Math. Res. Lett. **14** (2007), *no.* 5, 769–773

ASYMPTOTICS OF COINVARIANTS OF IWASAWA MODULES UNDER NON-NORMAL SUBGROUPS

Jordan S. Ellenberg and Adam Logan

Let G be a pro-p p-adic analytic group, thought of as a closed subgroup of $GL_N(\mathbb{Z}_p)$, and let Σ be a closed subgroup of G. Write Λ for the completed group algebra $\mathbb{Z}_p[[G]]$ and let M be a finitely generated Λ-module. Let $G = G^0 \supset G^1 \supset G^2 \supset \ldots$ be the descending sequence of principal congruence subgroups of G; write G_n for the finite quotient G/G^n. and Σ_n for the image of Σ in G_n. Write M_n for the coinvariant quotient of M under G^n. Then M_n is a module for the group algebra $\mathbb{Z}_p[G_n]$.

In Iwasawa theory, one often finds that the growth of arithmetic invariants of interest (e.g. class numbers, Mordell-Weil ranks) is controlled by a Λ-module M. In particular, the growth can be related to the $\mathbb{Z}_p$-ranks of the coinvariant quotients of M by various subgroups of G. Understanding these quotients is a purely algebraic problem. For instance, Harris [3, Theorem 1.10] shows that, if M is a Λ-torsion module,

$$\operatorname{rank}_{\mathbb{Z}_p} M_n = O(p^{n(\dim G - 1)}). \tag{1}$$

Note that if M is replaced by a free module of rank 1, we have

$$\operatorname{rank}_{\mathbb{Z}_p} \Lambda_{G^n} = |G_n| \sim p^{n \dim G}.$$

So one can read Harris's result as saying "the coinvariants of a torsion Λ-module by congruence subgroups grow more slowly than do the coinvariants of a free Λ-module." The goal of the present paper is to show a similar result for subgroups which are in some sense "far from normal." As corollaries, we show that induced modules are often faithful in the sense of Venjakob [7] and we give an upper bound for the growth of Mordell-Weil ranks of elliptic curves over certain non-Galois towers of field extensions.

Definition 1. We say $\Sigma \subset G$ is *eccentric* if

$$\lim_{n\to\infty} \frac{|\Sigma_n \backslash G_n / \Sigma_n|}{|G_n||\Sigma_n|^{-2}p^n} = 0.$$

Example 2. Suppose $G = K \rtimes \Sigma$, where K is isomorphic to $\mathbb{Z}_p^r$ and Σ to $\mathbb{Z}_p$. Then Σ is eccentric precisely when the action of Σ on K does not factor through a finite quotient of Σ.

Remark 3. It seems likely that the limit

$$\lim_{n\to\infty} \frac{\log |\Sigma_n \backslash G_n / \Sigma_n|}{n \log p}$$

Received by the editors July 8, 2006.

exists and is a non-negative integer, though this seems a bit complicated to prove. When this limit is an integer, it seems interesting to ask whether it is a “dimension” associated to the pair (G, Σ) in any cohomological sense.

Remark 4. The condition of eccentricity, as we have written it, depends on the structure of G as a subgroup of $GL_N(\mathbb{Z}_p)$; in fact, though we will not need this here, the condition is intrinsic to (G, Σ) and can be computed using the p-lower central series in place of the descending series of congruence subgroups.

We will prove the following theorem.

Theorem 5. *Let G be a pro-p p-analytic group with no p-torsion, and let M be a finitely generated torsion module for $\Lambda = \mathbb{Z}_p[[G]]$. Let Σ be an eccentric subgroup of G. Then*

$$\lim_{n\to\infty} \frac{\operatorname{rank}_{\mathbb{Z}_p}(M_n)_\Sigma}{\operatorname{rank}_{\mathbb{Z}_p}\Lambda(G)_{G^n\Sigma}} = 0.$$

Recall that a Λ-module M is called *faithful* if $\operatorname{Ann}_\Lambda M = 0$. When Λ is abelian, a torsion module cannot be faithful. By contrast, in the non-abelian cases, faithful torsion Λ-modules are quite prevalent; indeed they are ubiquitous among Λ-modules arising in arithmetic applications. Many examples of faithful torsion Λ-modules were constructed by Venjakob in [7]; for instance, he shows there that if G is a non-abelian semidirect product $K \rtimes \Sigma$ with $K \cong \Sigma \cong \mathbb{Z}_p$, then the induced module $\operatorname{Ind}_\Sigma^G \mathbb{Z}_p$ is a faithful Λ-module [7, Prop. 4.2]. In another example, he shows that if G is a pro-p subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$, and Σ is a maximal torus, then $\operatorname{Ind}_\Sigma^G \mathbb{Z}_p$ is again a faithful Λ-module. The following corollary generalizes these examples.

