Astérisque

JOHN COATES

Iwasawa algebras and arithmetic

Astérisque, tome 290 (2003), Séminaire Bourbaki, exp. n° 896, p. 37-52
<http://www.numdam.org/item?id=SB_2001-2002__44__37_0>

Séminaire BOURBAKI
54e année, 2001-2002, no 896, p. 37 à 52

Novembre 2001

IWASAWA ALGEBRAS AND ARITHMETIC

by **John COATES**

1. INTRODUCTION

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

$$\Lambda(G) = \varprojlim_U \mathbb{Z}_p[G/U]$$

where U runs over the open normal subgroups of G. Any compact $\mathbb{Z}_p$-module on which G acts continuously on the left has a unique structure as a left $\Lambda(G)$-module, extending the G-action. Thanks to this remark, modules over $\Lambda(G)$, where G is usually the image of Galois in a finite dimensional p-adic Galois representation, abound in arithmetic geometry. K. Iwasawa [Iw] was the first to study the structure theory of finitely generated $\Lambda(G)$-modules in the special case when $G = \mathbb{Z}_p$, and deduced from it his celebrated asymptotic formula for the growth of the order of the p-primary subgroup of the ideal class group in a $\mathbb{Z}_p$-extension of a number field. Almost immediately, J-P. Serre [Se1], [Se2] pointed out that, when $G = \mathbb{Z}_p^d$ for any integer $d \geqslant 1$, $\Lambda(G)$ is isomorphic to the local ring $\mathbb{Z}_p[[T_1, \ldots, T_d]]$ of formal power series in d variables with coefficients in $\mathbb{Z}_p$, and that Iwasawa's structure theorem for $\Lambda(G)$-modules could be re-proven for $d = 1$, and generalized to all $d \geqslant 1$, by using classical arguments in commutative algebra about the structure theory of modules up to pseudo-isomorphism ([B-CA], Chap. VII, § 4.4, Theorems 4 and 5).

Intuitively, one might expect that the structure theory for $\Lambda(G)$-modules would be very different in the commutative and non-commutative cases, but the aim of this seminar is to report on joint work of the author, P. Schneider and R. Sujatha [CSS] proving that, surprisingly, the two cases appear to be parallel in many ways. The first step towards elucidating the non-commutative theory was made by O. Venjakob [Ve1], [Ve2], who exploited ideas of J. Björk [Bj] to define in general the notion of a pseudo-null $\Lambda(G)$-module. If G is pro-p and has no element of order p, Venjakob defines

a finitely generated left $\Lambda(G)$-module M to be pseudo-null if it is $\Lambda(G)$-torsion (i.e. each element of M is annihilated by some non-zero element of $\Lambda(G)$), and, in addition, $Ext^1_{\Lambda(G)}(M, \Lambda(G)) = 0$. To establish our structure theory up to pseudo-isomorphism, we need to impose further conditions on G, and we are grateful to B. Totaro for pointing out to us that probably the most natural hypothesis is that G should possess a p-valuation in the sense of M. Lazard [La]. We recall that a p-valuation on G is a function $\omega : G \to (0, \infty]$ satisfying the following axioms for all x and y in G:

(i) $\omega(1) = \infty$, and $\frac{1}{p-1} < \omega(x) < \infty$ for $x \neq 1$;
(ii) $\omega(xy^{-1}) \geqslant \min\{\omega(x), \omega(y)\}$;
(iii) $\omega(x^{-1}y^{-1}xy) \geqslant \omega(x) + \omega(y)$;
(iv) $\omega(x^p) = \omega(x) + 1$.

We say that G is p-valued if it possesses a p-valuation. If G is p-valued, we remark that the compactness of G guarantees that G is complete with respect to the p-valuation ω in the following sense. For each $u > 0$, let G_u denote the subgroup of G consisting of all g such that $\omega(g) \geqslant u$. As J-P. Serre observed to us, G_u is open in G because, choosing $N > u$, G_u contains the subgroup of G generated by the p^N-th powers, and it is well known that this latter subgroup is a neighbourhood of the identity in a p-adic Lie group. Hence the family $\{G_u : u > 0\}$ form an open basis for the topology of G since their intersection is trivial, and the natural map from G to $\varprojlim G/G_u$ is an isomorphism because of the compactness of G. Moreover, Lazard [La] established the following basic facts. Any closed subgroup of a p-valued group is also p-valued. If G is p-valued, then it is pro-p, and has no element of order p. The classic example of a p-valued group is the group of matrices in $GL_n(\mathbb{Z}_p)$ which are congruent to the identity modulo p (resp. mod 4) if p is odd (resp. if $p = 2$). If $p > n + 1$, any pro-p closed subgroup of $GL_n(\mathbb{Z}_p)$ is p-valued.

THEOREM 1.1 ([CSS]). — *Let G be a p-valued compact p-adic Lie group, and let M be a finitely generated torsion $\Lambda(G)$-module. Let M_0 be the maximal pseudo-null submodule of M. Then there exist non-zero left ideals $L_1, \ldots, L_m$, and a $\Lambda(G)$-injection*

$$\phi : \bigoplus_{i=1}^{m} \Lambda(G)/L_i \longrightarrow M/M_0,$$

with Coker(ϕ) *pseudo-null.*

The special case of Theorem 1.1 in which M/M_0 is killed by some power of p was proven earlier by O. Venjakob [Ve1], [Ve2], and S. Howson [Ho]. In § 2, we shall give a sketch of a proof of Theorem 1.1 taken from [CSS], which is remarkably parallel to the classical commutative proof in [B-CA], and which exploits the fact that $\Lambda(G)$ is a filtered ring to which one can apply the techniques of the algebraic theory of micro-localization (see, for example, [LO]). After finding this proof, we also realized that Theorem 1.1 can be derived from the work of M. Chamarie [Ch1], [Ch2], on modules over maximal orders (see [CSS] for the details).

