q(E_i)_0,$$

and hence that $Q(E_i)_1$ is injective for any $i \geqslant 0$. Moreover, by [**6**, Remark 4.4 (ii)], the sequence

$$0 \to A_{C(P)} \otimes_A M \to A_{C(P)} \otimes_A E_0 \to A_{C(P)} \otimes_A E_1 \to \cdots$$

is, for any $P \in \mathcal{P}$, a 'minimal' injective resolution of the $A_{C(P)}$-module $A_{C(P)} \otimes_A M$. Since $A_{C(P)}$ as a principal ideal domain has global injective dimension less than or equal

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

to 1, we obtain that $A_{C(P)} \otimes_A E_i = 0$ for any $i \geqslant 2$ and any $P \in \mathcal{P}$. This means, by Lemma 5.2, that $Q(E_i)$ is completely faithful and hence that $Q(E_i)_1 = 0$ for any $i \geqslant 2$, and completes the proof of our claim. We mention that in the quotient category $\mathrm{Mod}(A)/\mathcal{C}_A^{1/2}$, every object has injective dimension less than or equal to 1 [**6**, Remark 4.4 (iii)]. □

Proposition 6.4. *Let M be a finitely generated A-module, and denote by $M_t \subseteq M$ the maximal A-torsion submodule. Suppose that* $\mathrm{K}_1\mathrm{dim}(A) \leqslant 1$ *and that $Q(M_t)$ does not contain any non-zero completely faithful subobject. Then*

$$Q(M) \cong Q(M_t) \oplus Q(M/M_t).$$

If, in addition, A is Auslander regular, then $Q(M/M_t) \cong Q(N)$ for some finitely generated reflexive A-module N.

Proof. By our assumptions and Proposition 5.1 (i), the object $Q(M_t)$ in $\mathrm{Mod}(A)/\mathcal{C}_A^1$ is bounded and of finite length and the A-module M/M_t is finitely generated and A-torsion free. It therefore follows from Proposition 6.2 that

$$Q(M) \cong Q(M_t) \oplus Q(M/M_t).$$

The canonical map $M \to M^{**}$ has kernel M_t [**30**, Proposition 3.4.7], and the A-module M^{**} is finitely generated and reflexive. If A is Auslander regular, then the cokernel of this map is pseudo-null [**41**, Corollary 1.5.7]. □

7. Iwasawa algebras

Let p be a prime number, and let G be a compact p-adic Lie group. We recall that the Iwasawa algebra $\Lambda(G)$ is defined to be the completed group ring

$$\Lambda(G) := \varprojlim_N \mathbb{Z}_p[G/N],$$

where N runs over the open normal subgroups of G. It seems fair to say that, until very recently, Iwasawa algebras have been largely neglected as concrete examples of non-commutative rings, even though they occur very naturally in many questions in arithmetic geometry. Under the assumption that G is p-valued in the sense of [**29**], we now show that $\Lambda(G)$ carries an exhaustive and complete filtration, and satisfies the axioms imposed on the ring A in the earlier parts of the paper. See also [**14**] for a proof of this result for a more restrictive class of G.

Definition 7.1 (cf. Chapter III, Definition 2.1.2 of [29]). A *p-valuation* on G is a function $\omega : G \to (0, \infty]$ satisfying the following axioms for all g and h in G.

(1) $\omega(1) = \infty$, and $1/(p-1) < \omega(g) < \infty$ for $g \neq 1$.

(2) $\omega(gh^{-1}) \geqslant \min\{\omega(g), \omega(h)\}$.

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

(3) $\omega(g^{-1}h^{-1}gh) \geqslant \omega(g) + \omega(h)$.

(4) $\omega(g^p) = \omega(g) + 1$.

We say that G is *p-valued* if it possesses a p-valuation. As B. Totaro emphasized to us, p-valued compact p-adic Lie groups G possess many useful properties. If G is p-valued, it is automatically pro-p and has no element of order p. Any closed subgroup of a p-valued group G is also p-valued. The classic example of a p-valued group is the subgroup of $GL_n(\mathbb{Z}_p)$ consisting of all matrices which are congruent to the identity modulo p (respectively, modulo 4) if p is odd (respectively, if $p = 2$). More generally, if $p > n + 1$, Lazard (see [**29**, p. 101]) has proven that every closed pro-p subgroup of $GL_n(\mathbb{Z}_p)$ is p-valued. The following result, whose proof we shall give below, is essentially contained in [**29**] (except that he uses decreasing instead of increasing filtrations), and we are grateful to B. Totaro for pointing it out to us.

Proposition 7.2. *Assume that G is a compact p-adic Lie group, which is p-valued. Then $\Lambda(G)$ possesses a complete, separated and exhaustive filtration $F.\Lambda(G)$ such that $\mathrm{gr}\,.\Lambda(G)$ is isomorphic as a graded ring to the polynomial ring $\mathbb{F}_p[X_0, \dots, X_d]$ in $d + 1$ variables, where $d = \dim(G)$, and the grading on the latter ring is given by assigning to each variable a certain strictly negative integer degree. In particular, $\Lambda(G)$ is a Noetherian Auslander regular maximal order without zero divisors, such that $\mathrm{K}_1\dim(\Lambda(G)) \leqslant 1$, and satisfies the axioms (C1), and (C2) of § 4.*

Proof. We assume for the rest of this section that G is p-valued, and begin the proof of Proposition 7.2. Let ω be any p-valuation on G and define, for each ν in $\mathbb{R}$, the closed normal subgroups

$$G_{\omega,\nu} = \{g \in G : \omega(g) \geqslant -\nu\}, \qquad G_{\omega,\nu^+} = \{g \in G : \omega(g) > -\nu\}.$$

As J.-P. Serre observed to us, as a consequence of [**29**, Chapter III. Corollary 3.1.4], these subgroups are open in G. In particular, the natural map $G \xrightarrow{\cong} \varprojlim G/G_{\omega,\nu}$ is an isomorphism because of the compactness of G.

