Cyclotomic Fields.

p will be a prime >2. μ_m = group of mth roots of unity in $\bar{\mathbb{Q}}$.

$F = \mathbb{Q}(\mu_p)$ $\quad \Theta: \Delta \hookrightarrow \mathrm{Aut}(\mu_p) = (\mathbb{Z}/p\mathbb{Z})^*$.

$\quad | \,)\Delta \qquad \sigma \mapsto (\zeta \mapsto \zeta^\sigma)$

$\mathbb{Q}$

Θ is onto by irreducibility of the cyclotomic equation.

$\Theta: \Delta \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^*$.

Θ as a canonical character of Δ with values in $\mathbb{F}_p$.

Θ^n, $n \in \mathbb{Z}$. n set of residues mod $(p-1)$

C = ideal class group of F.

C/C^p, a representation of Δ over $\mathbb{F}_p$.

Fundamental Question: Which of the characters Θ^n $(n \in \mathbb{Z})$ occur in representation on C/C^p. Easy: $\Theta^0, \Theta^1, \Theta^{-1}$ never occur.

Example: $p = 12613$. $\quad F \overset{12612}{|} \mathbb{Q}$ $\quad$ Fact: C/C^{12613} has dimension 4 over $\mathbb{F}_p$.
Θ^n occurs for $n = 2077, 3213, 12111, 12305$, with multiplicity 1.

Vandiver Conjecture: For every p, the only Θ^n which occur like this have n odd.

Iwasawa: $F_n = \mathbb{Q}(\mu_{p^{n+1}})$, $n = 0, 1, 2, \dots$ $\quad F_n \,|\,)\mathcal{G}_n\, \mathbb{Q}$ $\quad \mathcal{G}_n \hookrightarrow \mathrm{Aut}(\mu_{p^{n+1}}) = (\mathbb{Z}/p^{n+1}\mathbb{Z})^*$.
Irreducibility of cyclotomic equation $\Rightarrow$ this is an isomorphism.

$F_\infty = \bigcup_{n=0}^{\infty} F_n = \mathbb{Q}(\mu_{p^\infty})$. $\mathcal{G}_\infty = \mathrm{Gal}(F_\infty/\mathbb{Q}) = \varprojlim \mathcal{G}_n$

$\psi: \mathcal{G}_\infty \xrightarrow{\sim} \varprojlim (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \cong \mathbb{Z}_p^\times$ - cyclotomic character. $\sigma(\zeta) = \zeta^{\psi(\sigma)}$, $\zeta \in \mu_{p^\infty}$.

$\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$. $\quad 1 + p\mathbb{Z}_p \xrightarrow{\log} p\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}_p$.

Example: When $p = 12613$, p-primary part of ideal class group of $\mathbb{Q}(\mu_{p^\infty})$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^4$.

Two ingredients of "Main Conjecture":
(i) Analytic one: classical essentially and almost in Kummer.
(ii) Algebraic one.

Iwasawa formulated and proved "half" of it. Proved it if no Θ^n for n even occurs (for p) in C/C^p. (1964-70).
Early '80's: Mazur-Wiles gave first unconditional proof of whole Main Conjecture
Mid '80's: Thaine & Kolyvagin gave new variant of ideas of Kummer. (eg. Euler Systems).

Iwasawa algebra: G, profinite abelian group. Eg: $G = \mathbb{Z}_p^\times$ or $G = \mathbb{Z}_p^\times/\{\pm 1\}$.
Ω: set of open subsets of G.
Definition: $\Lambda(G)$ = Iwasawa algebra of G = $\varprojlim_{H \in \Omega} \mathbb{Z}_p[G/H]$.

May write $\Lambda(G) = \mathbb{Z}_p[[G]] \hookleftarrow \mathbb{Z}_p[G]$.
└ dense subalgebra.

Interpretation of elements of $\Lambda(G)$ as measures.

$\mathbb{C}_p$ = completion of an algebraic closure of $\mathbb{Q}_p$. $f: G \to \mathbb{C}_p$, continuous.

$\mu \in \Lambda(G)$ as measures on G with values in $\mathbb{Z}_p$. Want to define $\int_G f \, d\mu$.

Step 1: Locally constant $f: G \to \mathbb{C}_p$.

$\Rightarrow \exists H \in \Omega$ such that f is constant on G/H

For $H \in \Omega$, we have canonical map $\pi_H: \Lambda(G) \to \mathbb{Z}_p[G/H]$.

$\pi_H(\mu) = \sum_{\tau \in G/H} c_H(\tau)\tau$, $c_H(\tau) \in \mathbb{Z}_p$.

Define $\int_G f \, d\mu = \sum_{\tau \in G/H} c_H(\tau) f(\tau) \in \mathbb{C}_p$.

Consider $C(G, \mathbb{C}_p) = \{ f: G \to \mathbb{C}_p : f \text{ is continuous} \}$.

Can define norm $\|f\| = \sup_{x \in G} |f(x)|$.

For $H \in \Omega$, define $f_H: G/H \to \mathbb{C}_p$. Pick any set $\{\tau\}$ of representatives of G/H.

$f_H(\tau H) = f(\tau)$. Then $f_H \to f$ as $H \to 0$, with this norm.

Definition: $\int_G f \, d\mu = \lim_{H \to 0} \int_G f_H \, d\mu$.

Exercises: (i) $\mu = g \in G$. Dirac measure attached to g: $\int_G f \, dg = f(g)$.

(ii) $\Lambda(G)$ has a multiplication $\longleftrightarrow$ convolution of measures.

(iii) If $g \in G$, $\int_G f(gx) \, d\mu(x) = \int_G f(x) \, d(g\mu(x))$.

Integration of p-adic characters of G.

Definition: $X(G) = \mathrm{Hom}(G, \mathbb{C}_p^\times)$

For example, $\mathbb{Z}_p^\times \to \mathbb{C}_p^\times$; $x \mapsto x^m$ $(m \in \mathbb{Z})$.

Lemma: Let $\varphi \in X(G)$. Then φ can be extended uniquely to a continuous $\mathbb{Z}_p$-algebra homomorphism $\tilde{\varphi}: \Lambda(G) \to \mathbb{C}_p$.

Proof: Define $\tilde{\varphi}(\mu) = \int_G \varphi \, d\mu \quad \forall \mu \in \Lambda(G)$.

Pseudo-measure.

In general, $\Lambda(G)$ will have divisors of zero, eg. if $G = \mathbb{Z}_p^\times$.

$Q(G)$ = ring of fractions of $\Lambda(G) = \{ \frac{\alpha}{\beta} : \alpha, \beta \in \Lambda(G), \beta \text{ not a divisor of zero} \}$.

Definition: Take $\varphi \in X(G)$. We say $\mu \in Q(G)$ is a φ-pseudo-measure if $(\varphi(g) - g)\mu \in \Lambda(G) \quad \forall g \in G$.

If we can take φ = trivial character, call this a pseudo-measure.

Claim: Assume $\mu \in Q(G)$ which is a φ-pseudo-measure. Take any $\rho \in X(G)$, $\rho \neq \varphi$.
Then we define $\int_G \rho \, d\mu = \dfrac{\int \rho \, d((\varphi(g)-g)\mu)}{\varphi(g)-\rho(g)}$, for $g \in G$ such that $\varphi(g) \neq \rho(g)$.

Independence of the choice of g: Suppose $\varphi(g_i) = \rho(g_i)$, $i = 1,2$.

$$\int \rho \, d((\varphi(g_1)-g_1)\mu) \times (\varphi(g_2)-\rho(g_2)) \overset{(*)}{=} \int \rho \, d\left(\varphi(g_2)(\varphi(g_1)-g_1)\mu - g_2(\varphi(g_1)-g_1)\mu\right)$$

$(*)$: since $-\int \rho(g_2)\, \rho \, d((\varphi(g_1)-g_1)\mu) = -\int \rho \, d(g_2(\varphi(g_1)-g_1)\mu)$

$$= \int \rho \, d\left(\mu(\varphi(g_2)\varphi(g_1) - \varphi(g_2) g_1 - g_2 \varphi(g_1) + g_1 g_2)\right) \quad \text{- symmetric in } g_1, g_2.$$

So $\int \rho \, d\mu$ is well-defined.