Corollary 6. *Let G be as above and let Σ be an eccentric subgroup. Then*

$$\operatorname{Ann}_\Lambda \operatorname{Ind}_\Sigma^G \mathbb{Z}_p$$

is trivial.

Proof. Suppose $A = \operatorname{Ann}_\Lambda \operatorname{Ind}_\Sigma^G \mathbb{Z}_p$ is nontrivial. Equivalently, the nonzero two-sided ideal A is contained in the left augmentation ideal ΛI_Σ^I. Since Λ is isomorphic to its opposite algebra, there is a nonzero two-sided ideal B contained in the right augmentation ideal $I_\Sigma^r\Lambda$. Now take M to be the torsion module Λ/B. Then

$$M_{G^n\Sigma} = \Lambda/(B + I_\Sigma^r\Lambda + I_{G^n}) = \Lambda/(I_\Sigma^r\Lambda + I_{G^n}) = \Lambda(G)_{G^n\Sigma}$$

which contradicts Theorem 5. □

Remark 7. Venjakob also proves that certain modules for the completed group algebra $\mathbb{F}_p[[G]]$ have trivial annihilator. The method of the present paper does not work in characteristic p; it is an interesting question whether the analogue of Theorem 5 still holds.

Remark 8. When Σ is trivial, Theorem 5 follows from the theorem of Harris cited above. Note also that some form of the eccentricity hypothesis on Σ is certainly necessary: if Σ is normal, for instance, then $\mathbb{Z}_p[[G/\Sigma]]$ is a torsion Λ-module whose coinvariants are identical with those of the free module Λ.

Remark 9. Eccentricity of Σ implies that $\dim \Sigma \leq (1/2) \dim G$. If $\dim \Sigma$ is any larger, it is not clear that any version of Theorem 5 can hold. Indeed, it is an interesting open question whether $\mathrm{Ind}_\Sigma^G \mathbb{Z}_p$ is faithful in this case. This question seems substantially harder; in particular, it does not seem likely that it can be resolved by consideration of representation theory in characteristic 0, as in the present paper.

We now prove Theorem 5.

Proof. We know M is finitely generated, which is to say M is a quotient of Λ^C for some integer C; it follows that M_n is a quotient of $\mathbb{Z}_p[G_n]^C$. Write $M_n^{\mathbb{Q}}$ for $M_n \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then $\mathrm{Hom}_{G_n}(M_n^{\mathbb{Q}}, M_n^{\mathbb{Q}})$ is a quotient of $\mathrm{Hom}_{G_n}(M_n^{\mathbb{Q}}, \mathbb{Q}_p[G_n]^C)$, which has dimension $C \dim_{\mathbb{Q}_p} M_n^{\mathbb{Q}}$. Now by (1) we know

$$\dim_{\mathbb{Q}_p} \mathrm{Hom}_{G_n}(M_n^{\mathbb{Q}}.M_n^{\mathbb{Q}}) \leq Cp^{n \dim G - n} \sim C|G_n|p^{-n} \tag{2}$$

On the other hand, if $[G_n/\Sigma_n]$ is the permutation representation of G_n on the cosets of Σ_n (with $\mathbb{Q}_p$-coefficients) then

$$\dim_{\mathbb{Q}_p} \mathrm{Hom}_{G_n}([G_n/\Sigma_n], [G_n/\Sigma_n]) = |\Sigma_n \backslash G_n / \Sigma_n|. \tag{3}$$

Now $\mathrm{rank}_{\mathbb{Z}_p} M_n^{\Sigma_n}$ is precisely $\dim_{\mathbb{Q}_p} \mathrm{Hom}_{G_n}([G_n/\Sigma_n], M_n^{\mathbb{Q}})$. It follows from (2), (3), and the Cauchy-Schwarz inequality that

$$\dim_{\mathbb{Q}_p} \mathrm{Hom}_{G_n}([G_n/\Sigma_n], M_n^{\mathbb{Q}}) \leq (C|\Sigma_n \backslash G_n/\Sigma_n||G_n|p^{-n})^{1/2}$$

and the hypothesis that Σ is eccentric tells us exactly that the right hand side is $o(|G_n||\Sigma_n|^{-1})$.

