Compositio Mathematica **121:** 105–108, 2000.

Correction to p-adic Representations Arising from Descent on Abelian Varieties

MICHAEL HARRIS
U.F.R. de Mathématiques, Université Paris 7, 2, Pl. Jussieu, 75251 Paris Cedex 05, France.
e-mail: harris@mathp7.jussieu.fr

(Received: 15 April 1998; accepted in final form: 19 October 1998)

The article [1], which represents a part of my 1977 Harvard PhD thesis, contains a number of errors. I have known about these errors for some time, and have mentioned them to those who have expressed interest in the article. The Iwasawa theory of noncommutative p-adic Lie groups, the principal topic of [1], is now being revived, thanks to the work of J. Coates and his students. It therefore seems appropriate to point out the principal errors in [1] and to indicate which of them can be repaired. I thank B. Mazur and R. Taylor for encouraging me to do so, and B. Mazur again for looking over this erratum. I also thank J. Coates for his comments on [1] and on the first draft of this erratum, and S. Howson for sending a preprint of her work with Balister. This note was completed during a visit to RIMS and Kyoto University; I thank these institutions for their hospitality, and for providing an excellent working environment.

The errors in [1] are irrelevant to the other articles derived from the methods of my thesis, notably [2].

I refer to the notation and contents of [1] without comment. In particular, H is a p-adic analytic group with the property that its Iwasawa algebra Λ_H has no zero divisors; we call such an H *adequate*. Any p-adic analytic group has a subgroup of finite index with this property (cf. [1, 1.4]). In our case H is realized as a closed subgroup of the principal congruence subgroup Γ of $GL(N, \mathbb{Z}_p)$ of level p (or of level 4 if $p = 2$), for some N. We let $\Gamma(N)_i \subset \Gamma$ be the principal congruence subgroup of level p^{i+1} (resp. 2^{i+2} for $p = 2$) and let $H_i = H \cap \Gamma(N)_i$. Thus H_i/H_{i+1} is a finite abelian group of exponent p for all i, and $\Lambda_H = \varprojlim \mathbb{Z}_p[H/H_i]$ is a closed subalgebra of $\Lambda_{\Gamma(N)}$, which is known to be without zero divisors (cf. [1, 1.4] and the references there; it also follows from Theorem (2.3.3) of [4]). As in [1], we let $\Omega_H = \varprojlim \mathbb{F}_p[H/H_i]$. Both Λ_H and Ω_H are Noetherian (cf. the reference to Bourbaki's *Commutative Algebra* in [1]).

The principal error is contained in Corollary 1.7, where the argument in (ii) is incorrect. Indeed, Balister and Howson have given examples in [3] to show that

Corollary 1.7 fails whenever the Lie algebra of H is not solvable. The first half of Proposition 1.9 is false for the same reason.

Various proofs in [1] refer to Corollary 1.7 and Proposition 1.9. Most importantly they are used to argue, in certain cases, that the Selmer groups of elliptic curves over p-adic Lie extensions of number fields E with Galois group H are torsion modules over Λ_H. Since the criterion given in Corollary 1.7 for a module to be torsion is invalid, these examples, presented in sections 5.1 and 5.2, are also invalid. The second half of Corollary 2.10.1, used to mediate between Corollary 1.7 and the examples in section 5, is likewise invalid.

In other proofs, reference to Corollary 1.7 and Proposition 1.9 can be replaced by other arguments. This is notably the case with Theorems 1.10 and 3.3. The remainder of this note sketches new proofs of these theorems, which, in addition to making no reference to the offending assertions, are considerably simpler than the proofs given in [1]. (The original proof of Theorem 1.10 in [1] can easily be made correct.) I understand that Y. Ochi, in his 1998 Cambridge Ph.D. thesis, has also found new proofs of Theorem 1.10 and Theorem 3.3; his proof of Theorem 3.3 is substantially the same as the one given here.