Iwasawa-Kubota-Leopoldt pseudo-measure μ_B (p-adic avatar of $\zeta(s)$ etc.)

What is G in this case? Let $q = 4$ or p according as $p=2$ or $p>2$. Let $q_n = qp^n$ $(n = 0,1,2,\dots)$

$F_n = \mathbb{Q}(\mu_{q_n})$, $K_n = F_n \cap \mathbb{R}$. $[F_n : K_n] = 2$.

$F_\infty = \cup F_n = \mathbb{Q}(\mu_{p^\infty})$, $K_\infty = \cup K_n = F_\infty \cap \mathbb{R}$.

$\mathcal{G}_\infty = Gal(F_\infty/\mathbb{Q})$, $G_\infty = Gal(K_\infty/\mathbb{Q}) = \mathcal{G}/\langle 1, \tau \rangle$, τ = complex conjugation.

$\psi : \mathcal{G}_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times$, $\psi(\tau) = -1$. So $G_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times / \{\pm 1\}$.

$$\mathbb{Z}_p^\times = \begin{cases} \mu_4 \times (1 + 4\mathbb{Z}_2), & p = 2 \\ \mu_{p-1} \times (1 + p\mathbb{Z}_p) \end{cases}$$
Ψ
$x = \omega(x) \langle x \rangle$.

What is $Hom(\mathcal{G}_\infty, \mathbb{C}_p^\times)$? $= Hom(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$

$\mathbb{Z}_p^\times \to (\mathbb{Z}/q_n\mathbb{Z})^\times$, so a character of $(\mathbb{Z}/q_n\mathbb{Z})^\times$ composes to give a character for $\mathbb{Z}_p^\times$.

Example, $x \mapsto \langle x \rangle^s$, $s \in \mathbb{Z}_p$, composed with χ - Dirichlet character mod q_n.

All elements of $Hom(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$ are of form $\chi . \langle x \rangle^s$, for some χ of finite order, $s \in \mathbb{Z}_p$

Algebraic characters $\chi \psi^m$, $m \in \mathbb{Z}$, χ of finite order. This is a character of $G \iff \chi(\tau) = (-1)^m$.

χ of finite order of $\mathcal{G}_\infty \xleftrightarrow{\psi}$ character of $(\mathbb{Z}/q_n\mathbb{Z})^\times$ for some n.

Define $L(\chi, s) = \prod_{r \text{ primes}} \left(1 - \frac{\chi(r)}{r^s}\right)^{-1}$, $\quad r \neq p$, $\chi(r) = \chi(r \bmod q_n)$
$\quad r = p$, $\chi(p) = 0$, if $\chi \neq$ trivial character.
$\quad = 1$, if χ = trivial character.

primitive Dirichlet L-function of χ.

Fact: $\forall m \geq 0$, $L(\chi, -m) \in \overline{\mathbb{Q}}$

Main Analytic Theorem: There exists a unique pseudo-measure μ_B on G_∞ such that for all characters χ of finite order of $\mathcal{G}_\infty$ and all integers $k \geq 1$ such that $\chi(\tau) = (-1)^k$,
we have $\int_G \chi \psi^k \, d\mu_B = L(\chi, 1-k) \times (1 - \chi(p) . p^{k-1})$.

Preliminaries from complex theory

q_n, $n \geq 0$. $c \in (\mathbb{Z}/q_n\mathbb{Z})^\times$. Define partial zeta function $\zeta(c, q_n, s) = \sum_{\substack{n \in c \\ n \geq 1}} n^{-s}$.

Lemma: If χ is a Dirichlet character mod q_n, then
$$L(\chi,s)(1-\chi(p)\cdot p^{-s}) = \sum_{c\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi(c)\,\zeta(c,q_n,s).$$
$$\Big\|$$
$$\sum_{\substack{n=1\\(n,p)=1}}^{\infty} \frac{\chi(n)}{n^s}$$

if $u\in\mathbb{Z}_p^\times$, define $\zeta(u,q_n,s) = \zeta([u]_n, q_n, s)$.
$$\begin{array}{cc} \rotatebox{90}{$\in$} & \downarrow \\ [u]_n & (\mathbb{Z}/q_n\mathbb{Z})^\times \end{array}$$

Recall: $\frac{t}{e^t-1} = \sum_{m=0}^{\infty} \frac{B_m t^m}{m!}$, where B_m are the Bernoulli numbers.
The mth Bernoulli polynomial is given by: $\frac{te^{tx}}{e^t-1} = \sum_{m=0}^{\infty} B_m(x)\frac{t^m}{m!}$
$B_m(x) = \sum_{i=0}^{m}\binom{m}{i} B_i\, x^{m-i}$.

Let $s_n(u)$ = unique representative of $[u]_n$ with $0 < s_n(u) < q_n$.

Theorem: For each $u\in\mathbb{Z}_p^\times$, and all $n\geq 0$ and $k\geq 1$, we have
$$\zeta(u,q_n,1-k) = -\frac{q_n^{k-1}}{k} B_k\left(\frac{s_n(u)}{q_n}\right) \in \mathbb{Q}.$$
Proof: See Washington.

Definition: For $v,u\in\mathbb{Z}_p^\times$ and $k\geq 1$, we let $\Delta_k(u,v,q_n) = v^k\zeta(u,q_n,1-k) - \zeta(uv,q_n,1-k)$.

Theorem: (i) $\Delta_1(u,v,q_n)\in\mathbb{Z}_p$
(ii) $\Delta_k(u,v,q_n) \equiv (uv)^{k-1}\Delta_1(u,v,q_n) \bmod q_n$. $(n\geq 0,\ k\geq 1)$.

$B_1(x) = x-\frac{1}{2}$. $v\zeta(u,q_n,0) = -B_1\left(\frac{s_n(u)}{q_n}\right)\cdot v = \frac{v}{2} - \frac{s_n(u)}{q_n}v$.
$\zeta(uv,q_n,0) = \frac{1}{2} - \frac{s_n(uv)}{q_n}$

So $\Delta_1(u,v,q_n) = \frac{v-1}{2} + \frac{s_n(uv) - v\,s_n(u)}{q_n}$ But, $v s_n(u) \equiv uv \equiv s_n(uv) \bmod q_n$.
So $\Delta_1(u,v,q_n)\in\mathbb{Z}_p$.

Change notation:
Definition: $u,v\in\mathbb{Z}_p^\times$, $k\geq 1$, $n\geq 0$. $\Delta_k(u,v,q_n) = \zeta(u,q_n,1-k) - v^k\zeta(uv^{-1},q_n,1-k)$.
(If $\Delta_k'(u,v,q_n)$ is as defined last time, have $\Delta_k(u,v,q_n) = v^k\Delta_k'(u,v^{-1},q_n)$).

The theorem becomes:
Theorem: (i) $\Delta_1(u,v,q_n)\in\mathbb{Z}_p$. (Proof as before).
(ii) For all integers $k\geq 1$, we have $\Delta_k(u,v,q_n) \equiv u^{k-1}\Delta_1(u,v,q_n) \bmod q_n$.
Definition: Let p^e be the largest power of p dividing the denominator of any of
$B_1/k = \frac{-1}{2k}$, B_2/k, .., B_k/k.

Lemma 2: For all $n\geq 0$, we have $\zeta(u,q_{n+e},1-k) \equiv \frac{k-1}{k}\cdot\frac{u^k}{q_{n+e}} + u^{k-1}\cdot\zeta(u,q_{n+e},0) \bmod q_n$.
Proof: $\zeta(u,q_{n+e},1-k) = -\frac{q_{n+e}^{k-1}}{k}\cdot B_k\left(\frac{s_{n+e}(u)}{q_{n+e}}\right)$ .. $0 < s_{n+e}(u) < q_{n+e}$.