Put

$$\mathrm{gr}_\omega(G) = \bigoplus_{\nu \in \mathbb{R}} \frac{G_{\omega,\nu}}{G_{\omega,\nu^+}}.$$

The commutator induces a Lie bracket on $\mathrm{gr}_\omega(G)$, which we denote by $[\cdot,\cdot]_\omega$, and this makes $\mathrm{gr}_\omega(G)$ into a graded Lie algebra over $\mathbb{F}_p$. Let $\mathbb{F}_p[\pi]$ denote the polynomial ring in one variable π over $\mathbb{F}_p$, viewed as a graded $\mathbb{F}_p$-algebra with π of degree -1. The rule $gG_{\omega,\nu^+} \mapsto g^p G_{\omega,(\nu-1)^+}$ defines an $\mathbb{F}_p$-linear operator Π on $\mathrm{gr}_\omega(G)$, which is homogeneous of degree -1, and which satisfies $[\Pi\bar{g}, \bar{h}]_\omega = \Pi([\bar{g}, \bar{h}]_\omega)$ for homogeneous elements $\bar{g}$, $\bar{h}$ of $\mathrm{gr}_\omega(G)$. Letting π act as Π therefore makes $\mathrm{gr}_\omega(G)$ into a graded Lie algebra over $\mathbb{F}_p[\pi]$.

Lemma 7.3. *There exists a p-valuation ω' on G such that, for all $g \in G$ with $g \neq 1$, $\omega'(g) \in e^{-1}\mathbb{Z}$, for some fixed integer $e \geqslant 1$, and $\mathrm{gr}_{\omega'}(G)$ is an abelian Lie algebra over $\mathbb{F}_p[\pi]$.*

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Proof. We first convince ourselves that G is of finite rank in the sense of [**29**, Chapter III, Definition 2.1.3], i.e. that $\mathrm{gr}_\omega(G)$ is finitely generated as an $\mathbb{F}_p[\pi]$-module. By [**29**, Chapter III, Proposition 3.1.3 and Proposition 3.1.9] there is an open subgroup $H \subseteq G$ which is p-valued of finite rank with respect to the induced p-valuation $\omega|H$. Since $\mathrm{gr}_\omega(H)$ is of finite index in $\mathrm{gr}_\omega(G)$, we see that the latter is finitely generated over $\mathbb{F}_p[\pi]$ as well.

In this situation, [**29**, Chapter III, Proposition 3.1.11 and Proposition 3.1.12] ensure the existence of a p-valuation ω' on G such that $\omega'(g) \in \mathbb{Q}$ for all $g \neq 1$ and such that $\mathrm{gr}_{\omega'}(G)$ is an abelian Lie algebra. Using [**29**, Chapter III, Proposition 3.1.9] again, we obtain that $\mathrm{gr}_{\omega'}(G)$ also is finitely generated over $\mathbb{F}_p[\pi]$. It now follows from [**29**, Chapter III, Proposition 2.2.5 and Proposition 2.2.6] that $\omega'(G \setminus \{1\}) \subseteq a_1 + \mathbb{N}_0 \cup \cdots \cup a_r + \mathbb{N}_0$ for finitely many appropriate rational numbers $a_1, \ldots, a_r$. We finally let e be a common denominator for $a_1, \ldots, a_r$. □

Returning to the proof of Proposition 7.2, we see that, following [**29**, Chapter III, § 2.3], our p-valuation ω' on G determines a complete filtration on $\Lambda(G)$, which *a priori* is indexed by the additive group $\mathbb{R}$. On the other hand, by [**29**, Chapter III, Theorem 2.3.3], the associated graded ring for $\Lambda(G)$ with this filtration is isomorphic as a graded algebra to the universal enveloping algebra of the $\mathbb{F}_p[\pi]$-Lie algebra $\mathrm{gr}_{\omega'}(G)$. By Lemma 7.3, $\mathrm{gr}_{\omega'}(G)$ is an abelian Lie algebra, which is free over $\mathbb{F}_p[\pi]$ of rank $d = \dim(G)$, and so its universal enveloping algebra is a polynomial ring in d variables over $\mathbb{F}_p[\pi]$. Further, by Lemma 7.3, the degrees of the generators of the universal enveloping algebra belong to $e^{-1}\mathbb{Z}$, and thus Lazard's theorem implies that the filtration on $\Lambda(G)$ is also indexed by $e^{-1}\mathbb{Z}$. Clearly, we can now rescale the filtration on $\Lambda(G)$ so that it is indexed by $\mathbb{Z}$, and the proof of Proposition 7.2 is complete. □

It is now clear that the structure theory as developed in §§ 2–6 is applicable to finitely generated modules over the Iwasawa algebra $\Lambda(G)$ of a p-valued compact p-adic Lie group G. The most important open problem remains the classification of the prime c-ideals in $\Lambda(G)$. One might also ask under which additional conditions, $\Lambda(G)$ is a unique factorization ring.

