THE FORMULATION OF THE CYCLOTOMIC IWASAWA MAIN CONJECTURE IN MAZUR-WILES PAPER, PRELIMINARY VERSION

F.BARS AND I.BLANCO-CHACÓN

1. Algebraic side: Iwasawa modules and characteristic ideals in cyclotomic Iwasawa theory.

Let us fix p an odd prime once and for all.

By a p-adic Dirichlet character we mean a character $\chi : (\mathbb{Z}/N)^* \to \overline{\mathbb{Q}_p}^*$ and by $\mathcal{O}_\chi \subset \overline{\mathbb{Q}_p}$ we mean the ring extension of $\mathbb{Z}_p$ generated by the values of χ, where as usual $\mathbb{Q}_p$ are the p-adic numbers and $\mathbb{C}_p$ will denote the completion of $\overline{\mathbb{Q}_p}$. We assume, once and for all, that the conductor of χ, called f in the text, is not divisible by p^2 (i.e. χ is a character of first kind). As usual, the Teichmüller character $\omega : (\mathbb{Z}/p)^* = \mathbb{F}_p^* \to \mathbb{Z}_p^* \subseteq \overline{\mathbb{Q}_p}^*$ is the unique character of order $p-1$ such that $\omega(a) \equiv a (mod\ p)$.

Let μ_{p^n} be the group of p^n-th roots of unity and set

$$\mathbb{Q}(\mu_{p^\infty}) := \cup_{n=1}^{\infty} \mathbb{Q}(\mu_{p^n}).$$

Denote by $\mathbb{Q}_\infty/\mathbb{Q}$ the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$, where $[\mathbb{Q}(\mu_{p^\infty}) : \mathbb{Q}_\infty] = p-1$, and $\mathbb{Q}_n \subset \mathbb{Q}_\infty$ the subfield of degree p^n over $\mathbb{Q}$.

For a finite abelian extension $F/\mathbb{Q}$, write $F_\infty = F\mathbb{Q}_\infty$, and $F_n = F\mathbb{Q}_n$. The $\mathbb{Z}_p$-extension F_∞/F is called the cyclotomic extension of the number field F and denote by Γ the Galois group $\mathrm{Gal}(F_\infty/F)$.

Consider the Iwasawa algebra: $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/M)]] := \varprojlim_n \mathbb{Z}_p[\mathrm{Gal}(F_n/M)]$ with $\mathbb{Q} \subset M \subset F$ such that F_∞/M is abelian. Assume once and for all that $F \cap \mathbb{Q}_\infty = \mathbb{Q}$, (recall any χ of first kind is attached by class field theory to a field F with $F \cap \mathbb{Q}_\infty = \mathbb{Q}$).

We have

$$\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]] = \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})][[\mathrm{Gal}(F_\infty/F)]] \cong \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})][[\Gamma]].$$

For any $\mathbb{Z}_p$-module U which admits a continuous action of $\mathrm{Gal}(F_\infty/\mathbb{Q})$, the χ-part of U is the $\mathcal{O}_\chi[[\Gamma]]$-module obtained by change of scalars:

$$U_\chi = U \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]} \mathcal{O}_\chi.$$

Recall that we have a non-canonical isomorphism:

$$\sigma_\gamma : \mathcal{O}_\chi[[\Gamma]] \to \Lambda_\chi := \mathcal{O}_\chi[[T]]$$

mapping γ (a topological generator of Γ) to $1+T$, latter on we will fix this choice.

Recall the following statements on the theory of Λ_χ-modules of finite type:

(1) M, N are Λ_χ-pseudo-isomorphic if exists a Λ_χ-homomorphism from M to N with finite kernel and cokernel. We write $M \sim N$ if they are Λ_χ-pseudo-null, which is an equivalence relation for Λ_χ-torsion modules.

(2) M a Λ_χ-torsion (always of finite type), then

$$M \sim \oplus_{i=1}^{r} \Lambda_\chi/(h_i)$$

for some natural r where each $h_i \in \Lambda_\chi$. The invariant

$$(h_1 \cdots h_r) = Char_{\Lambda_\chi}(M)$$

is named the characteristic ideal of the Λ_χ-module M.

Recall that for any $\alpha \in \Lambda_\chi$, we can write

$$\alpha = \pi^\mu h(T) v(T)$$

where π is an uniformizer of $\mathcal{O}_\chi$, $h(T)$ a distinguished polynomial of degree λ (i.e. the reduction of $h(T)$ in $\Lambda_\chi/(p)$ is T^λ), and $v(T)$ a unit of Λ_χ.

For $Char_{\Lambda_\chi}(M) = (\alpha)$ with α as above, the number $\mu \in \mathbb{N}$ is called the μ-invariant of M, and $\lambda = degree_T(h(T))$ is named the λ-invariant of M.

Denote by $A_n(F)$ the p-primary component of the ideal class group of F_n and by $H_n(F)$ the Galois group of the p-Hilbert class field of F_n over F_n, a $\mathrm{Gal}(F/\mathbb{Q})$-module by the conjugation.

The inclusion of the divisor groups induces a map $\iota_n : A_n(F) \to A_{n+1}(F)$ and $A_\infty(F) := \varinjlim_{\iota_n} A_n(F)$ defines a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$-module.

