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

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 $\Lambda\xi$.

LEMMA 1.4. — *The localisation $\Lambda_{(\xi)}$ is a Noetherian local ring, with a unique prime ideal, generated by the image of ξ in $\Lambda_{(\xi)}$. It contains no zero divisors. The ideal $\xi\Lambda$ of Λ is a height one prime ideal.*

As in the commutative case, ideals and left and right ideals of $\Lambda_{(\xi)}$ correspond bijectively respectively with ideals or left or right ideals of Λ which contain no element of S. Similarly for prime ideals. See [15, § 2.1.16] for further details.

DEFINITION. — We define the left localisation of a left Λ-module M at ξ by $\Lambda_{(\xi)} \otimes_\Lambda M$, where $\Lambda_{(\xi)}$ is considered as a $\Lambda_{(\xi)}$-Λ bimodule. Similarly, the right localisation of a right Λ-module is given by $M \otimes_\Lambda \Lambda_{(\xi)}$. We use the notation $M_{(\xi)}$ for both.

There is a canonical Λ-module homomorphism

$$\iota : M \longrightarrow M_{(\xi)}, \quad m \longmapsto (1, m). \tag{10}$$

LEMMA 1.5. — (i) *The kernel of ι consists of the set of elements of M which are annihilated by some t not divisible by ξ (see* [15, § 2.1.17]*).*

(ii) *For any Λ-module, M, and any finite set of elements $\{a_i^{-1} \otimes m_i\}_{i=1}^n$, we can clear denominators. That is, there exists an element a, in Λ but not divisible by ξ, such that the same set of elements can be written $\{a^{-1} \otimes n_i\}_i$ for some set $\{n_i\}_i$ of elements of M. In particular, any element of $\Lambda_{(\xi)} \otimes_\Lambda M$ can be represented by $a^{-1} \otimes m$ for some m in M and some a in Λ which is not divisible by ξ (see* [15, § 2.1.16]*).*

(iii) *The localisation functor from Λ-modules to $\Lambda_{(\xi)}$-modules is flat (see* [15, § 2.1.16]*).*

COROLLARY 1.6. — *For any Λ-module N*

$$\operatorname{Tor}_i^\Lambda(\Lambda_{(\xi)}, N) = 0, \quad \textit{when } i \geqslant 1.$$

This localisation gives a functor from the category of Λ-modules to the category of $\Lambda_{(\xi)}$-modules. It is given on homomorphisms by

$$f : M \longrightarrow N \text{ induces } \tilde{f} : M_{(\xi)} \to N_{(\xi)}, \ \ a^{-1} \otimes m \mapsto a^{-1} \otimes f(m). \tag{11}$$

Because the original map f is a Λ-module homomorphism, this gives a well defined $\Lambda_{(\xi)}$-module homomorphism. Throughout the remainder, whenever we refer to a homomorphism between the localisation of two modules induced from a homomorphism between the original two modules, we mean via this construction.

1.2. Dimension of Modules. — Recall that if the dimension of G as a p-adic manifold is d, then Λ has global dimension equal to $d+1$. In [1] Björk has described a filtration on M which allows one to define a notion of the dimension of a module.

THEOREM 1.7 (Björk). — *There is a convergent spectral sequence*

$$E_2^{p,q} = \mathrm{Ext}^p_\Lambda\big(\mathrm{Ext}^{-q}_\Lambda(M,\Lambda),\Lambda\big) \Longrightarrow H^{p+q}\big(\Delta^\bullet(M)\big), \tag{12}$$

where $\Delta^\bullet(M)$ is a chain complex which is exact in all degrees except 0, whilst $H^0(\Delta^\bullet(M))$ equals M. Here $\mathrm{Ext}^i_\Lambda(-,\Lambda)$ is interpreted to be zero when i is strictly less than zero.

Thus the $E_\infty^{p,q}$ terms give a canonical filtration of M by Λ-submodules:

$$0 \subseteq T_0(M) \subseteq T_1(M) \subseteq \cdots \subseteq T_{d+1}(M) = M. \tag{13}$$

DEFINITION. — The value $\min\{i \mid T_i(M) = M\}$ is called the *dimension* of M, denoted $\delta(M)$.

In [23], Venjakob has pointed out that this gives a suitable definition of a module being pseudonull in this setting:

DEFINITION. — A module M is called *pseudonull* if it has codimension at least two, that is M has dimension at most two less than $d+1$, the dimension of Λ. A Λ-module homomorphism $f: M \to N$ is called a *pseudoisomorphism* when both $\mathrm{Ker}(F)$ and $\mathrm{Coker}(F)$ are pseudonull.

Thus M being pseudonull is equivalent to the statement $T_{d-1}(M) = M$.

In order for this definition to be convenient to work with one has to prove Λ satisfies a certain algebraic condition (the so-called Auslander condition – it can be interpreted as a non-Abelian generalisation of the notion of being regular) concerning the behaviour of the $\mathrm{Ext}^i_\Lambda(-,\Lambda)$ groups of Λ-modules. The precise nature of this condition need not concern us, we only need certain consequences. Venjakob [23] has shown this condition holds for the Iwasawa algebra of a p-adic, Lie group. In [1], Björk shows that when this condition holds the filtration by $T_i(M)$ satisfies the following properties:

Properties of the filtration of M by $T_i(M)$

(i) If $0 \to M' \to M \to M'' \longrightarrow 0$ is a short exact sequence of Λ-modules then $\delta(M')$ and $\delta(M'')$ are both less than or equal to $\delta(M)$.

(ii) For each i the quotient $T_{i+1}(M)/T_i(M)$ equals zero if and only if $\mathrm{Ext}^{d-i}_\Lambda(\mathrm{Ext}^{d-i}_\Lambda(M,\Lambda),\Lambda)$ vanishes also.

(iii) If we denote by $j(M)$ the minimal i such that $\mathrm{Ext}^i_\Lambda(M,\Lambda)$ is non zero then $\delta(M) + j(M)$ equals $d+1$, the global dimension of Λ.

Note, the first property holds more generally, without assuming the Auslander condition. For a list of other properties, and for proofs, see [1] and [23].

Proposition 1.8. — *Assume that $M(\xi) = M$, that is, every element of M is annihilated by some power of ξ. Then the following are equivalent:*

(i) $M_{(\xi)} = 0$,

(ii) *M is pseudonull.*

Proof. — Recall, [24, § 5.6], that if $f : R \to S$ is a homomorphism of rings then there is a first quadrant cohomological spectral sequence,

$$E_2^{p\,q} = \operatorname{Ext}^p_S\big(A, \operatorname{Ext}^q_R(S, B)\big) \Longrightarrow \operatorname{Ext}^{p+q}_R(A, B), \tag{14}$$

where B is an R-module, A an S-module and S is given the structure of an R-module via f. We apply this with $R = \Lambda$. For convenience we use the notation Ω for the ring $\Lambda/\xi\Lambda$, and take S to be Ω treated as a Λ-Ω bimodule via f the canonical projection.

We begin by assuming the power of ξ which annihilates M is actually one, and will complete by induction. We need the following elementary observations.

Lemma 1.9. — (i) *One has*

$$\operatorname{Ext}^p_\Lambda(\operatorname{Ext}^{-q}_\Lambda(N, \Lambda), \Lambda) = \begin{cases} 0 & \textit{if } \ p \leqslant 0 \ \textit{or } q \geqslant 0, \\ \operatorname{Ext}^{p-1}_\Omega(\operatorname{Ext}^{-q-1}_\Omega(N, \Omega), \Omega) & \textit{otherwise.} \end{cases} \tag{15}$$

(ii) *The right Ω-module $\operatorname{Hom}_\Omega(N, \Omega)$ is zero if and only if N is torsion as an Ω-module. If it is non zero then it is Ω-torsion free.*

Proof of (i). — Taking the long exact sequence of $\operatorname{Ext}^i_\Lambda(-, \Lambda)$ groups of the short exact sequence of Λ-modules

$$0 \to \Lambda \xrightarrow{\times \xi} \Lambda \longrightarrow \Omega \to 0, \tag{16}$$

we obtain

$$\operatorname{Ext}^i_\Lambda(\Omega, \Lambda) = \begin{cases} \Omega & i = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{17}$$

Substituting this into the spectral sequence (14), with B taken to be Λ and A taken to be N, the spectral sequence degenerates and gives

$$\operatorname{Ext}^p_\Lambda(N, \Lambda) = \begin{cases} 0 & p \leqslant 0, \\ \operatorname{Ext}^{p-1}_\Omega(N, \Omega) & p \geqslant 1. \end{cases} \tag{18}$$

Since each $\operatorname{Ext}^{p-1}_\Omega(N, \Omega)$ is also an Ω-module, we can apply this again, giving the formula in the lemma.

(ii) That N being Ω-torsion implies $\operatorname{Hom}_\Omega(N, \Omega)$ is zero is immediate, as Ω contains no zero divisors. Conversely, suppose that N is not torsion. Since Ω is Noetherian (it is a quotient of the Noetherian ring Λ) it satisfies the Ore condition and so the subset of N consisting of the Ω-torsion elements and zero is actually an Ω-submodule.

We have

$$\mathrm{Hom}_{\Omega}(N,\Omega) = \mathrm{Hom}_{\Omega}(N/N_{\mathrm{tor}},\Omega). \tag{19}$$

Since Ω is itself torsion free, it is clear that $\mathrm{Hom}_{\Omega}(N/N_{\mathrm{tor}},\Omega)$ is torsion free, completing the proof of Lemma 1.9. □

We can now easily prove Proposition 1.8 when M is annihilated by ξ. First, since M is Λ-torsion it follows that $\mathrm{Ext}^0_{\Lambda}(M,\Lambda)$, and hence also $\mathrm{Ext}^0_{\Lambda}(\mathrm{Ext}^0_{\Lambda}(M,\Lambda),\Lambda)$, vanishes. By Lemma 1.5, the assumption that $M_{(\xi)}$ vanishes is equivalent to M being torsion as an Ω-module.

