A note on central torsion Iwasawa-modules

GERGELY ZÁBRÁDI

28th February 2013

1 Notation and preliminaries

For the Galois group $\mathrm{Gal}(L/k)$ of a Galois extension L of the number field k and a prime v of k we write $\mathrm{Gal}(L/k)_v$ for the decomposition subgroup of v. Let $\mathcal{G}$ be any p-adic Lie group without elements of order p and with a closed normal subgroup $\mathcal{H} \lhd \mathcal{G}$ such that $\Gamma := \mathcal{G}/\mathcal{H} \cong \mathbb{Z}_p$. We are going to need the special case when $\mathcal{G}$ is a finite index subgroup of $\mathrm{Gal}(\mathbb{Q}(E[p^\infty])/\mathbb{Q})$ and also in the case when $\mathcal{G} \cong \mathbb{Z}_p$. The former embeds into $\mathrm{GL}_2(\mathbb{Z}_p)$ once we choose a $\mathbb{Z}_p$-basis of $T_p(E)$. We denote by $\Lambda(\mathcal{G})$ the Iwasawa $\mathbb{Z}_p$-algebra of $\mathcal{G}$ and by $\Omega(G)$ its $\mathbb{F}_p$-version.

Let S be the set of all f in $\Lambda(\mathcal{G})$ such that $\Lambda(\mathcal{G})/\Lambda(\mathcal{G})f$ is a finitely generated $\Lambda(\mathcal{H})$-module and

$$S^* = \bigcup_{n \geq 0} p^n S.$$

These are multiplicatively closed (left and right) Ore sets of $\Lambda(\mathcal{G})$ [2], so we can define $\Lambda(\mathcal{G})_S$, $\Lambda(\mathcal{G})_{S^*}$ as the localizations of $\Lambda(\mathcal{G})$ at S and S^*. We write $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$ for the category of all finitely generated $\Lambda(\mathcal{G})$-modules, which are S^*-torsion. A finitely generated left module M is in $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$ if and only if $M/M(p)$ is finitely generated over $\Lambda(\mathcal{H})$ [2]. It is conjectured that $X(E/F_\infty)$ always lies in this category provided that E has good ordinary reduction at p. We write $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G}))$ for the Grothendieck group of the category $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$. Similarly, let $\mathfrak{M}(\mathcal{G}, p)$ denote the category of p-power-torsion finitely generated $\Lambda(\mathcal{G})$-modules and $\mathfrak{N}_{\mathcal{H}}(\mathcal{G})$ the category of $\Lambda(\mathcal{G})$-modules that are finitely generated over $\Lambda(\mathcal{H})$.

Lemma 1.1. *Assume in addition that $\mathcal{G}$ is a pro-p group. Then we have $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G})) = K_0(\mathfrak{M}(\mathcal{G}, p)) \oplus K_0(\mathfrak{N}_{\mathcal{H}}(\mathcal{G}))$.*

Proof. By definition any module in $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$ is an extension of a module in $\mathfrak{M}(\mathcal{G}, p)$ and a module in $\mathfrak{N}_{\mathcal{H}}(\mathcal{G})$. Hence we have $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G})) = K_0(\mathfrak{M}(\mathcal{G}, p)) + K_0(\mathfrak{N}_{\mathcal{H}}(\mathcal{G}))$. Let M and N be $\Lambda(G)$-modules as above. Now we claim that the map $[M] \mapsto [M(p)]$ is well defined and extends to a homomorphism $K_0(\mathfrak{M}_{\mathcal{H}}(\mathcal{G})) \to K_0(\mathfrak{M}(\mathcal{G}, p))$. For this let

$$0 \to A \to B \to C \to 0$$

be a short exact sequence in $\mathfrak{M}_{\mathcal{H}}(\mathcal{G})$. Then we have $\mu(B) = \mu(A) + \mu(C)$ for their μ-invariants (as $\Lambda(G)$-modules) since p-power-torsion $\Lambda(G)$-modules that are finitely generated over $\Lambda(H)$ (ie. modules in $\mathfrak{M}(\mathcal{G}, p) \cap \mathfrak{N}_{\mathcal{H}}(\mathcal{G})$) clearly have trivial μ-invariant. Here the μ-invariant $\mu(M)$

of a finitely generated $\Lambda(G)$-module is defined by $\sum_{j=0}^{\infty}\mathrm{rk}_{\Omega(\mathcal{G})}(p^jM(p)/p^{j+1}M(p))$. Hence we have $[B(p)] = [A(p)] + [C(p)]$ in $K_0(\mathfrak{M}(\mathcal{G},p))$ by the main theorem of [1] applied to pro-p groups. The statement follows using again that modules in $\mathfrak{N}_{\mathcal{H}}(\mathcal{G})$ have trivial μ-invariant hence the homomorphism constructed is zero on $K_0(\mathfrak{N}_{\mathcal{H}}(\mathcal{G}))$. $\square$

