Iwasawa Theory and Projective Modules

Ralph Greenberg

University of Washington
Seattle, Washington, USA

Aug 10, 2010

Some references

R. Greenberg, *Iwasawa theory, projective modules, and modular representations*

J. Coates, P. Schneider, R. Sujatha, *Modules over Iwasawa algebras*

J. Coates, T. Fukaya, K. Kato, R. Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*

J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, *The* GL_2 *main conjecture for elliptic curves without complex multiplication*

The set-up

Suppose that F is a number field, that F_∞ is the cyclotomic $\mathbf{Z}_p$-extension of F, and that K is a finite Galois extension of F. We will assume that $K \cap F_\infty = F$. Let $K_\infty = KF_\infty$. Let

$$G = \mathrm{Gal}(K_\infty/F) \ , \qquad \Gamma = \mathrm{Gal}(F_\infty/F) \ \ ,$$

$$\Delta \ = \ \mathrm{Gal}(K/F) \ \ ,$$

the last of which is a finite group. We can identify Δ with $\mathrm{Gal}(K_\infty/F_\infty)$ and G with $\Delta \times \Gamma$.

Suppose that E is an elliptic curve defined over F. We will always assume that E has good ordinary reduction at the primes of F lying over p.

Selmer groups for E

The p-primary subgroup $\mathrm{Sel}_E(K_\infty)_p$ of the Selmer group for E over K_∞ is defined as the kernel of a map of the following form:

$$H^1(K_\infty, E[p^\infty]) \longrightarrow \bigoplus_v \mathcal{H}_v(K_\infty, E) \quad ,$$

where v runs over all the primes of F and $\mathcal{H}_v(K_\infty, E)$ is defined in a certain way in terms of local Galois cohomology groups. If Σ_0 is any finite set of primes of F, not containing primes above p or above ∞, then we define a *"non-primitive"* Selmer group by:

$$\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p \;=\; \ker\Big(H^1(K_\infty, E[p^\infty]) \longrightarrow \bigoplus_{v \notin \Sigma_0} \mathcal{H}_v(K_\infty, E)\Big) \quad .$$

Of course, one has an inclusion $\mathrm{Sel}_E(K_\infty)_p \subseteq \mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$. One has equality if $\mathcal{H}_v(K_\infty, E) = 0$ for all $v \in \Sigma_0$.

Some modules over groups rings

The discrete $\mathbf{Z}_p$-module $\mathrm{Sel}_E(K_\infty)_p$ has a natural action of G, Δ, and Γ. Let $X_E(K_\infty)$ denote the Pontryagin dual of $\mathrm{Sel}_E(K_\infty)_p$. Then we can regard $X_E(K_\infty)$ as a module over the group ring $\mathbf{Z}_p[\Delta]$, and also over the completed group rings $\mathbf{Z}_p[[G]]$ and $\Lambda = \mathbf{Z}_p[[\Gamma]]$. The latter ring is the usual Iwasawa algebra.

For any set Σ_0 as above, the Pontryagin dual of $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ will be denoted by $X_E^{\Sigma_o}(K_\infty)$ and is also a module over the above group rings. Over the ring $\Lambda = \mathbf{Z}_p[[\Gamma]]$, these modules are known to be finitely-generated.

The difference between the primitive and non-primitive Selmer groups

There is a conjecture of Mazur which asserts that $\mathrm{Sel}_E(K_\infty)_p$ is a cotorsion Λ-module. This means that $X_E(K_\infty)$ is a finitely-generated, torsion Λ-module. This conjecture turns out to imply that the map whose kernel is $\mathrm{Sel}_E(K_\infty)_p$ is surjective. As a consequence, it follows that

$$\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p/\mathrm{Sel}_E(K_\infty)_p \;\cong\; \bigoplus_{v\in\Sigma_0} \mathcal{H}_v(K_\infty, E) \;\; .$$

As we mention below, $\mathcal{H}_v(K_\infty, E)$ is a cofinitely-generated $\mathbf{Z}_p$-module. Its Pontryagin dual is a finitely-generated $\mathbf{Z}_p$-module. It is also a module over the various group rings mentioned above.

