Note on Nakayama's Lemma For Compact Λ-modules.

By P.N. Balister and S. Howson.

1. Introduction.

We discuss here two results which are widely used in the study of compact $\Lambda(G)$ modules, where $\Lambda(G) = \mathbb{Z}_p[[G]] = \varprojlim \mathbb{Z}_p[G/U]$ for G a suitable profinite group, and the inverse limit is taken over open normal subgroups U of G. The first result is a simple condition for a compact $\Lambda(G)$ module X to be finitely generated, the proof of which is essentially known. We recently noticed, however, that there is a slight gap in the proof usually quoted e.g., in [4], even in the case where $G = \mathbb{Z}_p$. The proof seems to originate in [2] where X is assumed to be profinite. We show how to extend this result to cover a wide class of examples, including the case considered in [4].

The second result concerns an important condition for X to be $\Lambda(G)$ torsion in the case of Abelian G. Unfortunately, this condition does not generalise to all uniform G, as has erroneously been claimed in [1]. We discuss here why that is, and explain when it does hold.

We would particularly like to thank Marcus du Sautoy for his help, especially for the suggestion that the second result extends to some non-Abelian groups.

2. Motivation.

The main application of these results in number theory occurs in Iwasawa Theory, where one attempts to study arithmetic objects over an infinite tower of fields.

As an example, let E be an elliptic curve defined over a number field K and assume that p is a prime at which E has good ordinary reduction. Let E_{p^n} be the group of p^n-division points on E, and $E_{p^\infty} = \cup E_{p^n}$. Define fields $K_n = K(E_{p^n})$ and let $K_\infty = \cup K_n$. Let $G = \mathrm{Gal}(K_\infty/K)$ be the infinite Galois group with open subgroups $G_n = \mathrm{Gal}(K_\infty/K_n)$. We will assume that E has no complex multiplication, so, by a theorem of Serre's [3], G will be an open subgroup of finite index in $GL_2(\mathbb{Z}_p)$. The situation when E has complex multiplication is well understood, and we shall say no more about that here.

We can define Selmer groups $S(E/K)$, $S(E/K_n)$ and $S(E/K_\infty)$ of the elliptic curve as subgroups of $H^1(K, E_{p^\infty})$, $H^1(K_n, E_{p^\infty})$ and $H^1(K_\infty, E_{p^\infty})$ respectively, given by the usual local triviality conditions. It is natural to ask about the size of these groups. We are ultimately interested in Selmer groups over number fields, but it is also useful to study $S(E/K_\infty)$. There is a natural action of G on $S(E/K_\infty)$ which can be extended by continuity to an action of the completed group algebra $\Lambda(G) = \varprojlim \mathbb{Z}_p[G/G_n]$. ¿From knowing the structure of $S(E/K_\infty)$ as a $\Lambda(G)$ module, we then try to deduce information about the $S(E/K_n)$. We try to proceed as follows:-

- In most cases, it is possible to show that the natural restriction homomorphism $H^1(K, E_{p^\infty}) \to H^1(K_\infty, E_{p^\infty})^G$ induces a map $S(E/K) \to S(E/K_\infty)^G$ with *finite* kernel and cokernel, see [6]. If $\widehat{M}$ denotes the Pontjagin dual of a $\Lambda(G)$ module, M, then this means there is a map $\widehat{S(E/K_\infty)}_G \to \widehat{S(E/K)}$ with finite kernel and cokernel. Here M_G means the G coinvariants of a $\Lambda(G)$ module, M, that is the maximal quotient of M on which G acts trivially. It is given by M/IM, where I denotes the augmentation ideal of $\Lambda(G)$, i.e., the kernel of the natural map $\Lambda(G) \to \mathbb{Z}_p[G/G] = \mathbb{Z}_p$ which arises from the definition of $\Lambda(G)$ as an inverse limit.
- Use some analogue of Nakayama's Lemma to deduce results about X. There are two 'results' that we are interested in:-

(1) If X/IX is a finitely generated $\mathbb{Z}_p$ module then X is a finitely generated $\Lambda(G)$ module.
(2) If X/IX is a finite $\mathbb{Z}_p$ module then X is a torsion $\Lambda(G)$ module.