($\Rightarrow$) By the above Lemma 1.9, the double Ext group, $\mathrm{Ext}^1_{\Lambda}(\mathrm{Ext}^1_{\Lambda}(M,\Lambda),\Lambda)$, vanishes. Thus, from the second of the above properties of the filtration of M by the submodules $T_i(M)$, we must have that $T_{d-1}(M)$ already equals M. In other words, M is pseudonull.

($\Leftarrow$) Suppose M is not Ω-torsion. By (i) of Lemma 1.9

$$\mathrm{Ext}^1_{\Lambda}\big(\mathrm{Ext}^1_{\Lambda}(M,\Lambda),\Lambda\big) = \mathrm{Hom}_{\Omega}\big(\mathrm{Hom}_{\Omega}(M,\Omega),\Omega\big),$$

and this is non zero by (ii) of the above lemma. Thus, again by the second property of the filtration of M by the $T_i(M)$, it follows that $T_d(M)/T_{d-1}(M)$ is non zero, and in particular $T_{d-1}(M)$ is strictly smaller than M, which is therefore not pseudonull.

Note that the above proof actually demonstrates that if M is an Ω-module then $M_{(\xi)}$ vanishes if and only if $\mathrm{Ext}^i_{\Lambda}(M,\Lambda)$ vanishes for i equal to both 1 and 2. We need this slightly stronger condition to continue the induction.

Proceeding by induction, we consider the short exact sequence

$$0 \to \xi M \longrightarrow M \longrightarrow M/\xi M \to 0. \tag{20}$$

By Lemma 1.5 part (iii) the module $M_{(\xi)}$ vanishes if and only if $(\xi M)_{(\xi)}$ and $(M/\xi M)_{(\xi)}$ both vanish.

($\Rightarrow$) Suppose this is the case. Then by induction $\mathrm{Ext}^1_{\Lambda}(\xi M,\Lambda)$ and $\mathrm{Ext}^1_{\Lambda}(m/\xi M,\Lambda)$ both vanish. Thus, by the long exact sequence of $\mathrm{Ext}^1_{\Lambda}(-,\Lambda)$ groups of the above short exact sequence (20), $\mathrm{Ext}^1_{\Lambda}(M,\Lambda)$ vanishes also. Again, since M is Λ-torsion we have $\mathrm{Ext}^0_{\Lambda}(M,\Lambda) = 0$. Thus both $\mathrm{Ext}^1_{\Lambda}(\mathrm{Ext}^1_{\Lambda}(M,\Lambda),\Lambda)$ and $\mathrm{Ext}^0_{\Lambda}(\mathrm{Ext}^0_{\Lambda}(M,\Lambda),\Lambda)$ vanish and so again by the second listed property of the filtration by $T_i(M)$ we have $T_{d-1}(M)$ is already equal to M and so M is pseudonull.

($\Leftarrow$) If M is pseudonull then, by the first listed property of the filtration by $T_i(M)$, both ξM and $M/\xi M$ have dimension at most $d-1$, that is they are pseudonull. By the inductive hypothesis it follows that they both vanish on localising at the ideal $\xi\Lambda$, and so $M_{(\xi)}$ vanishes also. This completes the proof of Proposition 1.8. □

Remark. — Recall $\mathfrak{M}$ denotes the maximal ideal of Λ. As in the commutative case we shall see that when ξ lies in $\mathfrak{M}$, but not in $\mathfrak{M}^2$, then Ω has finite global dimension, equal to the dimension d of G which is one less than the global dimension of Λ. The above arguments show in fact that Ω again satisfies the Auslander condition alluded to above in the definition above of pseudonull (see [23] for further details in the particular case $\xi = p$) and so part (i) of the lemma becomes

$$\dim_\Lambda(N) = \dim_\Omega(N).$$

For applications and for general interest we include a proof of

Theorem 1.10. — *Assume ξ lies in $\mathfrak{M}$ but not in $\mathfrak{M}^2$. Then the ring Ω has global dimension equal to d.*

Remark. — Of course, since Λ is a local ring, ξ must be an element of the maximal ideal $\mathfrak{M}$ otherwise it would be a unit.

Proof. — This follows as in the commutative case except that one has to specify consistently left Λ-modules. By [15, 7.3.7] it is sufficient simply to show that Ω has finite global dimension, since that Theorem then guarantees that it must actually be equal to $\mathrm{gldim}(\Lambda) - 1$, that is to d. Since ξ is an element of $\mathfrak{M}$ the ring Ω is again local. Let $\mathfrak{J}$ denote its maximal ideal, given by the image of $\mathfrak{M}$ in Ω. As in the proof of Theorem 2 in [17], since $\Omega/\mathfrak{J}$ is isomorphic to $\mathbb{F}_p$, the ideal $\mathfrak{J}$ satisfies the Artin-Rees property. That is, for any left ideal, L, of Ω there exists an integer k with $\mathfrak{J}^k \cap L$ contained in $\mathfrak{J}L$. It follows from a Theorem of Boratynsky in [2] that

$$\mathrm{gldim}\,(\Omega) \leqslant n \iff \mathrm{Ext}_\Omega^{n+1}(\mathbb{F}_p, \mathbb{F}_p) = 0, \tag{21}$$

thus it is sufficient to show that $\mathbb{F}_p$ has finite projective dimension as an Ω-module. In fact, by patching together a finite Ω-projective resolution of $\mathfrak{J}$ with

$$0 \longrightarrow \mathfrak{J} \longrightarrow \Omega \longrightarrow \mathbb{F}_p \longrightarrow 0 \tag{22}$$

we see that it is sufficient to show that $\mathfrak{J}$ has finite projective dimension as an Ω-module. But one easily sees that $\mathfrak{M}/\xi\mathfrak{M}$ has finite projective dimension as an Ω-module (or see [15, 7.3.6]) and so it is sufficient to show that $\mathfrak{J}$ is a direct summand of this.

Now $\mathfrak{M}/\mathfrak{M}^2$ is a finite dimensional $\mathbb{F}_p$-vector space and, by assumption, ξ maps to a non zero element of this. Extending to an $\mathbb{F}_p$-basis of $\mathfrak{M}/\mathfrak{M}^2$ and lifting we can find elements $\{\xi, x_2, \dots, x_r\}$ of $\mathfrak{M}$ which form a minimal set of generators of $\mathfrak{M}$ as a left Λ-module. Then, setting $\mathfrak{b} = \Lambda x_2 + \Lambda x_3 + \cdots + \Lambda x_r$, we obtain

$$\mathfrak{J} = \mathfrak{M}/\xi\Lambda = (\mathfrak{b} + \xi\Lambda)/\xi\Lambda \tag{23}$$

$$= \mathfrak{b}/\mathfrak{b} \cap \xi\Lambda \longrightarrow \mathfrak{M}/\xi\mathfrak{M} \longrightarrow \mathfrak{M}/\xi\Lambda = \mathfrak{J} \tag{24}$$

giving an explicit splitting $\mathfrak{M}/\xi\mathfrak{M} \cong \mathfrak{J} \oplus \mathbb{F}_p$ as left Λ-modules, proving the claim. □

For general Λ-modules M, N, $\mathrm{Hom}_\Lambda(M,N)$ does not have a natural structure as a Λ-module. Thus there can be no equivalent of the fact, in the commutative case, that localisation commutes with taking the Hom functor. However, an isomorphism between finitely generated modules over $\Lambda_{(\xi)}$ can, under certain circumstances, be lifted to a homomorphism over Λ. When the kernel and cokernel of this homomorphism are annihilated by a power of ξ this will be a pseudoisomorphism.

For any positive integer n we use the notation $\langle\xi^n\rangle$ for the ideal $\xi^n\Lambda$ (or $\xi^n\Lambda_{(\xi)}$) of Λ (respectively $\Lambda_{(\xi)}$) generated by ξ^n.

Proposition 1.11. — *Suppose*

$$\tilde{f} : M_{(\xi)} \xrightarrow{\sim} \Lambda_\xi^r \oplus \bigoplus_{i=1}^{t-r} \Lambda_\xi/\langle\xi^{n_i}\rangle \tag{25}$$

as left $\Lambda_{(\xi)}$-modules. Then there exists a Λ-module homomorphism:

$$f : M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^{t-r} \Lambda/\langle\xi^{n_i}\rangle \tag{26}$$

which induces $\tilde{f}$ upon extending to $M_{(\xi)}$ via $1\otimes f$. In particular, upon restricting to $M(\xi)$ this gives a pseudoisomorphism:

$$f_{|M(\xi)} : M(\xi) \longrightarrow \bigoplus_{i=1}^{t-r} \Lambda/\langle\xi^{n_i}\rangle \tag{27}$$

Remark. — We cannot conclude f itself is a pseudoisomorphism from the whole of M, as Proposition 1.8 only applies when M is annihilated by some power of ξ.

Proof. — We show that taking f to be the composition of the natural map, ι, from M to $M_{(\xi)}$ with the isomorphism in (25) restricted to the Λ-submodule of $M_{(\xi)}$ generated by the elements $1 \otimes m$ for m in M gives the homomorphism required in (26). The image of this map gives a Λ-submodule, which we denote by N, of $\Lambda_\xi^r \oplus \bigoplus \Lambda_\xi/\langle\xi^{n_i}\rangle$. This has the property that $N_{(\xi)}$ is isomorphic to $\Lambda_\xi^r \oplus \bigoplus \Lambda_\xi/\langle\xi^{n_i}\rangle$. Thus we have to show that any Λ-submodule with this property is a Λ-submodule of a Λ-module of the required form.