An often needed assumption in this talk

We will often need to assume that $\mathrm{Sel}_E(K_\infty)_p[p]$ is finite. This means that $\mathrm{Sel}_E(K_\infty)_p$ is a cofinitely-generated $\mathbf{Z}_p$-module. That is, $X_E(K_\infty)$ is a finitely-generated $\mathbf{Z}_p$-module. Thus, as a Λ-module, $X_E(K_\infty)$ is indeed a torsion module. Furthermore, the μ-invariant is 0.

It is not hard to show that $\mathcal{H}_v(K_\infty, E) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{\delta_v(K_\infty, E)}$ for any $v \nmid p, \infty$, where $\delta_v(K_\infty, E)$ is a non-negative integer. Hence $\mathcal{H}_v(K_\infty, E)$ is a cofinitely-generated $\mathbf{Z}_p$-module for all v in Σ_0. The above assumption then implies that $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p[p]$ is finite and that $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ is also a cofinitely-generated $\mathbf{Z}_p$-module.

Under the above assumption, $X_E(K_\infty)$ and $X_E^{\Sigma_0}(K_\infty)$ will be finitely-generated $\mathbf{Z}_p[\Delta]$-modules.

A theorem about projectivity

For simplicity, we will assume that p is odd. Define the following set:

$$\Phi_{K/F} \ = \ \{ v \mid v \nmid p, \infty, \ \text{ and } \ p | e_v(K/F) \ \} \ .$$

Here $e_v(K/F)$ denotes the ramification index for v in K/F.

If v is a prime of F lying above p, let $\overline{E}_v$ denote E modulo v and let k_v denote the residue field for a prime of K above v.

Theorem A. *Let us make the following assumptions:*

(a) $\mathrm{Sel}_E(K_\infty)[p]$ *is finite.*

(b) $\Phi_{K/F} \ \subseteq \ \Sigma_0$.

(c) $E(K_\infty)[p] = 0$ *and* $\overline{E}_v(k_v)[p] = 0$ *for all* $v|p$.

Then $X_E^{\Sigma_0}(K_\infty)$ *is a projective* $\mathbf{Z}_p[\Delta]$*-module.*

The multiplicity $\lambda_X(\sigma)$.

Suppose that X is a finitely-generated, projective $\mathbf{Z}_p[\Delta]$-module. Let $V = X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, a finite-dimensional representation space for Δ over $\mathbf{Q}_p$. For every absolutely irreducible representation σ of Δ (defined over a finite extension $\mathcal{F}$ of $\mathbf{Q}_p$), let $\lambda_X(\sigma)$ denote the multiplicity of σ in $V \otimes_{\mathbf{Q}_p} \mathcal{F}$.

If ρ is any representation of Δ over $\mathcal{F}$, then one can realize ρ over $\mathcal{O}$, the ring of integers in $\mathcal{F}$. One can reduce the resulting $\mathcal{O}$-representation modulo $\mathfrak{m}$, the maximal ideal in $\mathcal{O}$, obtaining a representation $\widetilde{\rho}$ over $\mathfrak{f} = \mathcal{O}/\mathfrak{m}$, the residue field for $\mathcal{F}$. Its semisimplification $\widetilde{\rho}^{ss}$ is well-defined.

A basic property of projective $\mathbf{Z}_p[\Delta]$-modules

Suppose that ρ_1 and ρ_2 are representions of Δ (over $\mathcal{F}$). For each $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, let $m_i(\sigma)$ denote the multiplicity of σ in ρ_i for $i = 1, 2$.

Proposition. *Assume that $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$. Then one has the linear relation*

$$\sum_{\sigma} m_1(\sigma)\lambda_X(\sigma) \;=\; \sum_{\sigma} m_2(\sigma)\lambda_X(\sigma) \quad ,$$

where σ varies over $\mathrm{Irr}_{\mathcal{F}}(\Delta)$.