It is these statements that are the principal subject of this paper.

- We would then wish to prove some kind of 'control theorem' relating $\widehat{S(E/K_\infty)}_{G_n}$ and $\widehat{S(E/K_n)}$ as n varies. Here X_{G_n} denotes the maximal quotient of X on which G_n acts trivially. A result of this kind would allow us to use general properties about finitely generated $\Lambda(G)$ modules to analyse the behaviour of $\widehat{S(E/K_n)}$ as n varies. Such a result is proved by Harris in [1] and we will discuss this stage no further.

It is instructive to recall the classical example for which the above philosophy works. Let $\mathbb{Q}_\infty$ denote the cyclotomic $\mathbb{Z}_p$ extension of $\mathbb{Q}$, where we continue to assume that p is a prime at which E has good, ordinary reduction, and let $S(E/\mathbb{Q}_\infty)$ denote the Selmer group of E over $\mathbb{Q}_\infty$. If $S(E/\mathbb{Q})$ is finite (for example this is known, by a deep theorem of Kolyvagin, to be true for all primes p when E is modular and the L-function of E does not vanish at $s = 1$) the argument proves that $\widehat{S(E/\mathbb{Q}_\infty)}$ is a torsion module over the completed group algebra of $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. In [7], Mazur proves a control theorem for this case and shows that the rank of the group $E(F)$, of F-rational points of E, is bounded as F ranges over all finite extensions of $\mathbb{Q}$ contained in $\mathbb{Q}_\infty$.

We return now to the case discussed above, with $G = \mathrm{Gal}(K_\infty/K)$. Then result (1) still holds, but, as noted above, result (2) now fails. The consequence of this is that we do not have a single example, for any choice of E with no complex multiplication and for any prime p, where we can prove $\widehat{S(E/K_\infty)}$ is a torsion $\Lambda(G)$ module. Some 'examples' were given in [1] but they all depended on a false proof of the result (2) claimed there.

That paper also relates the conjecture that $\widehat{S(E/K_\infty)}$ is a torsion $\Lambda(G)$ module to the longstanding conjecture that $\widehat{S(E/\mathbb{Q}_\infty)}$ is torsion as a $\Lambda(\Gamma)$ module. This conjecture can be proved quite easily in some cases, and Kato has recently announced a proof for all modular E and all ordinary p. Details of this have not been published yet, however. Specifically, the claim in [1] is that under the hypotheses on E and p made above, $\widehat{S(E/K_\infty)}$ being torsion as a $\Lambda(G)$ module is equivalent to $\widehat{S(E/\mathbb{Q}_\infty)}$ being torsion as a $\Lambda(\Gamma)$ module. Unfortunately, the arguments relating the two are incorrect for the same reason that the proof there of result (2) fails.

We should point out that there are some other results in [1] which rely on result (2). Most notably, calculations of the $\Lambda(G)$ rank of the Galois group of the maximal Abelian pro-p extension of K_∞ over K_∞ where K_∞ is an extension of either $\mathbb{Q}$ or $\mathbb{Q}_p$, with Galois group a p-adic Lie group and G a uniform pro-p subgroup. Most of these results can be proved by other means however.

3. (1) Condition for X to be Finitely Generated.