$B_k(x) = \sum_{i=0}^{k} \binom{k}{i} . B_i . x^{k-i} = x^k - \frac{1}{2}x^{k-1} + \dots$

So $\zeta(u, q_{n+e}, 1-k) \equiv \frac{-s_{n+e}(u)^k}{k\, q_{n+e}} + \frac{1}{2} s_{n+e}(u)^{k-1} \bmod q_n$.

$\equiv \frac{-s_{n+e}(u)^k}{k\, q_{n+e}} + \frac{1}{2} u^{k-1} \bmod q_n$, since $p^e/2 \in \mathbb{Z}_p$.

Write $u - s_{n+e}(u) = -q_{n+e}\, w$.

$s_{n+e}(u)^k = (u + q_{n+e} w)^k \equiv u^k + k q_{n+e}\, w . u^{k-1} \bmod q_{n+e}^2$. Put $w = \frac{s_{n+e}(u) - u}{q_{n+e}}$.

$\frac{s_{n+e}(u)^k}{k q_{n+e}} \equiv \frac{u^k}{k q_{n+e}} + u^{k-1}\left(\frac{s_{n+e}(u)-u}{q_{n+e}}\right) \bmod q_n$.

$\equiv \frac{1-k}{k} . \frac{u^k}{q_{n+e}} + u^{k-1} . \frac{s_{n+e}(u)}{q_{n+e}} \bmod q_n$.

So $\zeta(u, q_{n+e}, 1-k) \equiv \frac{k-1}{k} . \frac{u^k}{q_{n+e}} + u^{k-1} \underbrace{\left(\frac{1}{2} - \frac{s_{n+e}(u)}{q_{n+e}}\right)}_{= -B_1\left(\frac{s_{n+e}(u)}{q_{n+e}}\right)} \bmod q_n$

Corollary: $\Delta_k(u, v, q_{n+e}) = \zeta(u, q_{n+e}, 1-k) - v^k\, \zeta(uv^{-1}, q_{n+e}, 1-k)$.

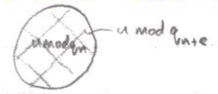
$\equiv u^{k-1} \zeta(u, q_{n+e}, 0) - u^{k-1} v^{1-k} . v^k . \zeta(uv^{-1}, q_{n+e}, 0) \bmod q_n$.

$\equiv u^{k-1} \Delta_1(u, v, q_{n+e}) \bmod q_n \quad \forall\, n \geq 0$.

Lemma: Given $u \in \mathbb{Z}_p^\times$ and $n \geq 0$, then for all $r \geq 0$, we have
$\sum_w \zeta(w, q_{n+e}, s) = \zeta(u, q_n, s)$, where w runs over any set of representatives of $(\mathbb{Z}/q_{n+r}\mathbb{Z})^\times$ which map to $u \bmod q_n$ in $(\mathbb{Z}/q_n\mathbb{Z})^\times$.

Proof: Obvious from Dirichlet series when $Re(s) > 1$.

RHS $= \sum_{\substack{m \geq 1 \\ (m,p)=1 \\ m \in u \bmod q_n}} m^{-s}$. LHS:



So we are summing over the same elements.

Apply with $r = e$. $\sum_w \Delta_k(w, v, q_{n+e}) = \Delta_k(u, v, q_n)$.

Now, $\Delta_k(w, v, q_{n+e}) \equiv w^{k-1} \Delta_1(w, v, q_{n+e}) \bmod q_n$. $\forall w$.

$\equiv u^{k-1}\, \Delta_1(w, v, q_{n+e}) \bmod q_n \quad \forall u$.

Sum over w: $\Delta_k(u, v, q_n) \equiv u^{k-1} \Delta_1(u, v, q_n) \bmod q_n$.

This proves theorem (ii).

Recall that we are trying to find a pseudo-measure on $G_\infty = Gal(K_\infty/\mathbb{Q}) = \mathcal{G}_\infty / \langle 1, c \rangle$, such that $\int_{G_\infty} \chi \psi^k d\mu_B = L(\chi, 1-k) . (1 - \chi(p) . p^{k-1})$, $\forall\, k \geq 1$ with $\chi(c) = (-1)^k$.
(χ of finite order of $\mathcal{G}_\infty$ and $\chi(c) = (-1)^k$).

We will first construct pseudo-measure μ_A with $\int_{G_\infty} \chi \psi^{k-2} d\mu_A = L(\chi, 1-k) . (1 - \chi(p) . p^{k-1})\ \forall\, k \geq 1$.

Note: If $g: G_\infty \to \mathbb{C}_p$, continuous, this gives a measure via $\int_{G_\infty} f(x) g(x)\, d\mu(x) = \int_{G_\infty} f(x)\, d\mu_g(x)$.
So we will take $\mu_B = \mu_A\, \psi^{-2}$, $\psi^{-2}: G_\infty \to \mathbb{C}_p$.

Recall: We have:

$$\begin{array}{l} \mathcal{G}_\infty \left(\begin{array}{l} F_\infty = \mathbb{Q}(\mu_{p^\infty}) \\ \ \ | \\ K_\infty = \mathbb{Q}(\mu_{p^\infty}) \\ \ \ | \ \ \Big) \ G_\infty \\ \ \mathbb{Q} \end{array} \right. \end{array}$$

Want to look at $\varprojlim \mathbb{Z}_p[G(K_n/\mathbb{Q})]$.

Have $\psi: \mathcal{G}_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times$

$\sigma_u \longmapsto u$

Write $\tau_u = \sigma_u | K_\infty$

$\sigma_{u,n} = \sigma_u | F_n \in G(F_n/\mathbb{Q})$

$\tau_{u,n} = \tau_u | K_n \in G(K_n/\mathbb{Q})$.

W_n - any set of representatives in $\mathbb{Z}_p^\times$ of $(\mathbb{Z}/q_n\mathbb{Z})^\times$. $v \in \mathbb{Z}_p^\times$.

Key Definition: $\lambda_{v,n} = (1 - v^2 \tau_{v,n}) . \sum_{u \in W_n} \zeta(u, q_n, -1) \tau_{u,n} \quad \in \mathbb{Q}_p[G_n]$.

So $\lambda_{v,n} = \sum_{u \in W_n} \Delta_2(u, v, q_n) \tau_{u,n}$, where $\Delta_2(u, v, q_n) = \zeta(u, q_n, -1) - v^2 \zeta(uv^{-1}, q_n, -1)$.

So $\lambda_{v,n} \in \mathbb{Z}_p[G_n]$. - Fact 1.

Fact 2: $(\lambda_{v,n}) \in \varprojlim \mathbb{Z}_p[G_n]$. We have: $\sum_w \Delta_2(w, v, q_{n+r}) = \Delta_2(u, v, q_n)$, any $r \geq 0$.

w such that under $(\mathbb{Z}/q_{n+r}\mathbb{Z})^\times \to (\mathbb{Z}/q_n\mathbb{Z})^\times$ have $w \longmapsto u \bmod q_n$.

Projective limit: $(1 - v^2 \tau_{v,n}) = 1 - v^2 \tau_v$ ~ not a zero divisor in $\Lambda(G_\infty)$ when v is not a root of unity. Write $(\lambda_{v,n}) = \lambda_v$.

Definition: $\mu_A = \lambda_v / (1 - v^2 \tau_v) \in$ ring of quotients of $\Lambda(G_\infty)$. $\psi^{-2}(\tau_v) = v^{-2}$.
It is a ψ^{-2}-pseudo-measure.

We want $\int_{G_\infty} \chi \psi^{k-2} d\mu_A \quad \forall \chi$ of finite order of $\mathcal{G}_\infty$ with $\chi(c) = (-1)^k$ and all $k \geq 1$.

Calculation: $\int_{G_\infty} \chi \psi^{k-2} d\lambda_v = \lim_{\substack{n \to \infty \\ (n \gg 0)}} \sum_{u \in W_n} \Delta_2(u, v, q_n) \chi(u) u^{k-2} \quad - (*)$

Now, $\Delta_k(u, v, q_n) \equiv u^{k-1} \Delta_1(u, v, q_n) \equiv u^{k-2} \Delta_2(u, v, q_n) \bmod q_n$.