Further, if M is a left $\Lambda(\mathcal{G})$-module, then by $M^{\#}$ we denote the right module defined on the same underlying set with the action of $\Lambda(\mathcal{G})$ via the anti-involution $\# = (\cdot)^{-1}$ on $\mathcal{G}$, i. e. for an m element in M and g in G, and the right action is defined by $mg := g^{-1}m$. By extending the right multiplication linearly to the whole Iwasawa algebra we get $mx = x^{\#}m$.

2 Central torsion Iwasawa-modules

In this section we are going to assume that $G' = H' \times Z$ is a compact pro-p p-adic Lie-group without elements of order p such that the centre $Z(G')$ is $Z \cong \mathbb{Z}_p$. So the above machinery applies to $\mathcal{G} := G'$ and $\mathcal{H} := H'$.

Lemma 2.1. *Let M be a finitely generated central torsion $\Lambda(G)$-module without p-torsion. Then M represents the trivial element in the $K_0(\mathfrak{M}_{H'}(G'))$ if and only if it is $\Lambda(H')$-torsion.*

Proof. One direction follows from the existence of a homomorphism

$$K_0(\mathfrak{M}_{H'}(G')) \to \mathbb{Z}$$

sending modules to their $\Lambda(H')$-rank. For the other direction assume that M is both $\Lambda(H')$- and $\Lambda(Z)$-torsion and choose (by the Weierstraß preparation theorem noting that M has no p-torsion) a distinguished polynomial $f(T)$ in $\mathbb{Z}_p[T] \subset \mathbb{Z}_p[[T]] \cong \Lambda(Z)$ annihilating M. We may assume without loss of generality that f is irreducible. Now we can take a projective resolution of M as a $\Lambda(G')/(f)$-module. Moreover, since $\Lambda(G')/(f)$ is a regular local ring we have $K_0(\Lambda(G')/(f))$ is isomorphic to $\mathbb{Z}$. On the other hand, the ring $\Lambda(G')/(f)$ is free of rank $\deg(f)$ over $\Lambda(H')$ and so M has trivial class in $K_0(\Lambda(G')/(f))$ as its rank is $\mathrm{rk}_{\Lambda(G')/(f)}(M) = \mathrm{rk}_{\Lambda(H)}(M)/\deg(f) = 0$. Since any finitely generated $\Lambda(G')/(f)$-module lies in $\mathfrak{M}_{H'}(G')$ the statement follows. $\square$

Lemma 2.2. *Let M be a $\Lambda(Z)$-torsion module in the category $\mathfrak{M}_{H'}(G')$. Then $\mathrm{Ext}^1_{\Lambda(G)}(M^{\#},\Lambda(G))$ is also $\Lambda(Z)$-torsion.*

Proof. By the long exact sequence of $\mathrm{Ext}(\cdot,\Lambda(G))$ we may assume without loss of generality that M is killed by a prime element f in the commutative algebra $\mathbb{Z}_p[[T]] \cong \Lambda(Z)$, ie. f is either a distinguished polynomial or $f = p$. Since $M^{\#}$ is then killed by $f^{\#}$ and finitely generated over $\Lambda(G)$, it admits a surjective $\Lambda(G)$-homomorphism from a finite free module over $\Lambda(G)/(f^{\#})$. So again by the long exact sequence of $\mathrm{Ext}(\cdot,\Lambda(G))$ it suffices to show the statement for $M^{\#} = \Lambda(G)/(f^{\#})$. However, we have $\mathrm{Ext}^1_{\Lambda(G)}(\Lambda(G)/(f^{\#}),\Lambda(G)) \cong \Lambda(G)/(f^{\#})$ therefore the statement. $\square$

Lemma 2.3. *Taking H'-coinvariants induces a homomorphism on the K_0-groups*

$$\begin{aligned} H_*(H',\cdot)\colon K_0(\mathfrak{M}_{H'}(G')) &\to K_0(\mathfrak{M}_1(Z)) \\ M &\mapsto \sum_{i=0}^{\dim H'+1}(-1)^i[H_i(H',M)] \end{aligned}$$

where $K_0(\mathfrak{M}_1(Z))$ denotes the category of finitely torsion $\Lambda(Z)$-modules.