Theorem. *Let Λ be a compact topological ring with 1 and let I be a (left) ideal with $I^n \to 0$ in Λ. Let X be a compact (Hausdorff) (left) Λ module and assume either that X is profinite, or that condition (B) below holds. If $IX = X$ then $X = 0$.*

Corollary. *Let Λ, X and I be as above. If X/IX is finitely generated as a Λ/I module then X is finitely generated as a Λ module.*

Proof (assuming Theorem).
Lift any finite set of generators of X/IX to X so that $X/IX = (\Lambda/I)x_1 + \cdots + (\Lambda/I)x_s$ with $x_i \in X$. Define $Y = \Lambda x_1 + \cdots + \Lambda x_s$. Since Y is a continuous image of a compact set, it is closed in X and so

X/Y is both compact and Hausdorff. By construction $I(X/Y) = (IX+Y)/Y = X/Y$, so $X/Y = 0$ and $X = Y$ is finitely generated. □

Proof of Theorem.
Assume $X \neq 0$ and let U be an open neighbourhood of 0 in X with $U \neq X$. Let $x \in X$. By continuity of the action of Λ, there exists a neighbourhood U_x of x in X such that for sufficiently large n, $I^n.U_x = \{ab : a \in I^n, b \in U_x\} \subseteq U$. Since X is compact, we can cover X with finitely many U_x, and so obtain $I^n.X = \{ab : a \in I^n, b \in X\} \subseteq U \subset X$ for some n. Now $IX = X$, so by induction $I^nX = X$. We wish to obtain a contradiction from $I^n.X \subseteq U \neq X$. Unfortunately, the IX in the statement of the lemma is not the set theoretic product of I and X, but is the submodule generated by products, $IX = \{\sum a_ib_i : a_i \in I, b_i \in X\}$ and so $I^nX = \{\sum a_ib_i : a_i \in I^n, b_i \in X\}$ is not the same as $I^n.X$ in general. To proceed we must make some additional assumptions.

(A) Strengthen the condition on X:- Assume X is profinite.

In this case we can take U to be an open subgoup under addition, and so $I^n.X \subseteq U$ implies $I^nX \subseteq U$. Also note that in the corollary, the quotient of a profinite group by a closed subgroup is still profinite.

This condition was assumed in [2]. It holds in the case of the Selmer groups since these are subsets of cohomology groups which are direct limits of finite groups. The duals are therefore profinite.

(B) Strengthen the condition on I:- Assume that we are given a descending chain of (left) ideals I_n such that $I_n = \langle f_{1,n}, \ldots, f_{d,n}\rangle$ are finitely generated by a fixed number of generators independent of n, also assume that $I_n \to 0$ and that for all n there exists an N with $I^N \subseteq I_n$.

In this case replace U in the above argument with V, an open neighbourhood of 0 in X such that $V + V + \cdots + V \subseteq U \subset X$, where there are d terms in the sum. Such a V exists by continuity of addition in X. Since $I_n \to 0$ as $n \to \infty$, for sufficiently large n $I_n.X \subseteq V$ by the argument above. Now $I^NX \subseteq I_nX = f_{1,n}X + \ldots f_{d,n}X \subseteq I_n.X + \ldots + I_n.X \subseteq V + \ldots + V \subseteq U \subset X$. The result then follows. □

We now note two cases where condition (B) is known to hold.

(B1) Λ is commutative and I is finitely generated.

If $I = \langle f_1, \ldots, f_d\rangle$, write $I_n = \langle f_1^n, \ldots, f_d^n\rangle$ and note that $I^{d(n-1)+1} \subseteq I_n \subseteq I^n$.

(B2) $\Lambda = \Lambda(G)$ with G a topologically finitely generated powerful pro-p group and I any proper ideal.

A pro-p group G is said to be *powerful* if the commutator subgroup $[G,G]$ is contained in the closure of the subgroup G^p generated by pth powers of elements of G (or G^4, 4th powers, in the case $p = 2$). ¿From now on we will abbreviate 'topologically finitely generated powerful pro-p' to 'f.g. powerful'. The result follows from the following basic facts known in this case (see [5]).