So $(*) = \lim_{n \to \infty} \sum_{u \in W_n} \Delta_k(u, v, q_n) \chi(u)$. Conductor of χ divides q_{n_0}.

So, $\sum_{w \in W_n} \Delta_k(w, v, q_n) \chi(w) = \sum_{u \in W_{n_0}} \Delta_k(u, v, q_{n_0}) \chi(u) \quad - (**)$

Let $L_{\{p\}}(\chi, s) = \prod_{r \neq p} \left(1 - \frac{\chi(r)}{r^s}\right)^{-1} = \sum_{\substack{n=1 \\ (n,p)=1}}^{\infty} \frac{\chi(n)}{n^s}$.

So $(**) = L_{\{p\}}(\chi, 1-k) - v^k \chi(v) L_{\{p\}}(\chi, 1-k) = (1 - v^k \chi(v)) . L(\chi, 1-k) . (1 - \chi(p) p^{k-1})$.
And this is thus $\int_{G_\infty} \chi \psi^{k-2} d\lambda_v$. Also, $\int_{G_\infty} \chi \psi^{k-2} d(1 - v^2 \tau_v) = (1 - v^k \chi(v))$.

Conclusion: $\exists$ a ψ^{-2}-pseudo-measure μ_A on G_∞ such that
$\int_{G_\infty} \chi \psi^{k-2} d\mu_A = L(\chi, 1-k) . (1 - \chi(p) p^{k-1})$, χ finite order, $\chi(c) = (-1)^k$, $k \geq 1$.

Structure of Iwasawa Algebras in some special cases

$\Lambda(G)$, G a profinite abelian group.

Case 1: $G \xrightarrow{\sim} \mathbb{Z}_p$. $G = \Gamma$. Look at $\Lambda(\Gamma)$.

$\mathbb{Z}_p[[T]]$ = ring of formal power series in T with coefficients in $\mathbb{Z}_p$.

Fix a topological generator γ of Γ.

Proposition: There exists a unique continuous homomorphism of $\mathbb{Z}_p$-algebras, $\varepsilon: \mathbb{Z}_p[[T]] \xrightarrow{\sim} \Lambda(\Gamma)$ such that $\varepsilon(1+T) = \gamma$. (Recall: $\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\Sigma_n]$, Σ_n = unique cyclic quotient of Γ of degree p^n).

Basic facts about $\mathbb{Z}_p[[T]]$. (See Washington or Bourbaki).

1. Division algorithm. Assume that f is of the form $f = \sum_{n=0}^{\infty} a_n T^n$ where $a_i \in p\mathbb{Z}_p$ $(0 \le i < r)$ and $a_r \in \mathbb{Z}_p^\times$. If g is any element of $\mathbb{Z}_p[[T]]$, then there exist unique α, β in $\mathbb{Z}_p[[T]]$ such that $g = \alpha f + \beta$, where $\deg \beta < r$.

$$\omega_n(T) = (1+T)^{p^n} - 1 = \underbrace{\sum_{i=0}^{p^n-1} \binom{p^n}{i} T^i}_{\uparrow \text{ divisible by } p} + T^{p^n}$$

Definition: We say $f(T) = \sum_{n=0}^{r} a_n T^n$ is distinguished if $a_i \in p\mathbb{Z}_p$ $(0 \le i < r)$ and $a_r = 1$.

Weierstrass Preparation Theorem: Every $g \in \mathbb{Z}_p[[T]]$ can be written uniquely in the form $g = p^\mu f w$, where $\mu \in \mathbb{Z}$, $\mu \ge 0$, f is a distinguished polynomial, and $w \in \mathbb{Z}_p[[T]]^\times$.

Corollary: Given $g \ne 0$ in $\mathbb{Z}_p[[T]]$, there exist only finitely many $x \in \mathbb{C}_p$ with $|x|_p < 1$ such that $g(x) = 0$.

$g(T) = \sum_{n=0}^{\infty} a_n T^n$, $g(x) = \sum_{n=0}^{\infty} a_n x^n$. $g(x) = 0 \Rightarrow f(x) = 0$.

Corollary: The natural map $\mathbb{Z}_p[T]/(\omega_n(T)) \longrightarrow \mathbb{Z}_p[[T]]/(\omega_n(T))$ is an isomorphism.

$\Lambda(\Gamma)$. $\Gamma = \varprojlim \Sigma_n$, $\Sigma_n \cong \mathbb{Z}/p\mathbb{Z}$.

$\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\Sigma_n]$

There is a unique isomorphism $\mathbb{Z}_p[T]/(\omega_n(T)) \xrightarrow{\sim} \mathbb{Z}_p[\Sigma_n]$

$1+T \bmod \omega_n(T) \longmapsto \gamma_n$ = image of γ in Σ_n.

Then $\Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[T]/(\omega_n(T))$

$\gamma \mapsto (1+T)$

$$\begin{array}{ccc} \text{So} \quad \Lambda(\Gamma) & \xrightarrow{\sim} & \varprojlim \mathbb{Z}_p[T]/(\omega_n(T)) \\ \gamma & \longmapsto & (1+T) \quad \uparrow i \\ & & \mathbb{Z}_p[[T]] \end{array}$$

– final step is to show i is an isomorphism.

i is injective by Weierstrass. i is surjective by completeness. Both spaces are compact. $\mathrm{Im}(i)$ is dense. i is continuous, so the image of a closed set is closed, and we get the whole set. So $\Lambda(\Gamma) \xrightarrow{\sim} \mathbb{Z}_p[[T]]$.

<u>Remark</u>: Given $f(T) \in \mathbb{Z}_p[[T]]$, and let $\varepsilon(f(T)) = \mu$ be the corresponding measure in $\Lambda(\Gamma)$. Take φ to be any element of $\mathrm{Hom}(\Gamma, \mathbb{C}_p^\times)$. This gives $\tilde{\varphi} : \Lambda(\Gamma) \to \mathbb{C}_p$.

(Recall $\tilde{\varphi}(\mu) = \int_\Gamma \varphi \, d\mu$).

Suppose $f(T) = \sum_{n=0}^{\infty} a_n T^n$ with $a_n \in \mathbb{Z}_p$.

Claim that $\tilde{\varphi}(\mu) = \sum_{n=0}^{\infty} a_n (\varphi(\gamma) - 1)^n \; .= f(\varphi(\gamma) - 1)$.

$\mathbb{Z}_p[[T]]$. Maximal ideal, $\mathfrak{m} = (p, T)$. $\wp$, prime ideal, has height 1, $\wp = (f)$, f an irreducible distinguished polynomial.

For $p > 2$, $G_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times / \{\pm 1\} \xrightarrow{\sim} \mu_{p-1}/\{\pm 1\} \times (1 + p\mathbb{Z}_p) \xrightarrow{\sim} \mu_{p-1}/\{\pm 1\} \times \mathbb{Z}_p$.

<u>Case 2</u>: Assume $G = \Delta \times \Gamma$, where Δ is finite, and $\Gamma \cong \mathbb{Z}_p$.

Let $\Omega = \mathbb{Z}_p[\Delta]$

<u>Definition</u>: $\Omega[[T]]$ = ring of all formal power series in T with coefficients in Ω.

$$f = \sum_{n=0}^{\infty} a_n T^n, \quad a_n = \sum_{\delta \in \Delta} c_{n,\delta} \delta, \quad c_{n,\delta} \in \mathbb{Z}_p.$$

Let γ be a fixed topological generator of Γ.

$\Omega \subset \mathbb{Z}_p[G] \subset \Lambda(G)$.

<u>Proposition</u>: There is a unique isomorphism of topological algebras $\varepsilon : \Omega[[T]] \to \Lambda(G)$ which preserves the natural inclusion of Ω in $\Lambda(G)$, and $\varepsilon(1+T) = \gamma$.

$\Gamma = \varprojlim \Sigma_n$. $\mathbb{Z}_p[\Delta \times \Sigma_n] = \Omega[\Sigma_n]$. $\Lambda(G) = \varprojlim \Omega[\Sigma_n]$.