Proof. First of all note that since we have $Z \cong \mathbb{Z}_p$, a finitely generated $\Lambda(Z)$-module N belongs to $\mathfrak{M}_1(Z)$ if and only if it has finite $\mathbb{Z}_p$-rank or, equivalently, if $N/N(p)$ is finitely generated over $\mathbb{Z}_p$. On the other hand, if M lies in $\mathfrak{M}_{H'}(G')$ then $H_i(H', M(p))$ is killed by a power of p and $H_i(H', M/M(p))$ is finitely generated over $\mathbb{Z}_p$. In particular both are $\Lambda(Z)$-torsion. The statement follows from the long exact sequence of H'-homology noting that H' has p-cohomological dimension $\leq \dim H' + 1$. $\square$

3 Selmer groups that are not central torsion

In this section E will be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication and with good ordinary reduction at the prime $p \geq 5$. We put $G := \mathrm{Gal}(\mathbb{Q}(E[p^\infty])/\mathbb{Q})$ and $H := \mathrm{Ker}((\cdot)^{p-1} \circ \det |_{G \leq \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))})$. Therefore G/H is isomorphic to a finite index subgroup of $1 + p\mathbb{Z}_p \cong \mathbb{Z}_p$ so that the machinery of section 1 applies. Moreover, $G' \leq G$ will be an open subgroup with the properties in section 2. For instance, we could take $G' := 1 + p^r M_2(\mathbb{Z}_p)$ (under an identification of G with an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$) for some integer r large enough to assure $G' \leq G$.

Proposition 3.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication and with good ordinary reduction at the prime p. Moreover, assume that the j-invariant of E is non-integral and the dual Selmer $X(E/F_\infty)$ is in the category $\mathfrak{M}_H(G)$. Then $X(E/F_\infty)$ is not annihilated by any element of $\Lambda(Z)$.*

Proof. We prove by contradiction and assume that $X(E/F_\infty)$ is $\Lambda(Z)$-torsion. We proceed in 3 steps.

Step 1. By Lemma 2.2 $\mathrm{Ext}^1(X(E/F_\infty)^\#, \Lambda(G))$ is also $\Lambda(Z)$-torsion. On the other hand, Theorem 5.2 in [3] provides us with $\Lambda(G)$-homomorphism

$$\varphi : X(E/F_\infty) \to \mathrm{Ext}^1(X(E/F_\infty)^\#, \Lambda(G))$$

such that $\mathrm{Ker}(\varphi)$ is finitely generated over $\mathbb{Z}_p$ (so it represents the trivial element in $\mathfrak{M}_H(G)$) and $\mathrm{Coker}(\varphi)$ represents the same element in $\mathfrak{M}_H(G)$ as

$$\bigoplus_{v_q(j_E)<0} \Lambda(G) \otimes_{\Lambda(G_q)} T_p(E)^{\mathrm{v}} =: \bigoplus_{v_q(j_E)<0} M_q \ . \tag{1}$$

Since the module in (1) has no p-torsion, we deduce that $\mathrm{Coker}(\varphi)(p)$ has trivial class in $K_0(\mathfrak{M}_{H'}(G'))$ by Lemma 1.1 for any pro-p open subgroup $H' \times Z = G' \leq G$ with $Z = Z(G') \cong \mathbb{Z}_p$. We are going to fix such a pro-p open subgroup G' later on depending on the ramification properties of $\mathbb{Q}(E[p^\infty])$ at the potentially multiplicative primes q. We are going to show that (1) is on one hand $\Lambda(H')$-torsion, on the other hand, it does not have a trivial class in $K_0(\mathfrak{M}_{H'}(G'))$. This will contradict to Lemma 2.1.

Step 2. In order to show that the class of (1) is nonzero in $K_0(\mathfrak{M}_{H'}(G'))$, we apply the homomorphism $H_*(H', \cdot)$ defined in Lemma 2.3 and show that its image

$$[H_*(H', \bigoplus_{v_q(j_E)<0} M_q)] = \sum_{v_q(j_E)<0} \sum_{i=0}^{4} (-1)^i [H_i(H', M_q)] \tag{2}$$

is nonzero, but has rank 0 over $\mathbb{Z}_p$. The latter implies that (1) is $\Lambda(H')$-torsion.

To compute the $\Lambda(Z)$-characteristic ideal of the right hand side of (2) we have the following

Lemma 3.2. *For any finitely generated $\Lambda(G_q)$-module N there is an isomorphism*

$$H_i(H', \Lambda(G) \otimes_{\Lambda(G_q)} N) \cong \Lambda(G/H') \otimes_{\Lambda(G_q/(H' \cap G_q))} H_i(H' \cap G_q, N) \tag{3}$$

of $\Lambda(G/H')$-modules.