Since $\mathrm{rank}_{\mathbb{Z}_p} \Lambda(G)_{G^n\Sigma}$ is precisely $|G_n||\Sigma_n|^{-1}$, we are done. □

Remark 10. We do not expect the given upper bound on $\mathrm{rank}_{\mathbb{Z}_p} M_n^{\Sigma}$ to be sharp, because the inequality

$$\dim_{\mathbb{Q}_p} \mathrm{Hom}_{G_n}(M_n^{\mathbb{Q}}, M_n^{\mathbb{Q}}) \leq \dim_{\mathbb{Q}_p} \mathrm{Hom}_{G_n}(M_n^{\mathbb{Q}}, \mathbb{Z}_p[G_n]^C)$$

is typically not sharp.

We conclude with an application to ranks of elliptic curves over towers of function fields. Let p be a rational prime, k a field of characteristic prime to $6p$, C a smooth (but not necessarily proper) geometrically integral curve over k, and $\pi : \mathcal{E} \to C$ a non-isotrivial elliptic surface with good reduction at all points of C. Suppose furthermore that the image of the absolute Galois group of $k(C)$ on $\mathcal{E}[p^\infty]$ has image a pro-p principal congruence subgroup G of $\mathrm{GL}_2(\mathbb{Z}_p)$. (This can be arranged by replacing C with a finite cover, as long as $\mathbb{G}_m[p^\infty](k)$ is finite.)

Now let P be an element of the Tate module $T_p\mathcal{E}$, and let V be a pro-cyclic subgroup of $T_p\mathcal{E}$ not containing P. Then let $k(C_n)$ be the minimal extension of $k(C)$ over which the projections of P and V to $T_p\mathcal{E}/p^nT_p\mathcal{E}$ are defined, and let C_n be the nonsingular curve with function field $k(C_n)$. Let $k(C_\infty)$ be the union of all the $k(C_n)$. Then $k(C_\infty)$ is an extension of $k(C)$, whose splitting field $k(C'_\infty)$ has Galois group G. (Note that $k(C'_\infty)$ is obtained from $k(C_\infty)$ by extending the constant field to include μ_{p^∞}.) Write G^n for the nth principal congruence subgroup of G, and $\Sigma \subset G$ for the subgroup whose fixed field is $k(C_\infty)$. Then Σ is the 1-dimensional subgroup of G consisting of diagonal matrices fixing $P \in T_pE$. It is easy to check that Σ is eccentric in G—-indeed $|\Sigma_n \backslash G_n/\Sigma_n| = O(p^{2n})$.

Now let $\pi_{\mathcal{A}} : \mathcal{A} \to C$ be a non-isotrivial elliptic surface over $k(C)$ with good reduction on C (for instance, $\mathcal{A}$ might be $\mathcal{E}$ itself.) A theorem of Shioda [4] shows that $\operatorname{rank}_{\mathbb{Z}} \mathcal{A}(k(C_n))$ is $O(p^{3n})$. Several papers (such as [2],[5],[6]) have shown that in many pro-p towers of curves, the Shioda bound can be substantially improved, but it does not seem that the methods there apply immediately to this case. However, Theorem 5 allows us to give a non-trivial upper bound for the growth of the rank of $\mathcal{A}$.

Corollary 11. *The Mordell-Weil rank of $\mathcal{A}$ over $k(C_n)$ is $o(p^{3n})$.*

Proof. Let $j : \eta \hookrightarrow C$ be the inclusion of the generic point, and write $\mathcal{F}$ for the sheaf $j_* j^* R^1(\pi_{\mathcal{A}})_* \mathbb{Q}_p/\mathbb{Z}_p$. Then we denote by $\mathcal{S}(C, \mathcal{A}[p^\infty])$ the Selmer group $H^1(C \times_k k^s, \mathcal{F})$ of $\mathcal{A}/C$, as in [2, §2]. Then $\operatorname{rank}_{\mathbb{Z}} \mathcal{A}(k(C)) \leq \operatorname{corank}_{\mathbb{Z}_p} \mathcal{S}(C, \mathcal{A}[p^\infty])^{\operatorname{Gal}(k^s/k)}$. We also write $\mathcal{S}(C_\infty, \mathcal{A}[p^\infty])$ for the direct limit of $H^1(C_i \times_k k^s, \mathcal{F})$ as C_i ranges over the curves between C and C_∞. Write K for the kernel of the determinant map in G, and K^n for $K \cap G^n$. Then $C_n \times_k k^s \to C_0 \times_k k^s$ is a Galois cover with group K/K^n.