If $\rho_1 \ncong \rho_2$, then the above linear relation is non-trivial. Such non-trivial linear relations always exist if Δ has order divisible by p.

The number of independent congruence relations

One can quantify this. Suppose that s is the number of conjugacy classes in Δ and t is the number of conjugacy classes of elements of Δ of order prime to p. Then the number of independent linear relations arising as above is $s - t$.

Suppose that Δ is a p-group. In this case, we have $t = 1$. In fact, if ρ_1 and ρ_2 are representations of Δ over $\mathcal{F}$, then $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$ if and only if ρ_1 and ρ_2 have the same degree. This is because the only irreducible representation of Δ over $\mathfrak{f}$ is the trivial representation.

In general, t is the number of isomorphism classes of irreducible representations of Δ over a sufficiently large finite field $\mathfrak{f}$.

If $|\Delta|$ is not divisible by p, then $t = s$ and there are no nontrivial congruence relations. One has $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$ if and only if $\rho_1 \cong \rho_2$.

An illustration

As an illustration, suppose that $\Delta = \Delta_r = PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$, where $r \geq 0$. Then Δ has a quotient $\Delta_0 \cong PGL_2(\mathbf{F}_p)$. It turns out that if ρ_1 is any representation of Δ over $\mathcal{F}$, then there exists a representation ρ_2 of Δ factoring through the quotient group Δ_0 such that $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$. Hence, under the assumption that X is a finitely-generated, projective $\mathbf{Z}_p[\Delta]$-module, one can determine $\lambda_X(\sigma)$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$ if one knows $\lambda_X(\sigma)$ for all $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)$.

The PGL_2 illustration continued

One can write down explicit congruence relations. Assume that p is odd. If σ is an irreducible representation of $\Delta = \Delta_r$ of degree $p^{r-1}(p-1)(p+1)$, and $r \geq 2$, then one has

$$\lambda_X(\sigma) \;=\; p^{r-2} \sum_{\alpha \in \mathrm{Irr}_{\mathcal{F}}(\Delta_0)} \deg(\alpha)\lambda_X(\alpha) \quad .$$

It turns out that $\deg(\alpha)$ is even for all but four irreducible representations of Δ_0. There are two 1-dimensional and two p-dimensional irreducible representations of Δ_0. If σ is as above, then one has a parity result:

$$\lambda_X(\sigma) \;\equiv\; \sum_{2 \nmid \deg(\alpha)} \lambda_X(\alpha) \pmod 2,$$

where the sum just has the four terms corresponding to the α's of degree 1 or p.

Quasi-projectivity

It is useful to have a broader form of the above proposition. Suppose that X is a finitely-generated $\mathbf{Z}_p[\Delta]$-module. The multiplicity $\lambda_X(\sigma)$ just depends on $V = X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Suppose that there are finitely-generated, projective $\mathbf{Z}_p[\Delta]$-modules X_1 and X_2 such that one has an exact sequence

$$0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V \longrightarrow 0 \quad ,$$

where $V_i = X_i \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ for $i = 1, 2$. We then say that X is quasi-projective.

Somewhat more generally, assume that X is a $\mathbf{Z}_p[\Delta]$-module which is possibly not finitely-generated. The above definition makes sense under the assumption that X/X_{tors} is a finitely-generated $\mathbf{Z}_p[\Delta]$-module. Then V is still a finite-dimensional representation space for Δ over $\mathbf{Q}_p$.

Congruence relations for quasi-projective $\mathbf{Z}_p[\Delta]$-modules

Proposition. *Assume that X is a projective or quasi-projective $\mathbf{Z}_p[\Delta]$-module. Assume that $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$. Then one has the linear relation*

$$\sum_{\sigma} m_1(\sigma)\lambda_X(\sigma) = \sum_{\sigma} m_2(\sigma)\lambda_X(\sigma) \quad ,$$

where σ varies over $\mathrm{Irr}_{\mathcal{F}}(\Delta)$ and $m_i(\sigma)$ denotes the multiplicity of σ in ρ_i for $i = 1, 2$.