8. Examples from elliptic curves

We believe that the abstract theory developed earlier in this paper can be fruitfully applied to many important modules over the Iwasawa algebras of p-adic Lie groups, which arise naturally in arithmetic geometry. For brevity, we shall only discuss here one of the most interesting classes of non-commutative examples, which are defined using elliptic curves without complex multiplication. These rather mysterious examples have already been studied (see [**11**, **21**, **34**]), but it seems certain that a deeper understanding of them, and especially their connection with special values of L-functions, will only be achieved by analysing further their structure as modules over the Iwasawa algebra.

Let F be a finite extension of $\mathbb{Q}$, and E an elliptic curve defined over F. We shall always assume that E has no complex multiplication (i.e. that the endomorphism ring of E over $\bar{\mathbb{Q}}$ is $\mathbb{Z}$). Let p be any prime number greater than or equal to 5. For each integer

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

$n \geqslant 1$, we write E_{p^n} for the group of p^n-division points on E, and E_{p^∞} for the group of all p-power division points on E. We define

$$F_\infty = F(E_{p^\infty}), \qquad G = G(F_\infty/F).$$

The action of G on E_{p^∞} defines an injection of G into $\mathrm{Aut}(E_{p^\infty}) \cong GL_2(\mathbb{Z}_p)$; and a celebrated theorem of Serre [**37**] asserts that G is open in $GL_2(\mathbb{Z}_p)$. Let μ_{p^∞} denote the subgroup of all p-power roots of unity. By the Weil pairing, the field $F(\mu_{p^\infty})$ is contained in F_∞, and we write Γ for the Galois group of $F(\mu_{p^\infty})$ over F. Henceforth, we shall always assume that the Galois group G is pro-p (this can always be achieved by replacing F by a finite extension, if necessary). This implies that Γ is pro-p, and hence that $F(\mu_{p^\infty})$ is itself the cyclotomic $\mathbb{Z}_p$-extension of F. For simplicity, we write $F^{\mathrm{cyc}} = F(\mu_{p^\infty})$.

The modules which interest us arise as follows from the classical Selmer groups, whose definition we now recall. Let L denote any intermediate field with $F \subseteq L \subseteq F_\infty$. As usual, if v is any finite place of L, we write L_v for the union of the completions at v of all finite extensions of F contained in L. If K is a field, $\bar{K}$ will always denote a fixed algebraic closure of K.

Definition 8.1. The *Selmer group* $\mathcal{S}(E/L)$ is defined as

$$\mathcal{S}(E/L) = \mathrm{Ker}\biggl(H^1(G(\bar{\mathbb{Q}}/L), E_{p^\infty}) \to \prod_v H^1(G(\bar{L}_v/L_v), E(\bar{L}_v))\biggr).$$

We also write $X(E/L)$ for the compact Pontryagin dual

$$X(E/L) = \mathrm{Hom}(\mathcal{S}(E/L), \mathbb{Q}_p/\mathbb{Z}_p).$$

If L is Galois over F, then $G(L/F)$ has a natural action on both $\mathcal{S}(E/L)$ and $X(E/L)$, and this extends to a natural action of $\Lambda(G(L/F))$ of the p-adic Lie group $G(L/F)$. Moreover, it is easy to see that $X(E/L)$ is a finitely generated module over $\Lambda(G(L/F))$. Lying much deeper, and still only proven in a very modest number of cases, are the following two conjectures. If E has good ordinary reduction at all primes v of F dividing p, it is conjectured that $X(E/F^{\mathrm{cyc}})$ is always $\Lambda(\Gamma)$-torsion (see [**33**]), and that $X(E/F_\infty)$ is $\Lambda(G)$-torsion (see [**11**, **18**]). We mention the two conjectures at the same time because one can study both by exploiting the connection between them. Put

$$H = G(F_\infty/F^{\mathrm{cyc}}),$$

so that $\Lambda(H)$ is a sub-algebra of $\Lambda(G)$. Then $\Lambda(G)$ is not finitely generated as a $\Lambda(H)$-module, because $\Gamma = G/H$ is infinite. Now the structure theory of finitely generated torsion $\Lambda(\Gamma)$-modules is very well known (see [**5**, **25**]). Indeed, if M is a finitely generated $\Lambda(\Gamma)$-module, this structure theory shows that M is a finitely generated $\mathbb{Z}_p$-module if and only if M is $\Lambda(\Gamma)$-torsion and the μ-invariant of M is zero. The following result is proven in [**11**].

Proposition 8.2. *Assume the following hypotheses are valid.*

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

(i) *$p \geqslant 5$.*

(ii) *G is pro-p.*

(iii) *E has good ordinary reduction at all places v of F dividing p.*

(iv) *$X(E/F^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module.*

Then $X(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module, and so, in particular, $X(E/F_\infty)$ is $\Lambda(G)$-torsion.