There are also minor errors. For example, Ballister and Howson point out in [3] that the standard proof of Nakayama's lemma in Iwasawa theory contains an error, and this error is repeated in Corollary 1.6 of [1]. However, the proof is correct when applied to profinite Λ_H-modules, which are the only ones considered in [1]. Apart from errors of this kind, only Corollary 1.7, Proposition 1.9 (first half), Corollary 2.10.1 (second half), and the examples in sections 5.1, 5.2, and 5.3 cannot be repaired.

For the reader's convenience, I repeat the statements of Theorems 1.10 and 3.3 here; for notation I refer to [1]. The statement of Theorem 1.10 has been modified to include Lemma 3.4.1.

THEOREM 1.10. *Let M be a finitely generated compact $\Lambda = \Lambda_H$-module. Let $n = \dim H$ and, for each i, let d_i denote the $\mathbb{Z}_p$-rank of the free part of the finitely generated $\mathbb{Z}_p$ module $M_i = M/I_{H_i}M$, where $I_{H_i} = \ker \Lambda_H \to \mathbb{Z}_p[H/H_i]$. Let r denote the rank of M as Λ-module (i.e., the rank of the quotient of M by its Λ-torsion submodule). Then $d_i = r[H : H_i] + O(p^{(n-1)i})$. In particular, for M to be a torsion Λ-module, it is necessary and sufficient that $d_i = O(p^{(n-1)i})$.*

Remark. There is a rational number $C > 0$ such that $[H : H_i] = Cp^{ni}$ for i sufficiently large.

Proof. First assume $r = 0$. We may assume M has no p-torsion. Then $d_i = \dim_{\mathbb{F}_p} \bar{M}/I_{H_i}\bar{M}$, where $\bar{M} = M/pM$ is a finitely generated torsion module over Ω_H. Thus it suffices to prove the estimate $d_i = O(p^{(n-1)i})$ for finitely generated torsion modules over Ω_H. There is a surjective map

$$\oplus_i \Omega_H/\Omega_H \cdot f_i \to \bar{M}$$

for a finite set of non-zero elements $f_i \in \Omega_H$. We thus reduce to the case

https://doi.org/10.1023/A:1001730616194 Published online by Cambridge University Press

$\bar{M} = \Omega_H/\Omega_H \cdot f$, for some non-zero $f \in \Omega_H$. Then $d_i = \dim \mathrm{Coker}\ f : \Omega_{H,i} \to \Omega_{H,i}$, where $\Omega_{H,i} = \Omega_H/I_{H_i}$. Let $\mathrm{Gr}(\Omega_H)$ be the associated graded algebra for the filtration by the (images of) I_{H_i}, and let $\mathrm{Gr}(\bar{M})$ (resp. $\mathrm{Gr}(\Omega_{H,i})$ be the corresponding associated graded module over $\mathrm{Gr}(\Omega_H)$ (resp. ideal in $\mathrm{Gr}(\Omega_H)$). As in [1], $\mathrm{Gr}(\Omega_H)$ is a polynomial ring. Let $f' \in \mathrm{Gr}(\Omega_H)$ be the leading term of f. Now the rank of an endomorphism of a finite dimensional filtered $\mathbb{F}_p$-vector space goes down upon passage to the associated graded space. Thus

$$d_i \leqslant d_i' = \dim \mathrm{Coker}\ f' : \mathrm{Gr}(\Omega_H)/\mathrm{Gr}(\Omega_{H,i}) \to \mathrm{Gr}(\Omega_H)/\mathrm{Gr}(\Omega_{H,i}).$$

The estimate for d_i' then follows from the theory of the Hilbert polynomial, as in the proof of Lemma 1.10.1.

In the general case, there is an exact sequence $0 \to T \to M \to M' \to 0$ with T torsion and M' torsion free of rank r. Then $d_i - \mathrm{rank}\ M'/I_{H_i}M' = \mathrm{O}(p^{(n-1)i})$ by the case of rank 0. Thus we may assume M is torsion free. Then there are Λ_H-free modules V and V' of rank r, and morphisms $M \to V$ and $V' \to M$ with torsion cokernel. The estimate for d_i then follows as in the proof of Lemma 3.4.1.