The invariants $\lambda_E(\sigma)$ and $\lambda_E^{\Sigma_0}(\sigma)$

The modules $X = X_E(K_\infty)$ and $X = X_E^{\Sigma_0}(K_\infty)$ defined previously are $\mathbf{Z}_p[\Delta]$-modules. If $\mathrm{Sel}_E(K_\infty)[p]$ is finite, then they are finitely-generated $\mathbf{Z}_p[\Delta]$-modules. For any $\sigma \in \mathrm{Irr}_{\mathcal{F}}(\Delta)$, the corresponding invariant $\lambda_X(\sigma)$ will be denoted by $\lambda_E(\sigma)$ and $\lambda_E^{\Sigma_0}(\sigma)$, respectively. They depend only on E, F, and σ, and Σ_0 for the non-primitive case.

Congruence relations for $\lambda_E^{\Sigma_0}(\sigma)$.

Theorem B. *Let us make the following assumptions:*

(a) $\mathrm{Sel}_E(K_\infty)[p]$ *is finite.*

(b) $\Phi_{K/F} \subseteq \Sigma_0$.

Then $X_E^{\Sigma_0}(K_\infty)$ *is a quasi-projective* $\mathbf{Z}_p[\Delta]$*-module. Consequently, with the same notation as above, if* $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$*, then one has the linear relation*

$$\sum_{\sigma} m_1(\sigma)\lambda_E^{\Sigma_0}(\sigma) = \sum_{\sigma} m_2(\sigma)\lambda_E^{\Sigma_0}(\sigma) \quad ,$$

where σ *varies over* $\mathrm{Irr}_{\mathcal{F}}(\Delta)$.

The case where Δ is a p-group

There is a theorem of Hachimori and Matsuno which relates the $\mathbf{Z}_p$-coranks of $\mathrm{Sel}_E(K_\infty)_p$ and $\mathrm{Sel}_E(F_\infty)_p$ in the case where K_∞/F_∞ is a p-extension. That theorem is equivalent to theorem B in the case where $|\Delta|$ is a power of p. Let σ_0 be the trivial representation of Δ. If ρ_1 is the regular representation of Δ and ρ_2 is $\sigma_0^{|\Delta|}$, then $\widetilde{\rho}_1^{ss} \cong \widetilde{\rho}_2^{ss}$.

Weakening the hypotheses

Proposition. *Suppose that* Σ_0 *is a finite set of non-archimedean primes of* F *which contains no prime over* p*. Let* $\Sigma_1 = \Sigma_0 \cup \Phi_{K/F}$

.

(i) Assume that all of the assumptions in theorem A are satisfied except for the inclusion $\Phi_{K/F} \subseteq \Sigma_0$*. If the Pontryagin dual of* $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ *is projective as a* $\mathbf{Z}_p[\Delta]$*-module, then* $\mathcal{H}_v(K_\infty, E) = 0$ *for all* $v \in \Sigma_1 - \Sigma_0$*. Therefore* $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p = \mathrm{Sel}_E^{\Sigma_1}(K_\infty)_p$*.*

(ii) Suppose that $p \geq 5$*. If the Pontryagin dual of* $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p$ *is quasi-projective as a* $\mathbf{Z}_p[\Delta]$*-module, then* $\mathcal{H}_v(K_\infty, E) = 0$ *for all* $v \in \Sigma_1 - \Sigma_0$*. Therefore* $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p = \mathrm{Sel}_E^{\Sigma_1}(K_\infty)_p$*.*

Weakening the hypotheses

Concerning the hypothesis that $\mathrm{Sel}_E(K_\infty)[p]$ is finite, it suffices to assume that $\mathrm{Sel}_E(K_\infty)[p^2]/\mathrm{Sel}_E(K_\infty)[p]$ is finite.

