Bull. Soc. math. France
130 (4), 2002, p. 507–535

STRUCTURE OF CENTRAL TORSION IWASAWA MODULES

BY SUSAN HOWSON

ABSTRACT. — We describe an approach to determining, up to pseudoisomorphism, the structure of a central-torsion module over the Iwasawa algebra of a pro-p, p-adic, Lie group containing no element of order p. The techniques employed follow classical methods used in the commutative case, but using Ore's method of localisation. We then consider the properties of certain invariants which may prove useful in determining the structure of a module. Finally, we describe the case of pro-p subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$ in detail and give a brief example from the theory of elliptic curves.

RÉSUMÉ (*Les structures des modules de torsion sur le centre d'une algèbre d'Iwasawa*)
Nous décrivons une méthode pour déterminer, à pseudo-isomorphisme près, la structure d'un module de torsion sur le centre d'une algèbre d'Iwasawa d'un pro-p groupe de Lie p-adique ne contenant pas d'élément d'ordre p. La méthode est semblable à celle utilisée dans le cas commutatif grâce au procédé de localisation de Ore. Nous étudions ensuite les propriétés de certains invariants qui peuvent être utiles pour déterminer la structure d'un tel module. Enfin nous traitons en détail le cas d'un pro-p sous-groupe de $\mathrm{GL}_2(\mathbb{Z}_p)$ et nous donnons un exemple d'application à la théorie des courbes elliptiques.

Texte reçu le 4 avril 2001, accepté le 7 novembre 2001

SUSAN HOWSON, School of Mathematical Sciences, University of Nottingham, University Park, Nottingham, NG7 2RD (U.K.) • *E-mail :* `sh@maths.nott.ac.uk`

2000 Mathematics Subject Classification. — 11R23, 16P50.

Key words and phrases. — Iwasawa Theory, Euler characteristics, Iwasawa Modules, Structure Theory.

Completed while the author was visiting Université de Paris 13, funded by a postdoctoral grant from an EU TMR network. The author thanks Paris 13, and Jacques Tilouine and Daniel Barsky in particular, for their hospitality.

Introduction

Let G be a pro-p, p-adic, compact Lie group, containing no element of order p. We are interested in the structure of modules finitely generated over its Iwasawa algebra, $\Lambda(G)$, defined by

$$\Lambda(G) := \varprojlim_{H \triangleleft_o G} \mathbb{Z}_p[G/H] \tag{1}$$

We describe a structure theorem for the ξ-torsion submodule of M, where ξ is an element of $\Lambda(G)$ which is

(i) a prime of Λ, and

(ii) lies in the centre of Λ.

The set of elements of M which are annihilated by some power of ξ will be denoted by $M(\xi)$. Because ξ is central, this does form a $\Lambda(G)$-submodule. Note that since Λ is Noetherian, and ξ is central, $M(\xi)$ is finitely generated over Λ and there exists some integer $n \geqslant 0$ such that $\xi^n M(\xi) = 0$. The main technique used is the Ore method of localisation.

In the case G is uniform, this applies to $\xi = p$. This is because $\Lambda(G)/p$, which is the $\mathbb{F}_p$-linear completed group algebra $\mathbb{F}_p[[G]]$, is known to contain no zero divisors in this case, see the second edition of [10, chap. 12]. (By convention, *zero itself is not considered a zero divisor.*)

We then glue this together, for the set of all such ξ, and discuss some properties. We consider certain invariants of Λ-torsion Iwasawa modules which we have called *generalised Euler Characteristics.* These may help in explicitly determining structures. In particular, in Section 3 we generalise results from an earlier paper [13] which considered invariants for the case $\xi = p$ in some detail.

In the final section we consider in more detail the case of pro-p open subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$, determining the centre and central primes. We conclude by giving an application to the study of the structure of the Selmer group of an elliptic curve, taking further an example already studied in [5], [7] and [13].

Since this paper has been written with applications to Number Theory in mind, in particular to Iwasawa Theory, rather more details of standard results in the theory of noncommutative Noetherian rings have been given than might otherwise have been the case. For convenience, most references for such standard material are to the book of McConnell and Robson [15]. For standard results on the structure of the classical Iwasawa algebra we refer to the book of Neukirch, Schmidt and Wingberg [16].