We mention in passing that it is not always true that $X(E/F_\infty)$ is finitely generated over $\Lambda(H)$ (many examples are known, see [**11**], where $X(E/F^{\mathrm{cyc}})$ has positive μ-invariant, and for these examples $X(E/F_\infty)$ cannot be finitely generated over $\Lambda(H)$).

A second basic result about $X(E/F_\infty)$ is due to Ochi and Venjakob [**34**].

Proposition 8.3. *Assume that hypotheses (i), (ii) and (iii) of Proposition 8.2 are valid. If $X(E/F_\infty)$ is $\Lambda(G)$-torsion, then it contains no non-zero pseudo-null submodule. In particular, if $X(E/F_\infty)$ is finitely generated over $\Lambda(H)$, then $X(E/F_\infty)$ has no non-zero pseudo-null submodule.*

Corollary 8.4. *Assume that hypotheses (i), (ii), (iii) and (iv) of Proposition 8.2 are valid. Then the $\Lambda(H)$-torsion submodule of $X(E/F_\infty)$ is zero, and $X(E/F_\infty)$ has positive $\Lambda(H)$-rank.*

Proof. It is proven in [**34**] that every $\Lambda(G)$-module which is finitely generated and torsion over $\Lambda(H)$ is pseudo-null as a $\Lambda(G)$-module. For the final assertion, we only need to note that it is shown in [**11**] that $X(E/F_\infty) \neq 0$ for all primes $p \geqslant 5$. □

We cannot resist mentioning a curious arithmetic consequence of Corollary 8.4, whose interest lies in the fact that it asserts a non-triviality result for all good ordinary primes $p \geqslant 5$. For this proposition alone, we drop our assumption that G is pro-p.

Proposition 8.5. *Let E be an elliptic curve over F without complex multiplication, whose j-invariant is an algebraic integer. Let p be any prime number $\geqslant 5$ such that E has good ordinary reduction at all primes v of F dividing p. Put $K = F(E_p)$. Then $\mathcal{S}(E/K^{\mathrm{cyc}})$ is infinite.*

Proof. Since the j-invariant of E is an integer in F, E has good reduction everywhere over $K = F(E_p)$ by the results of [**39**]. Put $G_K = G(F_\infty/K)$, so that G_K is pro-p. Let us assume that $\mathcal{S}(E/K^{\mathrm{cyc}})$ is finite, and derive a contradiction. Now Corollary 8.4 implies that $X(E/F_\infty)$ is a finitely generated $\Lambda(H_K)$-module, of strictly positive $\Lambda(H_K)$-rank, which we denote by r; here, $H_K = G(F_\infty/K^{\mathrm{cyc}})$. Now let L be a variable finite extension of K contained in F_∞, and put $H_L = G(F_\infty/L^{\mathrm{cyc}})$. A well-known algebraic argument (see [**19**]) then shows that, as $[L^{\mathrm{cyc}} : K^{\mathrm{cyc}}] \to \infty$, we have the asymptotic estimate

$$\mathbb{Z}_p\text{-rank of } X(E/F_\infty)_{H_L} = r[L^{\mathrm{cyc}} : K^{\mathrm{cyc}}] + o([L^{\mathrm{cyc}} : K^{\mathrm{cyc}}]).$$

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Here, $X(E/F_\infty)_{H_L}$ denotes the H_L-coinvariants of $X(E/F_\infty)$. We shall only need the very weak consequence of this result that $X(E/F_\infty)_{H_L}$ is not finite when $[L^{\mathrm{cyc}} : K^{\mathrm{cyc}}]$ is sufficiently large. On the other hand, if L is any finite Galois extension of K contained in F_∞, we can apply the formula of Hachimori and Matsuno (see [**17**] or [**21**, Corollary 2.12]) to the finite Galois p-extension $L^{\mathrm{cyc}}/K^{\mathrm{cyc}}$ to conclude, on recalling that E has good reduction everywhere over K, that $\mathcal{S}(E/L^{\mathrm{cyc}})$ is finite always. But the restriction map from $\mathcal{S}(E/L^{\mathrm{cyc}})$ to $\mathcal{S}(E/F_\infty)^{H_L}$ induces a homomorphism

$$f : X(E/F_\infty)_{H_L} \to X(E/L^{\mathrm{cyc}}).$$

A non-trivial arithmetic argument (see [**11**, § 6, Lemma 6.7]) shows that Ker(f) and Coker(f) are both finite, since E has no places of bad multiplicative reduction. Thus we conclude that $X(E/F_\infty)_{H_L}$ is finite for all finite Galois extensions L of K contained in F_∞, contradicting what we proved above. This completes the proof of the proposition. □

Example 8.6. Let E be the elliptic curve over $\mathbb{Q}$ given by

$$E : y^2 + xy = x^3 + x^2 - 2x - 7.$$

The conductor of E is 121 (E is the curve 121C1 in [**13**]), and the j-invariant of E is equal to -11^2. We mention in passing that Serre [**37**] has proven that G is isomorphic to $GL_2(\mathbb{Z}_p)$ for all primes $p \neq 11$, where $G = G(\mathbb{Q}(E_{p^\infty})/\mathbb{Q})$. The good ordinary primes for E are $2, 3, 5, 7, 13, 17, \ldots$ (the first supersingular prime is 43). Thus Proposition 8.5 can be applied to E and proves that for all ordinary primes $p \geqslant 5$, the Selmer group $\mathcal{S}(E/\mathbb{Q}(E_p, \mu_{p^\infty}))$ is infinite. Put $F = \mathbb{Q}(E_p)$. To illustrate the limits of our present knowledge, we still cannot prove that either $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion or $X(E/F_\infty)$ is $\Lambda(G)$-torsion for a single good ordinary prime $p \geqslant 5$ for this curve E.