For each n, we have a map

$$\mathcal{S}(C_n, \mathcal{A}[p^\infty]) \to \mathcal{S}(C_\infty, \mathcal{A}[p^\infty])^{K^n}$$

whose kernel is $H^1(K^n, \mathcal{A}[p^\infty](k^s(C_\infty)))$.

The coefficient module $\mathcal{A}[p^\infty](k^s(C_\infty))$ has $\mathbb{Z}_p$-corank at most 2, and the congruence subgroup K^n, being a uniform group of rank 3, is generated by 3 elements. It follows that $H^1(K^n, \mathcal{A}[p^\infty](k^s(C_\infty)))$ has $\mathbb{Z}_p$-corank at most 6. So the kernel of

$$\mathcal{S}(C_n, \mathcal{A}[p^\infty])^{\operatorname{Gal}(k^s/k)} \to (\mathcal{S}(C_\infty, \mathcal{A}[p^\infty])^{K^n})^{\operatorname{Gal}(k^s/k)}$$

also has $\mathbb{Z}_p$-corank at most 6. Now $N := \mathcal{S}(C_\infty, \mathcal{A}[p^\infty])^{\operatorname{Gal}(k^s/k(\mu_{p^\infty}))}$ is a module for $\Lambda(G)$; it is cofinitely generated when considered as a $\Lambda(K)$-module by [2, Prop. 3.3], which immediately implies that it is a cofinitely generated cotorsion $\Lambda(G)$-module – see for instance [1, Prop 2.3]. Now

$$\operatorname{rank}_{\mathbb{Z}} \mathcal{A}(k(C_n)) \leq \operatorname{corank}_{\mathbb{Z}_p} \mathcal{S}(C_n, \mathcal{A}[p^\infty])^{\operatorname{Gal}(k^s/k)} \leq \operatorname{corank}_{\mathbb{Z}_p} N^{\Sigma K^n} + 6.$$

Take M to be the finitely generated torsion Λ-module dual to N. Now

$$\operatorname{corank}_{\mathbb{Z}_p} N^{\Sigma K^n} = \operatorname{rank}_{\mathbb{Z}_p} M_{\Sigma K^n} = o(p^{3n})$$

by Theorem 5, and we are done. □

Indeed, the proof of Theorem 5 shows in this case that $\operatorname{rank}_{\mathbb{Z}}(\mathcal{A}(k(C_n)))$ is bounded above by a constant multiple of $(|\Sigma_n \backslash G_n/\Sigma_n||G_n|p^{-n})^{1/2}$, which is $O(p^{5n/2})$.

Acknowledgments

The first author was partially supported by NSF-CAREER Grant DMS-0448750 and a Sloan Research Fellowship; the second author was supported by an Awards to Newly Appointed Lecturers grant from the Nuffield Foundation and by MSRI in the context of their program on rational and integral points on higher-dimensional varieties during part of the preparation of this work. We are grateful to the CRM in Montreal and to MSRI for their hospitality.

References

[1] J. Coates, T. Fukaya, K. Kato, R.Sujatha, O. Venjakob, *The* GL_2 *main conjecture for elliptic curves without complex multiplication*, Publ. Math. Inst. Hautes Études Sci. No. 101, (2005), 163–208.

[2] J. S. Ellenberg, *Selmer groups and Mordell-Weil groups of elliptic curves over towers of function fields*, Compos. Math. **142** (2006), no. 5, 1215–1230.

[3] M. Harris, *Correction to: "p-adic representations arising from descent on abelian varieties*, Compositio Math. **121** (2000), no. 1, 105–108.

[4] T. Shioda, *Some remarks on elliptic curves over function fields.* Astérisque (1992), No. 209, 12, 99–114.

[5] J. Silverman, *A bound for the Mordell-Weil rank of an elliptic surface after a cyclic base extension*, J. Algebraic Geom. **9** (2000), no. 2, 301–308.

[6] ———, *The rank of elliptic surfaces in unramified abelian towers*, J. Reine. Angew. Math. **577** (2004), 153–169.

[7] O. Venjakob, *A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory*, J. Reine Angew. Math. **559** (2003), 153–191.

Department of Mathematics, University of Wisconsin, 480 Lincoln Drive, Madison, WI 53706, USA

E-mail address: `ellenber@math.wisc.edu`

Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON N2L 3G1, Canada

E-mail address: `a5logan@math.uwaterloo.ca`