The Main Conjecture of Iwasawa theory

Ravi Fernando – fernando@berkeley.edu

November 5, 2015*

1 Motivation

Iwasawa's main conjecture was motivated by the Weil conjectures, so let's briefly review what the Weil conjectures tell us. Let X be an algebraic variety over a finite field $\mathbb{F}_q$. Then the Weil conjectures state that the zeta function attached to X equals the alternating product of characteristic polynomials of the Frobenius Frob_q acting on the ℓ-adic cohomology groups $H^i(X, \mathbb{Q}_\ell)$; this also comes with a functional equation and a "Riemann hypothesis" restricting where the characteristic polynomials can vanish.

There is a strong analogy between number fields and function fields, so it is not unreasonable to expect an analogue of the Weil conjectures in our current setting. On the analytic side, the zeta function of the Weil conjectures will correspond to the p-adic L-function $L_p(\chi, s)$ defined in Dylan's talk last week. But on the algebraic side, we need to choose a suitable module to take the role of the étale cohomology groups (or Tate module). This role will be filled by an eigenspace of the $\mathbb{Z}_p[[T]]$-module X_∞.

In fact, one version of the main conjecture (which I won't be stating precisely, because I couldn't find a good reference for it) has a very nice analogy to the Weil conjectures. In this version, we consider the module X_∞ (actually X_∞^-) over $\mathbb{Z}_p[[T]]$, and tensor this up to $\mathbb{Q}_p[[T]]$. This decomposes as a direct sum of several eigenspaces, and the T-action respects this decomposition. Then the claim is that the characteristic polynomial of T on the $\omega\chi^{-1}$-eigenspace equals the p-adic L-function $L_p(\chi, s)$ up to a unit in $\mathbb{Z}_p[[T]]$. The analogies are as follows:

$$H^*(X, \mathbb{Q}_\ell) \longleftrightarrow (X_\infty^- \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^{(\omega\chi^{-1})} \tag{1}$$

$$\text{Frob}_p \longleftrightarrow T \tag{2}$$

In this talk, we will see a different version of the statement; both versions were proved by Mazur and Wiles in 1984.

*Notes for a talk given in Berkeley's Student Number Theory Seminar, focusing on Iwasawa theory. Main reference: Romyar Sharifi, *Notes on Iwasawa theory.*

2 Setup

We begin with some setup. In this talk, p will be an odd prime and F will be an abelian CM field whose degree over $\mathbb{Q}$ is prime to p. (Reminder: a CM field[1] is a totally imaginary quadratic extension of a totally real number field; in particular, this means that complex conjugation is uniquely defined on F.) We consider the cyclotomic $\mathbb{Z}_p$-extension $F = F_0 \subset F_1 \subset \cdots \subset F_\infty$ of F.

Recall a few of the objects we have studied, first on the algebraic side: A_n is the p-part of the class group of F_n, and $X_\infty = \lim_{\leftarrow n} A_n$, where the inverse limit is taken with respect to the norm maps $N_n : A_{n+1} \to A_n$. (Recall that X_∞ is also the Galois group $\mathrm{Gal}(L_\infty/F_\infty)$.) In particular, X_∞ is a module over $\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$. It will be important for us today that X_∞ also admits an action of the finite abelian group $\Delta = \mathrm{Gal}(F/\mathbb{Q})$: for example, view each A_n as $\mathrm{Gal}(L_n/F_n)$ and let Δ act on it by lifting and conjugating.[2] This action commutes with the $\mathbb{Z}_p$-module structure (trivially, because it commutes with the $\mathbb{Z}/p^n\mathbb{Z}$-module structure on A_n) and also with the Γ-action (because Γ_n and Δ commute in $\mathrm{Gal}(F_n/\mathbb{Q}) \cong \Gamma_n \times \Delta$).