It is now natural to try and compare these arithmetic results about the module $X(E/F_\infty)$ with the algebraic theory established earlier in this paper. All we can do at present is to pose the following rather obvious questions. For simplicity, let us assume that our elliptic curve E over F and the prime p satisfy hypotheses (i)–(iv) of Proposition 8.2, so that we know that $X(E/F_\infty)$ is $\Lambda(G)$-torsion. In addition, let us assume that G is a p-valued group in the sense of § 7 (if this is not the case, it can always be achieved by replacing F by a finite extension contained also in F_∞). Then, by the results of § 7, $A = \Lambda(G)$ is a Noetherian Auslander regular maximal order, without zero divisors, satisfying $\mathrm{K}_1\mathrm{dim}(A) \leqslant 1$. Take $M = X(E/F_\infty)$, and as before, we write $Q(M)$ for the corresponding object in the quotient category $\mathrm{Mod}(A)/\mathcal{C}_A^1$, where $A = \Lambda(G)$. By Proposition 5.1, we have the canonical decomposition,

$$Q(M) = Q(M)_0 \oplus Q(M)_1,$$

where $Q(M)_0$ is completely faithful, and $Q(M)_1$ is bounded. At present, we do not know a single example of an elliptic curve E over F satisfying hypotheses (i)–(iv) of Proposition 8.2 and a prime p satisfying our hypothesis for which we can prove that a given one of the direct summands $Q(M)_i$ $(i = 0, 1)$ is non-zero. Of course, one at least

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

of the two direct summands must be non-zero, since Proposition 8.3 and Corollary 8.4 show that $Q(M)$ is non-zero. It follows from Corollary 3.5 and Proposition 8.3 that there exist non-zero left ideals $L_1, \dots, L_m$ of $\Lambda(G)$ such that we have an exact sequence of $\Lambda(G)$-modules,

$$0 \to \bigoplus_{i=1}^{m} \Lambda(G)/L_i \to X(E/F_\infty) \to Z \to 0,$$

where Z is pseudo-null. We stress that there appears to be great interest arithmetically in studying the left ideals $L_1, \dots, L_m$. One can hope eventually to give a description of these left ideals in terms of the values at $s = 1$ of the twists of the complex L-function of E over F by Artin characters of G (i.e. those characters of G which factor through a finite quotient). A more modest goal at present is to attempt to determine these ideals in some simple numerical examples. We now discuss one such example in more detail.

Example 8.7. Let E be the elliptic curve $X_1(11)$, namely $E : y^2 + y = x^3 - x^2$, of conductor 11. Take $p = 5$, and let F be the field obtained by adjoining the fifth roots of unity to $\mathbb{Q}$. Thus $F_\infty = \mathbb{Q}(E_{5^\infty})$, and $F^{\text{cyc}} = \mathbb{Q}(\mu_{5^\infty})$, and we have

$$G = G(F_\infty/F), \qquad H = G(F_\infty/\mathbb{Q}(\mu_{5^\infty})).$$

It can easily be shown (see [**15**]) that the image of G in $\mathrm{Aut}(E_{5^\infty})$ can be identified with the subgroup of all matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in $GL_2(\mathbb{Z}_5)$ with $a \equiv d \equiv 1 \bmod 5$, and $c \equiv 0 \bmod 5^2$, and this group in turn is isomorphic to the group of all matrices in $GL_2(\mathbb{Z}_5)$ which are congruent to the identity modulo 5. Hence G is pro-5, and also a 5-valued group in the sense of § 7. As 5 is an ordinary prime for E, and it is well known that $\mathcal{S}(E/\mathbb{Q}(\mu_{5^\infty})) = 0$ (see [**12**, Chapter 5]), we see that hypotheses (i)–(iv) of Proposition 8.2 are valid in this case.

Proposition 8.8. *In the above example, $X(E/F_\infty)$ is a torsion $\Lambda(G)$-module, with no non-zero pseudo-null submodule. It is finitely generated over $\Lambda(H)$ of rank 4, its $\Lambda(H)$-torsion submodule is zero, but it is not a free $\Lambda(H)$-module.*

The proof that $X(E/F_\infty)$ has $\Lambda(H)$-rank 4 hinges on the remarkable fact that we can determine the exact $\mathbb{Z}_5$-rank of the H_L-coinvariants of $X(E/F_\infty)$ for any finite Galois extension L of F contained in F_∞, where $H_L = G(F_\infty/L^{\text{cyc}})$. The following result which depends crucially on the ideas of [**17**], summarizes what is proven in § 7 of [**11**].