Let $\{v_i\}$ be a minimal set of generators of $\Lambda_\xi^r \oplus \bigoplus \Lambda_\xi/\langle\xi^{n_i}\rangle$. It is most convenient if we assume this is a 'canonical' basis, by which we mean the first r generators are generators of a free $\Lambda_{(\xi)}$-module, and each of the other v_i generates one of the $\Lambda_{(\xi)}/\langle\xi^{n_i}\rangle$. Let $\{m_i\}$ be a set of generators of M. Then the $\{1 \otimes m_i\}$ generate $M_{(\xi)}$ as a $\Lambda_{(\xi)}$-module, and N as a Λ-module. Since the v_i are generators, each $\tilde{f}(1 \otimes m_i)$ can be written

$$\tilde{f}(1 \otimes m_i) = \sum_{j=1}^{t} a_{i\,j}^{-1} b_{i\,j} v_j$$

for some $a_{i\,j}, b_{i\,j}$ in Λ with the $a_{i\,j}$ not divisible by ξ. By Lemma 1.5 we can clear the denominators in this sum, and rewrite it

$$\tilde{f}(1 \otimes m_i) = \sum_{j=1}^{t} b'_{i\,j} a^{-1} v_j$$

for a single a in Λ, not divisible by ξ. Thus N is a Λ-submodule of the Λ-module generated by the $a^{-1}v_j$. But this module has the required form. Denote this module by R. Then by the original choice of generators $\{v_i\}$ there is a Λ-module surjection

$$\Lambda^r \bigoplus \bigoplus_{i=1}^{t-r} \Lambda/\langle \xi^{n_i} \rangle \longrightarrow R, \quad (e_1, \ldots, e_t) \longmapsto (e_1 a^{-1} v_1, \ldots, e_t a^{-1} v_t).$$

Since this becomes an isomorphism on localising at $\xi\Lambda$, every element in the kernel of this map must be annihilated by some element in Λ not divisible by ξ. But there are no such elements in the module on the left hand side, and so this map is also injective.

That $1 \otimes f$ induces the original isomorphism $\tilde{f}$ is immediate from the construction of f. Since localising at $\xi\Lambda$ is exact, and since the localisation of f restricted to $M(\xi)$ is an isomorphism, the localisations of the kernel and cokernel in (27) vanish. Since they are also both annihilated by some power of ξ, it follows from Proposition 1.8 that they are pseudonull. □

1.3. Non-Abelian Principal Ideal Domains.

— We give a brief review of this theory and how it applies to $\Lambda_{(\xi)}$.

Definition. — Denote by υ the following function from $\Lambda_{(\xi)} \backslash \{0\}$ to $\mathbb{N}$. By Lemma 1.1 every non zero x in Λ can be uniquely written as $b\,\xi^n$, with b contained in S. Then υ is defined by

$$\upsilon : a^{-1} b\, \xi^n \longmapsto n. \tag{28}$$

We extend to the whole of $\Lambda_{(\xi)}$ by setting $\upsilon(0) = \infty$.

Lemma 1.12. — *The function υ defined above is well-defined and satisfies the following properties for a non-Archimedean valuation, making $\Lambda_{(\xi)}$ into a (non-Abelian) discrete valuation ring:*

(i) $\upsilon(\alpha\beta) = \upsilon(\alpha) + \upsilon(\beta) \geqslant \max(\upsilon(\alpha), \upsilon(\beta))$ *for all non zero α, β in $\Lambda_{(\xi)}$.*

(ii) $\upsilon(\alpha + \beta) \leqslant \max(\upsilon(\alpha), \upsilon(\beta))$ *for all α and β in $\Lambda_{(\xi)}$.*

(iii) *For all α, β in $\Lambda_{(\xi)}$ either $\alpha = \beta\gamma$ and $\alpha = \gamma'\beta$ for some γ, γ' in $\Lambda_{(\xi)}$, or $\upsilon(\alpha) < \upsilon(\beta)$.*

Proof. — This is essentially immediate from Lemma 1.1. We check it is well defined. Suppose $a^{-1}b = c^{-1}d$ in $\Lambda_{(\xi)}$. First note that $a^{-1}b = 0$ if and only if $b = 0$, and similarly $c^{-1}d = 0$ if and only if $d = 0$, and we assume now this is not the case. Let a_1, c_1 in S be chosen, as usual, so that $a_1c = c_1a$. Then the assumption $a^{-1}b = c^{-1}d$ is equivalent to $c_1b = a_1d$. Write $b = b_1\xi^n$ for some b_1 in S. That is $\upsilon(a^{-1}b) = n$. Then $a_1d = c_1b_1\xi^n$. Since ξ is prime, a_1 an element of S and Λ contains no zero divisors, this implies $d = d_1\xi^n$ with d_1 an element of S. Thus $\upsilon(c^{-1}d) = \upsilon(c^{-1}d_1\xi^n) = n$, also.

That υ satisfies the properties given is immediate from the definition. The only non units in $\Lambda_{(\xi)}$ are powers of the image of ξ in $\Lambda_{(\xi)}$. □

Corollary 1.13. — *All right and left ideals of $\Lambda_{(\xi)}$ are principal.*

Definition. — Let R denote a Noetherian ring, not necessarily commutative, containing no zero divisors and for which every right and left ideal is principal. Whenever we refer to a *Principal Ideal Domain* we mean a ring with these properties.

Lemma 1.14. — *If N is a submodule of a finitely generated, free R-module, F, then N is also free, of rank at most equal to that of F.*

This follows exactly the usual proof for Abelian principal ideal domains, see for example [9, § 10.6].

Definition. — Recall that in a principal ideal domain the notion of highest common factor and least common multiple can be defined. If a and b are two elements in R then a *highest common right, resp. left, factor* of a and b is a generator of $Ra + Rb$, resp. $aR + bR$. A *least common left, resp. right, multiple* of a and b is a generator of $Ra \cap Rb$, resp. $aR \cap bR$.

Theorem 1.15. — *For all finitely generated R-modules, M, there exists a finite set of non zero elements $\{a_i\}$ of R, and an integer $r \geqslant 0$, such that there is an isomorphism*

$$M \cong \Big(\bigoplus_{i=1}^{r} \frac{R}{Ra_i}\Big) \bigoplus R^r. \tag{29}$$

For the proof see [15, § 5.7.19].

Remark. — It is not necessarily true that the $\{a_i\}$ are unique in this general setting. See the discussion in § 5.7.18–19 of [15]. This difficulty does not, however, arise for us:

Definition. — Two elements of R are said to be *equivalent* if they generate the same left ideal.

Lemma 1.16. — *For the ring $\Lambda_{(\xi)}$, the set $\{a_i\}$ in Theorem 1.15 is uniquely defined up to reordering, equivalence and redundancy ($Ra_i = R$). By Lemma 1.12 and the comments after Lemma 1.4 they may all be taken to be powers of ξ.*

Indeed, in $\Lambda_{(\xi)}$ the only proper left ideals are of the form $\Lambda\xi^n$, for integers $n \geqslant 1$. Since ξ is central, these are also right ideals, thus there are no faithful torsion $\Lambda_{(\xi)}$-modules. The lemma can thus be reduced to a special case of the structure theorem for modules over an Artinian principal ideal domain. See [15, § 5.7.17].

2. General Structure Theorem for Central Prime Torsion

Let M now denote any finitely generated, left, Λ-module. We first restate Proposition 1.11 above as the following:

Corollary 2.1. — *If $(M(\xi))_{(\xi)}$ is non zero then there is a non zero homomorphism*

$$M \longrightarrow \bigoplus_{i=1}^{t} \frac{\Lambda}{\langle \xi^{n_i} \rangle}, \tag{30}$$

which restricts to a pseudoisomorphism on $M(\xi)$.

Proposition 2.2. — *Let ξ be any central prime of Λ, as defined in the introduction. Then there is a pseudoisomorphism*

$$M \longrightarrow \bigoplus_{i=1}^{t} \frac{\Lambda}{\langle \xi^{n_i} \rangle} \oplus \frac{M}{M(\xi)}. \tag{31}$$

Proof. — This is similar to the argument of 5.1.7 (page 224) of [16]. Let f be the homomorphism in (30) of Corollary 2.1. Let ϕ denote the Λ-module homomorphism from the module M to $\bigoplus \Lambda/\xi^{n_i}\Lambda \oplus M/M(\xi)$, given by $(f_{|M(\xi)}, can)$ where *can* denotes the canonical surjection of M onto $M/M(\xi)$. We have the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & M(\xi) \arrow[r] \arrow[d, "f_{|M(\xi)}"] & M \arrow[r] \arrow[d, "\phi"] & \frac{M}{M(\xi)} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \bigoplus_{i=1}^{t} \frac{\Lambda}{\langle \xi^{n_i} \rangle} \arrow[r] & \bigoplus_{i=1}^{t} \frac{\Lambda}{\langle \xi^{n_i} \rangle} \oplus \frac{M}{M(\xi)} \arrow[r] & \frac{M}{M(\xi)} \arrow[r] & 0.
\end{tikzcd} \tag{32}$$

Then, by the snake lemma

$$\mathrm{Ker}(\phi) = \mathrm{Ker}(f_{|M(\xi)}), \quad \mathrm{Coker}(\phi) = \mathrm{Coker}(f_{|M(\xi)}).$$

By the last line of Corollary 2.1, f restricted to $M(\xi)$ is a pseudoisomorphism, thus both of these modules are pseudonull, and so ϕ is also a pseudoisomorphism. □

The following is an immediate consequence of the behaviour of the dimension $\delta(M)$ of the Λ-modules in exact sequences quoted in the list of properties of the filtration $T_i(M)$ of M in Section 1.2.

LEMMA 2.3. — *The composition of two pseudoisomorphisms is also a pseudoisomorphism.*

We now put this together for all central primes, ξ.