Notation. — Throughout the remainder, G represents a pro-p, p-adic, Lie group, whose dimension as a p-adic manifold is finite, equal to d. Excepting the final section, G remains fixed and we will omit it from the notation, writing simply Λ for $\Lambda(G)$. We use always ξ to denote a central prime, by which we mean a prime element of Λ which lies in the centre of Λ.

Acknowledgements. — We note that in [23] Otmar Venjakob has used a different approach to structure theorems of the sort contained in this paper, to prove a slightly weaker version of our Theorem 2.5 in the case of $\xi = p$ and when the module is annihilated by a power of p, see [23]. John Coates, Peter Schneider and R. Sujatha have also recently developed a structure theory along similar lines to that considered in § 2 of this paper. Their results hold more generally than Theorem 2.5 as they apply to *all* torsion modules over the Iwasawa algebra of an extra powerful pro-p, p-adic Lie group (a slightly stronger restriction on the group than the results in the present paper.) They do not, however, obtain uniqueness of the structures, and can not give explicit pseudoisomorphisms in the category of finitely generated Λ-modules. Their structures are determined in the quotient category, of torsion Λ-modules quotiented by the subcategory of pseudonull submodules. See § 1.2 for the definition of pseudonull, following the work of Venjakob, in this case. Finally, I wish to thank Ralph Greenberg and Chris Brookes for helpful conversations concerning the explicit determination of the centre of the Iwasawa algebra of a pro-p, open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ given in § 4 and Ken Brown for pointing out an error in an earlier version of this paper.

1. Background Algebra

1.1. Properties of Localisations. — We start by quoting some elementary properties of Λ which are essential for the remainder.

Recall that the (*left/right*) *projective dimension* of a (left/right) Λ-module is the least integer n such that it has a projective resolution of length n. The *global dimension* of Λ is the supremum of the projective dimensions of all Λ-modules. We do not need to specify whether left or right global dimension since for Noetherian rings the supremum over left modules and over right modules coincide. That Λ is Noetherian is proven in [10]. Brumer has shown in [4] that Λ has finite global dimension equal to $d+1$. Both these last two properties do not require that G be pro-p, only that it be p-adic analytic with, for the finite global dimension property, no element of order p. This last condition is needed to ensure G has finite cohomological dimension, equal to d, [20]. Also, if G is pro-p but possibly containing an element of order p, then Λ is a local ring, with unique maximal ideal given by the kernel of the canonical map

$$\Lambda \xrightarrow{\varepsilon} \mathbb{Z}_p \longrightarrow \mathbb{F}_p, \tag{2}$$

where the first map is the augmentation map, sending every element of G to 1. We denote the maximal ideal of Λ by $\mathfrak{M}$. If we insist that G contain no element of any finite order (other than the identity) then Neumann has proven in [17] that Λ contains no zero divisors.

Throughout this section we fix a choice of central prime, ξ. For ξ in the centre of Λ, λ any element of Λ, the statement ξ divides λ is unambiguous, and means $\lambda = \xi a = a\xi$, for some a in Λ. We do not need to specify whether ξ is a right or left divisor. To consider modules in this non commutative situation we must be careful to distinguish between left and right actions. We will make an arbitrary choice, thus, except where specified otherwise, all ideals and Λ-modules are left ideals and modules. The entire theory is symmetrical.

LEMMA 1.1. — *If ξ is a central prime in Λ then every element of Λ can be uniquely written as $a\xi^r$ for some finite integer $r \geqslant 0$, and some a in Λ such that ξ does not divide a.*

Proof. — The definition of prime requires that ξ is not a unit, thus ξ is an element of the maximal ideal, $\mathfrak{M}$, of Λ. The $\mathfrak{M}^n$ form a base of neighbourhoods of zero in Λ, and so $\bigcap_{n\geqslant 0} \mathfrak{M}^n = \{0\}$. Let λ be a non zero element of Λ. Since ξ is an element of $\mathfrak{M}$, there exists some n such that λ is contained in $\mathfrak{M}^{n-1}$ and not contained in $\mathfrak{M}^n$. Then the maximal power of ξ which can divide λ is bounded by $n-1$.