Claim $\varprojlim \Omega[\Sigma_n] \cong \varprojlim \Omega[T]/(\omega_n)$.

We need: (i) $\Omega[T]/(\omega_n) \xrightarrow{\sim} \Omega[[T]]/(\omega_n(T))$

(ii) $\Omega[[T]] \xrightarrow{\sim} \varprojlim \Omega[[T]]/(\omega_n(T))$.

$(\mathbb{Z}_p[T]/(\omega_n))^r \qquad (\mathbb{Z}_p[[T]]/(\omega_n))^r \qquad r = \#(\Delta)$

<u>Remark</u>: $f(T) = \sum_{n=0}^{\infty} a_n T^n \in \Omega[[T]]$, $a_n \in \Omega$, $\varepsilon(f(T)) = \mu$.

$\varphi \in \mathrm{Hom}(G, \mathbb{C}_p^\times)$, $\tilde{\varphi}(\mu) = \int_G \varphi \, d\mu = \sum_{n=0}^{\infty} \theta(a_n)(\varphi(\gamma) - 1)^n$ where $\theta = \varphi|_\Delta$.

<u>Uniqueness of L.K.I pseudo-measure.</u>

$\mathcal{G}_\infty = G(F_\infty/\mathbb{Q})$, $G_\infty = \mathcal{G}_\infty / \langle 1, c \rangle$

$$\Psi : \mathcal{G}_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times \xrightarrow{\sim} \begin{cases} \mu_2 \times (1 + 4\mathbb{Z}_2) & \text{when } p = 2 \\ \mu_{p-1} \times (1 + p\mathbb{Z}_p) & \text{when } p > 2. \end{cases}$$

$$G_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times/\{\pm 1\} \xrightarrow{\sim} \begin{cases} 1 + 4\mathbb{Z}_2 & \text{when } p = 2 \\ \mu_{p-1}/\{\pm 1\} \times (1 + p\mathbb{Z}_p) & \text{when } p > 2. \end{cases}$$

$\mathcal{G}_\infty = \mathcal{D} \times \Gamma$, $\mathcal{D} \xrightarrow{\sim} G(F_0/\mathbb{Q})$ $\qquad \theta = \Psi|_{\mathcal{D}}$ $\quad \mathrm{Hom}(\mathcal{D}, \mathbb{C}_p^\times) = \{\theta^i, \ i \bmod 2 \text{ if } p = 2, \ i \bmod p-1, (p>2)\}$

$G_\infty = D \times \Gamma$ $\quad D \xrightarrow{\sim} G(K_0/\mathbb{Q})$ $\qquad \mathrm{Hom}(D, \mathbb{C}_p^\times) = \{\theta^i, \ i \text{ even} \bmod p-1\}$.

Lemma: Suppose μ_1, μ_2 are two elements of $\Lambda(G)$. Then

(i) If $p=2$ and $\int_{\mathcal{G}_\infty} \psi^n d\mu_1 = \int_{\mathcal{G}_\infty} \psi^n d\mu_2$ for infinitely many even $n \in \mathbb{Z}$, then $\mu_1 = \mu_2$.

(ii) If $p>2$ and $\int_{\mathcal{G}_\infty} \psi^n d\mu_1 = \int_{\mathcal{G}_\infty} \psi^n d\mu_2$ for infinitely many $n \in \mathbb{Z}$ lying in each even residue class mod $p-1$, then $\mu_1 = \mu_2$.

Proof: (ii) $\Lambda(\mathcal{G}_\infty) \xrightarrow{\sim} \Omega[[T]]$, $\Omega = \mathbb{Z}_p[D]$

$\mu_i \longleftrightarrow f_i = \sum_{k=0}^{\infty} a_{k,i} T^i$, $a_{k,i} \in \Omega$

γ - topological generator of Γ. k even, $\chi = \theta^k$, $n \equiv k \mod p-1$.

$\int_{\mathcal{G}_\infty} \psi^n d\mu_1 = \sum_{k=0}^{\infty} \chi(a_{k,i})(\psi(\gamma)^n - 1)^k$, $k = 0, 1, \ldots$ $\forall \chi \in \mathrm{Hom}(D, \mathbb{C}_p^\times)$

$\Rightarrow \sum_{k=0}^{\infty} \chi(a_{k,1}) T^n = \sum_{k=0}^{\infty} \chi(a_{k,2}) T^n \Rightarrow \chi(a_{k,1}) = \chi(a_{k,2}) \Rightarrow a_{k,1} = a_{k,2}$ $\forall k \geq 0 \Rightarrow \mu_1 = \mu_2$.

Hence μ_A and $\mu_B = \psi^{-2} \mu_A$ are unique.

2. Local Theory. $(p>2)$.

$$\begin{array}{ccl} \wp_n & \Phi_n = \mathbb{Q}_p(\mu_{p^{n+1}}) & \\ | & | \quad \big) \mathcal{G}_n & \cong \mathrm{Aut}(\mu_{p^{n+1}}) = (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times. \\ p & \mathbb{Q}_p & \end{array}$$

Let $\Phi_\infty = \bigcup \Phi_n = \mathbb{Q}_p(\mu_{p^\infty})$
$\mathcal{G}_\infty = G(\Phi_\infty / \mathbb{Q}_p)$

Let U_n = units of (ring of integers of) Φ_n which are $\equiv 1 \mod \wp_n$. - $\mathbb{Z}_p$ - module.
$\mathcal{G}_n$ - module structure. $\mathbb{Z}_p[\mathcal{G}_n]$ - structure.

$m \geq n$: $N_{m,n} : \Phi_m^\times \to \Phi_n^\times$

Definition: $U_\infty = \varprojlim U_n$. - a $\mathbb{Z}_p[\mathcal{G}_\infty]$ - module. $\mathbb{Z}_p[\mathcal{G}_\infty] \subset \Lambda(\mathcal{G}_\infty)$.

Let G be any profinite abelian group, X a compact $\mathbb{Z}_p$ - module on which G acts continuously.
Let Ω = set of all open subgroups of G. $H \in \Omega$.

Definition: $(X)_H$ = largest quotient of X on which H acts trivially.

Claim: $X = \varprojlim_{H \in \Omega} (X)_H$.

For now, accept this. If we have $x \in X$, $\xi \in \Lambda(G)$. x has image x_H in $(X)_H$, ξ has image ξ_H in $\mathbb{Z}_p[G/H]$. Then $\xi . x = (\xi_H . x_H)$.

Recall: $\hat{X} = \mathrm{Hom}_{cts}(X, \mathbb{Q}_p/\mathbb{Z}_p)$. X compact $\Rightarrow$ $\hat{X}$ discrete. G acts on $X \Rightarrow G$ acts continuously on $\hat{X}$. $(\sigma f)(x) = f(\sigma^{-1} x)$.

$\hat{X}$ a discrete G-module. $\hat{X} = \bigcup_{H \in \Omega} (\hat{X})^H = \varinjlim_{H \in \Omega} (\hat{X})^H$. $X = \varprojlim_{H} \widehat{(\hat{X})^H}$

$X \times \hat{X} \to \mathbb{Q}_p / \mathbb{Z}_p$. $X = \varprojlim_{H} (X)_H$.

$(X)_H$ $(\hat{X})^H$

So $\mathcal{U}_\infty = \varprojlim \mathcal{U}_n$ is a $\Lambda(\mathcal{G}_\infty)$-module.

(i) Weak way: use Class Field Theory, and Structure Theory of $\Lambda(\mathcal{G}_\infty)$-modules.
(ii) Strong way: We will construct a canonical $\Lambda(\mathcal{G}_\infty)$-homomorphism $\iota_\infty : \mathcal{U}_\infty \to \Lambda(\mathcal{G}_\infty)$.

$\forall n \geq 0$, choose ζ_n - generator of $\mu_{p^{n+1}}$, $\zeta_n^p = \zeta_{n-1}$ $\forall n \geq 0$. Choose such a compatible system (ζ_n). $\zeta_n - 1$ is a local parameter (has order 1) of Φ_n for all $n \geq 0$.
$u_n \in \mathcal{U}_n$, clearly exists. $f_n(T) \in \mathbb{Z}_p[[T]]$, $f_n(\zeta_n - 1) = u_n$. (f_n is not unique).