DEFINITION. — For a finite set of central primes, $\{\xi_1,\dots,\xi_n\}$, we define $M(\xi_1,\dots,\xi_n)$ to be the module generated by elements of M annihilated by a monomial in the ξ_i, where i varies between 1 and n. Denote by $M(\{\xi\})$ the module generated by elements of M annihilated by any product of central primes.

LEMMA 2.4. — *There exists a finite set of central primes, $\{\xi_i\}_{i=1}^r$, such that*

$$M\big(\{\xi\}\big)=M(\xi_1,\dots,\xi_r).$$

Proof. — Recall Λ is Noetherian, and M is finitely generated over Λ. Since $M(\{\xi\})$ is a Λ-submodule of M, it is also Noetherian. Thus the ascending chain

$$0\subset M(\xi_1)\subset M(\xi_1,\xi_2)\subset\cdots \tag{33}$$

terminates after a finite number of terms, giving $M(\{\xi\})$. □

THEOREM 2.5. — *Let M be any finitely generated, left, Λ-module. Then there exists a pseudoisomorphism,*

$$M\longrightarrow\bigoplus_{\xi}\bigg(\bigoplus_{i_\xi=1}^{r_\xi}\frac{\Lambda}{\langle\xi^{n_{i_\xi}}\rangle}\bigg)\oplus\frac{M}{M(\{\xi\})}, \tag{34}$$

where $M(\{\xi\})$ denotes the module generated by the $M(\xi)$, for all central primes ξ, and in the direct sum ξ runs over all central primes ξ_i. For all but finitely many ξ, the exponent n_{i_ξ} is zero for all i_ξ. In particular, if $\{\xi_1,\dots,\xi_n\}$ is a finite set of central primes generating $M(\{\xi\})$ then for all central primes not in this set, n_{i_ξ} is zero for all i. This representation is unique, in the sense that the ideals, $\{\langle\xi^{n_{i_\xi}}\rangle\}$, in (34) are uniquely defined, up to redundancy ($n_{i_\xi}=0$) and renumbering, by M and ξ.

Proof. — We let $N_0=M$ and proceed inductively, running through all the central primes ξ. Let $\{\xi_1,\cdots,\xi_n\}$ be a finite set of central primes as in Lemma 2.4.

Then for $i \leqslant n$ we define M_i to be $M/M(\xi_1, \dots, \xi_i)$, where $M(\xi_1, \dots, \xi_i)$ is as defined above. By Proposition 2.2, there is a pseudoisomorphism

$$f_i : M_{i-1} \longrightarrow \bigoplus_{j=1}^{r_{\xi_i}} \frac{\Lambda}{\langle \xi_i^{n_{j,i}} \rangle} \oplus M_i. \tag{35}$$

If we have a pseudoisomorphism

$$\phi_{i-1} : M \longrightarrow \bigoplus_{k=1}^{i-1} \Big(\bigoplus_{j=1}^{r_{\xi_k}} \frac{\Lambda}{\langle \xi_k^{n_{j,k}} \rangle} \Big) \oplus M_{i-1}, \tag{36}$$

then composing this with (id, f_i) gives ϕ_i. This is the required pseudoisomorphism, since M_n is equal to $M(\{\xi\})$. It remains to show this representation is independent of the choice of generating set $\{\xi_1, \dots, \xi_n\}$ and in particular that the exponents are intrinsically defined by M, independent of the choices made.

Lemma 2.6. — *Let ξ_1 and ξ_2 be two* distinct *central primes. Let ϕ be the pseudoisomorphism as constructed in Proposition* 2.2*:*

$$M \longrightarrow \bigoplus_{i=1}^{t} \frac{\Lambda}{\langle \xi_1^{n_i} \rangle} \oplus \frac{M}{M(\xi_1)}. \tag{37}$$

Then, localising at ξ_2, ϕ induces an isomorphism

$$M_{\xi_2} \longrightarrow \Big(\frac{M}{M(\xi_1)} \Big)_{(\xi_2)}. \tag{38}$$

This is immediate by Lemma 1.5 since, by the construction of ϕ in Proposition 2.2, both the kernel and cokernel of ϕ are ξ_1-torsion.

The uniqueness part of the statement of Theorem 2.5 now follows from the uniqueness of the structure of $\Lambda_{(\xi)}$-modules, as explained in Lemma 1.16. □

3. Properties

Suppose first that every element of M is annihilated by a product of some central primes, *i.e.* $M = M(\{\xi\})$. Let $\{\xi_j\}_{j=1}^n$ be a set of central primes as in Lemma 2.4. In this case we define the *characteristic element* of M by

$$\mathrm{Char}(M) = \prod_{j=1}^{n} \Big(\prod_{i_j=1}^{r_j} \xi_j^{n_{i_j}} \Big), \tag{39}$$

where the indices n_{i_j} and the limits r_j for each central prime ξ_j are as defined in Theorem 2.5 above. Although this is not itself uniquely defined, the *characteristic ideal* $\langle \mathrm{Char}(M) \rangle$, of Λ is uniquely defined for each M, by the uniqueness statement in Theorem 2.5.

Definition. — More generally, for any Λ-module, M, we define the following element of Λ associated to M

$$z(M) = \mathrm{Char}\,\bigl(M\bigl(\{\xi\}\bigr)\bigr). \tag{40}$$

We consider invariants of M which may help us find further information about $z(M)$ in some cases. Let V denote a finite dimensional $\mathbb{Q}_p$-vector space upon which G acts via a continuous representation

$$\rho : G \longrightarrow \mathrm{GL}(V)$$

with G acting upon V on the *right*. Let T denote a $\mathbb{Z}_p$-lattice in V, fixed under the action of G. Since T is compact, ρ extends to a homomorphism $\Lambda \to \mathrm{End}(V)$ and T becomes naturally a right Λ-module.

Definition. — We consider the following *generalised Euler Characteristics*. For any finitely generated, torsion Λ-module, M, with V as described above, define

$$\chi(G,V,M) = \prod_{i\geqslant 0} \bigl(\#\,\mathrm{Tor}_i^{\Lambda}(T,M)\bigr)^{(-1)^i}, \tag{41}$$

for some lattice T in V, if this product is finite. Otherwise we simply refer to this Euler characteristic as being undefined, or infinite. Since Λ has finite global dimension the product contains only finitely many terms, at most $d+2$. In common with the notation in earlier work [5], [13], when V is the trivial representation $\mathbb{Q}_p$ we omit the V and use the notation $\chi(G,M)$.

The value of $\chi(G,V,M)$ depends, *a priori*, upon the choice of lattice T in V, but for torsion M this is not, in fact, the case.

Lemma 3.1. — *If M is a finitely generated, torsion Λ-module then $\chi(G,V,M)$ is independent of choice of lattice, T, in V.*

Proof. — Suppose T_1 and T_2 are two G-equivariant $\mathbb{Z}_p$-lattices in V. Since $T_1 \cap T_2$ is also a G-equivariant $\mathbb{Z}_p$-lattice we may assume T_1 is a sublattice of T_2 with T_2/T_1 a finite G-module. Furthermore, since we have assumed throughout that G is pro-p one knows that the only simple finite G-module is $\mathbb{F}_p$, with trivial G action, thus we may assume also that T_2/T_1 is isomorphic to $\mathbb{F}_p$. First note that $\mathrm{Tor}_i^{\Lambda}(\mathbb{F}_p,M)$ is finite for all i and all finitely generated Λ-modules, M. Indeed, taking a finite, free presentation of M

$$0 \to \Lambda^{n_{d+1}} \longrightarrow \cdots \longrightarrow \Lambda^{n_0} \longrightarrow M \to 0, \tag{42}$$

and observing that $\mathrm{Tor}_i^{\Lambda}(\mathbb{F}_p,\Lambda)$ vanishes for i at least 1, while $\mathrm{Tor}_0^{\Lambda}(\mathbb{F}_p,\Lambda)$ is isomorphic to $\mathbb{F}_p$, we see (*cf.* the results in [13]) that

$$\log_p\Bigl(\prod_{i\geqslant 0}\bigl(\#\,\mathrm{Tor}_i^{\Lambda}(\mathbb{F}_p,M)\bigr)^{(-1)^i}\Bigr) = \sum_{i\geqslant 0}(-1)^i n_i, \tag{43}$$

which is simply the rank of M as a Λ-module, thus is zero under the assumption that M is torsion. The lemma follows upon taking $\mathrm{Tor}_i^{\Lambda}(-, M)$ of the short exact sequence

$$0 \to T_1 \longrightarrow T_2 \longrightarrow \mathbb{F}_p \to 0. \qquad \square$$

Since we will only use the notation (41) in the case M is Λ-torsion there will be no confusion in not specifying the lattice, however the proof of the lemma clearly describes precisely in terms of the Λ-rank of M how the general Euler characteristics change when M is not Λ-torsion. Finally, we remark that if one does not insist G be pro-p then the behaviour of these invariants is far more subtle, and currently not well understood (*cf.* § 2.1 of [13] and similar results in Chapter 1 of [23].) Calculations of some specific Euler characteristics for G not pro-p and V taken to be $\mathbb{Q}_p$ are given in [5] and [6], [8], [21] and [22] for 'small' representations.