Now we need to discuss the eigenspaces of X_∞. Let χ be a character $\Delta \to \overline{\mathbb{Q}_p}^\times$, which must in particular take values that are prime-to-p roots of unity. We can ask for elements $x \in X_\infty$ on which every element $\delta \in \Delta$ acts by $\delta \cdot x = \chi(\delta) \cdot x$; i.e. the χ-eigenspace of X_∞. But there's a problem: although X_∞ is a $\mathbb{Z}_p$-module, this might not be enough: since $\mathbb{Z}_p$ only contains $p-1$ roots of unity, the image of χ may not be contained in it. To fix this problem, we extend scalars. Let $\mathscr{O}_\chi = \mathbb{Z}_p[\mathrm{im}\,\chi]$, i.e. $\mathbb{Z}_p$ with some finite number of prime-to-p roots of unity adjoined, which is isomorphic to $\mathbb{Z}_{p^n}$ for some n. Then we define the *χ-eigenspace* $X_\infty^{(\chi)}$ to consist of elements of $X_\infty \otimes_{\mathbb{Z}_p} \mathscr{O}_\chi$ on which the action of Δ agrees with multiplication by $\chi(\Delta)$. Note that this can also be realized as the tensor product $X_\infty \otimes_{\mathbb{Z}_p[\Delta]} \mathscr{O}_\chi$, where the map $\mathbb{Z}_p[\Delta] \to \mathscr{O}_\chi$ is given by $\chi : \Delta \to \mathscr{O}_\chi$.

3 Statement of theorem

Theorem 3.1. *(The main conjecture over $\mathbb{Q}$,[3] Mazur-Wiles 1984.) Continue the notation above, but let χ be a nontrivial even character of $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. Let $\Lambda_\chi = \mathscr{O}_\chi[[T]]$. Then the characteristic ideal of the Λ_χ-module $X_\infty^{(\omega\chi^{-1})}$ equals the ideal generated by f_χ, where $f_\chi \in \Lambda_\chi$ is the element defined by $f_\chi((1+p)^s - 1) = L_p(\chi, s)$ for $s \in \mathbb{Z}_p$.*

Some explanation here:

[1] The reason for the terminology: recall that when an elliptic curve has complex multiplication, its endomorphism ring is an order in an imaginary quadratic field. The analogue for higher-dimensional abelian varieties is a simple abelian variety of dimension n whose endomorphism ring is commutative with rank $2n$ over $\mathbb{Z}$, which is as large as possible. In this case, the endomorphism ring must be an order in a CM field, and conversely all orders in CM fields appear in this way.

[2] More precisely, we have a short exact sequence $0 \to A_n \to \mathrm{Gal}(L_n/\mathbb{Q}) \to \mathbb{Z}/p^n\mathbb{Z} \times \Delta \to 0$; the middle term acts on A_n by conjugation, and the action of A_n itself is trivial.

[3] "Over $\mathbb{Q}$" in the sense that all fields involved are abelian over $\mathbb{Q}$, even though F itself need not equal $\mathbb{Q}$.

- X_∞ was originally a $\mathbb{Z}_p[[T]]$-module, but its eigenspaces live over the extended ring of scalars $\mathscr{O}_\chi[[T]]$.
- We originally defined characteristic ideals (in Bertie's talk) for modules over $\Lambda = \mathbb{Z}_p[[T]]$, but all of that theory works essentially without change for any complete local Noetherian ring with finite residue field of characteristic p, and Λ_χ certainly satisfies these properties.
- The character ω is the Teichmüller character $\Delta \to \mu_{p-1} \subset \mathbb{Z}_p^\times$ defined as follows: for $\delta \in \Delta$, we only need to specify $\omega(\delta)$ modulo p, and we choose it so that $\delta(\zeta) = \zeta^{\omega(\delta)}$ for all pth roots of unity ζ. (Confusion: does F contain pth roots of unity? The introduction suggests that $F = \mathbb{Q}(\mu_p)$ is the most important case, but we aren't assuming that here.)
- Recall that the map $s \mapsto (1+p)^s$ is a bijection $\mathbb{Z}_p \to 1 + p\,\mathbb{Z}_p$, so it makes sense to define f_χ by specifying it on the points $(1+p)^s - 1$. Note also that since we want f_χ to be a formal power series, its input must be in $p\,\mathbb{Z}_p$ rather than just $\mathbb{Z}_p$.

4 Consequences and further results

The statement I gave in this talk was the main conjecture over $\mathbb{Q}$, in the sense that the fields involved are cut out by abelian characters of $G_\mathbb{Q}$. There exist generalizations to totally real fields, CM fields, elliptic curves, and so on.

An interesting consequence of the main conjecture is the Herbrand-Ribet theorem. For this, we take $F = \mathbb{Q}(\zeta_p)$, and note that every character χ of Δ is a power of the Teichmüller character ω. Herbrand proved in the early 1900s that if the ω^n-eigenspace of the class group of F is nontrivial, then p divides the Bernoulli number B_{p-n}. Later, Ribet proved the more difficult theorem that the converse holds. The eventual proof of the main conjecture was modeled on Ribet's proof, and yielded his theorem as a corollary.