Facts about f.g. powerful groups.

a. *G is topologically finitely generated. Write $\{a_1, \ldots, a_d\}$ for a generating set.*

b. *G has a decreasing sequence of normal open subgroups G_n where G_n is topologically generated by $\{a_1^{p^{n-1}}, \ldots, a_d^{p^{n-1}}\}$.*

c. *There exist constants c, d such that for sufficiently large n, $(G : G_n) = p^{dn+c}$. Write $d = \dim G$.*

d. *Let I_n be the kernel of the projection map $\Lambda(G) \to (\mathbb{Z}_p/p^n\mathbb{Z}_p)[G/G_n]$. Then I_n is generated as a $\Lambda(G)$ module by $\{b_{0,n}, \ldots, b_{d,n}\}$ where $b_{0,n} = p^n$ and $b_{i,n} = a_i^{p^{n-1}} - 1$ for $1 \le i \le d$.*

e. *I_1 is the (unique) maximal ideal of $\Lambda(G)$.*

f. *Both $\{I_n\}$ and $\{I_1^n\}$ form a base of neighbourhoods of 0 in $\Lambda(G)$. In particular, for all n there exists an N with $I_1^N \subseteq I_n \subseteq I_1^n$.*

Note that any proper ideal I will be contained in I_1 and so $I^N \subseteq I_n$.

4. (2) Condition for X to be Λ-torsion.

We now consider the stronger version of Nakayama's lemma. Let $I = \operatorname{Ker}(\Lambda(G) \to \mathbb{Z}_p)$ be the augmentation ideal of $\Lambda = \Lambda(G)$. It is well known that, in the case of $G = \mathbb{Z}_p$ and with X as above, if X/IX is finite then X is actually a torsion Λ module. This is immediate from the structure theorem for Λ modules that we have in this case. This result does not, however, extend to other pro-p groups in general.

We first note that the concept of a torsion module is only useful when Λ has no zero divisors. In order to ensure this, we will assume that G is a uniform pro-p group. G is said to be *uniform* if it is a f.g. powerful group in which the orders of the finite p-groups G_n/G_{n+1} are constant, independent of n. The following facts are known (see [5]).

Facts about uniform groups.

a. *If G is a f.g. powerful group then the following are equivalent, (a) G is uniform, (b) G has no p torsion elements and (c) the map $g \mapsto g^p$ is injective.*

b. *Any f.g. powerful group contains an open subgroup that is uniform.*

c. *Any p-adic analytic group contains an open subgroup that is uniform.*

d. *If G is uniform then $\Lambda(G)$ has no zero divisors.*

e. *If X is a finitely generated $\Lambda(G)$ module, then there exists a map $X \to \Lambda(G)^r$ with both kernel and cokernel $\Lambda(G)$ torsion. The integer r is uniquely defined and called the* rank *of X.*

We will show that, for a uniform group G, result (2) holds if and only if G is soluble. First we will prove some general results about f.g. powerful groups.

Proposition. *Let G be a f.g. powerful group.*

(1) *If H is a closed normal subgroup of G then G/H is a f.g. powerful group and $\dim(G/H) \leq \dim G$ with equality if and only if H is finite.*

(2) *If G is not soluble, there exists a closed normal subgroup $H \neq 1$ with $H/\overline{[H,H]}$ finite.*

(3) *If G is uniform, soluble and non-trivial, there exists a closed normal subgroup H isomorphic to $\mathbb{Z}_p^r$ for some $r > 0$ and with G/H a soluble uniform group with $\dim G/H < \dim G$.*

Proof.
(1) The fact that G/H is f.g. powerful is clear from the definition of a f.g. powerful group.

$$(G\colon G_n) = (G\colon G_nH)(G_nH\colon G_n) = (G/H\colon (G/H)_n)(H\colon H \cap G_n).$$

So for some constant c and sufficiently large n, $(H\colon H \cap G_n) = p^{(\dim G - \dim(G/H))n + c}$.
But $(H\colon H \cap G_n) \geq 1$ and $(H\colon H \cap G_n) \to \infty$ if and only if H is infinite (recall $\cap G_n = 1$). The result follows.
(2) Let $G^{(0)} = G$ and $G^{(n+1)} = \overline{[G^{(n)}, G^{(n)}]}$. Since G is not soluble, $G^{(n)} \neq 1$. If $G^{(n)}/G^{(n+1)}$ is infinite then $\dim G/G^{(n+1)} > \dim G/G^{(n)}$ by part (1), but $\dim G/G^{(n+1)}$ is bounded by $\dim G$, so eventually $G^{(n)}/G^{(n+1)}$ must be finite. Let $H = G^{(n)}$ so that $H \neq 1$ and $H/\overline{[H,H]}$ is finite.