Concerning the initial set-up of fields, it suffices to assume that $G = \mathrm{Gal}(K_\infty/F)$ fits into an exact sequence

$$1 \longrightarrow \Delta \longrightarrow G \longrightarrow \Gamma \longrightarrow 1 \ .$$

Then $\Delta = \mathrm{Gal}(K_\infty/F_\infty)$ is a normal subgroup of G and G will be isomorphic to a semidirect product $\Delta \rtimes \Gamma$. The hypotheses must be restated in a suitable way. For example, one replaces $\Phi_{K/F}$ by Φ_{K_∞/F_∞} (with the same definition in terms of ramification indices).

Weakening the hypotheses

One can also take Δ to be a p-adic Lie group for theorem A. In defining $\Phi_{K/F}$ (or Φ_{K_∞/F_∞}), one should replace the statement that $p|e_v(K/F)$ by the statement that the inertia subgroup of Δ for a prime above v contains a non-trivial pro-p subgroup.

Interestingly, if that inertia subgroup contains an infinite pro-p-subgroup (which must then be isomorphic to $\mathbf{Z}_p$), it follows that $\mathcal{H}_v(K_\infty, E) = 0$. If Δ is a p-adic Lie group and has no elements of order p, then $\mathcal{H}_v(K_\infty, E) = 0$ for all $v \in \Phi_{K/F}$. If one takes $\Sigma_0 = \Phi_{K/F}$, then $\mathrm{Sel}_E^{\Sigma_0}(K_\infty)_p = \mathrm{Sel}_E(K_\infty)_p$.

As for theorem **B**, we don't yet know how to extend this to the case where Δ is an infinite p-adic Lie group.

The difference $\lambda_E^{\Sigma_0}(\sigma) - \lambda_E(\sigma)$

We denote that difference by $\delta_E(\Sigma_0, \sigma)$. It is equal to the multiplicity of σ in the representation space

$$\bigoplus_{v \in \Sigma_0} \widehat{\mathcal{H}}_v(K_\infty, E) \otimes_{\mathbf{Z}_p} \mathcal{F}$$

of Δ, where $\widehat{\mathcal{H}}_v(K_\infty, E)$ denoted the Pontryagin dual of $\mathcal{H}_v(K_\infty, E)$. This multiplicity can be studied in a straightforward way. Thus, the difference between $\lambda_E^{\Sigma_0}(\sigma)$ and $\lambda_E(\sigma)$ can determined by studying local Galois cohomology groups. We won't discuss this today.

In summary, if Σ_0 is chosen suitably and if $\mathrm{Sel}_E(K_\infty)[p]$ is assumed to be finite, then one can study the non-primitive λ-invariants $\lambda_E^{\Sigma_0}(\sigma)$ by using the congruence relations, and thereby one can get information about the invariants $\lambda_E(\sigma)$.

Invariants over K

One can use information about the $\lambda_E(\sigma)$'s to study the action of Δ on $\mathrm{Sel}_E(K)_p$. Let $s_E(\sigma)$ denote the multiplicity of σ in the representation space $X_E(K) \otimes_{\mathbf{Z}_p} \mathcal{F}$, where $X_E(K)$ denotes the Pontryagin dual of $\mathrm{Sel}_E(K)_p$. If the Tate-Shafarevich group for E over K is finite, then $s_E(\sigma) = r_E(\sigma)$, where $r_E(\sigma)$ is the multiplicity of σ in $E(K) \otimes_{\mathbf{Z}} \mathcal{F}$. Of course, $r_E(\sigma)$ doesn't depend on p.
By definition, one has

$$\mathrm{rank}(E(K)) = \sum_{\sigma} deg(\sigma) r_E(\sigma) \quad ,$$

$$\mathrm{corank}_{\mathbf{Z}_p}(\mathrm{Sel}_E(K)_p) = \sum_{\sigma} deg(\sigma) s_E(\sigma) \quad ,$$

where σ varies over $\mathrm{Irr}_{\mathcal{F}}(\Delta)$.