Theorem: Assume $u = (u_n)$ is any element of $\mathcal{U}_\infty = \varprojlim \mathcal{U}_n$. Then there exists a unique power series $f_n(T) \in \mathbb{Z}_p[[T]]$ such that $f(\zeta_n - 1) = u_n$ $\forall n \geq 0$.

The uniqueness is obvious by the Weierstrass Preparation Theorem. Existence:

Proof (due to Coleman): We have given $\mathbb{Z}_p[[T]]$ the $\mathfrak{m}$-adic topology, where $\mathfrak{m}$ is the maximal ideal, $= (p, T)$.

Lemma: $\exists$ unique map $N : \mathbb{Z}_p[[T]] \to \mathbb{Z}_p[[T]]$ such that $(Nf)((1+T)^p - 1) = \prod_{\zeta \in \mu_p} f(\zeta(1+T) - 1)$.
Proof: Uniqueness is obvious from WPT.
Existence: Let $g(T) =$ power series on RHS, $\in \mathbb{Z}_p[[T]]$. Must show we can write $g(T) = h((1+T)^p - 1)$ for some $h \in \mathbb{Z}_p[[T]]$.
Note that $\forall \rho \in \mu_p$, $g(\rho(1+T) - 1) = g(T)$. $\Rightarrow g(T) = g(0) + ((1+T)^p - 1)g_1(T)$, since $g(T) - g(0)$ vanishes at every $\rho \in \mu_p$.
Claim: Can write $g(T) = \sum_{i=0}^{n-1} a_i((1+T)^p - 1)^i + ((1+T)^p - 1)^n g_n(T)$.
True for $n = 1$. $g_n(\rho(1+T) - 1) = g_n(T)$ $\forall \rho \in \mu_p$.
$\Rightarrow g_n(T) = g_n(0) + ((1+T)^p - 1)h_n(T)$. Continue induction.

$f \in \mathbb{Z}_p[[T]]$. $\Phi_m \xrightarrow{N_{m,n}} \Phi_n$.
$N_{n,n-1}(f(\zeta_n - 1)) = \prod_{\sigma \in G(\Phi_n | \Phi_{n-1})} (\sigma f)(\zeta_n - 1) = \prod_\sigma f(\sigma(\zeta_n) - 1)$

$[\sigma(\zeta_n) = \zeta \zeta_n, \ \zeta \in \mu_p.]$ $\qquad = \prod_{\zeta \in \mu_p} f(\zeta \zeta_n - 1) = (Nf)(\zeta_{n-1} - 1)$.

$f_u(\zeta_n - 1) = u_n$ $\forall n \geq 0$, $N_{n,n-1}(u_n) = u_{n-1}$. We need $Nf = f$.
$f(0) \equiv 1 \bmod p$. $(f(\zeta_n - 1)) \in \mathcal{U}_\infty$.

Take $f \in \mathbb{Z}_p[[T]]$. Show $N^k f$ $(k = 0, 1, 2, \ldots)$ converges to some $h \in \mathbb{Z}_p[[T]]$. Then $Nh = h$.

Lemma: Assume $f \in \mathbb{Z}_p[[T]]$ satisfies $f((1+T)^p - 1) \equiv 1 \bmod p^k \mathbb{Z}_p[[T]]$ for some $k \geq 1$.
Then $f(T) \equiv 1 \bmod p^k \mathbb{Z}_p[[T]]$.
Proof: $f(T) = 1 + p^\mu \sum_{n=0}^\infty a_n T^n$, $\mu \geq 0$, maximal. $\exists$ an integer $r \geq 0$ such that $a_0, \ldots, a_{r-1}$ are divisible by p, but $a_r \in \mathbb{Z}_p^\times$.
$\sum_{n=0}^\infty a_n((1+T)^p - 1)^n \equiv a_r T^{pr} + \sum_{n > r} a_n T^{pn} \bmod p\mathbb{Z}_p[[T]]$. (*) $(1+T)^p - 1 = T^p +$ (terms all divisible by p),
so (*) $\not\equiv 0 \bmod p\mathbb{Z}_p[[T]]$, as a_r isn't. So $f((1+T)^p - 1) - 1 = p^\mu \times h$, $h \notin p\mathbb{Z}_p[[T]]$, so $\mu \geq k$.

f a unit in $\mathbb{Z}_p[[T]] \iff f(0)$ a unit in $\mathbb{Z}_p^\times$.
$\Downarrow$
Nf a unit in $\mathbb{Z}_p[[T]]$. $Nf(0) = \prod f(\zeta - 1) \in \mathbb{Z}_p^\times$.

Lemma: Assume that f is a unit in $\mathbb{Z}_p[[T]]$. Then for all integers $k \geq 0$, we have $\frac{N^k f}{f} \equiv 1 \bmod p\,\mathbb{Z}_p[[T]]$.

Proof: $\frac{N^k f}{f} = \frac{N(N^{k-1}f)}{N^{k-1}f} \cdot \frac{N(N^{k-2}f)}{N^{k-2}f} \cdots \frac{Nf}{f}$, so we may assume $k=1$.

$Nf((1+T)^p - 1) = \prod_{\zeta \in \mu_p} f(\zeta(1+T) - 1)$. $f(\zeta(T+1)-1) \in \mathcal{O}_{\Phi_0}[[T]]$, $\wp_0 = (\zeta_0 - 1)$

So $\zeta(1+T) - 1 = \zeta T + \zeta - 1 \equiv T \bmod \wp_0$.

So $f(\zeta(1+T) - 1) \equiv f(T) \bmod \wp_0$.

So $Nf((1+T)^p - 1) \equiv f(T)^p \bmod \wp_0 \mathcal{O}_{\wp_0}[[T]] \equiv f(T)^p \bmod p\,\mathbb{Z}_p[[T]]$. $(*)$

Claim $(*) \equiv f(T^p) \bmod p\,\mathbb{Z}_p[[T]]$. For, we have $(a_0 + a_1 T + \dots)^p$ and $a_i^p \equiv a_i \bmod p$.

So $Nf((1+T)^p - 1) \equiv f(T^p) \bmod p\,\mathbb{Z}_p[[T]]$. But $(1+T)^p - 1 \equiv T^p \bmod p\,\mathbb{Z}_p[[T]]$.

So $\hookrightarrow \equiv f((1+T)^p - 1) \bmod p\,\mathbb{Z}_p[[T]]$.

Let $h(T) = \frac{Nf}{f}$. Then $h(T) \equiv 1 \bmod p\,\mathbb{Z}_p[[T]]$.

Lemma: Assume that f satisfies $f \equiv 1 \bmod p^k \mathbb{Z}_p[[T]]$ for some integer $k \geq 1$. Then $Nf \equiv 1 \bmod p^{k+1}\mathbb{Z}_p[[T]]$.

Proof: Suffices to show that $Nf((1+T)^p - 1) \equiv 1 \bmod p^{k+1}\mathbb{Z}_p[[T]]$. We have $\zeta(1+T) - 1 \bmod \wp_0$.

$\Rightarrow f(\zeta(1+T) - 1) \equiv f(T) \bmod \wp_0 p^k \mathcal{O}_{\wp_0}[[T]]$.

$Nf((1+T)^p - 1) \equiv f(T)^p \bmod p^{k+1}\mathbb{Z}_p[[T]] \equiv 1 \bmod p^{k+1}\mathbb{Z}_p[[T]]$.

Lemma: Assume $f \in \mathbb{Z}_p[[T]]^\times$ and $k_2 \geq k_1 \geq 0$. Then $N^{k_2} f \equiv N^{k_1} f \bmod p^{k_1+1}\mathbb{Z}_p[[T]]$.

Proof: By last time, $\frac{N^{k_2-k_1}f}{f} \equiv 1 \bmod p\,\mathbb{Z}_p[[T]]$. So $N^{k_1}\left(\frac{N^{k_2-k_1}f}{f}\right) \equiv 1 \bmod p^{k_1+1}\mathbb{Z}_p[[T]]$.