We assume for the rest of this exposé that G is a p-valued compact p-adic Lie group. In particular, it follows that $\Lambda(G)$ is Noetherian, and has no zero divisors. Let $\mathrm{Mod}(G)$ denote the category of all finitely generated left $\Lambda(G)$-modules, and $C^1(G)$ the subcategory whose objects are the pseudo-null modules ($C^1(G)$ is closed under taking subobjects, quotients, and extensions). To discuss questions about the uniqueness of the decomposition in Theorem 1.1, we have to pass to the quotient category

$$\mathfrak{M}(G) = \mathrm{Mod}(G)/C^1(G).$$

We write $Q : \mathrm{Mod}(G) \longrightarrow \mathfrak{M}(G)$ for the canonical functor. If M is an object of $\mathrm{Mod}(G)$, we define its annihilator, which we denote by $\mathrm{ann}_{\Lambda(G)}(M)$, to be the two sided ideal consisting of all r in $\Lambda(G)$ such that $r.M = 0$. We then define the annihilator of the object $Q(M)$ of the quotient category $\mathfrak{M}(G)$, which we denote by $\mathrm{ann}(Q(M))$, to be the sum of all the ideals $\mathrm{ann}_{\Lambda(G)}(N)$, where N runs over all objects of $\mathrm{Mod}(G)$ such that $Q(N)$ is isomorphic to $Q(M)$ in $\mathfrak{M}(G)$. In fact, a lemma of Robson [Ro] shows that

$$\mathrm{ann}(Q(M)) = \mathrm{ann}_{\Lambda(G)}(M/M_0),$$

where, as above, M_0 denotes the maximal pseudo-null submodule of M. Yet another description of $\mathrm{ann}(Q(M))$ can be given in terms of the left ideals $L_1, \ldots, L_m$ appearing in Theorem 1.1. Let J_i be the maximal two-sided ideal of $\Lambda(G)$ which is contained in L_i, and let $J = \cap_{i=1}^m J_i$. Then $J_i = \mathrm{ann}_{\Lambda(G)}(\Lambda(G)/L_i)$, and we have

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

in particular, we see that $J \neq 0$ if and only if $J_i \neq 0$ for $i = 1, \ldots, m$.

It is in questions of annihilators that we find a basic difference between the commutative and non-commutative case. R. Greenberg (unpublished) has given an example of a p-valued open subgroup of $GL_2(\mathbb{Z}_p)$, and a finitely generated torsion $\Lambda(G)$-module M such that $\mathrm{ann}(Q(M)) = 0$. Following Chamarie [Ch2], we therefore define $Q(M)$ to be *bounded* (resp. *completely faithful*) if $\mathrm{ann}(Q(M)) \neq 0$ (resp. if $\mathrm{ann}(Q(N)) = 0$ for every torsion $\Lambda(G)$-module N such that $Q(N)$ is a non-zero subquotient of $Q(M)$). It is proven in [Ch2] that, for every finitely generated torsion $\Lambda(G)$-module M, we have a canonical decomposition

$$Q(M) = Q(U) \oplus Q(V),$$

where $Q(U)$ is completely faithful and $Q(V)$ is bounded. Very little is known about completely faithful objects in $\mathfrak{M}(G)$ beyond the fact that Greenberg's example shows that they exist, and also it is shown in [Ch2] that they are cyclic, i.e. isomorphic in $\mathfrak{M}(G)$ to $Q(\Lambda(G)/L)$ where L is a non-zero left ideal. However, Y. Hachimori and O. Venjakob [HV] have recently given examples of completely faithful $\Lambda(G)$-modules which arise naturally in arithmetic geometry, and one suspects that their occurrence in number theory may be rather common.

We write $\mathfrak{M}_b(G)$ for the full subcategory of $\mathfrak{M}(G)$ consisting of the bounded objects, and we define $\mathcal{D}_b(G)$ to be the Grothendieck group of $\mathfrak{M}_b(G)$. In fact, $\mathfrak{M}_b(G)$ is also an abelian category in which every object has finite length, and the Jordan-Hölder theorem shows that $\mathcal{D}_b(G)$ is the free abelian group on the set of isomorphism classes of simple objects in $\mathfrak{M}_b(G)$. It is natural to ask whether we can relate $\mathcal{D}_b(G)$ to a natural group of divisors of the ring $\Lambda(G)$, parallel to the classical theory for commutative, integrally closed, integral domains ([B-CA], Chap. VII, § 4.5, Proposition 11). As we shall now explain, this is indeed the case. Let $K(G)$ denote the skew field of fractions of $\Lambda(G)$, which is well known to exist because $\Lambda(G)$ is Noetherian and has no divisors of zero. Then $\Lambda(G)$ is a *maximal order* (this is the non-commutative analogue of being integrally closed) in the sense that, if B is any intermediate ring with $\Lambda(G) \subset B \subset K(G)$ such that there exist non-zero elements u, v in $K(G)$ with $uBv \subset \Lambda(G)$, then necessarily $B = \Lambda(G)$ (see [CSS], Lemma 2.6). For any left (resp. right) $\Lambda(G)$- module M, we put $M^* = \mathrm{Hom}_{\Lambda(G)}(M, \Lambda(G))$ for the dual right (resp. left) $\Lambda(G)$-module, and we say M is *reflexive* if the natural map from M to M^{**} is an isomorphism. A non-zero left (resp. right) $\Lambda(G)$-submodule L of $K(G)$ is called a *fractional* left (resp. right) ideal if there is a non-zero v in $K(G)$ such that $L \subset \Lambda(G)v$ (resp. $L \subset v\Lambda(G)$). A *fractional ideal* of $\Lambda(G)$ is a subset I of $K(G)$ which is both a fractional left and a fractional right ideal. Finally, we define a fractional c-ideal of $\Lambda(G)$ to be a reflexive fractional ideal of $\Lambda(G)$, and we write $\mathcal{C}(G)$ for the set of fractional c-ideals. As a special case of general results about maximal orders, Asano ([As]) has shown that $\mathcal{C}(G)$ is an abelian group with respect to the product $I.J = (IJ)^{**}$. We recall that a two-sided ideal $\mathfrak{p}$ of $\Lambda(G)$ is said to be *prime* if, whenever x and y are elements of $\Lambda(G)$ such that $x\Lambda(G)y \subset \mathfrak{p}$, we always have x is in $\mathfrak{p}$ or y is in $\mathfrak{p}$. It is then also proven in [As] that $\mathcal{C}(G)$ is the free abelian group on the set $\mathcal{P}$ of all non-zero prime c-ideals, and that every prime c-ideal has height 1 (i.e. is a minimal non-zero prime ideal). There would be great interest in giving an explicit description of this set $\mathcal{P}$ (for example, when G is a p-valued open subgroup of $SL_2(\mathbb{Z}_p)$).