Proof. The commutative diagram

$$\begin{array}{ccc} G_q & \longrightarrow & G \\ \downarrow & & \downarrow \\ G_q/(H' \cap G_q) & \longrightarrow & G/H' \end{array}$$

induces two spectral sequences

$$E^2_{p,q}(N) = \mathrm{Tor}_p^{\Lambda(G)}(\Lambda(G/H'), \mathrm{Tor}_q^{\Lambda(G_q)}(\Lambda(G), N))$$
$$E^2_{p,q}(N) = \mathrm{Tor}_p^{\Lambda(G_q/(H' \cap G_q))}(\Lambda(G/H'), \mathrm{Tor}_q^{\Lambda(G_q)}(\Lambda(G_q/(H' \cap G_q)), N))$$

both computing $\mathrm{Tor}_{p+q}^{\Lambda(G_q)}(\Lambda(G/H'), N)$. The result follows noting that $\Lambda(G)$ (respectively $\Lambda(G/H')$) is flat over $\Lambda(G_q)$ (respectively over $\Lambda(G_q/(H' \cap G_q))$). □

Step 3. By Lemma 3.2 we are reduced to computing the local homology groups $H_i(H' \cap G_q, T_p(E)^\vee)$. By the theory of the Tate curve there exists a finite extension of $\mathbb{Q}_q(\mu_p) \leq F_q$ contained in $\mathbb{Q}_q(E[p^\infty])$ over which E achieves split multiplicative reduction and $E[p^\infty]$ is isomorphic to $(\mu_{p^\infty} \times t^{\mathbb{Z}/p^\infty})/t^{\mathbb{Z}}$ as a $\mathrm{Gal}(\overline{\mathbb{Q}_q}/F_q)$-module for some element $t \in F_q^\times$ with $|t|_q < 1$. Hence the image $G_{q,0}$ of the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}_p}/F_q) \leq \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ in G_q has the following properties:

(*i*) $G_{q,0} \cong H_{q,0} \rtimes \Gamma_{q,0}$ with $H_{q,0} \cong \Gamma_{q,0} \cong \mathbb{Z}_p$ such that the conjugation action of $\Gamma_{q,0}$ on $H_{q,0}$ is given by the cyclotomic character $\chi_{q,cyc}$;

(*ii*) $\Gamma_{q,0} \cap H' = \{1\}$;

(*iii*) there exists a $\mathbb{Z}_p$-basis of $T_p(E)$ inducing an inclusion $G_q \leq G \leq \mathrm{GL}_2(\mathbb{Z}_p)$ such that $H_{q,0} \leq H_{q,1} := \begin{pmatrix} 1 & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix} \leq G \leq \mathrm{GL}_2(\mathbb{Z}_p)$.

Therefore the local $H_{q,1} \rtimes \Gamma_{q,0}$-module $T_p(E)^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(T_p(E), \mathbb{Z}_p) \cong T_p(E)(-1)$ fits into the exact sequence

$$0 \to X\mathbb{Z}_p[[X]] \to X^{-1}\mathbb{Z}_p[[X]] \to T_p(E)^\vee \to 0$$

where we identified $\mathbb{Z}_p[[X]]$ with $\Lambda(H_{q,1})$. Since $H_{q,0}$ has finite index in $H_{q,1}$ the above is a projective resolution of $T_p(E)^\vee$ as a $\Lambda(H_{q,0})$-module. Hence we may compute explicitely its $H_{q,0}$-homology as a $\Gamma_{q,0}$-module to obtain isomorphisms

$$H_0(H_{q,0}, T_p(E)^\vee)/H_0(H_{q,0}, T_p(E)^\vee)(p) \cong \mathbb{Z}_p(-1)\ ; \tag{4}$$
$$H_1(H_{q,0}, T_p(E)^\vee)/H_1(H_{q,0}, T_p(E)^\vee)(p) \cong \mathbb{Z}_p(1)\ ; \tag{5}$$

and $H_i(H_{q,0}, T_p(E)^{\mathrm{v}}) = 0$ for $i > 1$.