Corollary: For each $f \in \mathbb{Z}_p[[T]]^\times$, $g = \lim_{k\to\infty} N^k f$ exists, and satisfies $Ng = g$.

$u = (u_n) \in \varprojlim U_n$. $f_u(\zeta_n - 1) = u_n \ \forall n$. For each $n \geq 0$, $\exists\, f_n(T) \in \mathbb{Z}_p[[T]]$ such that $f_n(\zeta_n - 1) = u_n$.

Definition: $g_m(T) = (N^m f_{2m})(T) \quad \forall m \geq 0$.

$(N^k f_n)(\zeta_{n-k} - 1) = N_{n,n-k}\, f_n(\zeta_n - 1)$ (by defining property of N)
$= u_{n-k}. \quad \forall\, 0 \leq k \leq n$.

$(N^{m-n} g_m)(\zeta_n - 1) = (N^{2m-n} f_{2m})(\zeta_n - 1) = u_n$, $m \geq n \geq 0$.

$N^{m-n} g_m = N^{2m-n} f_{2m} \equiv \underset{g_m}{\underset{\parallel}{N^m f_{2m}}} \bmod p^{m+1}\mathbb{Z}_p[[T]]$

So $N^{m-n} g_m \equiv g_m \bmod p^{m+1}\mathbb{Z}_p[[T]]$.

$T = \zeta_n - 1$: $g_m(\zeta_n - 1) \equiv u_n \bmod p^{m+1}\mathcal{O}_{\Phi_n}$, $m \geq n$.

Fix n: $\lim_{m\to\infty} g_m(\zeta_n - 1) = u_n$. Have $\{g_m\} \in \mathbb{Z}_p[[T]]$

Convergent subsequence $\{g_{m_i}\}$. $g_{m_i} \to h \in \mathbb{Z}_p[[T]]$

$h(\zeta_n - 1) = u_n \ \forall n$.

Logarithm map in $1 + \mathfrak{m}$. $\log : 1 + \mathfrak{m} \to \mathbb{Q}_p[[T]]$. $f(T) = 1 + h(T)$, $h(T) \in \mathfrak{m} = (p, T)$.

$\log(f(T)) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{h(T)^n}{n}$

$u = (u_n) \in \mathcal{U}_\infty$. $f_u(\zeta_n - 1) = u_n$. $f_u(T) \in 1 + \mathfrak{m}$.

Definition: $l_u(T) = \mathrm{Log}\, f_u(T) - \frac{1}{p}\sum_{\zeta \in \mu_p} \mathrm{Log}\, f_u(\zeta(1+T)-1) \in \mathbb{Q}_p[[T]]$.

Lemma: $l_u(T) \in \mathbb{Z}_p[[T]]$ $\forall u \in \mathcal{U}_\infty$.

Proof: $\prod_{\zeta\in\mu_p} f_u(\zeta(1+T)-1) \equiv f_u(T)^p \mod p\mathbb{Z}_p[[T]]$ Let $h_u(T) = \dfrac{f_u(T)^p}{\prod_{\zeta\in\mu_p} f_u(\zeta(1+T)-1)}$

$h_u(T) = 1 + p k_u(T)$, $k_u(T) \in \mathbb{Z}_p[[T]]$.

$\mathrm{Log}\, h_u(T) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{p^n \cdot k_u(T)}{n} \in p\mathbb{Z}_p[[T]]$.

Claim: $np \mid p^n$ $\forall n \geq 1$.

$l_u(T) = \frac{1}{p}\mathrm{Log}\, h_u(T) \in \mathbb{Z}_p[[T]]$.

Mahler's Theorem: Let $f: \mathbb{Z}_p \to \mathbb{C}_p$ be any continuous function. Then $f(x)$ can be written uniquely as $f(x) = \sum_{n=0}^{\infty} a_n(f)\binom{x}{n}$, $\binom{x}{n} = \frac{x\cdot(x-1)\cdots(x-n+1)}{n!}$, where $a_n(f) \to 0$ as $n \to \infty$

Proof: $a_n(f) = \Delta^n f(0)$. $\Delta f(x) = f(x+1) - f(x)$. Hard: $a_n(f) \to 0$ as $n \to \infty$.

Given $\mu \in \Lambda(\mathbb{Z}_p)$, Let $c_n(\mu) = \int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x)$ $(n = 0, 1, \ldots)$

$\mu \mapsto h_\mu(T) := \sum_{n=0}^{\infty} c_n(\mu) T^n = \int_{\mathbb{Z}_p} (1+T)^x d\mu(x)$

Here we have a map: $\Lambda(\mathbb{Z}_p) \to \mathbb{Z}_p[[T]]$ - totally canonical.

$\mu \longmapsto h_\mu(T)$.

Lemma: Assume $f(x) = \sum_{n=0}^{\infty} a_n(f)\binom{x}{n}$. Then $\int_{\mathbb{Z}_p} f(x)\, d\mu(x) = \sum_{n=0}^{\infty} a_n(f)\, c_n(\mu)$.

Proof: $\int_{\mathbb{Z}_p} f(x)\, d\mu(x) = \sum_{n=0}^{\infty} a_n(f) \cdot \int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x) = \sum a_n(f) c_n(\mu)$.

Exercise: $f: \mathbb{Z}_p \to \mathbb{C}_p$. (i) $\int_{\mathbb{Z}_p} f\, d\mu_{T^n} = \Delta^n f(0)$

(ii) $\int_{\mathbb{Z}_p} f\, d\mu_{(1+T)} = f(n)$, $n \in \mathbb{Z}_p$.

Recall, we had: $\Lambda(\mathbb{Z}_p) \xrightarrow{\sim} \mathbb{Z}_p[[T]]$

$$\begin{aligned} \mu &\longmapsto h_\mu(T) = \sum_{n=0}^{\infty} T^n \int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x) \\ \mu_{h(T)} &\longleftarrow h(T) \\ \sigma_1 &\longmapsto 1+T \quad , \quad \int_{\mathbb{Z}_p} f(x)\, d\mu_{1+T} = f(1) \end{aligned}$$

Notation: X, open subset of $\mathbb{Z}_p$. $\int_X d\mu := \int_{\mathbb{Z}_p} \varepsilon_X\, d\mu$, $\mu \in \Lambda(\mathbb{Z}_p)$

$\varepsilon_X(x) = \begin{cases} 1 & \text{if } x \in X \\ 0 & \text{if } x \notin X. \end{cases}$ $0 \leq k \leq p^n - 1$, $\int_{k+p^n\mathbb{Z}_p} d\mu_{f(T)}$.

$f(T) = \sum_{k=0}^{p^n-1} c_{n,k}(1+T)^k \mod \omega_n(T)$, $c_{n,k} \in \mathbb{Z}_p$, $\omega_n(T) = (1+T)^{p^n} - 1$.

Corollary: $\int_{k+p^n\mathbb{Z}_p} d\mu_{f(T)} = c_{n,k}$ $(n \geq 1,\ 0 \leq k \leq p^n - 1)$

Proof: Obvious. $\mu = \mu_{f(T)}$. $\Lambda(\mathbb{Z}_p)$

$$\begin{array}{ccc} \mu = \mu_{f(T)} & & \Lambda(\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ \sum_{k=0}^{p^n-1} c_{n,k}\tilde{\sigma}_1 & & \Lambda(\mathbb{Z}_p/p^n\mathbb{Z}_p) \end{array}$$

$\tilde{\sigma}_1$ = image of 1 in $\mathbb{Z}_p/p^n\mathbb{Z}_p$.

$\mathcal{G}_\infty \xrightarrow[\sim]{\psi} \mathbb{Z}_p^\times \subset \mathbb{Z}_p$. $\quad \tilde{\mu} \in \Lambda(\mathbb{Z}_p)$

$\mu \in \Lambda(\mathbb{Z}_p)$. $\quad \varepsilon$ = characteristic Function of $\mathbb{Z}_p^\times$.

