ASIAN J. MATH..
Vol. 1, No. 2, pp. 224–229, June 1997

NOTE ON NAKAYAMA'S LEMMA FOR COMPACT Λ-MODULES*

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,

*Received February 26, 1997; accepted for publication April 9, 1997.
†Department of Pure Mathematics and Mathematical Statistics, 16 Mill Lane, Cambridge CB21SB, United Kingdom (balister@pmms.cam.ac.uk, S.Howson@pmms.cam.ac.uk).