The restriction maps $Res_{n+1}: H_{n+1}(F) \to H_n(F)$ allow us to define the $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$-module:

$$H_\infty(F) := \varprojlim_{Res_n} H_n(F).$$

We have an isomorphism compatible with the $\mathrm{Gal}(F/\mathbb{Q})$-action $A_n(F) \to^{\cong} H_n(F)$, satisfying the following commutative diagrams:

$$\begin{array}{ccc} A_{n+1}(F) & \to^{\cong} & H_{n+1}(F) \\ \downarrow Norm & & \downarrow Res \\ A_n(F) & \to^{\cong} & H_n(F) \end{array} \qquad \begin{array}{ccc} A_n(F) & \to^{\cong} & H_n(F) \\ \downarrow \iota_n & & transfer \\ A_{n+1}(F) & \to^{\cong} & H_{n+1}(F) \end{array}$$

Recall that $Hom(A_\infty(F), \mathbb{Q}_p/\mathbb{Z}_p)$ is a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$-module with action given by $(\tau \cdot f)(a) := \tau f(\tau^{-1}a) = f(\tau^{-1}a)$. Iwasawa proved that:

$$Hom(A_\infty(F), \mathbb{Q}_p/\mathbb{Z}_p)_{\chi^{-1}} \sim H_\infty(F)^{\#}_{\chi}$$

as Λ_χ-modules (through the above fixed isomorphism σ_γ) and they are Λ_χ-finite modules finitely generated, where $\#$ denotes the same group but with the $\mathrm{Gal}(F_\infty/\mathbb{Q})$ action given by the rule $\tau h^{\#} := \tau^{-1}h$.

Therefore, we can define by $h_p(F, \chi, T)$ the generator of $char_{\Lambda_\chi}(H_\infty(F)_\chi)$ as the product of π^μ (with a fixed uniformizer for $\mathcal{O}_\chi$) and a distinguished polynomial.

Proposition 1. *We have the following results,*

$$char_{\Lambda_\chi}(H_\infty(F)^{\#}_{\infty,\chi}) = (h_p(\chi, (1+T)^{-1} - 1))$$

$$char_{\Lambda_\chi}(Hom(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)_\chi = (h_p(\chi^{-1}, (1+T)^{-1} - 1))$$

Remark 2. *Usually there is another Λ_χ-Iwasawa module for which the main conjecture is formulated. Consider M_n the maximal abelian p-extension of F_n which is unramified except possibly at the primes of F_n lying above p. Consider $M_\infty := \cup_{n\geq 0} M_n$ and denote by $X_\infty = Gal(M_\infty/F_\infty)$ which is a $\mathbb{Z}_p[[Gal(F_\infty/F)]]$-module as usual action by conjugation.*

Then $X_{\infty,\chi}$ is a finitely generated Λ_χ-module and it is a torsion module if χ is an even character, and under that assumption, we have an isomorphism of Λ_χ-modules:

$$X_{\infty,\chi} \cong Hom(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1))_\chi \cong Hom(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)_{\omega^{-1}\chi},$$

where $\mathbb{Q}_p/\mathbb{Z}_p(1) = \mu_{p^\infty} = \cup_{n\geq 0}\mu_{p^n}$ (the first Tate twist) and ω denotes the Teichmüller character. Therefore, for χ even we have:

$$char_{\Lambda_\chi}(X_{\infty,\chi}) = (h_p(\omega\chi^{-1}, u(1+T)^{-1} - 1))$$

where u is $\kappa(\gamma) \in \mathbb{Z}_p^*$ where κ is the p-cyclotomic character restricted to $\Gamma = Gal(F_\infty/F)$, and γ a fixed topological generator of Γ.

For some computations, Mazur and Wiles work with Fitting ideals instead of characteristic ideals, see §5 for few details of the role that plays in the paper. (For a survey on Fitting ideals, see [3]).

Definition 3. *Let Z be a finitely generated Λ_χ-module and let*

$$\Lambda_\chi^a \to^{\psi} \Lambda_\chi^b \twoheadrightarrow Z$$

be a presentation, where the map ψ can be represented by an $a \times b$-matrix Φ_Z with entries in Λ_χ.

In this setting, the Fitting ideal of Z is the ideal generated by all the determinants of the $b \times b$-minors of Φ_Z if $a \geq b$ and otherwise is the zero ideal. We denote this ideal by $Fitt_{\Lambda_\chi}(Z)$.

And recall the following result

Lemma 4. *Let Z be a finitely generated Λ_χ-module having no $\mathcal{O}_\chi$-torsion. Then,*

$$char_{\Lambda_\chi}(Z) = Fitt_{\Lambda_\chi}(Z).$$

An more general we have

Lemma 5. *Let Z be a finitely generated torsion Λ_χ-module such that $\mu = 0$. Then we have,*

$$char_{\Lambda_\chi}(Z)(\pi, T)^{lenght_{\Lambda_\chi}(tor_{\mathcal{O}_\chi}(Z))} \subseteq Fitt_{\Lambda_\chi}(Z) \subseteq char_{\Lambda_\chi}(Z).$$

Concerning our involved Iwasawa modules in order to relate Fitting ideals with characteristic ideals we have the following result

Proposition 6. *For each odd character χ, we have:*

(1) *(Iwasawa)* $H_{\infty,\chi}$ *and* $Hom(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)_\chi$ *have no finite* Λ_χ*-submodules,*
(2) *(Ferrero-Washington) The* μ*-invariant for* $H_{\infty,\chi}$ *and* $Hom(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)_\chi$ *are zero, in particular both are of finite type as* $\mathbb{Z}_p$*-modules.*

2. Analytic side: p-adic L-functions and Iwasawa main conjecture

Let χ be a Dirichlet character associated to F with conductor f,

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s};\ Re(s) > 1.$$

From the functional equation, we have for $m \geq 1$ integer:

$$L(1-m,\chi) \begin{cases} \neq 0 \ if \ m \equiv \delta (mod\ 2) \\ = 0 \ otherwise \end{cases}$$

where $\delta = 0$ if χ even and 1 if χ is odd.