Our aim is to construct a canonical homomorphism

$$\chi : \mathcal{D}_b(G) \to \mathcal{C}(G),$$

and for this we need to localize $\Lambda(G)$ at the prime ideals in $\mathcal{P}$. We recall that a multiplicatively closed subset S of non-zero elements of $\Lambda(G)$ is said to be a right and left Ore set if, for each s in S and a in $\Lambda(G)$ both $aS \cap s\Lambda(G)$ and $Sa \cap \Lambda(G)s$ are non-empty. For each $\mathfrak{p}$ in $\mathcal{P}$, let $S(\mathfrak{p})$ denote the set of all elements of $\Lambda(G)$ whose residue class in $\Lambda(G)/\mathfrak{p}$ is not a zero divisor. Chamarie [Ch1] has proven that $S(\mathfrak{p})$ is a left and right Ore set, and that the localization of $\Lambda(G)$ by $S(\mathfrak{p})$, which we denote by $\Lambda(G)_{\mathfrak{p}}$, is a bounded maximal order, with Jacobson radical $\mathfrak{p}\Lambda(G)_{\mathfrak{p}}$. Moreover, every left and right ideal in $\Lambda(G)_{\mathfrak{p}}$ is principal. Now, up to isomorphism, the objects of finite length in $\mathfrak{M}_b(G)$ are of the form $Q(M)$, where M is a finitely

generated torsion $\Lambda(G)$-module. Hence the localization $M_{\mathfrak{p}} = \Lambda(G)_{\mathfrak{p}} \otimes_{\Lambda(G)} M$ is a finitely generated torsion $\Lambda(G)_{\mathfrak{p}}$-module, which has finite length because $\Lambda(G)_{\mathfrak{p}}$ is a principal ideal domain. Denoting the length of $M_{\mathfrak{p}}$ by $\ell_{\mathfrak{p}}(Q(M))$, we then define

$$\chi(Q(M)) = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\ell_{\mathfrak{p}}(Q(M))},$$

and we call $\chi(Q(M))$ the *characteristic ideal* of $Q(M)$. This is well defined, as it is proven in [Ch2], Lemma 4.2.1 that, for any finitely generated torsion $\Lambda(G)$-module M, we have that $M_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$ in $\mathcal{P}$ if and only if $Q(M)$ is completely faithful. Moreover, it is shown in [CSS] that $\mathrm{ann}(Q(M))$ is a c-ideal such that $\chi(Q(M)) \subset \mathrm{ann}(Q(M))$, and such that $\chi(Q(M))$ and $\mathrm{ann}(Q(M))$ have the same prime factors in $\mathcal{P}$. In addition, the exactness of localization and the additivity of the length function show that χ induces a homomorphism from $\mathcal{D}_b(G)$ to $\mathcal{C}(G)$.

THEOREM 1.2 ([CSS]). — *The homomorphism*

$$\chi : \mathcal{D}_b(G) \longrightarrow \mathcal{C}(G)$$

is an isomorphism. In particular, χ induces a bijection between the set of isomorphism classes of simple objects in $\mathfrak{M}_b(G)$ and the set $\mathcal{P}$ of all non-zero prime c-ideals of $\Lambda(G)$.

As far as all finitely generated $\Lambda(G)$-modules are concerned, only the following partial result is proven in [CSS]. If M is an arbitrary finitely generated $\Lambda(G)$-module, we write M_t for its $\Lambda(G)$-torsion submodule. It is shown in [Ve2] that the natural map from $M/M_t \to (M/M_t)^{**}$ is injective and has pseudo-null cokernel.

THEOREM 1.3 ([CSS]). — *Let M be a finitely generated $\Lambda(G)$-module such that $Q(M_t)$ is bounded. Then we have an isomorphism*

$$Q(M) \xrightarrow{\sim} Q(M_t) \oplus Q(M/M_t),$$

where $Q(M/M_t)$ is reflexive in the sense that it is isomorphic to $Q((M/M_t)^{**})$ in the quotient category $\mathfrak{M}(G)$.

The fundamental question left open by [CSS] is whether every prime ideal $\mathfrak{p}$ in $\mathcal{P}$ is principal. This is true when $G = \mathbb{Z}_p^d$, for any integer $d \geqslant 1$, thanks to the Weierstrass Preparation Theorem, and we strongly suspect that it remains true for all compact, p-valued p-adic Lie groups G.

2. SKETCH OF THE PROOF OF THEOREM 1.1

One of the nicest parts of Bourbaki's treatise on commutative algebra is his elegant proof of the analogue of Theorem 1.1 for all finitely generated torsion modules over any Noetherian, integrally closed, integral domain (see [B-CA], Chap. VII, § 4.4, Theorem 5). We now briefly explain how simple ideas from the algebraic theory of

micro-localization allow one to extend these arguments to modules over a wide class of non-commutative filtered rings. Following the spirit of Bourbaki, we proceed axiomatically, and leave to the end of this section the verification that our concrete ring $\Lambda(G)$ satisfies the axioms we impose.

Let A be an associative ring with unit elements, which will not, in general, be commutative. We assume that A is endowed with a filtration $F_\bullet A = \{F_n A : n \in \mathbb{Z}\}$, but we shall be unfaithful to Bourbaki and always assume our filtrations are increasing, i.e. $F_n A \subset F_{n+1} A$ for all n in $\mathbb{Z}$. This filtration will always be assumed to be exhaustive (i.e. $\bigcup_{n\in\mathbb{Z}} F_n A = A$) and separated (i.e. $\bigcap_{n\in\mathbb{Z}} F_n A = 0$). We write

$$\mathrm{gr}_\bullet A = \bigoplus_{n\in\mathbb{Z}} F_n A/F_{n-1}A, \qquad \widehat{A} = \varprojlim A/A_n$$

for the associated graded ring, and the completion of A with respect to the filtration, respectively. We follow the non-commutative literature ([LO], Chap. II, Theorem 2.2), and define A to be a *Zariski ring* if $\mathrm{gr}_\bullet A$ is left and right Noetherian, and $\widehat{A}$ is a faithfully flat left and right A-module.

For the rest of this section, we shall assume that the ring A satisfies the following axioms:

(C1) A is complete with respect to $F_\bullet A$, i.e. the natural injection from A to $\widehat{A}$ is an isomorphism;

(C2) $\mathrm{gr}_\bullet A$ is isomorphic as a graded ring to $k[T_1, \ldots, T_r]$, the ring of polynomials in a finite number of variables with coefficients in a field k, graded by assigning to each of the variables a strictly negative integer as its degree.

Axioms (C1) and (C2) imply that A is left and right Noetherian and has no zero divisors, and that A is a Zariski ring.