Parity

Assuming that E has good ordinary reduction at the primes of F above p and that Mazur's conjecture for $\mathrm{Sel}_E(K_\infty)_p$ is true, one can prove the following parity result:

If σ is an irreducible orthogonal representation of Δ, then

$$s_E(\sigma) \equiv \lambda_E(\sigma) \pmod 2 \quad .$$

An irreducible representation σ is said to be orthogonal if σ can be realized by orthogonal matrices over a suitable large field. Such representations are self-dual.

As examples, all of the irreducible representations of dihedral groups are orthogonal. The same is true for all the irreducible representations of $\Delta_r = PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for $r \geq 0$ and p odd.

The parity conjecture

This refers to the conjecture that the sign in the (conjectural) functional equation for the Hasse-Weil L-function $L(E/K, s)$ is $(-1)^{\mathrm{rank}\left(E(K)\right)}$. A refinement of this conjecture is that if σ is a self-dual irreducible representation of Δ, then the sign in the (conjectural) functional equation for the twisted Hasse-Weil L-function $L(E/F, \sigma, s)$ is $(-1)^{r_E(\sigma)}$. There is a conjectural value for this sign given by Deligne, and spelled out by Rohrlich.

For any prime p, there is a conjecture involving the invariants $s_E(\sigma)$, namely that the conjectural sign in the functional equation for $L(E/F, \sigma, s)$ is $(-1)^{s_E(\sigma)}$. This is a conjecture about the parity of $s_E(\sigma)$, and hence (under suitable assumptions) the parity of $\lambda_E(\sigma)$. We refer to this as the p-Selmer version of the parity conjecture.

Compatibility with congruence relations

With the assumptions in theorems A or B, and an additional assumption that E has semistable reduction at primes of F lying above 2 and 3, one can show that the parity conjecture is compatible with the congruence relations (viewed as equations over $\mathbf{F}_2$). The proof involves a careful study of the $\delta_v(E, \sigma)$'s.

Suppose that $\Delta \cong PGL_2(\mathbf{Z}/p^{r+1}\mathbf{Z})$ for $r \geq 0$. Let K_0 be the subfield of K such that $\Delta_0 = \mathrm{Gal}(K_0/F) \cong PGL_2(\mathbf{F}_p)$. One can show that if $\mathrm{Sel}_E(K_{0,\infty})[p]$ is finite, then $\mathrm{Sel}_E(K_\infty)[p]$ is finite too. Thus, it will be enough to assume the finiteness of $\mathrm{Sel}_E(K_{0,\infty})[p]$. Suppose that Σ_0 contains $\Phi_{K/F}$. Under all of these assumptions, one proves the following result.

If the p-Selmer version of the parity conjecture is true for all irreducible representations of Δ_0, then it is also true for all irreducible representations of Δ.

Other results on the parity conjecture

The p-Selmer version of the parity conjecture has been studied by Birch-Stephens, Kramer-Tunnell, Monsky, Nekovar, B.D. Kim, V. and T. Dokchitser, Coates-Fukaya-Kato-Sujatha, and Mazur-Rubin. The results in [CFKS] are somewhat parallel to the results just mentioned, although the hypotheses and approach are different.

The results of Mazur and Rubin concern dihedral extensions of degree $2p^r$. If Δ is isomorphic to D_{2p^r}, then the irreducible representations of Δ have degree 1 or 2. The two 1-dimensional representations factor through the quotient Δ_0 of Δ of order 2. If σ has degree 2, and ρ is the direct sum of the two 1-dimensional representations then $\widetilde{\sigma}^{ss} \cong \widetilde{\rho}^{ss}$. In essence, under certain mild assumptions, they show that if the parity conjecture holds for the two 1-dimensional representations of Δ_0, then it also holds for σ.

Projective dimension

Recall the assumptions in theorem A.

(a) $\mathrm{Sel}_E(K_\infty)[p]$ is finite.

(b) $\Phi_{K/F} \subseteq \Sigma_0$.

(c) $E(K_\infty)[p] = 0$ and $\overline{E}_v(k_v)[p] = 0$ for all $v|p$.