We can relate these special values to the generalized Bernoulli numbers, namely, recall that $B_{n,\chi}$ are defined by

$$\sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!},$$

Proposition 7. *For* $m \geq 1$ *we have* $L(1-m,\chi) = -\frac{B_{m,\chi}}{m}$.

The Bernoulli polynomials $B_n(X)$ defined by

$$\frac{te^{Xt}}{e^t-1} = \sum_{n=0}^{\infty} B_n(X) \frac{t^n}{n!},$$

which satisfy

$$B_{n,\chi} = f^{n-1} \sum_{a=1}^{f} \chi(a) B_n(\frac{a}{f})$$

and play a key role in order to construct a series named p-adic L-function, and that we write $L_p(s,\chi)$ with $s \in \mathbb{C}_p$ in some range of convergence such that

$$L_p(1-m,\chi) = -(1-\chi\omega^{-n}(p)p^{m-1}) \frac{B_{m,\chi\omega^{-m}}}{m},$$

for $m \geq 1$.

Recall that $L_p(T,\chi) \in Frac(\mathcal{O}_\chi)[[T]]$, where $Frac(R)$ denotes the field of fractions of a domain R. For further details on $L_p(s,\chi)$, as its classical construction, se for example §3.4[1].

In section §4, following the classical work of Iwasawa, we construct a formal power series $G_p(T,\chi) \in \mathcal{O}_\chi[[T]]$ which should interpolate the p-adic L-functions as a measure, in particular in order to simplify, χ is assumed to be of first kind (i.e. $p^2 \nmid f$ the conductor).

The power series $G_p(T,\chi)$ is characterized by the property

$$G_p(\chi, u^s - 1) = L_p(\chi, s),\ \forall s \in \mathbb{Z}_p.$$

The following formulation of a Cyclotomic Iwasawa Main Conjecture (IMC in the following in the text) was formulated by Greenberg:

Conjecture 8 (IMC)**.** *Let* χ *be an even primitive Dirichlet character of first kind. Then, as ideals of* $\mathcal{O}_\chi[[T]]$*, we have*

$$(h_p(\omega\chi^{-1}, T)) = (G_p(\chi, T)).$$

3. Iwasawa theory in terms of components

Let us denote by $G = G_p \times G'_p$ a finite abelian group of order k where G_p the p-primary component and G'_p the product of all ℓ-primary components with $\ell \neq p$. Consider

$$R = \mathbb{Z}_p[G] = \mathbb{Z}_p[G_p] \otimes \mathbb{Z}_p[G'_p]$$

a complete ring, product of local rings (i.e., a semi-local ring).

There is a bijection between any of the sets in the list:

(1) connected components of $Spec(R)$

(2) irreducible idempotents of R,

(3) maximal ideals of R,

(4) $\mathbb{Q}_p$-conjugacy classes of $\overline{\mathbb{Q}_p}^*$-valued characters of G'_p.

Write Π_R for the set of connected components of $Spec(R)$ and let us refer to its elements as *components*.

For each $\mathfrak{m} \in \Pi_R$, $R_\mathfrak{m}$ denotes the completion of R with respect to the corresponding maximal ideal and $e_\mathfrak{m}$ the irreducible idempotent. We have

$$R = \prod_{\mathfrak{m}\in\Pi_R} R_\mathfrak{m}.$$

Denote by Σ_R the set of irreducible components of $Spec(R)$, and we have a bijectivity with $\mathbb{Q}_p$-conjugacy classes of $\overline{\mathbb{Q}_p}^*$-valued characters of G. The elements of Σ_R are called *sheets* and we have a surjection:

$$\Sigma_R \twoheadrightarrow \Pi_R.$$

The basic *sheet* of a *component* $\mathfrak{m}$ (corresponding to a $\mathbb{Q}_p$-conjugacy of a character χ' on G'_p) is the sheet corresponding to the $\mathbb{Q}_p$-conjugacy of the character of G obtained from χ' with the projection $G \to G'_p$.

Observe that the basic sheet corresponds to the characters of G in $\mathfrak{m}$ of order prime to p, these characters are named basic characters.

Fix an integer a prime to p and set $G_{a,n} := (\mathbb{Z}/ap^n)^*$, and $R_{a,n} = \mathbb{Z}_p[G_{a,n}]$. Define from the natural projections $R_{a,n+1} \twoheadrightarrow R_{a,n}$,

$$R_{a,\infty} := \varprojlim_n R_{a,n}$$

and since $(G_{a,n})'_p = (G_{a,1})'_p$ we have (componentwise):

$$R_{a,\infty,\mathfrak{m}} := \varprojlim_n (R_{a,n})_\mathfrak{m}.$$

A component $\mathfrak{m}$ of $R_{a,\infty,\mathfrak{m}}$ is primitive or (a-primitive) if the conductor of any basic character is either a or ap.