For the remainder of the proof, M will denote an arbitrary finitely generated torsion A-module. We endow M with a *good filtration* $F_\bullet M = \{F_n M : n \in \mathbb{Z}\}$. This means that we have

$$F_n M = \sum_{i=1}^{r} F_{n-k_i} A \cdot w_i \qquad (n \in \mathbb{Z}),$$

where $w_1, \ldots, w_r$ is some fixed set of A-generators of M, and $k_1, \ldots, k_r$ are fixed integers. Since $F_\bullet M$ is a good filtration, basic properties of Zariski rings show that not only is $F_\bullet M$ separated, but also any submodule N of M is closed in the filtration topology [LO]). Also, defining the $\mathrm{gr}_\bullet A$ module $\mathrm{gr}_\bullet M$ as usual by

$$\mathrm{gr}_\bullet M = \bigoplus_{n\in\mathbb{Z}} F_n M/F_{n-1}M,$$

we have that $\mathrm{gr}_\bullet M$ is a finitely generated $\mathrm{gr}_\bullet A$-module, which is plainly $\mathrm{gr}_\bullet A$-torsion.

The starting point of our proof is to apply the classical commutative theory to the finitely generated torsion $\mathrm{gr}_\bullet A$-module $\mathrm{gr}_\bullet M$. We write Ass $(\mathrm{gr}_\bullet M)$ for the set of prime ideals $\mathfrak{p}$ in $\mathrm{gr}_\bullet A$ which are the exact annihilator of some non-zero element of

$\mathrm{gr}_\bullet M$. Note that the zero ideal is not in Ass $(\mathrm{gr}_\bullet M)$, because $\mathrm{gr}_\bullet M$ is $\mathrm{gr}_\bullet A$-torsion. As $\mathrm{gr}_\bullet M$ is a graded $\mathrm{gr}_\bullet A$-module, every ideal in Ass $(\mathrm{gr}_\bullet M)$ is graded. We define

$$W(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$$

to be the set of prime ideals of height 1 in Ass $(\mathrm{gr}_\bullet M)$. It is not difficult to see that $W(M)$ is independent of the very non-canonical choice of the good filtration $F_\bullet M$. We define $S = S(M)$ to be the set of all non-zero homogeneous elements of $\mathrm{gr}_\bullet A$ which do not belong to $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_m$. We can localize $\mathrm{gr}_\bullet A$ with respect to the multiplicative set of S of non-zero homogeneous elements, and obtain in this way the graded ring $S^{-1}\mathrm{gr}_\bullet A$ ([B-CA], Chap. II, § 2.9), which we denote by $(\mathrm{gr}_\bullet A)_S$. The following lemma (see [CSS], Proposition 3.4) is easily established.

LEMMA 2.1. — *The non-zero graded prime ideals of* $(\mathrm{gr}_\bullet A)_S$ *are precisely the* $S^{-1}\mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$, *and these all have height* 1. *Every proper graded ideal of* $(\mathrm{gr}_\bullet A)_S$ *is contained in one of the* $S^{-1}\mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$.

COROLLARY 2.2. — *Every graded ideal in* $(\mathrm{gr}_\bullet A)_S$ *is principal.*

To deduce the corollary, we first note that, as A is factorial by axiom (C2), so is its localization $(\mathrm{gr}_\bullet A)_S$. Now, if $\mathfrak{b}$ is any non-zero graded ideal of $(\mathrm{gr}_\bullet A)_S$, every element of Ass $((\mathrm{gr}_\bullet A)_S/\mathfrak{b})$ must be graded prime ideal of $(\mathrm{gr}_\bullet A)_S$, and therefore of height 1 by Lemma 2.1. But then (see [B-CA], Chap. VII, § 1.6, Proposition 10) the ideal $\mathfrak{b}$ is divisorial, and so principal because $(\mathrm{gr}_\bullet A)_S$ is factorial.

The heart of our proof is the following observation on Ore sets, which we understand goes back to Kashiwara [Ka]. As usual, if $x \in F_n A \backslash F_{n-1} A$, we define its principal symbol $\sharp(x)$ by $\sharp(x) = x + F_{n-1}A$. Let us define

$$T = \{t \in A : \sharp(t) \in S\};$$

here S is the multiplicative set of non-zero elements of A defined above.

PROPOSITION 2.3. — T *is a left and right Ore set in* A.

We omit the proof (see [Li] or the last part of [WK]), which uses the fact that A is a Zariski ring. In view of Proposition 2.3, it makes sense to take either the left or the right localization of A with respect to T. As they are isomorphic, we write A_T for either localization. Moreover, as is explained in [Li], A_T is endowed with a natural separated and exhaustive filtration $F_\bullet A_T$, with the property that $\mathrm{gr}_\bullet(A_T) = (\mathrm{gr.A})_S$. Even though we have imposed the axiom that A is complete, it will not in general be true that A_T is complete with respect to the filtration $F_\bullet A_T$. Nevertheless, the filtration $F_\bullet A_T$ makes A_T into a Zariski ring (see [Li]), and this weaker result suffices for our purposes. Finally, if N is any finitely generated A-module endowed with a good filtration $F_\bullet N$, then its localization $N_T = A_T \otimes_A N$ is a finitely generated A_T-module, which (see [Li]) is also endowed with a natural filtration $F_\bullet N_T$ such that $\mathrm{gr}_\bullet(N_T) = (\mathrm{gr}_\bullet N)_S$.

PROPOSITION 2.4. — *Every left and right ideal in A_T is principal.*

To prove this, we can, by symmetry, restrict our attention to left ideals L of A_T. Taking any such left ideal, we endow it with the induced filtration $F_\bullet L$ given by $F_n L = L \cap F_n A_T$. By a basic property of Zariski rings, $F_\bullet L$ is again a good filtration. Plainly $\mathrm{gr}_\bullet L$ is a graded ideal in $\mathrm{gr}_\bullet A_T = (\mathrm{gr}_\bullet A)_S$, and so is principal by Corollary 2.2. Thus we can find a homogeneous z in $\mathrm{gr}_\bullet L$ such that $\mathrm{gr}_\bullet L = (\mathrm{gr}_\bullet A)_S \cdot z$. Now pick w to be any element of L such that $\sharp(w) = z$. But, thanks to a remarkable property of Zariski rings ([LO], Chap. I, § 5, Corollary 5.5), we conclude that $L = A_T w$ (note that we are able to carry out this last step without passing to the completion of A_T).