PROPOSITION 3.2. — *Assume $M = M(\xi_1, \dots, \xi_r)$ for some finite set of central primes $\{\xi_1, \dots \xi_r\}$ each of which lies in $\mathfrak{M}$ but not in $\mathfrak{M}^2$. Let (ρ, V) be a finite dimensional right representation of G such that* $\det(\rho(\mathrm{Char}(M)))$ *is non zero. Then $\chi(G, V, M)$ is a finite power of p given by*

$$\mathrm{ord}_p\big(\chi(G, V, M)\big) = \mathrm{ord}_p\big(\det \rho\big(\mathrm{Char}(M)\big)\big). \tag{44}$$

We prove two special cases first:

LEMMA 3.3. — *Let f be any element of Λ, and let M be the left Λ-module $\Lambda/\Lambda f$. Then the generalised Euler characteristic $\chi(G, V, \Lambda/\Lambda f)$ is finite if and only if* $\det(\rho(f))$ *is non zero, in which case the two values have the same p-part.*

Proof. — Let M here denote $\Lambda/\Lambda f$. Consider the short exact sequence of left Λ-modules

$$0 \longrightarrow \Lambda \xrightarrow{\times f} \Lambda \longrightarrow M \to 0$$

where Λ itself is considered as a Λ-bimodule and the multiplication by f map is on the right. Tensoring on the left with a lattice, T, in V we find

$$0 \to \mathrm{Tor}_1^{\Lambda}(T, M) \longrightarrow T \xrightarrow{\rho(f)} T \longrightarrow T \otimes_\Lambda M \to 0 \tag{45}$$

and $\mathrm{Tor}_i^{\Lambda}(T, M) = 0$ for i greater than 1. The sequence (45) comes about because $\mathrm{Tor}_i^{\Lambda}(T, \Lambda)$ vanishes for i greater than zero, and because $T \otimes_\Lambda \Lambda$ is canonically isomorphic to T as a $\mathbb{Z}_p$-module, with the homomorphism f becoming the action of $\rho(f)$. It follows that the $\mathrm{Tor}_i^{\Lambda}(T, M)$ for i equal to 0 and 1 are both finite if and only if $\rho(f)$ is non singular and then we have the claimed equality. □

REMARK. — We have not assumed that f is central here, and so Lemma 3.3 holds in general. This gives another proof of the independence of $\chi(G, V, M)$ on the choice of lattice T for the special case of the 'standard' modules, M, of the form $\Lambda/\Lambda f$, which holds without assuming G be torsion free so long as f is a non zero divisor in Λ. It would be interesting to know other cases where this number is independent of choice of T for general, not necessarily pro-p, G.

LEMMA 3.4. — *If M is ξ-torsion for a single central prime ξ which lies in the maximal ideal $\mathfrak{M}$ but not in $\mathfrak{M}^2$, then the proposition holds. If we assume furthermore that M is also pseudonull then if* $\det(\rho(\xi))$ *is non zero,* $\chi(G,V,M)$ *must equal* 1.

Proof. — This mirrors exactly section 1.2 of [13] which deals with the case ξ equal to p. We will only sketch the argument here, and the extra points needed to generalise to this case.

First note that in this case $\mathrm{Char}(M)$ is a power of ξ and so $\det(\rho(\mathrm{Char}(M)))$ equals zero if and only if $\det(\rho(\xi))$ equals zero. For M annihilated by ξ itself, since ξ is not in $\mathfrak{M}^2$ we can apply 1.10 to find a finite, free resolution of M by Ω-modules, where Ω denotes $\Lambda/\xi\Lambda$.

$$0 \to \Omega^{n_d} \longrightarrow \cdots \longrightarrow \Omega^{n_0} \longrightarrow M \to 0. \tag{46}$$

The lemma immediately above applies to Ω itself. If $\det(\rho(\xi))$ is non zero then by the above Lemma 3.3 and considering $\mathrm{Tor}_i^{\Lambda}(T,-)$ of the resolution (46) we obtain

$$\mathrm{ord}_p\big(\chi(G,V,M)\big) = \big(\textstyle\sum_{i\geqslant 0}(-1)^i n_i\big)\ \mathrm{ord}_p\big(\det(\rho(\xi))\big), \tag{47}$$

and $\sum_{i\geqslant 0}(-1)^i n_i$ gives the rank of M as an Ω-module. By Proposition 1.8 and Lemma 1.5, M is pseudonull if and only if every element of M has a non trivial annihilator in Ω. In which case M has zero Ω-rank and so by (47), $\chi(G,V,M)$ equals 1. This, together with the existence of the pseudoisomorphism $M \to \Omega^n$ in this case (a special case of Corollary 2.1) gives the lemma when $\xi M = 0$. It extends inductively to general ξ-torsion modules M upon considering

$$0 \to \xi M \to M \to M/\xi M \to 0. \qquad \square$$

Proof of 3.2. — The rest of the proposition now follows immediately. By the above Lemma 3.3 it holds for the standard modules on the righthand side of (34), in the case $M(\{\xi\}) = M$. By the method of construction of the pseudoisomorphism in Theorem 2.5 any element, x, of the kernel or cokernel of the pseudoisomorphism is annihilated both by some ξ^n with ξ a non zero factor in $\mathrm{Char}(M)$, and also some non zero element of Λ not divisible by ξ. Since $\det(\rho(\mathrm{Char}(M)))$ is non zero and both ρ and det are multiplicative functions, by Lemma 3.4 above $\chi(G,V,\Lambda x)$ equals one. Since this is true for every element x in the kernel and cokernel of the pseudoisomorphism, and since both are finitely generated Λ-modules, if $\det(\rho(\mathrm{Char}(M)))$ is non zero then $\chi(G,V,N)$ equals zero for N either the kernel of cokernel. Proposition 3.2 now follows by the multiplicativity of $\chi(G,V,M)$ in exact sequences. □

Lemma 3.5. — *If* $0 \to A \to B \to C \to 0$ *is a short exact sequence of* Λ-*modules which are all* Λ-torsion *then the ideals* $\langle z(B)\rangle$ *and* $\langle z(A) \times z(C)\rangle$ *coincide.*

Proof. — This follows immediately from the proof of Theorem 2.5, since the contribution of each central prime, ξ, to $z(M)$ is given in terms of the $\Lambda_{(\xi)}$-module structure of $M_{(\xi)}$, and localising at $\xi\Lambda$ is flat, by Lemma 1.5 part (iii). If ξ is any such prime then we have

(48)
$$\begin{tikzcd}
0 \arrow[r] & A_{(\xi)} \arrow[r] \arrow[d, "\wr"] & B_{(\xi)} \arrow[r] \arrow[d, "\wr"] & C_{(\xi)} \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & \bigoplus \dfrac{\Lambda}{\langle \xi^{a_i}\rangle} \arrow[r] & \bigoplus \dfrac{\Lambda}{\langle \xi^{b_i}\rangle} \arrow[r] & \bigoplus \dfrac{\Lambda}{\langle \xi^{c_i}\rangle} \arrow[r] & 0
\end{tikzcd}$$

from which the lemma follows by the uniqueness in Lemma 1.16. □

4. Subgroups of $\mathbf{GL_2}(\mathbb{Z}_p)$ and an Application to Elliptic Curves

Throughout the whole of this section we assume that G is a pro-p open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ with p at least 3, unless otherwise specified. If p equals 3 we assume G is sufficiently small to contain no element of order p (recall this is always the case when $p \geqslant 5$). As there will be some variation in the choice of group throughout this section, we now include G in the notation, $\Lambda(G)$, for the Iwasawa algebra of G as defined in (1). In this case G is the direct product of the centre of G and the closed subgroup of G given by the kernel of the determinant function. We will use the notation $Z(G)$ to denote the centre of G. Then it is well known that $Z(G)$ consists of the scalar matrices only in this case. There is an inverse to the determinant function given by $a \mapsto \left(\begin{smallmatrix} a^{1/2} & 0 \\ 0 & a^{1/2}\end{smallmatrix}\right)$, where $a^{1/2}$ is the square root of a such that this matrix is an element of $Z(G)$. This is well defined since, by the assumption that G contains no element of order 2, $Z(G)$ is canonically isomorphic to an open subgroup of $\mathbb{Z}_p^\times$ containing no element of order 2, thus is uniquely divisible by 2 under the assumption that $p \geqslant 3$. Since the determinant function is continuous, the kernel of the determinant map is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$.

Though we will not give the details here, this section generalises to any group which is a direct product of $\mathbb{Z}_p^n$ with a pro-p, p-adic, Lie group which has the property that the only element in a finite conjugacy class is the identity. In the case of Proposition 4.2 one has to proceed by induction on n and the argument is similar to that given for the case of p equal to 2 just preceding Lemma 4.3 below.

Lemma 4.1. — *Assume p is at least* 3. *If G is an open subgroup of* $\mathrm{GL}_2(\mathbb{Z}_p)$ *containing no element of order* 2, *and H is the kernel of the determinant function, then $\Lambda(G)$ is non-canonically isomorphic as a topological $\mathbb{Z}_p$-algebra* *to $\Lambda(H)[[T]]$, the ring of power series in a single variable which commutes with $\Lambda(H)$.*

Proof. — As explained in the above discussion, G is isomorphic to $H \times Z(G)$ and so $\Lambda(G)$ is isomorphic to $\Lambda(H)\widehat{\otimes}_{\mathbb{Z}_p}\Lambda(Z(G))$ which is isomorphic to $\Lambda(H)[[Z(G)]]$, where $\widehat{\otimes}$ denotes the completed tensor product. Under our assumptions on G the centre $Z(G)$ is isomorphic to $\mathbb{Z}_p$, and we choose a topological generator γ of $Z(G)$. Then it is well known that the map

$$\Lambda\big(Z(G)\big) \longrightarrow \mathbb{Z}_p[[T]], \quad \gamma \longmapsto T+1 \tag{49}$$

gives an isomorphism of topological $\mathbb{Z}_p$-algebras. The proof of continuity is given, for example, in [16], Proposition 5.3.5. This extends to the required isomorphism

$$\Lambda(H)\widehat{\otimes}_{\mathbb{Z}_p}\Lambda\big(Z(G)\big) \cong \Lambda(H)\widehat{\otimes}_{\mathbb{Z}_p}\mathbb{Z}_p[[T]] \cong \Lambda(H)[[T]]. \tag{50}$$

□

PROPOSITION 4.2. — *Assume G is a pro-p open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ (we do not here restrict to $p \geqslant 3$ or require that G contains no element of order p). Then the centre of $\Lambda(G)$ is the completed group algebra of the centre of G. Since this is isomorphic to either $\mathbb{Z}_p$, or possibly $\mathbb{Z}_2 \times \mathbb{Z}/2$ when p is equal to 2, the centre of $\Lambda(G)$ is isomorphic to $\mathbb{Z}_p[[T]]$ for p at least 3 while for $p = 2$ it is isomorphic to $\mathbb{Z}_2[\Delta][[T]]$ where Δ is either $\mathbb{Z}/2$ or trivial, depending upon whether G contains the identity or not.*

Similarly, if G is a pro-p open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ then for $p \geqslant 3$ the centre of $\Lambda(G)$ consists of the $\mathbb{Z}_p$-scalar multiples of the identity of G only, while for $p = 2$ it is isomorphic to $\mathbb{Z}_2[\Delta]$ where again Δ is either $\mathbb{Z}/2$ or trivial, depending upon whether G contains the identity or not.