A component $\mathfrak{m}$ of $R_{a,\infty,\mathfrak{m}}$ is pseudo-primitive if there is some character of $\mathfrak{m}$ whose conductor is a or ap.

A component $\mathfrak{m}$ is even (resp. odd) if every character belonging to $\mathfrak{m}$ is even (resp. odd).

Examples 9. *We give different examples of the above concepts.*

(1) *Take $p = 3$ and $a = 11$. Consider a character of conductor 33*

$$\chi : (\mathbb{Z}/33)^* \cong (\mathbb{Z}/3)^* \times (\mathbb{Z}/11)^* \cong C_2 \times C_{10} \to \mathbb{C}_3^*.$$

(recall that the finite subgroup in $\mathbb{Z}_3^*$ of square roots of unity is $\{\pm 1\}$). The character χ is primitive if it does not vanish on C_2, and χ^2 has conductor 11, in particular, χ^2 is a pseudo-primitive character in this case.

(2) *Take $p = 3$ and $a = 2$, take the character*

$$\chi : (\mathbb{Z}/6)^* \to \mathbb{Z}_3^* \subseteq \mathbb{C}_3^*$$

of order 2 given by $5 \mapsto -1$. It is a basic character of conductor 3, in particular it is not primitive. It is neither a Galois conjugate, because the image is in $\mathbb{Z}_3^*$, thus it is not pseudo-primitive.

(3) *Take p an odd prime and $a = 1$. Then, we have the Teichmüller character*

$$\omega : (\mathbb{Z}/p)^* \to \mathbb{Z}_p^*.$$

The conductor of ω^j with $(j, p-1) = 1$ is p and hence, it is primitive, and a basic character because the Galois conjugation is exactly the same character.

Write $\Gamma_a := ker(\mathbb{Z}_{p,a}^* := \varprojlim_n \mathbb{Z}/ap^n \to (\mathbb{Z}/pa\mathbb{Z})^*)$, a free pro-$p$-group on one generator u such that $u \not\equiv 1 (mod\ ap^2)$, and $\Gamma_a/\Gamma_a^{p^n} \times (\mathbb{Z}/ap)^* \cong G_{a,n-1}$, therefore we have:

$$R_{a,\infty,\mathfrak{m}} \cong R_{a,1,\mathfrak{m}}[[\Gamma_a]]$$

$$R_{a,n,\mathfrak{m}} \cong R_{a,1,\mathfrak{m}}[\Gamma_a/\Gamma_a^{p^{n-1}}].$$

Definition 10. *For $k \in \mathbb{Z}$, the k-twisted yoke*

$$\rho_k : \mathbb{Z}_p[[Gal(\overline{\mathbb{Q}}/\mathbb{Q})]] \to R_{a,\infty}$$

is the unique continuous ring homomorphism such that

$$\rho_k(g) = \varepsilon_{p,1}^k(g)[\varepsilon_{p,a}(g)]$$

where

$$\varepsilon_{p,a} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_{p,a}^*$$

defined by the property $\zeta_{ap^n}^{\varepsilon_{p,a}(g)} = g(\zeta_{ap^n})$ for every ap^n-th root ζ_{ap^n} of 1 in $\overline{Q}$, and observe

$$\alpha \circ \varepsilon_{p,a} = \varepsilon_{p,1}$$

where $\alpha : \mathbb{Z}_{p,a}^* \to \mathbb{Z}_{p,1}^* = \mathbb{Z}_p^*$ *the natural projection.*

The conjugate k*-twisted yoke is defined by* $\overline{\rho}_k(g) := \varepsilon_{p,1}^k(g)[\varepsilon_{p,a}(g)]^{-1}$*. Now if* $\mathfrak{m}$ *is a component of* $R_{a,\infty}$ *we denote by* $\eta_{k,\mathfrak{m}}$ *(and* $\overline{\eta}_{k,\mathfrak{m}}$*) the composition of* ρ_k *(resp.* $\overline{\rho}_k$*) with the projection to the factor* $R_{a,\infty,\mathfrak{m}}$*.*

Remark 11. *Consider the restriction of* $\varepsilon_{p,a}$ *to* $Gal(\mathbb{Q}(\mu_a)_\infty/\mathbb{Q}) \cong Gal(\mathbb{Q}(\mu_a)_\infty/\mathbb{Q}(\mu_a)) \times Gal(\mathbb{Q}(\mu_a)/\mathbb{Q})$ *and defines and isomorphism between* $Gal(\mathbb{Q}(\mu_a)_\infty/\mathbb{Q}(\mu_a))$ *to* Γ_a*, this isomorphism is named* κ *when* $a = 1$*, and* κ_a *in general.*

We choose once and for all a topological generator γ_a *of* $Gal(\mathbb{Q}(\mu_a)_\infty/\mathbb{Q}(\mu_a))$ *such that* $\kappa_a(\gamma_a) = u$ *a fix topological generator of* Γ_a*, and in particular* $\alpha(u) = \kappa(\gamma) = \kappa_a(\gamma_a)$*.*