These assumptions imply that $X_E^{\Sigma_0}(K_\infty)$ has a free resolution of length 1 as a $\mathbf{Z}_p[[G]]$-module, where $G = \mathrm{Gal}(K_\infty/F) \cong \Delta \times \Gamma$. In fact, this is true if one replaces (a) by the assumption that $\mathrm{Sel}_E(K_\infty)_p$ has finite $\mathbf{Z}_p$-corank (as conjectured by Mazur). The other assumptions are needed in full strength.

We will write R for $\mathbf{Z}_p[[G]]$ and X for $X_E^{\Sigma_0}(K_\infty)$. Thus, under the above assumptions, one has an exact sequence

$$0 \longrightarrow R^d \longrightarrow R^d \longrightarrow X \longrightarrow 0 \quad ,$$

where $d \geq 1$.

A final remark

This is a remark related to the paper *The GL_2 main conjecture for elliptic curves without complex multiplication*

The map $R^d \longrightarrow R^d$ is given by right-multiplication by a $d \times d$ matrix with entries in R. The determinant of such a matrix, if it makes sense, should be a *"characteristic element"* for the R-module X.

This does make sense if G is commutative. And so the above exact sequence gives a characteristic element ξ in $R = \mathbf{Z}_p[[G]]$. One can think of such an element as a $\mathbf{Z}_p$-valued measure on the Galois group $G = \Delta \times \Gamma$. One can identify R with $\Lambda[\Delta]$. If $\sigma : \Delta \to \mathcal{O}^\times$ is a character of Δ, then σ induces a ring homomorphism $\sigma : R \to \mathcal{O}[[\Gamma]]$ and $\sigma(\xi)$ is an element of $\mathcal{O}[[\Gamma]] = \Lambda_{\mathcal{O}}$.

If G is non-commutative, then one can define a "determinant" ξ in some K_1. For a ring $\mathfrak{R}$, one defines $K_1(\mathfrak{R})$ as a certain abelian quotient of the direct limit of the groups $GL_n(\mathfrak{R})$ under the map sending an $n \times n$ matrix A to the $(n+1) \times (n+1)$ matrix $\begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}$.

Assuming that $G = \Delta \times \Gamma$, one can identify $R = \mathbf{Z}_p[[G]]$ with $\mathbf{Z}_p[[\Gamma \times \Delta]] = \Lambda[\Delta]$. Recall that $\Lambda = \mathbf{Z}_p[[\Gamma]]$. If S is a multiplicatively closed subset of the nonzero elements of Λ containing an annihilator of X, Then one can left-tensor the above exact sequence with $\mathfrak{R} = R_S = \Lambda_S[\Delta]$, obtaining an isomorphism

$$\mathfrak{R}^d \longrightarrow \mathfrak{R}^d \quad .$$

This defines a $d \times d$ matrix and hence an element ξ in $K_1(\mathfrak{R})$. Note that the matrix can be taken with entries in R.

An integrality property of ξ

One can think of ξ as a characteristic element for the R-module X. It has a nice integrality property, namely if $\sigma : \Delta \to GL_n(\mathcal{O})$ is any irreducible representation of Δ, then σ induces ring homomorphisms:

$$\sigma : \mathbf{Z}_p[\Delta] \to M_n(\mathcal{O}), \qquad \sigma : \Lambda[\Delta] \to M_n(\Lambda_{\mathcal{O}}) \quad ,$$

where $\Lambda_{\mathcal{O}} = \mathcal{O}[[\Gamma]]$. This extends to a ring homomorphism

$$\sigma : \mathfrak{R} \to M_n(\Lambda_{\mathcal{O},S}) \quad .$$

One then gets a homomorphism Φ_σ from $K_1(\mathfrak{R})$ to

$$K_1\big(M_n(\Lambda_{\mathcal{O},S})\big) = K_1(\Lambda_{\mathcal{O},S}) = \Lambda_{\mathcal{O},S}^{\times} \quad .$$

The remark is that $\Phi_\sigma(\xi)$ is in $\Lambda_{\mathcal{O}}$.