(3) In this case there exists an n with $G^{(n+1)} = 1$ and $G^{(n)} \neq 1$, so $N = G^{(n)}$ is an Abelian normal subgroup of G. Let $H = \{g \in G : g^{p^n} \in N \text{ for some } n\}$. We will show that H is also an Abelian normal subgroup of G. If $x, y \in H$ with $x^{p^n}, y^{p^n} \in N$ then $(x^{p^n} y x^{-p^n})^{p^n} = x^{p^n} y^{p^n} x^{-p^n} = y^{p^n}$. Since the map $g \mapsto g^p$ is injective, $x^{p^n} y x^{-p^n} = y$. Thus $(y^{-1}xy)^{p^n} = y^{-1} x^{p^n} y = x^{p^n}$ and so similarly $y^{-1}xy = x$. Therefore $xy = yx$ and $(xy)^{p^n} = x^{p^n} y^{p^n} \in N$ and $xy \in H$, from which it follows that H is an Abelian subgroup of G. It is normal since $(gxg^{-1})^{p^n} = gx^{p^n}g^{-1} \in N$ and so $gxg^{-1} \in H$. We know that G, and hence all $G^{(n)}$, are topologically finitely generated pro-p groups. Also G, and hence H, has no p torsion. Therefore H is isomorphic to $\mathbb{Z}_p^r$ for some $r > 0$. By part (1), G/H is a f.g. powerful group with $\dim G/H < \dim G$. Since G/H has no p torsion, it must also be uniform. □

Theorem. *If G is a non-soluble uniform pro-p group then result (2) fails. In particular we can find a non-trivial ideal J of $\Lambda(G)$ with J/IJ finite.*

Proof.
Let H be as in part (2) of the proposition. Let $I(H)$ denote the augmentation ideal of $\Lambda(H)$ considered as a subgroup of $\Lambda(G)$. Consider the map $\phi : H \to I(H)$ given by $\phi(g) = g - 1$. Then

$$\phi(ghg^{-1}h^{-1}) = (gh - hg)h^{-1}g^{-1} = ((g-1)(h-1) - (h-1)(g-1))h^{-1}g^{-1} \in I(H)^2$$

(note that h and g are invertible elements of $\Lambda(H)$). ϕ therefore induces a map $\bar{\phi} : H/\overline{[H,H]} \to I(H)/I(H)^2$, and it easy to see that this is a group homomorphism. The image of this map is both compact and dense, so $\bar{\phi}$ is surjective and $I(H)/I(H)^2$ is finite. But the map

$$I(H)/I(H)^2 \to (I(H) + II(H))/II(H) = \Lambda I(H)/I\Lambda I(H)$$

is clearly well defined and surjective ($I(H) \subseteq I$). So if we take $J = \Lambda I(H)$, J/IJ is finite. But J is an ideal of Λ, and Λ has no zero divisors, so J is not torsion. □

As an example, it is easy to check that if $H_i = \{x \in SL_n(\mathbb{Z}_p) : x \equiv 1 \mod p^i\}$ is the ith congruence kernel of $SL_n(\mathbb{Z}_p)$ and if $i \geq 1$ and $p \geq 3$, then $[H_i, H_i] = H_{2i}$ and has finite index in H_i. Result (2) will then fail for any uniform G containing one of these groups. In particular it fails for uniform open subgroups of $GL_n(\mathbb{Z}_p)$, e.g., congruence subgroups of the form $\{x \in GL_n(\mathbb{Z}_p) : x \equiv 1 \mod p^i\}$ for $i \geq 1$, $p \geq 3$.