Once we have established that A_T is a principal ideal domain, we can rapidly complete the proof of Theorem 1.1, following closely the classical commutative argument. As the localized module $M_T = A_T \otimes_A M$ is a finitely generated torsion A_T-module, an old result of Jacobson (see [Ja], Chap. 3, Theorem 10) shows that there exist elements $w_1, \ldots, w_m$ in M_T such that

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

Let $\psi : M \to M_T$ be the canonical A-homomorphism given by $\psi(m) = 1 \otimes m$, and let $M' = \mathrm{Im}(\psi)$, $N = \mathrm{Ker}(\psi)$. Since N is precisely the set of T-torsion elements of M, we have $N_T = 0$, and so N is pseudo-null by Proposition 2.5 below. Now M' is an A-submodule of M_T with $M'_T = M_T$. We are clearly free to multiply any of the elements $w_1, \ldots, w_m$ above by any element of T, and thus we can assume that $w_1, \ldots, w_m$ all belong to M'. We then define the A-submodule M'' of M' by

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

where the sum is clearly direct because $w_1, \ldots, w_m$ are even linearly independent over A_T. But $N' = M'/M''$ is a quotient of M with $N'_T = 0$, and so N' is also pseudo-null by Proposition 2.5. Now 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

$$\rho : \bigoplus_{i=1}^{m} A/L'_i \xrightarrow{\sim} \bigoplus_{i=1}^{m} Aw_i = M'' \subset M' = M/N$$

is an injective A-homorphism with pseudo-null cokernel. Let L_i be the unique left ideal such that L_i/L'_i is the maximal pseudo-null submodule of A/L_i. We deduce easily that ρ induces an injection of A-modules

$$\varphi : \bigoplus_{i=1}^{m} A/L_i \longrightarrow M/M_0,$$

where M_0 is the maximal pseudo-null submodule of M, and $\mathrm{Coker}(\varphi)$ is pseudo-null. Thus we have established Theorem 1.1 with $\Lambda(G)$ replaced by our ring A satisfying axioms (C1) and (C2).

PROPOSITION 2.5. — *Let U be any A-subquotient of the A-torsion module M. Then $U_T = 0$ implies that U is pseudo-null. The converse statement holds if A is assumed to be Auslander regular.*

In fact, the notion of a module over an arbitrary ring A with identity element being pseudo-null is defined in [CSS]. We refer the reader to [CSS] for the somewhat delicate proof of Proposition 2.5, as well as a discussion of the notion of Auslander regularity.

The fact that $\Lambda(G)$ satisfies axioms (C1) and (C2) when G is a compact p-valued p-adic Lie group is a consequence of the following result, which is essentially contained in the important but difficult paper of M. Lazard [La]. The explanation given in [CSS] of how to derive this result from Lazard's work was given to us by B. Totaro. The last assertion of Proposition 2.6 is due to O. Venjakob [Ve1], [Ve2].

PROPOSITION 2.6. — *Assume that G is a compact p-adic Lie group, which is p-valued. Then $\Lambda(G)$ possesses a complete, separated and exhaustive filtration $F_\bullet\Lambda(G)$ such that $\mathrm{gr}_\bullet\Lambda(G)$ is isomorphic as a graded ring to the polynomial ring $\mathbb{F}_p[X_0, \ldots, X_d]$ in $d+1$ variables, where d is the dimension of G; here the grading on $\mathbb{F}_p[X_0, \ldots, X_d]$ is given by assigning to each of the variables X_i a strictly negative integer degree. In particular, $\Lambda(G)$ satisfies axioms (C1) and (C2). In addition, $\Lambda(G)$ is Auslander regular.*

3. ARITHMETIC EXAMPLES

Concrete examples of finitely generated torsion $\Lambda(G)$-modules, which are of great arithmetic interest, abound in arithmetic geometry. Because of lack of space, we only discuss two classes of examples. In both cases, G is non-commutative, and is the image of Galois in a 2-dimensional p-adic Galois representation; thus, by Lazard [La], G is automatically p-valued provided G is pro-p and $p \geqslant 5$.

Example 1. — Let $p \geqslant 5$, and let $\mu_{p^n} (1 \leqslant n \leqslant \infty)$ denote the group of all p^n-th roots of unity. We write F for any finite extension of $\mathbb{Q}$ containing μ_p, and define

$$F^{\mathrm{cyc}} = F(\mu_{p^\infty}), \quad \Gamma = G(F^{\mathrm{cyc}}/F).$$

Now fix a non-zero element α of F, which is not a root of unity, and define

$$K_\infty = F^{\mathrm{cyc}}(\alpha^{1/p^n} : n = 1, 2, \ldots), \quad G = G(K_\infty/F).$$

If we define H to be $G(K_\infty/F_{\mathrm{cyc}})$, then both H and Γ are isomorphic to $\mathbb{Z}_p$, so that G is a p-adic Lie group of dimension 2, which is p-valued. Moreover, G is not commutative. Let $\psi : \Gamma \to \mathbb{Z}_p^\times$ bethe character giving the action of Γ on μ_{p^∞}. Then, as α belongs to F, Kummer theory shows that the natural action of Γ on H via inner automorphism is given by the character ψ. One can study many left $\Lambda(G)$-modules

which are of arithmetic interest, but the simplest is probably the following. Let L_∞ denote the maximal unramified abelian p-extension of K_∞, and put $X = G(L_\infty/K_\infty)$. As usual, there is a continuous left action of G on X via inner automorphism (if σ is in G and x in X, we define $\sigma \cdot x = \widetilde{\sigma} x \widetilde{\sigma}^{-1}$, where $\widetilde{\sigma}$ denotes any lifting of σ to the Galois group of L_∞ over F). Y. Ochi [Oc] has proven that X is a finitely generated torsion $\Lambda(G)$-module. At present, very little else is known about the module $\Lambda(G)$; in particular, it seems that at present no example is known in which we can prove that X is not pseudo-null as a $\Lambda(G)$-module. In the special case $F = \mathbb{Q}(\mu_p)$ and $\alpha = p$, one can easily show that $X \neq 0$ if and only if p is an irregular prime. Moreover, in this case, O. Venjakob [Ve3] has shown that if X is pseudo-null, then the p-primary subgroup of the ideal class group of K_∞ is zero.