We note that this argument also gives a proof of the second part of Proposition 1.9, which states that, if $\bar{M}$ is a torsion Ω_H-module, then M is a torsion Λ_H-module. Indeed, if $\bar{M}$ is a torsion Ω_H-module, then $\dim_{\mathbb{F}_p} \bar{M}/I_{H_i}\bar{M} = \mathrm{O}(p^{(n-1)i})$. As above, this implies that $d_i = \mathrm{O}(p^{(n-1)i})$, hence M is of rank 0.

THEOREM 3.3. *Let K be a finite field extension of $\mathbb{Q}$, and K'/K a Galois extension of number fields such that $H = \mathrm{Gal}(K'/K)$ is an adequate p-analytic group. Assume that only a finite set T of primes in K ramify in K' and let L be the maximal unramified pro-p Abelian extension of K'. Let $\mathrm{Iw}(K'/K) = \mathrm{Gal}(L/K')$, endowed with its natural structure as Λ_H-module. Then $\mathrm{Iw}(K'/K)$ is a torsion Λ_H-module.*

Remark. In the statement of Theorem 3.3 in [1] it is assumed that K contains a primitive pth root of 1, since the statement (Proposition 3.2) that $Iw(K'/K)$ is a finitely generated Λ_H module is only proved in that case. However, as the referee remarked, this hypothesis is unnecessary. For example, one can reduce the general case to Proposition 3.2 by replacing K by $K(\zeta_p)$ and then taking invariants under $\mathrm{Gal}(K(\zeta_p)/K)$.

Proof. Write $M = \mathrm{Iw}(K'/K)$ for simplicity. For $i = 0, 1, \ldots$, let $K_i \subset K'$ be the fixed field of H_i. Let $L_i \subset L$ be the fixed field of $I_{H_i}M$. Then there is an exact sequence of p-adic Lie groups

$$1 \to M_i \to Y_i = \mathrm{Gal}(L_i/K_i) \to H_i \to 1.$$

Let F_i be the maximal abelian extension of K_i contained in L_i; thus $\mathrm{Gal}(F_i/K_i) = Y_i/[Y_i, Y_i]$. But Y_i is a central extension of H_i by M_i. I claim there is a constant C, independent of i, such that

$$\dim Y_i/[Y_i, Y_i] \geqslant \mathrm{rank}\ M_i - C.$$

https://doi.org/10.1023/A:1001730616194 Published online by Cambridge University Press

Here dim refers to the dimension as p-adic Lie group. Indeed, it suffices to verify the corresponding estimate for the Lie algebras. Extending a basis of $Lie(M_i)$ to a basis X_α of Lie(Y_i), we see immediately that the number of non-vanishing brackets $[X_\alpha, X_\beta]$ is bounded above by $C = \dim(H)^2$, from which the estimate follows.

By Theorem 1.10, we thus have to show that the $\mathbb{Z}_p$-rank of $\mathrm{Gal}(F_i/K_i)$ grows as $O(p^{(n-1)i})$, with $n = \dim H$. By the argument preceding (3.3.2), we find that

$$\text{rank } \mathrm{Gal}(F_i/K_i) \leqslant n \cdot |T_i|,$$

where T_i is the set of primes of K_i above T. But the paragraph between (3.3.2) and (3.3.3) remains valid in the present setting, yielding the estimate $|T_i| = \mathrm{O}(p^{(n-1)i})$, which completes the proof.

References

1. Harris, M.: p-adic representations arising from descent on abelian varieties, *Compositio Math.* **39** (1979), 177–245.
2. Harris, M.: Systematic growth of Mordell–Weil groups of abelian varieties in towers of number fields, *Invent. Math.* **51** (1979), 123–141.
3. Balister, P. N. and Howson, S.: Note on Nakayama's lemma for compact Λ-modules, *Asian J. Math.* **1** (1997), 224–229.
4. Lazard, M.: Groups analytiques p-adiques, *Publ. Math. IHES* **26** (1965).