In this setting we have the "Tate" twist automorphism,

$$\tau : R_{a,\infty} \to R_{a,\infty},\ [g] \mapsto \alpha(g)[g],$$

which clearly satisfies

$$\tau^{-1}\rho_k = \rho_{k+1}.$$

Remark 12. *Consider* M *a* $R_{a,\infty}$*-module and a* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-module such that its Galois action is obtained from* $R_{a,\infty}$ *by composition with a homomorphism* $h : \mathbb{Z}_p[[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]] \to R_{a,\infty}$*. Consider the Tate-twisted module* $M(1) := M \otimes_{\mathbb{Z}_p} \mu_{p^\infty}$ *with* $R_{a,\infty}$*-structure by action on the first module, then its Galois-module action is given via* τh*.*

Definition 13. *Let* M *be a* $R_{a,\infty,\mathfrak{m}}$*-module with a commuting action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*. We say that* M *is a* $\overline{n}_{-1}$*-yoked bimodule (or it admits a yoked bimodule structure) if its* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-structure is obtained from its* $R_{a,\infty,\mathfrak{m}}$*-structure via the homomorphism* $\overline{\eta}_{-1,\mathfrak{m}}$ *.*

Let us emphasize that $\overline{\eta}_{-1,\mathfrak{m}}$ is a surjective morphism characterized by the formula

$$\overline{\eta}_{-1,\mathfrak{m}}(Frob_\ell) = \ell^{-1}[\ell]^{-1}$$

where ℓ is any prime coprime with ap, and $Frob_\ell$ any Frobenius element in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ associated to ℓ, and $[\ell]$ refers the image in $R_{a,\infty,\mathfrak{m}}$ of $[l] \in \mathbb{Z}_p[[\mathbb{Z}_{p,a}^*]]$.

Definition 14. *Consider an algebraic* p*-abelian extension* L/K*. We say that* L/K *is of type* $\mathfrak{m}$ *if the kernel of*

$$\overline{\eta}_{-1} : \mathbb{Z}_p[[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]] \twoheadrightarrow R_{a,\infty,\mathfrak{m}}$$

annihilates the module $\mathrm{Gal}(L/K)$ *viewed as a* $\mathbb{Z}_p[[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]]$*-module via conjugation.*

Let us consider a component $\mathfrak{m}$. Set S be the set of Dirichlet characters of conductor dividing ap belonging to $\mathfrak{m}$, and always assume that it is an even component. Let $F_{\mathfrak{m}}^+$ be the finite abelian extension of $\mathbb{Q}$ characterized by

$$\mathrm{Gal}(\overline{\mathbb{Q}}/F_{\mathfrak{m}}^+) = \cap_{\chi \in S} ker(\chi).$$

Definition 15. *A finite extension* L/K *is said to be* **everywhere** *unramified if there exist algebraic number fields of finite degree* $K' \subset K$ *and* $L' \subset L$ *containing* K' *such that* $L = L'K$ *and* L'/K' *is an unramified extension.*[1]*. In general* L/K *is said* **everywhere** *unramified if it is a union of finite* **everywhere** *unramified extensions.*

Define by $K_{\mathfrak{m},\infty} := \mathbb{Q}_\infty F_{\mathfrak{m}}^+(\zeta_p)$, and let $L_{\mathfrak{m},\infty}$ the maximal **everywhere** unramified abelian extension of $K_{\mathfrak{m},\infty}$ of type $\mathfrak{m}$ and denote by

$$H_{\mathfrak{m}} := \mathrm{Gal}(L_{\mathfrak{m},\infty}/K_{\mathfrak{m},\infty}).$$

Consider a character ψ of $\mathfrak{m}$ of conductor dividing ap. Denote by $H_{\mathfrak{m},\psi}$ the $\mathcal{O}_\psi[[T]]$-module obtained from $H_{\mathfrak{m}}$ via the change of scalars:

$$R_{a,\infty,\mathfrak{m}} = R_{a,1,\mathfrak{m}}[[\Gamma_a]] \to \mathcal{O}_\psi[[\Gamma_a]] \to^{\sigma_u} \mathcal{O}_\psi[[T]]$$

where the first map is the natural one for the Dirichlet character, and the second one maps a topological generator u of Γ_a to $(1 + T)$.

Mazur and Wiles claims the obviousness of the following statement

[1]It seems that in the definition on Wiles-Mazur is unclear the use of the term everywhere unramified

Proposition 16 (Mazur-Wiles). *The natural map $H_\infty \to H_{\mathfrak{m}}$ induces an isomorphism of $\mathcal{O}_{(\psi\omega)^{-1}}$-modules*

$$\beta : H_{\infty,(\psi\omega)^{-1}}(F^+_{\mathfrak{m}}(\zeta_p)) \cong H_{\mathfrak{m},\psi}$$

where

$$u\beta((1+T)x) = (1+T)^{-1}\beta(x)$$

for $x \in H_{\infty,(\psi\omega)^{-1}}$, where $u \in \mathbb{Z}_p^*$ meaning $\kappa(\gamma)$.

Mazur-Wiles will work on quotients of $H_{\mathfrak{m},(\psi\omega)^{-1}}$ in order to prove IMC when $\mathfrak{m}$ is a primitive component.

For pseudo-primitive components Mazur-Wiles introduce a new module $H^\flat_{\mathfrak{m}} := Gal(L^\flat_{\mathfrak{m},\infty}/K_{\mathfrak{m},\infty})$ where $L^\flat_{\mathfrak{m},\infty}$ is the maximal virtually unramified extension of $K_{\mathfrak{m},\infty}$ of type $\mathfrak{m}$, where an abelian extension is called virtually unramified of type $\mathfrak{m}$ if is of type $\mathfrak{m}$ and it is unramified expect possible at primes of residual characteristic dividing a.