Example 2. — Let F be a finite extension of $\mathbb{Q}$, and E an elliptic curve defined over F, with $\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$. Let $p \geqslant 5$, and let E_{p^n} $(1 \leqslant n \leqslant \infty)$ denote the group of p^n-division points on E. We define

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

The action of G on E_{p^∞} defines an injection of G into $\mathrm{Aut}(E_{p^\infty}) \xrightarrow{\sim} GL_2(\mathbb{Z}_p)$, and, by a theorem of Serre [Se3], the image of G is open in $GL_2(\mathbb{Z}_p)$. By the Weil pairing, $F^{\mathrm{cyc}} = F(\mu_{p^\infty})$ is contained in F_∞, and we put

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

We shall assume from now on that G is pro-p (this can always be achieved, if necessary, by replacing F by a finite extension, e.g. by $F(E_p)$). Hence Γ is pro-p, and so is isomorphic to $\mathbb{Z}_p$.

For each intermediate field L with $F \subseteq L \subseteq F_\infty$, we recall that the *Selmer group* of E over L is defined by

$$S(E/L) = \mathrm{Ker}(H^1(G(\overline{\mathbb{Q}}/L), E_{p^\infty}) \longrightarrow \prod_v H^1(G(\overline{L_v}/L_v), E(\overline{L_v})),$$

where v runs over all finite places of L, and L_v denotes the union of the completions at v of all finite extensions of F contained in L. As usual, we have the exact sequence

$$0 \longrightarrow E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow S(E/L) \longrightarrow Ш(E/L)(p) \longrightarrow 0,$$

where $Ш(E/L)(p)$ denotes the p-primary subgroup of the Tate-Shafarevich group of E over L. We write

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

for the compact Pontrjagin dual of the discrete p-primary module $S(E/L)$. If L is Galois over F, then the Galois group $G(L/F)$ of L over F has a natural action on both $S(E/L)$ and $X(E/L)$, and it is easily seen that $X(E/L)$ is always a finitely generated $\Lambda(G(E/L))$-module. We shall be primarily interested in the $\Lambda(G)$-module $X(E/F_\infty)$. If E has good ordinary reduction at all places v of F dividing p, old conjectures due

to B. Mazur [Ma] and M. Harris [Ha] affirm, respectively, that $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and $X(E/F_\infty)$ is $\Lambda(G)$-torsion. It is easy to see that the validity of Mazur's conjecture for all finite extensions L of F contained in F_∞ implies the validity of Harris' conjecture for F_∞, but this is of little use in practice since the number of cases in which we can prove Mazur's conjecture remains very limited (the best result to date is K. Kato's [Kat] theorem that $X(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion when E is an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at p, and F is an abelian extension of $\mathbb{Q}$). In [CH], an alternative approach is given which does enable one to give the first proven examples of Harris' conjecture, and to deduce new examples of Mazur's conjecture.

THEOREM 3.1. — *Assume that* (i) $p \geqslant 5$, (ii) G *is pro-p,* (iii) E *has good ordinary reduction at all places* v *of* F *dividing* p, *and* (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, where* $H = G(F_\infty/F^{\mathrm{cyc}})$. *In particular,* $X(E/F_\infty)$ *is a torsion* $\Lambda(G)$*-module.*

Remark 1. — Every $\Lambda(G)$-module, which is finitely generated over $\Lambda(H)$, is automatically $\Lambda(G)$-torsion. This is because $\Lambda(G)$ is not finitely generated over $\Lambda(H)$, since G/H is infinite.

Remark 2. — In the general framework and notation of Theorem 1.1, we say that the $\Lambda(G)$-module M has μ-invariant zero if none of the left ideals $L_1, \ldots, L_m$ appearing in Theorem 1.1 is of the form $\Lambda(G)p^k$ for some integer $k \geqslant 1$. If Γ is a group isomorphic to $\mathbb{Z}_p$, it follows from Theorem 1.1 and the Weierstrass preparation theorem that a $\Lambda(\Gamma)$-module Y is a finitely generated $\mathbb{Z}_p$-module if and only if Y is $\Lambda(\Gamma)$-torsion and has μ-invariant zero. Note also that if M is a finitely generated $\Lambda(H)$-module, then it must have μ-invariant zero, because $\Lambda(G)/\Lambda(G)p^k$ is not a finitely generated $\Lambda(H)$-module when $k \geqslant 1$.

A second important result about $X(E/F_\infty)$ is due to Y. Ochi and O. Venjakob [OV].

THEOREM 3.2. — *Assume that hypotheses* (i), (ii), (ii), *and* (iv) *of Theorem 3.1 are valid. Then* $X(E/F_\infty)$ *contains no non-zero pseudo-null submodule, the* $\Lambda(H)$*-torsion submodule of* $X(E/F_\infty)$ *is zero, and* $X(E/F_\infty)$ *has strictly positive* $\Lambda(H)$*-rank.*

To prove the last assertion of Theorem 3.2, we must use the fact that always $X(E/F_\infty) \neq 0$ (this was first remarked by R. Greenberg, and a proof is given in the Appendix of [CH]). Assume now that E over F satisfies hypotheses (i), (ii), (ii), and (iv) of Theorem 3.1. We conclude from the above results and Theorem 1.1 that there exist non-zero left ideals $L_1, \ldots, L_m$ of $\Lambda(G)$ such that we have an exact sequence of $\Lambda(G)$-modules

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

where D is pseudo-null. We stress that there is great arithmetic interest in studying the left ideals $L_1, \ldots, L_m$, even in particular numerical examples. Of course, one imagines that these left ideals must be related to 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 which factor through finite quotients of G). On a much more elementary level, one can ask whether or not $\mathrm{ann}_{\Lambda(G)}(X(E/F_\infty)) \neq 0$. This still has not been settled in a single numerical example when $F_\infty = F(E_{p^\infty})$. Surprisingly, when K_∞ and G are as defined in Example 1 above, Hachimori and Venjakob [HV] have recently given many examples of elliptic curves E over K_∞ such that the dual of the Selmer group of E over K_∞ is a finitely generated torsion $\Lambda(G)$-module, which is not pseudo-null, but which is completely faithful. For example, they prove that this is the case for the elliptic curve $E = X_1(11)$ given below, when $p = 5$, and K_∞ is the field obtained by adjoining to $\mathbb{Q}$ all 5-power roots of unity and all 5-power roots of 11.

We end by discussing two specific numerical examples of elliptic curves over their field of p-power division points.