Lemma 8.9. *Let L be any finite Galois extension of F contained in F_∞. Then*

(i) *$X(E/L^{\text{cyc}})$ is a free $\mathbb{Z}_5$-module of rank $4 \cdot [L^{\text{cyc}} : F^{\text{cyc}}] - r_L$, where r_L denotes the number of primes of L^{cyc} above 11;*

(ii) *$X(E/F_\infty)_{H_L}$ has $\mathbb{Z}_5$-rank equal to $4 \cdot [L^{\text{cyc}} : F^{\text{cyc}}]$, and its $\mathbb{Z}_5$-torsion submodule contains a group having the same order as $E_{5^\infty}(L^{\text{cyc}})$.*

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

The only new ingredient in the proof of Lemma 8.9 is the result of Matsuno [**32**] that $X(E/L^{\mathrm{cyc}})$ contains no $\mathbb{Z}_5$-torsion, and we do not repeat the proof here. Let C denote the centre of G which is easily seen to be isomorphic to the multiplicative group $1+5\mathbb{Z}_5$. We have $G \cong C \times H$. By a result of Howson [**20**], the Iwasawa algebra $\Lambda(C)$ is precisely the centre of $\Lambda(G)$. Does any non-zero element of $\Lambda(C)$ annihilate $X(E/F_\infty)$? At present we can only prove the following much weaker result in this direction. Fix a topological generator σ_C of C. As usual, we have a unique continuous ring isomorphism $\rho : \Lambda(C) \xrightarrow{\sim} \mathbb{Z}_5[[T_C]]$ with $\rho(\sigma_C) = 1 + T_C$. We define a power series in $\mathbb{Z}_5[[T_C]]$ to be *special* if it is non-zero and can be written in the form

$$u(T_C) \cdot p^\mu \prod_{i=1}^{m} (T_C - \alpha_i),$$

where $u(T_C)$ is a unit in $\mathbb{Z}_5[[T_C]]$, μ is an integer $\geqslant 0$, and either (i) every α_i is of the form $\zeta_i - 1$ with some 5-power root of unity ζ_i in the algebraic closure of $\mathbb{Q}_5$, or (ii) every α_i belongs to $5\mathbb{Z}_5$. We define an element $\xi \in \Lambda(C)$ to be *special* if its image $\rho(\xi)$ is a special power series. It is easily seen that the set of special elements of $\Lambda(C)$ does not depend on the choice of the generator σ_C.

Proposition 8.10. *In the above example, the $\Lambda(G)$-module $X(E/F_\infty)$ is not annihilated by any special element of $\Lambda(C)$. In particular, C does not act trivially on $X(E/F_\infty)$.*

The proof of Proposition 8.10 rests on the following simple observation. Let K_∞ denote the fixed field of C. Let L be a finite Galois extension of F which is contained in K_∞. Then we have

$$F_\infty = K_\infty(\mu_{5^\infty}), \qquad K_\infty \cap L^{\mathrm{cyc}} = L,$$

and C is mapped isomorphically onto $\Gamma_L := G_L/H_L$, where $G_L = G(F_\infty/L)$, under the natural surjection, yielding a canonical isomorphism

$$\theta_L : \Lambda(C) \xrightarrow{\cong} \Lambda(\Gamma_L).$$

It is convenient to take $\theta_L(\sigma_C)$ to be a topological generator of Γ_L, and this enables us to identify both $\Lambda(C)$ and $\Lambda(\Gamma_L)$ with $\mathbb{Z}_5[[T_C]]$.

Lemma 8.11. *Let $\xi \in \Lambda(C)$ be a non-zero element which annihilates $X(E/F_\infty)$. For each finite Galois extension $L \subseteq K_\infty$ of F, the element $\theta_L(\xi)$ annihilates $X(E/L^{\mathrm{cyc}})$. In particular, each zero of the characteristic power series of $X(E/L^{\mathrm{cyc}})$ must also be a zero of $\rho(\xi)$.*

Proof. We know (see the Appendix of [**12**]) that the restriction map from $\mathcal{S}(E/L^{\mathrm{cyc}})$ to $\mathcal{S}(E/F_\infty)^{H_L}$ has finite kernel. Dualizing, we obtain a map from $Y := X(E/F_\infty)_{H_L}$ to $X(E/L^{\mathrm{cyc}})$ with finite cokernel. Clearly, $\theta_L(\xi)$ annihilates Y. Hence, as the characteristic power series of $X(E/L^{\mathrm{cyc}})$ divides the characteristic power series of Y, and as $X(E/L^{\mathrm{cyc}})$ is a free $\mathbb{Z}_5$-module by Lemma 8.9, we deduce easily that $\theta_L(\xi)$ must annihilate $X(E/L^{\mathrm{cyc}})$, proving our assertion. □

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

Let $Z(E/F)$ denote the set of all zeros of absolute value strictly less than one in the algebraic closure of $\mathbb{Q}_5$ of the characteristic power series of the $X(E/L^{\mathrm{cyc}})$, as L ranges over all finite extension of F which are contained in K_∞. If $Z(E/F)$ is infinite, Lemma 8.11 shows that $X(E/F_\infty)$ has no non-zero annihilator in $\Lambda(C)$. Unfortunately we do not see how to prove that $Z(E/F)$ is infinite at present. We can only prove the weaker result given in Proposition 8.10 by the following beautiful infinite descent results of Fisher [**15**]. Let E' denote the elliptic curve of conductor 11 with the equation

$$E' : y^2 + y = x^3 - x^2 - 7\,820x - 263\,580.$$

Define

$$L_1 := F(E_5), \qquad L_2 := F(E'_5).$$

Then (see [**15**]) both L_1 and L_2 are cyclic extensions of F of degree 5, which are contained in K_∞. As usual, we write $\text{Ш}(E/L)$ for the Tate–Shafarevich group of E over any finite extension L of F.