Proposition 17. *Let $\mathfrak{m}$ be a primitive or pseudo-primitive component and ψ a character belonging to $\mathfrak{m}$ such that a divides the conductor of ψ. Then, the natural surjection*

$$H^\flat_{\mathfrak{m},\psi} \twoheadrightarrow H_{\mathfrak{m},\psi}$$

has finite kernel (which is zero if $\mathfrak{m}$ is primitive).

In particular the characteristic ideal of $H^\flat_{\mathfrak{m},\psi}$ coincides with the characteristic ideal of $H_{\mathfrak{m},\psi}$.

4. Stickelberger elements and Stickelberger ideals: p-adic L-functions á la Iwasawa

Denote by $<x>$ the real number $\equiv x \bmod \mathbb{Z}$ with $0 \leq <x> < 1$. The k-th Stickelberger element is defined by:

$$\vartheta_k(b,N) := (N^{k-1}/k) \sum_{t=1, gcd(t,N)=1}^{N} B_k(<bt/N>)[t]^{-1} \in \mathbb{Q}[(\mathbb{Z}/N)^*]$$

for any positive integer N and any integer b. As usual in group rings, denote:

$$\hat{\vartheta}_k(b,N) := (N^{k-1}/k) \sum_{t=1, gcd(t,N)=1}^{N} B_k(<bt/N>)[t] \in \mathbb{Q}[(\mathbb{Z}/N)^*].$$

The k-th Stickelberger ideal is defined via:

$$S_k(N) := \mathbb{Z}[(\mathbb{Z}/N)^*] \cap \sum_{b\in\mathbb{Z}} \vartheta_k(b;N)\mathbb{Z}[(\mathbb{Z}/N)^*],$$

$$S_k(N)' := \mathbb{Z}[(\mathbb{Z}/N)^*] \cap \sum_{b\in\mathbb{Z}, gcd(b,p)=1} \vartheta_k(b;N)\mathbb{Z}[(\mathbb{Z}/N)^*],$$

and similarly $\hat{S}_k(N)$ and $\hat{S}_k(N)'$.

It is known that

$$\vartheta_{k,c}(b;N) := (1 - c^k[c]^{-1})\vartheta_k(b;N) \in \mathbb{Z}[(\mathbb{Z}/N)^*].$$

Let us get back to $R_{a,\infty}$, and take $N = ap^n$. We can define

$$\vartheta_{k,c}(b;ap^\infty) := \varprojlim_n \vartheta_{k,c}(b;ap^n) \in R_{a,\infty}$$

because in $R_{a,n+1} \to R_{a,n}$ we have $\vartheta_{k,c}(b,ap^{n+1}) \mapsto \vartheta_{k,c}(b;ap^n)$.

We have the relation via the twist automorphism: $\vartheta_{k,c}(1;ap^\infty) = \tau\vartheta_{k+1,c}(1;ap^\infty)$.

Now we follow Iwasawa for the construction of the p-adic L-function through k-th Stickelberger elements.

Recall that χ is a Dirichlet character of first kind of conductor dividing ap. Define by

$$G_{p,k,c}(\chi,T) \in \mathcal{O}_\chi[[T]] := \alpha_\chi(\vartheta_{k,c}(1;ap^\infty)), \text{ where}$$

$$\alpha_\chi : R_{a,\infty} = R_{a,1}[[\Gamma_a]] \to \mathcal{O}_\chi[[\Gamma_a]] \to^{\sigma_u} \mathcal{O}_\chi[[T]]$$

is the composition of the map taking into account $\chi : (\mathbb{Z}/ap)^* \to \mathcal{O}_\chi^*$ and σ_u defined by $[u] \mapsto 1+T$. Recall that u is a fixed topological generator of Γ_a chosen so that $\alpha(u) = \kappa(\gamma) \in \mathbb{Z}_p^*$, and we identify in all this lecture $\Gamma_a \cong \Gamma_1$ via $u \mapsto \gamma$ and by abuse in notation, $u \in \mathbb{Z}_p^*$ represents the element $\alpha(u)$.

If $\chi\omega^{-k}$ is not of p-power order, then $(1 - c^k[c]^{-1})$ defines a unit power series $u_{p,k,c} \in \mathcal{O}_\chi[[T]]$, and under this hypothesis one defines the k-th Stickelberger power series

$$G_{p,k}(\chi,T) := G_{p,k,c}(\chi,T)/u_{p,k,c} \in \mathcal{O}_\chi[[T]]$$

which is independent of c.

Theorem 18 (Iwasawa). *Let χ be a Dirichlet character of first kind. Then*

$$L_p(\chi, s) = G_p(\chi, \kappa(\gamma)^s - 1), \forall s \in \mathbb{Z}_p$$

where $G_p(\chi, T) = -G_{p,1}(\chi^{-1}\omega, T)$.