Numerical example 1. — I am grateful to T. Fisher for first pointing out this example to me. Let E be the elliptic curve over $\mathbb{Q}$

$$E : y^2 + xy = x^3 - x - 1.$$

This is the curve $B1$ of conductor 294 in [Cr1]. Take $F = \mathbb{Q}(\mu_7)$ and $p = 7$. Although E has bad reduction at 7 over $\mathbb{Q}$, it is easily seen that E has good ordinary reduction at the unique prime of F above 7. Moreover, μ_7 is a Galois submodule of E_7, whence we see easily that $F_\infty = \mathbb{Q}(E_{7^\infty})$ is a pro-7 extension of F. Fisher [Fi1] has shown that $S(E/F) = 0$. One can then use arguments from Iwasawa theory ([CS], p. 83) to deduce that we also have $S(E/F^{\mathrm{cyc}}) = 0$. Hence hypotheses (i), (ii), (iii), and (iv) of Theorem 3.1 are valid for E over F and $p = 7$. We conclude that $X(E/F_\infty)$ is a torsion $\Lambda(G)$-module, with μ-invariant equal to zero, and with no non-zero pseudo-null submodule. Moreover, $X(E/F_\infty)$ is finitely generated over $\Lambda(H)$, its $\Lambda(H)$-torsion submodule is zero, and it has positive $\Lambda(H)$-rank. Here $G = G(\mathbb{Q}(E_{7^\infty})/\mathbb{Q}(\mu_7))$ and $H = G(\mathbb{Q}(E_{7^\infty}/\mathbb{Q}(\mu_{7^\infty})))$.

Numerical example 2. — Let E be the elliptic curve $X_1(11)$ over $\mathbb{Q}$, namely

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

Then E has good ordinary reduction at 5. Take $F = \mathbb{Q}(\mu_5)$ and $p = 5$. As $(0, 0)$ is a rational point of order 5 on E, $F_\infty = \mathbb{Q}(E_{5^\infty})$ is a pro-5 extension of F. Indeed, it is well known and easy to see that the image of G in $\mathrm{Aut}(E_{5^\infty})$ can be identified with the subgroup of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $GL_2(\mathbb{Z}_5)$ with $a \equiv d \equiv 1 \mod 5$, and $c \equiv 0 \mod 5^2$, 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. Finally, it is well known that, in this

case, $S(E/F^{\mathrm{cyc}}) = 0$ (see [CS], Chap. 5). Hence hypotheses (i), (ii), (iii), and (iv) of Theorem 3.1 hold for E over F, and we conclude that $X(E/F_\infty)$ is a torsion $\Lambda(G)$-module, with μ-invariant equal to zero, and with no non-zero pseudo-null submodule. In fact, the following stronger result is true.

PROPOSITION 3.3. — *Take $E = X_1(11)$, $p = 5$, $F = \mathbb{Q}(\mu_5)$ and $H = G(F_\infty/\mathbb{Q}(\mu_{5^\infty}))$. Then $X(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module of rank 4, its $\Lambda(H)$-torsion submodule is zero, but it is not a free $\Lambda(H)$-module.*

For each finite Galois extension L of F which is contained in F_∞, we write

$$G_L = G(F_\infty/L), \quad H_L = G(F_\infty/L^{\mathrm{cyc}}),$$

so that G_L ranges over the open normal subgroups of G, and H_L ranges over the open normal subgroups of H. The proof of Proposition 3.3 hinges on the remarkable fact that one can use ideas of Y. Hachimori and K. Matsuno [HM] to determine the exact $\mathbb{Z}_5$-rank of the H_L-coinvariants of $X(E/F_\infty)$ for every finite Galois extension L of F contained in F_∞. In particular, the following result is proven in § 7 of [CH].

PROPOSITION 3.4. — *For each finite Galois extension L of F contained in F_∞, $X(E/L^{\mathrm{cyc}})$ is a free $\mathbb{Z}_5$-module of rank 4. $[L^{\mathrm{cyc}} : F^{\mathrm{cyc}}] - \tau_L$, where τ_L denotes the number of prime of L^{cyc} above 11. In particular, Mazur's conjecture is true for E over L^{cyc}, and $E(L^{\mathrm{cyc}})$ is a finitely generated abelian group of rank at most $4 \cdot [L^{\mathrm{cyc}} : F^{\mathrm{cyc}}] - \tau_L$.*

One deduces easily from this proposition that $X(E/F_\infty)_{H_L}$ has $\mathbb{Z}_5$-rank equal to $4 \cdot [L^{\mathrm{cyc}} : F^{\mathrm{cyc}}]$ for all L. At the same time, one shows that the $\mathbb{Z}_5$-torsion subgroup of $X(E/F_\infty)_{H_L}$ is never zero, which shows that $X(E/F_\infty)$ is not a free $\Lambda(H)$-module.

By contrast, it is a deep arithmetic problem to determine the exact $\mathbb{Z}_5$-rank of the G_L-coinvariants of $X(E/F_\infty)$ for all L. In particular, the following lemma is not difficult to prove using the methods of [CH].

LEMMA 3.5. — *Let L be any finite Galois extension of F contained in F_∞. Then $X(E/F_\infty)_{G_L}$ is finite if and only if both $E(L)$ and the 5-primary subgroup of the Tate-Shafarevich group of E over L are finite.*

We have already used the classical fact that $X(E/F_\infty)_G$ is finite. By some remarkable explicit descent calculations, T. Fisher [Fi2] has recently shown that $X(E/F_\infty)_{G_L}$ is finite for L ranging over the following three cyclic extensions of F of degree 5 which are contained in F_∞:

$$L_1 = \mathbb{Q}(X_1(11)_5), \quad L_2 = \mathbb{Q}(X_2(11)_5), \quad L_3 = FQ(\mu_{11})^+;$$

here $X_2(11)$ denotes the unique elliptic curve of conductor 11 over $\mathbb{Q}$ which has no non-zero rational point, and $\mathbb{Q}(\mu_{11})^+$ denotes the maximal real subfield of $\mathbb{Q}(\mu_{11})$. The field L_1 is the splitting field of the polynomial

$$x^5 + 2x^4 + 6x^3 - 2x^2 + 4x - 1.$$

Then T. Fisher's descent calculations [Fi2] show that $E(L_1)$ is finite, and

$$Ш(E/L_1)(5) = (\mathbb{Z}/5\mathbb{Z})^2.$$

However, it does not seem possible to extend his explicit calculations even to the field $K_2 = L_1(\mu_{5^2})$, which has degree 100 over $\mathbb{Q}$. Nevertheless, if

$$K_n = L_1(\mu_{5^{n+1}}) \qquad (n = 0, 1, \ldots),$$

T. Fisher, R. Greenberg and myself have shown that simple theoretical arguments from the Iwasawa theory of elliptic curves do enable one to prove that, for all integers $n = 0, 1, \ldots, E(K_n)$ is finite and $Ш(E/K_n)(5)$ is finite of order 5^{16n+2}.