Proposition 8.12 (cf. [15]). *We have:*

(i) $E(L_1) \cong (\mathbb{Z}/5\mathbb{Z})^2$, $\text{Ш}(E/L_1)(5) \cong (\mathbb{Z}/5\mathbb{Z})^2$;

(ii) $E(L_2) \cong \mathbb{Z}/5\mathbb{Z}$, $\text{Ш}(E/L_2)(5) = 0$.

We now complete the proof of Proposition 8.10. Let $f_i(T)$ denote the characteristic power series of $X(E/L_i^{\mathrm{cyc}})$. By Lemma 8.9 (i), $X(E/L_i^{\mathrm{cyc}})$ is a free $\mathbb{Z}_5$-module of rank 16, and so we can assume that each $f_i(T)$ is a distinguished polynomial of degree 16. Let $\Delta_i := G(L_i/\mathbb{Q})$. As Δ_i has order 20, one sees that Δ_i has one irreducible representation of degree 4, and four irreducible representations of degree 1, which factor through $G(F/\mathbb{Q})$. As $X(E/F^{\mathrm{cyc}}) = 0$, one deduces easily that none of the representations of degree 1 of Δ_i can occur in $X(E/L_i^{\mathrm{cyc}}) \otimes_{\mathbb{Z}_5} \bar{\mathbb{Q}}_5$, where $\bar{\mathbb{Q}}_5$ denotes an algebraic closure of $\mathbb{Q}_5$. As the actions of Δ_i and of $G(L_i^{\mathrm{cyc}}/L_i)$ commute with each other, it also follows easily that we have

$$f_i(T) = h_i(T)^4$$

for some distinguished polynomial $h_i(T)$ of degree 4 (we thank R. Greenberg for making this remark to us). The next key step in the proof is to use the well-known classical formula (see [**12**]) for the $G(L_i^{\mathrm{cyc}}/L_i)$-Euler characteristic of $X(E/L_i^{\mathrm{cyc}})$ to compute $f_i(0)$ up to a 5-adic unit. The data needed for this formula are given by Proposition 8.12, together with the decomposition of the prime number 5 in L_i, which is also determined in [**15**] (there are five primes of L_1 above 5, each with residue field $\mathbb{F}_5$, and there is a unique prime of L_2 above 5, with residue field $\mathbb{F}_5$), and we find

$$f_1(0) = 5^{12}v_1, \qquad f_2(0) = 5^4 v_2,$$

where v_1, v_2 are 5-adic units. It follows that

$$h_1(0) = 5^3 u_1, \qquad h_2(0) = 5u_2,$$

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

where u_1, u_2 are 5-adic units. As $h_1(T)$ has degree 4, it cannot be the same as $((1+T)^5-1)/T$ by the first formula, and so no root of $h_1(T)$ can be of the form $\zeta - 1$ for a 5-power root of unity ζ. Also, the above formula for $h_2(0)$ shows that $h_2(T)$ is an Eisenstein polynomial, and therefore irreducible over $\mathbb{Q}_5$, and so $h_2(T)$ can have no root in $5\mathbb{Z}_5$. Thus Proposition 8.10 now follows from these results and Lemma 8.11.

Acknowledgements. We express our warmest thanks both to O. Venjakob and S. Howson for keeping us fully informed of their work. J.C. and R.S. are also deeply grateful to H. Li and F. van Oystaeyen for their infinite patience in answering their inexpert questions on the algebraic theory of microlocalization. J.C. thanks both Columbia University and the long-suffering audience of his Eilenberg lectures there in the spring of 2001 for supporting this research so generously. P.S. gratefully acknowledges the support of the Tata Institute.

Note added in proof

Let p be an odd prime, and let G be the kernel of the reduction map from $SL_2(\mathbb{Z}_p)$ to $SL_2(\mathbb{F}_p)$. Let $B \subseteq G$ be the subgroup of lower triangular matrices. The induced module

$$M = \Lambda(G) \otimes_{\Lambda(B)} \mathbb{Z}_p$$

is pseudo-null. In his article in *J. Algebra* **67** (1980), 68–71, M. Harris proved that M is bounded, i.e. that its annihilator ideal I is non-zero. In his Cambridge PhD thesis, K. Ardakov has recently proven that I is a prime c-ideal in the sense of § 5. Apart from the evident prime c-ideal $p\Lambda(G)$, this is the only known prime c-ideal in $\Lambda(G)$.