From the commutativity of the diagram:

$$\begin{array}{lccc} R_{a,\infty} & \to^{\alpha_\chi} & \mathcal{O}_\chi[[T]] & T \\ \tau^{-1}\downarrow & & \downarrow & \downarrow \\ R_{a,\infty} & \to^{\alpha_{\chi\omega}} & \mathcal{O}_\chi[[T]] & u^{-1}(1+T)-1 \end{array}$$

we obtain,

$$G_p(\chi, T) = -G_{p,k}(\chi^{-1}\omega^k, u^{k-1}(1+T) - 1),$$

where u in the last two statements means the element $\kappa(\gamma) \in \mathbb{Z}_p^*$.

For later convenience in the seminar let us study the generators of the 2-th Stickelberger ideals in $R_{a,n,\mathfrak{m}}$.

Denote by $\vartheta_{2,\mathfrak{m}}(b; ap^n)$ the image of $\vartheta_2(b; ap^n)$ in $R_{a,n,\mathfrak{m}} \otimes \mathbb{Q}_p$. If ω^2 does not belong to $\mathfrak{m}$, there exists c such that $(1 - c^2[c]^{-1})$ projects to a unit in $R_{a,n,\mathfrak{m}}$, therefore

$$\vartheta_{2,\mathfrak{m}}(b; ap^n) \in R_{a,n,\mathfrak{m}}.$$

Denote by $S_2(ap^n)_\mathfrak{m}$ the ideal in $R_{a,n,\mathfrak{m}}$ generated by the images of $S_2(ap^n)$ in $R_{a,n,\mathfrak{m}}$. Similar definitions for $S_2(ap^n)'_\mathfrak{m}$, $\hat{S}_2(ap^n)_\mathfrak{m}$ and $\hat{S}_2(ap^n)'_\mathfrak{m}$.

Proposition 19. *Let $\mathfrak{m}$ be a component.*

(1) *If $\mathfrak{m}$ is pseudo-primitive and not associated to ω^2 or the trivial character, then $S_2(ap^n)'_\mathfrak{m}$ is generated by $\vartheta_{2,\mathfrak{m}}(d; ap^n)$ where d runs through those divisors of r where ap/r is the reduced conductor.*
(2) *If $\mathfrak{m}$ is pseudo-primitive and not associated to ω^{-2} or the trivial character, then $\hat{S}_2(ap^n)'_\mathfrak{m}$ is generated by $\hat{\vartheta}_{2,\mathfrak{m}}(d; ap^n)$ where d runs through those divisors of r where ap/r is the reduced conductor.*
(3) *If $\mathfrak{m}$ is a-primitive and not associated to ω^2 or the trivial character, then $S_2(ap^n)'_\mathfrak{m}$ is principal ideal generated by $\vartheta_{2,\mathfrak{m}}(1; ap^n)$ (the principal Stickelberger element).*

There are also results for the remaining pseudo-primite $\mathfrak{m}$ that coincide with $\omega^{\pm 2}$ or trivial character but we do not reproduce them here.

Finally, we show the relation between 2-th Stickelberger ideal and the p-adic L-function à la Iwasawa.

Proposition 20. *Let χ be a non-trivial even-character of conductor a or ap and $\chi \neq \omega^{-2}$. If $a = 1$, then*

$$\alpha_{\mathfrak{m},\chi}(\hat{S}_2(ap^\infty)'_\mathfrak{m}) = G_{p,2}(\chi^{-1}, (1+T)^{-1} - 1)$$

where recall that $\alpha_{\mathfrak{m},\chi} : R_{a,\infty,\mathfrak{m}} \to \mathcal{O}_\chi[[T]]$ follows from α_χ with the projection $R_{a,\infty} \to R_{a,\infty,\mathfrak{m}}$.

5. The IMC follows from a inclusion on Fitting ideals

Consider $G_p(\psi\omega^2, T)$, which is not a unit power series for any ψ character associated to the pseudo-primitive component $\mathfrak{m}$, (this allows Mazur-Wiles to suppose different restrictions, for example, when $a = 1$, they assume that $\mathfrak{m}$ does not contain as basic character ω^{-2} or the trivial character).

The big work of Mazur and Wiles is to construct an ideal $\mathfrak{b}_{n,\mathfrak{m}} \subseteq R_{a,n,\mathfrak{m}}$ and a virtually unramified extension of type $\mathfrak{m}$ $L_\mathfrak{m}^{(n)}/K_\mathfrak{m}$ such that $\mathrm{Gal}(L_\mathfrak{m}^{(n)}/K_\mathfrak{m})$ is an $R_{a,\infty,\mathfrak{m}}$-module which satisfies the following properties:

- we have a relation that in the simplest case of $\mathfrak{m}$ primitive reads as:

  $$(1 - l[l])^k \mathfrak{b}_\mathfrak{m}^{(n)} \subseteq \hat{S}_2(ap^n)'_\mathfrak{m},$$

  where l and k are technical elements, see the precise definition in [4, Chp 4§3,Chp5§5], for example $k = 0$ if $\psi = \psi'_p\omega^k$ and $k \not\equiv -1 (mod\ p-1)$, (moreover, in that situation we have that $\mathfrak{b}_\mathfrak{m}^{(n)} = \hat{S}_2(ap^n)'_\mathfrak{m}$ which is principal generated by the principal Stickelberger element $\hat{\vartheta}_2(ap^n)_\mathfrak{m}$).