Proof. — Let $Z(G)$ denote the centre of G, and let H be $G/Z(G)$. Then H is isomorphic to an open subgroup of $\mathrm{PGL}_2(\mathbb{Z}_p)$ or $\mathrm{PSL}_2(\mathbb{Z}_p)$. It is sufficient to prove the centre of $\mathbb{F}_p[[H]]$ consists of just the $\mathbb{F}_p$-scalar multiples of the identity. Indeed, assuming this, if ζ is an element of the centre of $\Lambda(G)$ then the image of ζ under the canonical surjection to $\mathbb{F}_p[[H]]$ lies in the set of $\mathbb{F}_p$-scalar multiples of the identity. Let $\overline{\zeta}$ denote the image of ζ in $\mathbb{F}_p[[G]]$. We first show that the centre of $\mathbb{F}_p[[G]]$ is just $\mathbb{F}_p[[Z(G)]]$. For $p \geqslant 3$ the centre of G is either zero, in which case G is isomorphic to H and so we are done, or isomorphic to $\mathbb{Z}_p$. In the second case we let γ denote a topological generator of $Z(G)$. Then $\overline{\zeta} = x\,\mathrm{id}_G + (\gamma-1)\overline{\zeta'}$ where x is an element of $\mathbb{F}_p$ and $\overline{\zeta'}$ is again central. Repeating, we find $\overline{\zeta}$ lies in $\mathbb{F}_p[[Z(G)]] + \mathbb{F}_p[[G]](\gamma-1)^n$ for all n. Since G is pro-p, $\mathbb{F}_p[[G]]$ is a local ring with maximal ideal given by the augmentation ideal $\mathfrak{M}$, the kernel of the natural map $\mathbb{F}_p[[G]] \to \mathbb{F}_p$. But G is also a p-adic, Lie group and so the $\mathfrak{M}$-adic topology is equivalent to the profinite topology on $\mathbb{F}_p[[G]]$. Thus

$$\bigcap_n \mathbb{F}_p[[G]](\gamma-1)^n = 0, \tag{51}$$

and so $\overline{\zeta}$ lies in $\mathbb{F}_p[[Z(G)]]$. This shows that the centre of $\mathbb{F}_p[[G]]$ is $\mathbb{F}_p[[Z(G)]]$ in the case $p \geqslant 3$.

If p is equal to 2 then the centre of G is isomorphic to one of $\mathbb{Z}_2$, $\mathbb{Z}/2$ or $\mathbb{Z}_2 \times \mathbb{Z}/2$. For the first two cases the argument is as above, since the centre is (topologically) cyclic. In the third case let $Z(G) \cong \Gamma \times \Delta$, where Δ is isomorphic to $\mathbb{Z}/2$ with generator δ and Γ is isomorphic to $\mathbb{Z}_2$ with topological generator γ. The above argument shows that the centre of $\mathbb{F}_2[[G/\Gamma]]$ is $\mathbb{F}_2[\Delta]$. Proceeding similarly, $\overline{\zeta} = x\,\mathrm{id}_G + y\delta + (\gamma-1)\overline{\zeta'}$ where x and y are elements of $\mathbb{F}_2$. Since $x\,\mathrm{id}_G$, $y\delta$ and γ are all central in $\mathbb{F}_2[[G]]$ so must $\overline{\zeta'}$ be. Thus again

$$\overline{\zeta} \in \mathbb{F}_2[[Z(G)]] + \bigcap_n \mathbb{F}_2[[G]](\gamma-1)^n. \tag{52}$$

Once more, the assumption that G is pro-2 means that $(\gamma-1)^n$ is an element of $\mathfrak{M}^n$ for all n and so the intersection on the right hand side of (52) is zero, proving again that the centre of $\mathbb{F}_2[[G]]$ is just $\mathbb{F}_2[[Z(G)]]$.

Now an identical argument lifts back to $\Lambda(G)$. As above, $\zeta = \alpha + p\zeta'$, with α an element of $\mathbb{Z}_p[[Z(G)]]$, ζ' also central in $\Lambda(G)$. Repeating, ζ is an element of $\mathbb{Z}_p[[Z(G)]] + \Lambda(G)p^n$, and again p is contained in the maximal ideal of $\Lambda(G)$ and so p^n tends to zero in the profinite topology on $\Lambda(G)$.

We need the following fact.

Lemma 4.3. — *For H any open subgroup of $\mathrm{PGL}_2(\mathbb{Z}_p)$ or $\mathrm{PSL}_2(\mathbb{Z}_p)$, the only finite conjugacy class in H is that consisting of the identity element only.*

Indeed, any open subgroup of either $\mathrm{PGL}_2(\mathbb{Z}_p)$ or $\mathrm{PSL}_2(\mathbb{Z}_p)$ has trivial centre. But if α is any element of H in a finite conjugacy class then the centraliser of α has finite index in H. Since it is closed it is also open, and contains α in the centre. Thus by the first remark applied to the centraliser of α in H, we see that α must be the identity.

Thus it remains to prove that for H a pro-p, p-adic Lie group whose only element in a finite conjugacy class is the identity, then the centre of $\mathbb{F}_p[[H]]$ is the set $\{\lambda i\}$ where i is the identity in H, λ an element of $\mathbb{F}_p$. For convenience we will omit i from the notation and refer to these as elements of $\mathbb{F}_p$. We will also denote $\mathbb{F}_p[[H]]$ by Ω.

Recall now that for a finite group, Δ, the centre of $\mathbb{F}_p[\Delta]$ is the free $\mathbb{F}_p$-module generated by the elements C_γ where γ runs over representatives of each conjugacy class of Δ and C_γ is defined by

$$C_\gamma = \sum \tau \tag{53}$$

with τ running over the conjugates of γ in Δ. We denote by $|C_\gamma|$ the number of terms in this sum, *i.e.* the order of the conjugacy class of γ in Δ.

Suppose now that ζ is an element of the centre of Ω. Let H_n denote a filtration of H by open, normal subgroups which give a base of neighbourhoods for the profinite topology of H. For example, we could take the descending, central p-series, $H_n = \overline{H_{n-1}^p[H_{n-1}, H_{n-1}]}$, see [10]. Let $\mathcal{H}_n$ be the finite groups H/H_n for each n, thus $H = \varprojlim \mathcal{H}_n$. Let ζ_n be the image of ζ in $\mathcal{H}_n$. Since ζ is central, each ζ_n is central in $\mathbb{F}_p[\mathcal{H}_n]$ and we denote these latter rings by Ω_n.

By the above comment for finite groups, for each n

$$\zeta_n = \sum_{\gamma_n} \alpha_{\gamma_n} C_{\gamma_n} \tag{54}$$

where γ_n runs over representations of the conjugacy classes in $\mathcal{H}_n$ and α_{γ_n} are scalars in $\mathbb{F}_p$. We show that the coefficient α_{γ_n} is zero unless γ_n is the identity.

Fix a positive integer n and an element γ_n of $\mathcal{H}_n$. Let n_1 be any integer strictly larger than n. Let h be any element of $\mathcal{H}_{n_1}$ which maps to some element in the same $\mathcal{H}_n$-conjugacy class as γ_n under the canonical surjection $\mathcal{H}_{n_1} \to \mathcal{H}_n$. Then the conjugacy class of h in $\mathcal{H}_{n_1}$ surjects on to the conjugacy class of γ_n in $\mathcal{H}_n$. This is true for any such h. Thus

$$\alpha_{\gamma_n} = \sum_{h \in \mathfrak{S}} \Big\{ \frac{|C_h|}{|C_{\gamma_n}|} \bmod p \Big\} \alpha_h \tag{55}$$

where $\mathfrak{S}$ denotes the set of representatives of conjugacy classes in $\mathcal{H}_{n_1}$ which map to the conjugacy class of γ_n in $\mathcal{H}_n$ under the canonical surjection. Since the order of the conjugacy class of any element in a finite group is the index of its centraliser in that group, and since the $\mathcal{H}_n$ are all p-groups, the index $|C_h|/|C_{\gamma_n}|$ is either 0 or 1, as an element of $\mathbb{F}_p$.

Taking $n_1 = n+1$, it follows that $\alpha_{\gamma_n} = 0$ unless there exists some element h_1 in $\mathcal{H}_{n+1}$ such that the conjugacy class of h_1 in $\mathcal{H}_{n+1}$ has the same order as that of γ_n in $\mathcal{H}_n$, and the coefficient α_{h_1} of C_{h_1} in ζ_{n+1} is non-zero. Furthermore, since the conjugacy class of h_1 surjects onto that of γ_n and since ζ_{n+1} is a sum of $C_{\gamma_{n+1}}$ we can replace h_1 with another representative of the $\mathcal{H}_{n+1}$-conjugacy class and so assume both that h_1 itself maps to γ_n and that the coefficient α_{h_1} of C_{h_1} in ζ_{n+1} is non zero as an element of $\mathbb{F}_p$.