References

1. G. Q. Abbasi, S. Kobayashi, H. Marubayashi and A. Ueda, Non-commutative unique factorization rings, *Commun. Alg.* **19** (1991), 167–198.
2. K. Asano, Zur Arithmetik in Schiefringen, *Osaka J. Math.* **1** (1949), 98–134.
3. M. Auslander and M. Bridger, *Stable homotopy theory*, Memoirs of the American Mathematical Society, vol. 94 (1969).
4. J.-E. Björk, Filtered Noetherian rings, in *Noetherian rings and their applications*, Mathematical Survey Monographs, vol. 24, pp. 59–97 (American Mathematical Society, Providence, RI, 1987).
5. N. Bourbaki, *Commutative algebra* (Hermann, Paris, 1972).
6. K. A. Brown, A. Haghany and T. H. Lenagan, Reflexive ideals and injective modules over Noetherian *v-H* orders, *Proc. Edinb. Math. Soc.* **34** (1991), 31–43.
7. W. Bruns and J. Herzog, *Cohen–Macaulay rings* (Cambridge University Press, 1993).
8. M. Chamarie, Sur les ordres maximaux au sens d'Asano, Vorlesungen FB Math., Uni. Essen, Heft 3 (1979).
9. M. Chamarie, Anneaux de Krull non commutatifs, *J. Alg.* **72** (1981), 210–222.
10. M. Chamarie, Modules sur les anneaux de Krull non commutatifs, in *Sém. d'Algèbre* (ed. P. Dubreil and M.-P. Malliavin), Lecture Notes in Mathematics, vol. 1029, pp. 283–310 (Springer, 1983).
11. J. Coates and S. Howson, Euler characteristics and elliptic curves, II, *J. Math. Soc. Jpn* **53** (2001), 175–235.

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

12. J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, TIFR-AMS Lecture Notes (Narosa Publishing House, 2000).
13. J. Cremona, *Algorithms for modular elliptic curves*, 2nd edn (Cambridge University Press, 1997).
14. J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p-groups* (Cambridge University Press, 1999).
15. T. Fisher, Descent calculations for the elliptic curves of conductor, *Proc. Lond. Math. Soc.* **11**, to appear.
16. P. Gabriel, Des catégories abéliennes, *Bull. Soc. Math. France* **90** (1962), 323–448.
17. Y. Hachimori and K. Matsuno, An analogue of Kida's formula for the Selmer groups of elliptic curves, *J. Alg. Geom.* **8** (1999), 581–601.
18. M. Harris, p-adic representations arising from descent on abelian varieties, *Compositio Math.* **39** (1979), 177–245.
19. S. Howson, Iwasawa theory for elliptic curves for p-adic Lie extensions, PhD thesis, University of Cambridge (1998).
20. S. Howson, Structure of central torsion Iwasawa modules, submitted.
21. S. Howson, Euler characteristics as invariants of Iwasawa modules, submitted.
22. L. Huishi, Lifting ore sets of Noetherian filtered rings and applications, *J. Alg.* **179** (1996), 686–703.
23. L. Huishi and F. van Oystaeyen, *Zariskian filtrations* (Kluwer, Dordrecht, 1996).
24. Y. Hachimori and O. Venjakob, Completely faithful Selmer groups over Kummer extensions, submitted.
25. K. Iwasawa, On Γ-extensions of number fields, *Bull. Am. Math. Soc.* **65** (1959), 183–226.
26. N. Jacobson, Theory of rings, in *Math. surveys*, vol. 2, (American Mathematical Society, Providence, RI, 1943).
27. M. Kashiwara, Algebraic study of systems of partial differential equations, Masters thesis, University of Tokyo (1971).
28. J. Lambek and G. O. Michler, The torsion theory at a prime ideal of a right Noetherian ring, *J. Alg.* **25** (1973), 364–389.
29. M. Lazard, Groupes analytiques p-adique, *Publ. Math. IHES* **26** (1965), 389–603.
30. J. C. McConnell and J. C. Robson, *Noncommutative Noetherian rings* (Wiley, 1987).
31. H. Marubayashi, A Krull type generalization of HNP rings with enough invertible ideals, *Commun. Alg.* **11** (1983), 469–499.
32. K. Matsuno, Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic extensions, submitted.
33. B. Mazur, Rational points of abelian varieties in towers of number fields, *Invent. Math.* **18** (1992), 183–266.
34. Y. Ochi and O. Venjakob, On the structure of Selmer groups over p-adic Lie extensions, *J. Alg. Geom.* **11** (2002), 547–576.
35. J. C. Robson, Cyclic and faithful objects in quotient categories with applications to Noetherian simple or Asano rings, in *Noncommutative ring theory, Kent state 1975*, Lecture Notes in Mathematics, vol. 545, pp. 151–172 (Springer, 1976).
36. J.-P. Serre, Classes des corps cyclotomiques (d'aprés K. Iwasawa), *Sém. Bourbaki* **174** (1958/1959) (Oeuvres, I, 569–576).
37. J.-P. Serre, Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331 (Oeuvres, III, 1–73).
38. J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics, vol. 5 (Springer, 1973).
39. J-P. Serre and J. Tate, Good reduction of abelian varieties, *Ann. Math.* **88** (1968), 492–517 (Oeuvres, II, 472–517).
40. B. Stenström, *Rings of quotients* (Springer, 1975).

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press

41. O. Venjakob, Iwasawa theory of p-adic Lie Extensions, PhD thesis, University of Heidelberg (2000).

42. O. Venjakob, On the structure of Iwasawa algebra of a p-adic Lie group, *J. Eur. Math. Soc.* **4** (2002), 271–311.

43. O. Venjakob, A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory, *Crelle's J.*, to appear.

44. E. Wexler-Kreindler, Microlocalization, platitude et theorie de torsion, *Commun. Alg.* **16** (1988), 1813–1852.

https://doi.org/10.1017/S1474748003000045 Published online by Cambridge University Press