  We define

  $$\mathfrak{b}_\mathfrak{m}^{(\infty)} = \varprojlim_n \mathfrak{b}_\mathfrak{m}^{(n)} \subset R_{a,\infty,\mathfrak{m}}$$

  through the natural maps $R_{a,n+1,\mathfrak{m}} \to R_{a,n,\mathfrak{m}}$.

  Thus, in the simplest case we have the inclusion

  $$(1 - l[l])^k \mathfrak{b}_\mathfrak{m}^{(\infty)} \subseteq \hat{S}_2(ap^\infty)'_\mathfrak{m}$$

  Now, applying the result of Proposition 20 we obtain:

$$(1 - l\psi(l)[l])^k \alpha_{\mathfrak{m},\psi}(\mathfrak{b}_\mathfrak{m}^{(\infty)}) \subseteq (G_{p,2}(\psi^{-1}, (1+T)^{-1} - 1)). \quad (1)$$

- we have a ideal $\mathfrak{U}_{\mathfrak{m}} \subset R_{a,\infty,\mathfrak{m}}$ of finite index (independent of n) such that:
$$\mathfrak{U}_{\mathfrak{m}} Fitt_{R_{a,\infty,\mathfrak{m}}}(Gal(L_{\mathfrak{m}}^{(n)}/K_{\mathfrak{m}})) \subseteq \mathfrak{b}_{\mathfrak{m}}^{(\infty)}$$
Now, the projective limit of Fitting ideals not always gets the Fitting ideal, but in complete local noetherian rings does ([4, Apendix (10)] or [3]), thus:

$$\mathfrak{U}_{\mathfrak{m}} Fitt_{R_{a,\infty,\mathfrak{m}}}(H_{\mathfrak{m}}^{\flat}) \subseteq \mathfrak{b}_{\mathfrak{m}}^{(\infty)}. \quad (2)$$

And in order to get back to characteristic ideals and because $H_{\mathfrak{m}}$ is pseudo-isomorphic to $H_{\mathfrak{m}}^{\flat}$ (we have epimorphism between them with finite kernel) applying Lemma 5 (or [4, cor. prop.2 Appendix]):

$$\mathfrak{U}'_{\mathfrak{m}} char_{\mathcal{O}_{\psi}[[T]]}(H_{\mathfrak{m},\psi}) \subseteq \alpha_{\mathfrak{m},\psi}(\mathfrak{b}_{\mathfrak{m}}^{(\infty)}) \quad (3)$$

where $\mathfrak{U}'_{\mathfrak{m}} \subseteq R_{a,\infty,\mathfrak{m}}$ an ideal of finite index.

Now combining equations (1) and (3):

$$(1 - l\psi(l)[l])^k char_{\mathcal{O}_{\psi}[[T]]}(H_{\mathfrak{m},\psi}) \subseteq (G_{p,2}(\psi^{-1}, (1+T)^{-1} - 1)). \quad (4)$$

Now take $\psi := \chi\omega^{-2}$. Now by Proposition 16 one deduces
$$Char_{\mathcal{O}_{\psi}[[T]]}(H_{\infty,\hat{\chi}=\omega\chi^{-1}}) = (h_{\mathfrak{m},\psi}(u^{-1}(1+T)^{-1} - 1)$$
where $Char_{R_{a,\infty,\mathfrak{m}}}(H_{\infty,\psi}) = (h_{\mathfrak{m},\psi}(T))$, generated by the corresponding distinguished polynomial (we are with μ-invariant zero), and therefore we read equation (4) as follows:

$$(1 - \psi(l)[l](u^{-1}(1+T)^{-1} - 1))^k Char_{\mathcal{O}_{\psi}[[T]]}(H_{\infty,\hat{\chi}}) \subseteq (G_{p,2}(\psi^{-1} = \omega^2\chi^{-1}, u(1+T) - 1)) = (G_p(\chi, T)).$$

For the simplest case $k = 0$ we have an inclusion, (and in the general statement need analysis to the zeroes of $(1 - \psi(l)[l](u^{-1}(1+T)^{-1} - 1))$ and similar factors.

This allows to prove that
$$G_p(\chi, T) \textit{ divides } h_p(\hat{\chi}, T),$$
where $h_p(\hat{\chi}, T)$ is the distinguished polynomial such that $Char_{R_{a,\infty,\mathfrak{m}}}(H_{\infty,\hat{\chi}}) = (h_p(\hat{\chi}, T))$, (for this one use that in $\mathcal{O}_{\chi}[[T]]$ one have that if $\mathfrak{a}(f) \subset (g)$ with $f, g \in \mathcal{O}_{\chi}[[T]]$ and $\mathfrak{a}$ an ideal of $\mathcal{O}_{\chi}[[T]]$ of finite index then g divides f, see [4, Lemma3, Appendix]).[2].

The other divisibility follows for the analytic class number formula proving the IMC.

References

[1] H. Castillo, *Kubota-Leopoldt p-adic L-function*, see www.algant.eu/documents/theses/castillo.pdf

[2] J. Coates, *The work of Mazur-Wiles*, Bourbaki talk 475,...

[3] F. Nuccio,*Fitting ideals*, pp83–95 In *The Iwasawa theory of totally real fields*, LNS vol.12, Ramanujan math. society, (2010).

[4] B.Mazur and A.Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Inventiones math. **76** (1984), 179–330.

[2]Recall that the Fitting ideal is not always principal, and we need to replace it by the characteristic ideal in order to use the above Lemma 3 in the appendix of Mazur-Wiles