Repeating, with γ_n replaced by h_1, we obtain a sequence of elements $h_i \in \mathcal{H}_{n+i}$ lifting γ_n such that 1) for all i the corresponding h_{i+1} maps to h_i under the map $\mathcal{H}_{n+i+1} \to \mathcal{H}_{n+i}$, 2) the conjugacy class of each h_i in the $\mathcal{H}_{n+1}$ has order $|C_{\gamma_n}|$, fixed independant of i and 3) the coefficient of C_{h_i} in ζ_{n+i} is a non zero element of $\mathbb{F}_p$. Since the h_i are compatible under the maps $\mathcal{H}_{n+i+1} \to \mathcal{H}_{n+i}$, the set $\{h_i\}$ gives an element in $H = \varprojlim \mathcal{H}_i$ which maps to γ_n in $\mathcal{H}_n$. Thus Proposition 4.2 follows from the next lemma, which shows that this is only possible if this element (and thus γ_n) is the identity in H (respectively $\mathcal{H}_n$). □

LEMMA 4.4. — *Let β be an element of H such that for each positive integer n its image, β_n, in $\mathcal{H}_n$ lies in a conjugacy class of order less than some fixed bound N, where N is independant of n. Then β is the identity element in H.*

Proof. — Since H contains no elements in a finite conjugacy class, other than the identity, it is sufficient to prove that β lies in a finite conjugacy class. But if not then there are at least $N+1$ distinct conjugates β^σ of β in H. The profinite topology on H is Hausdorff, with a basis of open normal subgroups which we can take to be the H_n as above, and so there exists some integer ℓ for which the β^σ have distinct images in $\mathcal{H}_\ell$. Since the β^σ are conjugate to β in H, their images all lie in the same conjugacy class as β_n in $\mathcal{H}_\ell$, which therefore must have order at least $N+1$ contradicting the hypothesis on β that the conjugacy classes of its images in all the $\mathcal{H}_n$ were of order bounded by N. □

DEFINITION. — A ring R is called a *polynomial identity ring* (*P.I. ring*) if there exists a polynomial f in the free algebra $\mathbb{Z}\langle x_1,\dots,x_n\rangle$ in n non commuting variables, for some n, such that $f(r_1,\dots,r_n)=0$ for all r_i in R. We then say that R *satisfies* f.

Then Proposition 4.2 has the following consequence:

COROLLARY 4.5. — *For H any open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$, G any open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$, none of $\Lambda(G)$, $\Lambda(H)$, $\mathbb{F}_p[[G]]$ or $\mathbb{F}_p[[H]]$ is a polynomial identity ring.*

Proof. — It is sufficient to show that $\mathbb{F}_p[[H]]$ is not a P.I. ring for H an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$, since if R is a P.I. ring, satisfying f, then so is any subring or quotient of R. By the Theorem in § 13.6.4 of [15], in a P.I. ring any non zero ideal has non zero intersection with the centre. But by the proof of Proposition 4.2 above, the only non zero elements in the centre of $\mathbb{F}_p[[H]]$ are invertible. Since the augmentation ideal, given by the kernel of the natural map $\mathbb{F}_p[[H]]\to\mathbb{F}_p$, is a non zero, proper ideal of $\mathbb{F}_p[[H]]$, it cannot contain an invertible element, and thus $\mathbb{F}_p[[H]]$ is not a P.I. ring. □

REMARK. — In fact, although the definition of a P.I. ring assumes f lies in $\mathbb{Z}\langle x_1,\dots,x_n\rangle$, for a ring upon which the action of $\mathbb{Z}$ extends to an action of $\mathbb{Z}_p$ no point in the proof of 13.6.4 of [15] fails if we only assume that f lies in a free $\mathbb{Z}_p$-algebra, $\mathbb{Z}_p\langle x_1,\dots,x_n\rangle$, for some n. Thus we can conclude that none of $\Lambda(G)$, $\Lambda(H)$, $\mathbb{F}_p[[G]]$ or $\mathbb{F}_p[[h]]$ satisfy a polynomial in $\mathbb{Z}_p\langle x_1,\dots,x_n\rangle$, for any n.

LEMMA 4.6. — *Assume that p is at least 3 and that G is a pro-p, open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ containing no element of order p. Then any element in the Iwasawa* *algebra of the centre of G which is a prime in that ring is also a prime in $\Lambda(G)$ and we have prime factorisation in the centre of $\Lambda(G)$. That is, any element of $\Lambda(Z(G))$ can be written as a product of primes.*

Proof. — The second statement is a well known property of $\mathbb{Z}[[T]]$, which has unique factorisation (see, for example, [3, § 5.2.5]). The first is clear from the isomorphism (49) in Lemma 4.1 above, together with the identification, in Proposition 4.2, of the centre of $\Lambda(G)$ as the completed group algebra of the centre of G. □

We have a full structure theorem for the central torsion submodule of any $\Lambda(G)$-module. If M is a finitely generated $\Lambda(G)$-module, denote by $M(Z(G))$ the set of elements of M which are annihilated by some element of the centre of $\Lambda(G)$. This is a $\Lambda(G)$-submodule, and the annihilator of any torsion element in $M/M(Z(G))$ contains no element in the centre of $\Lambda(G)$. Note that this does not imply that it is $\Lambda(H)$-torsion. Consider, for example, $\Lambda(G)/\{\Lambda(G)(\gamma - h)\}$, where γ is an element of the centre of G, h a non zero element of the subgroup H of G.

Theorem 4.7. — *Let G be a pro-p open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ for p at least 3 and such that G contains no element of finite order other than 1. Let M be a finitely generated $\Lambda(G)$-module. Then if we choose a topological generator γ of $Z(G)$ and make the identification $\Lambda(G) \cong \Lambda(H)[[T]]$ as in Lemma 4.1, there exists a finite set of elements $\{f_k\}_{k=1}^n$ of $\Lambda(H)[[T]]$ which are contained in the subring $\mathbb{Z}_p[[T]]$ and which are primes in this ring, such that there is a pseudoisomorphism*

$$M \longrightarrow \bigoplus_{k=1}^{n}\Big(\bigoplus_{j=1}^{r_k}\frac{\Lambda(H)[[T]]}{\langle f_k^{n_{j,k}}\rangle}\Big)\oplus\frac{M}{M(Z(G))}. \tag{56}$$

The ideal $\big\langle \prod\limits_{k,j} f_k^{n_{j,k}}\big\rangle$ is uniquely defined by M.

Proof. — This is an immediate translation of Theorem 2.5 to this situation, together with Lemma 4.6 showing that any element in the centre of $\Lambda(G)$ can be written as a product of central primes of $\Lambda(G)$. □

Remark. — It is well known that the set of prime ideals in $\mathbb{Z}_p[[T]]$ consists of the ideals (p) and (f), where f is an irreducible Weierstrass polynomial (see [16, Lemma 5.3.7]). Under the isomorphism of Lemma 4.1 this describes further the set $\{f_k\}_{k=1}^n$ appearing in the above theorem.

Example. — We conclude by applying the above theory to a concrete example of a module of interest, coming from the theory of elliptic curves. We will restrict to a single example with particularly nice properties.

Take E to be the elliptic curve $X_0(11)$ of conductor 11 defined over $\mathbb{Q}$ by a minimal Weierstrass equation:

$$E : y^2 + y = x^3 - x^2 - 10x - 20. \tag{57}$$

Fix p equal to 5 for the remainder, and G to be the Galois group of $\mathbb{Q}_\infty$ over $\mathbb{Q}(E_p)$, where E_p denotes the p torsion points of E, and $\mathbb{Q}_\infty$ is the field of definition of E_{p^∞}, the set of all p-power torsion points on E. Recall the p^∞-Selmer group of E over $\mathbb{Q}_\infty$, $\mathcal{S}_p(E/\mathbb{Q})$, is defined by the exactness of

$$0 \to \mathcal{S}_p(E/\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}_\infty, E_{p^\infty}) \longrightarrow \prod_\nu H^1(\mathbb{Q}_{\infty,\nu}, E), \tag{58}$$

where $\mathbb{Q}_{\infty,\nu}$ denotes the completion of $\mathbb{Q}_\infty$ at a place ν. For any discrete $\Lambda(G)$-module, D, we denote by $\widehat{D}$ its compact dual $\mathrm{Hom}_{\mathbb{Z}_p}(D, \mathbb{Q}_p/\mathbb{Z}_p)$ where '$\mathrm{Hom}_{\mathbb{Z}_p}$' here refers to continuous, $\mathbb{Z}_p$-module homomorphisms. We take X to be the compact $\Lambda(G)$-module $\widehat{\mathcal{S}_p(E/\mathbb{Q})}$.

The results in [13], in particular the final example at the end of § 3, show that p^2 divides $z(X)$. (The power of p is 2 because by Part I, § 8 of [14] our ground field $\mathbb{Q}(E_p)$ is in this case equal to $\mathbb{Q}(\mu_p)$, which is of course a degree 4 extension of $\mathbb{Q}$.) Recall that E is isogenous to $X_1(11)$ via a degree 5 isogeny. Let E' denote the elliptic curve $X_1(11)$, which is given by a Weierstrass equation:

$$E' : y^2 + y = x^3 - x^2. \tag{59}$$

Let $\mathcal{S}_p(E'/\mathbb{Q})$ denote the p^∞-Selmer group of E', defined as in (58), and X' denote its compact dual, $\widehat{\mathcal{S}_p(E'/\mathbb{Q})}$. Then it is shown in [5, Corollary 7.3], that X' is finitely generated over the subring $\Lambda(H)$ of $\Lambda(G)$, where $\Lambda(H)$ is the Iwasawa algebra of $H = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}^{\mathrm{cyc}})$. Here $\mathbb{Q}^{\mathrm{cyc}}$ denotes the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(E_p)$, equal in this case to $\mathbb{Q}(\mu_{p^\infty})$, the field obtained by adjoining all the p-power roots of unity to $\mathbb{Q}$.