When this exposé was given in November 2001, I naively imagined that perhaps $X_1(11)$ had no points of infinite order in the whole tower F_∞ of 5-division points. I am very grateful to K. Matsuno (unpublished) for producing overwhelming numerical evidence that this is not true. Take the field L_3 above, and let $H_2 = L_3(\mu_{5^2})$, so that H_2 is an abelian extension of $\mathbb{Q}$ of degree 100. K. Matsuno calculated the complex L-function of $X_1(11)$ over H_2, and proved that it has a zero at $s = 1$ of order 4. Thus, unless the conjecture of Birch and Swinnerton-Dyer is false (which I do not for one moment believe), $X_1(11)$ should have rank 4 over H_2. So far, no point of infinite order has been found, nor has Fisher been able to extend his explicit descent calculations to $X_1(11)$ over H_2. Thus, in conclusion, two important questions remain unanswered about the arithmetic of $X_1(11)$ over its field F_∞ of 5-power division points. Is the dual of the Selmer group of $X_1(11)$ over F_∞ a completely faithful $\Lambda(G)$-module? What is the $\mathbb{Z}$-rank of the group $X_1(11)(F_\infty)$ of F_∞-rational points modulo its torsion subgroup?

REFERENCES

[As] K. ASANO – Zur Arithmetik in Schiefringen, *Osaka J. Math.* **2** (1949), p. 98–134.

[Bj] J.-E. BJÖRK – Filtered Noetherian Rings, in *Noetherian rings and their applications*, Math. Survey Monographs, vol. 24, AMS, 1987, p. 59–97.

[B-CA] N. BOURBAKI – *Algèbre Commutative*, Paris, Hermann, 1972.

[Ch1] M. CHAMARIE – Anneaux de Krull non commutatifs, *J. Algebra* **72** (1981), p. 210–222.

[Ch2] ———, Modules sur les anneaux de Krull non commutatifs, in *Sém. d'Algèbre P. Dubreil et M.-P. Malliavin 1982*, Springer Lecture Notes, vol. 1029, Springer, 1983, p. 283–310.

[CH] J. COATES & S. HOWSON – Euler characteristics and elliptic curves II, *J. Math. Soc. Japan* **53** (2001), p. 175–235.

[CSS] J. COATES, P. SCHNEIDER & R. SUJATHA – Modules over Iwasawa algebras, *J. Inst. Math. Jussieu* **2** (2003), p. 73–108.

[CS] J. COATES & R. SUJATHA – *Galois cohomology of elliptic curves*, Lecture Notes, vol. 88, TIFR-AMS, 2000.

[Cr1] J. CREMONA – *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997.

[Fi1] T. FISHER – On 5 and 7 descents for elliptic curves, Ph.D. Thesis, Cambridge University, 2000.

[Fi2] ———, Descent calculations for the elliptic curves of conductor 11, *Proc. London Math. Soc.* **86** (2003), p. 583–606.

[HM] Y. HACHIMORI & K. MATSUNO – An analogue of Kida's formula for the Selmer groups of elliptic curves, *J. Alg. Geometry* **8** (1999), p. 581–601.

[HV] Y. HACHIMORI & O. VENJAKOB – Completely faithful Selmer groups over Kummer extensions, to appear.

[Ha] M. HARRIS – p-adic representations arising from descent on abelian varieties, *Compositio Math.* **30** (1979), p. 177–245.

[Ho] S. HOWSON – Structure of central torsion Iwasawa modules, *Bull. Soc. math. France* **130** (2002), no. 4, p. 507–535.

[Iw] K. IWASAWA – On Γ-extensions of number fields, *Bull. AMS* **65** (1959), p. 183–226.

[Ja] H. JACOBSON – *Theory of rings*, Math. Surveys, vol. 2, AMS, Providence, 1943.

[Ka] M. KASHIWARA – Algebraic study of systems of partial differential equations, Master thesis, Tokyo University, 1971, English translation in Mem. Soc. math. France (N.S.), vol. 63 (1995).

[Kat] K. KATO – p-adic Hodge theory and values of zeta functions of modular forms, to appear.

[La] M. LAZARD – Groupes analytiques p-adiques, *Publ. Math. IHÉS* **26** (1965), p. 380–603.

[Li] LI HUISHI – Lifting Ore sets of Noetherian filtered rings and applications, *J. Algebra* **179** (1996), p. 686–703.

[LO] LI HUISHI & F. VAN OYSTAEYEN – *Zariskian Filtrations*, Kluwer, Dordrecht, 1996.

[Ma] B. MAZUR – Rational points of abelian varieties in towers of number fields, *Invent. Math.* **18** (1992), p. 183–266.

[Oc] O. OCHI – Iwasawa modules via homotopy theory, Ph.D. Thesis, Cambridge University, 1999.

[OV] Y. OCHI & O. VENJAKOB – On the structure of Selmer groups over p-adic Lie extensions, *J. Alg. Geom* **11** (2002), p. 547–576.

[Ro] J.C. ROBSON – Cyclic and faithful objects in quotient categories with applications to Noetherian simple or Asano rings, in *Noncommutative Ring Theory*, Springer Lecture Notes, vol. 545, Springer, 1976, p. 151–172.

[Se2] J.-P. SERRE – Letter to K. Iwasawa, dated August 27th 1958.

[Se3] ———, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), p. 259–331.

[Se1] ———, Classes des corps cyclotomiques (d'après K. Iwasawa), in *Sém. Bourbaki*, Collection hors série, vol. 5, Société mathématique de France, 1995, exp. n° 174, décembre 1958, p. 83–93.

[Ve1] O. VENJAKOB – Iwasawa Theory of p-adic Lie Extensions, Thesis, Heidelberg University, 2000.

[Ve2] ———, On the structure of the Iwasawa algebra of a p-adic Lie group, *J. European Math. Soc* **4** (2002), p. 271–311.

[Ve3] ———, A non-commutative Weierstrass preparation theorem and its applications to Iwasawa theory, *J. reine angew. Math.* **559** (2003), p. 153–191.

[WK] E. WEXLER-KREINDLER – Microlocalisation, platitude et théorie de torsion, *Comm. Algebra* **16** (1988), p. 1813–1852.

John COATES

Cambridge University
DPMMS
Wilberforce Road
GB-Cambridge, CB3 0WB
U.K.
E-mail : J.H.Coates@dpmms.cam.ac.uk