Theorem. *If G is a soluble uniform pro-p group then result (2) holds. I.e., if X is a compact (Hausdorff) Λ module and X/IX is finite then X is a torsion $\Lambda(G)$ module.*

Proof.
Proceed by induction on $\dim G$. The case $G = 1$ is trivial, so let H be as in part (3) of the proposition, and assume the result holds for G/H. Let X be a compact $\Lambda = \Lambda(G)$ module with X_G finite. By the results of section 1, X is finitely generated. Hence there is a map $X \to \Lambda^r$ with torsion kernel and cokernel. If X is not torsion then $r > 0$ and hence, by projecting onto any factor of Λ^r, there is a non-trivial map $\phi : X \to \Lambda$. Let $J = \Lambda I(H) = I(H)\Lambda$ be the two-sided ideal of Λ generated by the augmentation ideal $I(H)$ of $\Lambda(H)$. (H is normal in G). Since $\cap J^n = \{0\}$, there exists an $n \geq 0$ such that $\phi(X) \subseteq J^n$, but $\phi(X) \nsubseteq J^{n+1}$. Then $X' = (\phi(X) + J^{n+1})/J^{n+1}$ is a non-trivial submodule of $F = J^n/J^{n+1}$. F is invariant under H, so both X' and F are $\Lambda(G/H)$ modules. X' is a quotient of X, so $X'_{G/H} = X'_G$ is a quotient of X_G and hence finite. Since the result holds for G/H, X' must be a non-trivial torsion $\Lambda(G/H)$ module. We will show that F is a free $\Lambda(G/H)$ module, which will give the required contradiction.
$J = \Lambda I(H) = \Lambda \otimes_{\Lambda(H)} I(H)$, so $J^n/J^{n+1} = \Lambda \otimes_{\Lambda(H)} I(H)^n/I(H)^{n+1}$. Since $\Lambda \otimes_{\Lambda(H)} \mathbb{Z}_p = \Lambda(G/H)$, it is enough to show that $I(H)^n/I(H)^{n+1}$ is a free $\mathbb{Z}_p$ module (with trivial H action). The triviality

of the H action follows from the fact that $I(H)^n/I(H)^{n+1} = I(H)_H$. The $\mathbb{Z}_p$ module stucture can be obtained using the isomorphisms $H \cong \mathbb{Z}_p^r$ and $\Lambda(H) \cong \mathbb{Z}_p[[T_1, \ldots, T_r]]$. $I(H)$ corresponds to the ideal $(T_1, \ldots, T_r)$, and $I(H)^n/I(H)^{n+1} \cong \bigoplus_{\sum a_i = n} T_1^{a_1} \ldots T_r^{a_r} \mathbb{Z}_p$ is a free $\mathbb{Z}_p$ module. □

References.

[1] M. Harris, *P-adic representations arising from descent on Abelian Varieties.* Harvard PhD Thesis 1977, also Comp. Math. **39** (1979), 177–245.

[2] J-P. Serre, *Classes des Corps Cyclotomiques (d'après K.Iwasawa).* Séminaire Bourbaki **174** 1958/59. Also, Collected Papers, volume I, no. 41.

[3] J-P. Serre, *Propriétés Galoisiennes des Points d'order Fini des Courbes Elliptiques.* Invent Math **15** 1972, 259–331. Also, Collected Papers, volume III, no. 94.

[4] L. Washington. *Introduction to Cyclotomic Fields.* Springer-Verlag GTM **83**.

[5] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p Groups.* LMS Lecture Notes **157** CUP. + 2nd edition, in preparation.

[6] J.H. Coates and S. Howson, *Euler Characteristics and Elliptic Curves.* To appear in The proceedings of the National Academy of Sciences.

[7] B. Mazur, *Rational Points of Abelian Varieties with Values in Towers of Number Fields.* Invent Math **18** 1972, 183–266.