By a well known theorem of Serre, since E does not have complex multiplication G embeds as an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. In fact, Lang and Trotter [14] have explicitly determined G in this case and shown it to be precisely the set of elements of $\mathrm{GL}_2(\mathbb{Z}_p)$ congruent to one modulo p. Denote this set by $\mathcal{G}$. Since, as remarked already, $\mathbb{F}_p[[G]]$ contains no zero divisors in this case, it follows that p is prime in $\Lambda(G)$, and we may apply the theory described in the preceding sections to this choice of central prime.

Let ϕ denote the isogeny:

$$\phi : E' \longrightarrow E.$$

It has degree 5. In order to further determine the structure of X upto pseudoisomorphism we consider the following diagram:

$$\begin{tikzcd} 0 \arrow[r] & X'(p) \arrow[r] & X' \arrow[r] & X'/X'(p) \arrow[r] & 0 \\ 0 \arrow[r] & X(p) \arrow[r] \arrow[u, "f"] & X \arrow[r] \arrow[u, "g"] & X/X(p) \arrow[r] \arrow[u, "h"] & 0 \end{tikzcd} \tag{60}$$

where the map g is the dual of the map $\mathcal{S}_p(E'/\mathbb{Q}) \to \mathcal{S}_p(E/\mathbb{Q})$ induced by ϕ. As explained in the proof of Theorem 3.1 of [13], since ϕ has degree 5 both the kernel and cokernel of g are annihilated by 5.

THEOREM 4.8. — *With notation as defined above, there exists a pseudoisomorphism as* $\Lambda(G)$*-modules*

$$X \longrightarrow \left(\frac{\Lambda(G)}{\langle 5\rangle}\right)^2 \bigoplus X'. \tag{61}$$

REMARK. — In fact, since it follows from a theorem of Ochi and Venjakob [18] that the compact dual of $\mathcal{S}_5(X_0(11)/\mathbb{Q}_\infty)$ contains no pseudonull submodules, this must be an injection. Furthermore from a slight modification of Corollaries 7.3 and 7.10 of [5], the $\Lambda(G)$-module X' is a finitely generated $\Lambda(H)$-module of rank 4. Finally, in [23, Lemma 1.5.18], Venjakob has shown that any $\Lambda(H)$-torsion in a $\Lambda(G)$-module which is finitely generated as a $\Lambda(H)$-module is in fact pseudonull, thus X' is $\Lambda(H)$-torsion free.

Proof. — First note that since all the modules on the top row of (60) are finitely generated over $\Lambda(H)$, so also are the cokernels of f, g and h. Furthermore, they are also annihilated by some power of p, from which it follows that they are pseudonull (Lemma 1.10 of [13] or 1.5.18 of [23]) as also is $X'(p)$. Since the kernel of g is p-torsion, it lies in $X(p)$ and thus equals the kernel of f. Thus by the snake lemma the kernel of h is pseudonull, and so h is a pseudoisomorphism. In [13] the μ-invariant of a finitely generated $\Lambda(G)$-module was defined by

$$\mu(M) = \sum_{i\geqslant 0} \operatorname{rank}_\Omega\bigl(p^i M(p)/p^{i+1}M(p)\bigr) \tag{62}$$

where $\Omega = \mathbb{F}_p[[G]]$. It was also shown that $\mu(X)$ equals 2 in this case (eqn. 102 of [13]). Since, by Proposition 1.9 of [13], for Λ-torsion modules the alternating sum of μ-invariants adds to zero along exact sequences, $\mu(X) = \mu(\mathrm{Ker}(g))$. This, together with the fact that $X'(p)$ is pseudonull and $\mathrm{Ker}(g)$ is annihilated by p ensures that the pseudoisomorphism implied by Proposition 2.2 is of the form

$$X \longrightarrow \left(\frac{\Lambda(G)}{\langle 5\rangle}\right)^2 \bigoplus \frac{X}{5\text{-tor}} \tag{63}$$

Composing with the pseudoisomorphism, h, and noting by the remark above that $X'(p)$ is zero, gives the theorem. □

We conclude by remarking that it seems extremely hard to elicit further information about the structure of $\mathcal{S}_5(X_1(11)/\mathbb{Q}_\infty)$ without more detailed knowledge of how the centre of G acts upon it. We also remark that it is not immediately clear that one can use the map in (61) directly to obtain any more than very weak asymptotic information for the structure of $\mathcal{S}_5(X_0(11)/\mathbb{Q}(E_{5^n}))$ as an Abelian group as n varies. The difficulty comes from the appearance of the pseudonull submodule appearing as the cokernel in (61) and about which we currently have little information. In the classical case for modules over the Iwasawa algebra of a group isomorphic to $\mathbb{Z}_p$, a module is pseudonull if and only if it is finite. In this case, if G_n denotes the Galois group of $\mathbb{Q}(E_{5^n})$ over $\mathbb{Q}(\mu_5)$ then the possible behaviour of the G_n-coinvariants of a general pseudonull submodule is unknown, beyond asymptotic upper bounds on the $\mathbb{Z}_p$-ranks as given originally by M. Harris in [12]. More direct approaches to understanding the behaviour of the 5-Selmer groups at these intermediate fields have, however, been considered directly in [5], [11] and [13].

BIBLIOGRAPHY

[1] Björk (J.-E.) – *Filtered Noetherian Rings*, in *Noetherian Rings and their Applications*, Math. Surv. Monogr., vol. 24, Oberwolfach/FRG, 1983, pp. 59–97.

[2] Boratynsky (M.) – *A Change of Rings Theorem and the Artin-Rees Property*, Proc. Amer. Math. Soc., t. **53** (1975), pp. 307–310.

[3] Bosch (S.), Guntzer (U.) & Remmert (R.) – *Non-Archimedean Analysis*, Grundlehren der mathematischen Wissenschaften, vol. 261, Springer Verlag, 1984.

[4] Brumer (A.) – *Pseudocompact Algebras, Profinite Groups and Class formations*, J. Algebra, t. **4** (1966), pp. 442–470.

[5] Coates (J.H.) & Howson (S.) – *Euler Characteristics and Elliptic Curves II*, J. Math. Soc. Japan, t. **53** (2001), no. 1, pp. 175–235.

[6] Coates (J.H.) & Sujatha (R.) – *Euler-Poincaré Characteristics of Abelian Varieties*, C. R. Acad. Sci. Paris Sér. I Math., t. **329** (1999), no. 4, pp. 309–313.

[7] ———, *Galois Cohomology of Elliptic Curves*, Lecture Notes at the Tata Institute of Fundamental Research, 2000.

[8] Coates (J.H.), Sujatha (R.) & Wintenberger (J-P.) – *On the Euler-Poincaré Characteristics of Finite Dimensional p-adic Galois Representations*, Publ. Math. IHES, t. **93** (2001), pp. 107–143.

[9] Cohn (P.M.) – *Algebra*, vol. 1, Wiley, 1993.

[10] Dixon (J.D.), duSautoy (M.P.F.), Mann (A.) & Segal (D.) – *Analytic pro-p groups*, 2$^{\text{nd}}$ ed., Cambridge Studies in Advanced Mathematics, vol. 61, C.U.P., 1999.

[11] HACHIMORI (Y.) & MATSUNO (K.) – *An Analogue of Kida's Formula for the Selmer Group of Elliptic Curves*, J. Alg. Geom., t. **8** (1999), pp. 581–601.

[12] HARRIS (M.) – *p-adic Representations Arising from Descent on Abelian Varieties*, Compositio Math., t. **39** (1979), no. 2, pp. 177–245.

[13] HOWSON (S.) – *Euler Characteristics as Invariants of Iwasawa Modules*, preprint to appear in Proc. London Math. Soc., 2002.

[14] LANG (S.) & TROTTER (H.) – *Frobenius Distributions in* GL_2*-extensions: Distribution of Frobenius automorphisms in* GL_2*-extensions of the Rational Numbers*, LNM, vol. 504, Springer Verlag, 1976.

[15] MCCONNELL (J.C.) & ROBSON (J.C.) – *Noncommutative Noetherian Rings*, Wiley-Interscience, 1987.

[16] NEUKIRCH (J.), SCHMIDT (A.) & WINGBERG (K.) – *Cohomology of Number Fields*, Grundlehren der mathematischen Wissenschaften, vol. 323, Springer Verlag, 2000.

[17] NEUMANN (A.) – *Completed group algebras without zero divisors*, Arch. Math., t. **51** (1988), pp. 496–499.

[18] OCHI (Y-H.) & VENJAKOB (O.) – *On the Structure of Selmer Groups over p-adic Lie Extensions*, J. Alg. Geom., t. **11** (2002), no. 3, pp. 547–580.

[19] SCHOLL (A.J.) & TAYLOR (R.L.), eds. – *Galois Representations in Arithmetic and Geometry*, L.M.S., C.U.P., 1998, Papers from the Durham Colloquium, 1996.

[20] SERRE (J-P.) – *Sur la dimension cohomologique des groupes profinis*, Topology, t. **3** (1965), pp. 413–420.

[21] ———, *La distribution d'Euler-Poincaré d'un groupe profini*, in *Galois Representations in Arithmetic and Geometry*, 1998, See [19].

[22] TOTARO (B.) – *Euler Characteristics for p-adic Lie Groups*, Publ. Math. IHES (1999), pp. 169–225.

[23] VENJAKOB (O.) – *Dissertation*, Ph.D. Thesis, Heidelberg, 2000.

[24] WEIBEL (C.A.) – *An Introduction to Homological Algebra*, Cambridge Studies in Advanced Mathematics, 38, C.U.P., 1994.