Moreover, we may choose the open subgroup $G' = H' \times Z \leq G$ sufficiently small (depending on all the prime numbers q at which E has potentially multiplicative reduction) so that (by possibly further increasing F_q for some q) we have $G_{q,0} = G' \cap G_q$, $H_{q,0} = H' \cap G_q$ and the composite map $\Gamma_{q,0} \hookrightarrow G_{q,0} \hookrightarrow G' \twoheadrightarrow Z = G'/H'$ is an isomorphism for all prime numbers q in question. Further, by the local and global Weil pairings, the local, resp. global cyclotomic characters $\chi_{q,cyc}$ and χ_{cyc} both factor through the determinant map on $\mathrm{GL}_2(\mathbb{Z}_p)$ and therefore are independent of the choice of a $\mathbb{Z}_p$-basis of $T_p(E)^{\mathrm{v}}$. In particular, the above isomorphism fits into the commutative diagram

$$\begin{array}{ccc} \Gamma_{q,0} & \xrightarrow{\sim} & Z \\ {\scriptstyle \chi_{q,cyc}}\downarrow & & \downarrow{\scriptstyle \chi_{cyc}} \\ \mathbb{Z}_p^\times & \xrightarrow{=} & \mathbb{Z}_p^\times \end{array} .$$

We deduce that the isomorphisms (4) and (5) also hold as $\Lambda(Z)$-modules. Using Lemma 3.2 with $N = T_p(E)^{\mathrm{v}}$ the right hand side of (2) equals

$$\sum_{v_q(j_E)<0} |G : G_q H'| \left([\mathbb{Z}_p(-1)] - [\mathbb{Z}_p(1)]\right) \tag{6}$$

in $K_0(\mathfrak{M}_1(Z))$. Indeed, since Z lies in the centre of G we have the isomorphism

$$\Lambda(G/H') \otimes_{\Lambda(G_q/(H'\cap G_q))} H_i(H' \cap G_q, T_p(E)^{\mathrm{v}}) \cong \bigoplus_{j=1}^{|G:G_qH'|} H_i(H' \cap G_q, T_p(E)^{\mathrm{v}})$$

of $\Lambda(Z)$-modules for $i = 0, 1$.

Since both $\mathbb{Z}_p(-1)$ and $\mathbb{Z}_p(1)$ have rank 1 over $\mathbb{Z}_p$ we immediately see that (1) is $\Lambda(H')$-torsion. On the other hand, the characteristic ideal of $\mathbb{Z}_p(-1)$ is $(z - \chi_{cyc}(z^{-1})) \lhd \Lambda(Z)$ that is clearly different from the characteristic ideal $(z - \chi_{cyc}(z))$ of $\mathbb{Z}_p(1)$ where z denotes a topological generator of the group Z. So the characteristic power series of (6) equals $\left(\frac{T+1-\chi_{cyc}(z^{-1})}{T+1-\chi_{cyc}(z)}\right)^{\sum_q |G:G_qH'|}$ which is not a unit in $\mathbb{Z}_p[[T]] \cong \Lambda(Z)$. □

Corollary 3.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication and with good ordinary reduction at the prime p. Moreover, assume that the j-invariant of E is non-integral, the dual Selmer $X(E/F_\infty)$ has no nonzero $\Lambda(H)$-torsion submodule and has rank 1 over $\Lambda(H)$. Then $X(E/F_\infty)$ has no nonzero $\Lambda(Z)$-torison submodule either. In particular, it is completely faithful.*

Proof. Assume that $0 \neq M \leq X(E/F_\infty)$ is the $\Lambda(Z)$-torsion part of $X(E/F_\infty)$. As $X(E/F_\infty)$ has no $\Lambda(H)$-torsion, M also has rank 1 over $\Lambda(H)$. In particular, $X(E/F_\infty)/M$ is $\Lambda(H)$-torsion. Choose an arbitrary element $x \in X(E/F_\infty)$. The we have $0 \neq \lambda_1 \in \Lambda(H)$ such that $\lambda_1 x \in M$ hence there is a $\lambda_2 \in \Lambda(Z)$ such that $\lambda_2\lambda_1 x = 0$. Since λ_2 lies in the centre, we conclude that $\lambda_1(\lambda_2 x) = 0$. Since $X(E/F_\infty)$ has no $\Lambda(H)$-torsion, we have $\lambda_2 x = 0$ and $x \in M$. □

References

[1] K. Ardakov, S. Wadsley, Characteristic elements for p-torsion Iwasawa modules, *J. Algebraic Geom.* **15** (2006) 339–377.

[2] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, The GL_2 main conjecture for elliptic curves without complex multiplication, *Publ. Math.* IHES **101** (2005), 163–208.

[3] G. Zábrádi, Pairings and functional equations over the GL_2-extension, *Proc. London Math. Soc.* (2010) **101** (3), 893–930.