We can certainly write $\lambda = \xi^r a$, such that ξ does not divide a. Suppose we can do this in two ways:

$$\xi^r a = \xi^s b. \tag{3}$$

We may assume that r is less than or equal to s. Then

$$\xi^r(a - \xi^{s-r}b) = 0. \tag{4}$$

Since Λ contains no zero divisors, we must have $a = \xi^{s-r}b$, and so $a = b$ and $r = s$. □

DEFINITION. — Let R be a ring, S any subset of R. We say that S satisfies the *Ore Condition* if for any element a in R and any element b in the subset S both the following conditions are satisfied:

(i) there exists a_1 in R and b_1 in S such that

$$b_1 a = a_1 b \tag{5}$$

(ii) there exists a_2 in R and b_2 in S such that

$$ab_2 = ba_2 \tag{6}$$

(The first condition is known as the *left* Ore condition, the second the *right* Ore condition.)

LEMMA 1.2. — *If we take the subset S to be the set of elements of Λ which are not contained in $\xi\Lambda$, in other words the set of elements not divisible by ξ, then S satisfies the Ore condition above.*

Proof. — We consider only the first condition, the proof of the second is entirely symmetrical. Let a be any element of Λ and b an element of S. If a equals zero then we may take any b_1, with a_1 also equal to zero. Thus we assume a is non zero. Since Λ is both left and right Noetherian, and contains no zero divisors, it is known that the set of non zero elements in Λ satisfies the Ore condition, [15]. Thus we may write

$$b'a = a'b \tag{7}$$

for some non zero element b' in Λ. By Lemma 1.1, we can write $b' = \xi^m b_1$, for some b_1 contained in S. Thus (7) becomes $\xi^m b_1 a = a'b$. Since ξ is central and prime, and by the assumption that b is not divisible by ξ, this implies that

$$a' = \xi^m a_1, \quad \text{and so} \quad \xi^m b_1 a = \xi^m a_1 b, \tag{8}$$

for some a_1 contained in Λ. Since Λ contains no zero divisors, we may cancel ξ^m, giving

$$b_1 a = a_1 b \tag{9}$$

where b_1 is an element of S as required in the Ore condition, (i). □

Definition. — Let S be a multiplicatively closed subset of Λ, A *left localisation* of Λ at S is a ring Λ_S together with a homomorphism $\theta : \Lambda \to \Lambda_S$, such that

(i) $\theta(s)$ is a unit in Λ_S for all s in S,

(ii) all q in Λ_S can be written $q = \theta(s)^{-1}\theta(\lambda)$ for some s in S, λ in Λ and

(iii) $\mathrm{Ker}(\theta) = \{\lambda \in \Lambda \mid \lambda s = 0 \text{ for some } s \text{ in } S\}$.

One can similarly define a right localisation.

Since the ring, Λ, which interests us contains no zero divisors, condition (iii) becomes the statement 'θ is an injection'.

Theorem 1.3 (See [15, § 2.1.12]). — *If S is a multiplicatively closed subset of Λ then the left localisation Λ_S exists if S satisfies the left Ore condition. Similarly, a right localisation exists if S satisfies the right Ore condition. If a localisation exists then it is unique up to canonical isomorphism. In particular, if both the left and right localisations exist then they are isomorphic.*

Thus in the case of interest here it will not be necessary to distinguish between a left or right localisation of Λ.

For the remainder of this section we fix S to be the set $\Lambda\backslash\xi\Lambda$. It is multiplicatively closed by the assumption that ξ is prime. Many of the general properties of localisation discussed hold for localisation with respect to any suitable set S, and the general statements are given in [15]. We have restricted to $S = \Lambda\backslash\xi\Lambda$ for ease of exposition.

Definition. — We will use the notation $\Lambda_{(\xi)}$ for the localisation of Λ at S, where S is taken to be the set of elements of Λ not contained in the ideal $\Lambda\xi$.