<u>Definition:</u> $\tilde{\mu}$ is defined by: $\int_{\mathbb{Z}_p} f(x)\, d\tilde{\mu}(x) = \int_{\mathbb{Z}_p} f(x)\, \varepsilon(x)\, d\mu(x)$

Define V: $\mathbb{Z}_p[[T]] \to \mathbb{Z}_p[[T]]$ by $(Vf)(T) = f(T) - \frac{1}{p}\sum_{\zeta \in \mu_p} f(\zeta(1+T)-1) \in \mathbb{Z}_p[[T]]$.

<u>Lemma:</u> For every $f(T) \in \mathbb{Z}_p[[T]]$, we have $\tilde{\mu}_f = \mu_{V(f)}$.

$$\left.\begin{array}{l} f(T) = \sum_{k=0}^{p^n-1} c_{n,k}(1+T)^k \bmod \omega_n(T) \\ (Vf)(T) = \sum_{\substack{k=0 \\ (k,p)=1}}^{p^n-1} c_{n,k}(1+T)^k \bmod \omega_n(T). \end{array}\right\} \Rightarrow \forall n \geq 1, \text{ we have } \int_{k+p^n\mathbb{Z}_p} d\mu_{V(f)} = \begin{cases} 0 & \text{if } p \mid k \\ \int_{k+p^n\mathbb{Z}_p} d\mu_f & \text{if } (p,k)=1. \end{cases}$$

So, $\tilde{\mu}_f = \mu_{V(f)}$.

<u>Definition:</u> We say $\mu \in \Lambda(\mathbb{Z}_p)$ is <u>centred</u> on $\mathbb{Z}_p^\times$ if $\tilde{\mu} = \mu$.

$\Lambda(\mathbb{Z}_p^\times)$ identified with a subset of $\Lambda(\mathbb{Z}_p)$

$\Updownarrow$

$Vf = f \qquad \varphi \in \Lambda(\mathbb{Z}_p)$, μ_φ

$\int_{\mathbb{Z}_p} f(x)\, d\mu_\varphi = \int_{\mathbb{Z}_p} f(x)\, d\varphi(x)$

$u = (u_n) \in \mathcal{U}_\infty = \varprojlim \mathcal{U}_n$.

$f_u(T)$. $\quad l_u(T) = \log f_u(T) - \frac{1}{p}\sum_{\zeta\in\mu_p} \log f_u(\zeta(1+T)-1) \in \mathbb{Z}_p[[T]]$.

<u>Lemma:</u> $\forall u \in \mathcal{U}_\infty$, $Vl_u = l_u$, ie μ_{l_u} is centred on $\mathbb{Z}_p^\times$.

<u>Proof:</u> $\rho \in \mu_p$. $l_u(\rho(1+T)-1) = \log f_u(\rho(1+T)-1) - \frac{1}{p}\Delta(\log f_u)$, $\quad Vl_u = l_u$.

$\iota_\infty : \mathcal{U}_\infty \to \Lambda(\mathcal{G}_\infty)$. $\mathcal{G}_\infty = G(\Phi_\infty/\mathbb{Q}_p) \xrightarrow[\sim]{\psi} \mathbb{Z}_p^\times$. $\quad [\zeta_n$ primitive p^{n+1} root of 1, $\zeta_n^p = \zeta_{n-1}\ \forall n]$.

$\mu_{l_u(T)} \in \Lambda(\mathbb{Z}_p^\times)$. $\widetilde{\mu_{l_u(T)}} = \mu_{l_u(T)}$

<u>Definition:</u> $\forall u \in \mathcal{U}_\infty$, $l_\infty(u) \in \Lambda(\mathcal{G}_\infty)$ is the unique measure defined by

$$l_u(T) = \sum_{n=0}^{\infty} T^n \int_{\mathcal{G}_\infty} \binom{\psi(\sigma)}{n}\, d l_\infty(u)(\sigma).$$

<u>Lemma:</u> $l_\infty : \mathcal{U}_\infty \to \Lambda(\mathcal{G}_\infty)$ is a $\Lambda(\mathcal{G}_\infty)$-homomorphism

<u>Proof:</u> (i) $u_1, u_2 \in \mathcal{U}_\infty \Rightarrow f_{u_1 u_2}(T) = f_{u_1}(T) f_{u_2}(T)$, so $l_{u_1u_2}(T) = l_{u_1}(T) + l_{u_2}(T)$.

$\lambda \in \mathbb{Z}_p$, $f_{\lambda u}(T) = f_u(T)^\lambda$, so $l_{u^\lambda}(T) = \lambda l_u(T)$.

(ii) $\mathcal{G}_\infty$-homomorphism? $\tau \in \mathcal{G}_\infty$. $f_{\tau(u)} = f_u((1+T)^{\psi(\tau)} - 1)$

$\tau(u_n) = \sum_{n=0}^{\infty} a_n (t(\zeta_n) - 1)^n$, $a_n \in \mathbb{Z}_p$. $\quad t(\zeta_n) = \zeta_n^{\psi(\tau)}$

So, $l_\infty(\tau(u)) = \tau\, l_\infty(u) \in \Lambda(\mathcal{G}_\infty)$

$$\begin{array}{ccc} \Lambda(\mathbb{Z}_p) & \xrightarrow{\sim} & \mathbb{Z}_p[[T]] \\ \sigma_1 & \longmapsto & 1+T \\ \psi(t)\sigma_1 & \longleftarrow & (1+T)^{\psi(t)} \end{array}$$

So we have $l_\infty : \mathcal{U}_\infty \to \Lambda(\mathcal{G}_\infty)$. How close is it to an isomorphism?

$$0 \to T_p(\mu) \to \mathcal{U}_\infty \xrightarrow{i_\infty} \Lambda(\mathcal{G}_\infty) \to T_p(\mu) \to 0.$$

$T_p(\mu) = \varprojlim \mu_{p^n}$

Theorem: We have the canonical exact sequence $0 \to T_p(\mu) \to U_\infty \xrightarrow{l_\infty} \Lambda(\mathcal{G}_\infty) \to T_p(\mu) \to 0$.

$j_\infty(\mu) = (\zeta_n)^{\int_{\mathcal{G}_\infty} \Psi(\sigma)\, d\mu(\sigma)}$. $\quad l_u(T) = \log f_u(T) - \frac{1}{p} \sum_{\zeta \in \mu_p} \log f_u(\zeta(1+T)-1)$

$l_u(T) = \sum_{n=0}^{\infty} T^n \int_{\mathcal{G}_\infty} \binom{\Psi(\sigma)}{n}\, d l_\infty(u)(\sigma)$.

Obvious that j_∞ is surjective.

Claim: $\mathrm{Ker}(l_\infty) = T_p(\mu) \subset U_\infty$.

(i) $u = (\rho_n) \in T_p(\mu)$. $\rho_{n+1}^p = \rho_n \quad \forall n \geq 0$.

Want $l_\infty(u) = 0$. $u = (\zeta_n)^a$ for some $a \in \mathbb{Z}_p$, ie $\rho_n = \zeta_n^a$ for $n \geq 0$. $\Rightarrow f_u(T) = (1+T)^a$.

Recall: $N f_u = f_u \Rightarrow f_u((1+T)^p - 1) = \prod_{\zeta \in \mu_p} f_u(\zeta(1+T)-1)$

$l_u(T) = \log f_u(T) - \frac{1}{p} \log f_u(\zeta(1+T)-1)$ $\quad$ So $l_u(T) = 0 \Rightarrow l_\infty(u) = 0$.

(ii) $u = (u_n) \in U_\infty$ with $l_\infty(u) = 0$, ie $p \log f_u(T) = f_u((1+T)^p - 1)$.

$\log\left[\frac{f_u(T)^p}{f_u((1+T)^p-1)}\right] = 0. \quad \Rightarrow f_u(T)^p = f_u((1+T)^p - 1) \qquad f_u(0) \equiv 1 \bmod p.$

$\Rightarrow \begin{cases} u_n^p = u_{n-1}, & n \geq 1 \\ f_u(0) = u_0^p. \end{cases}$

Lemma: $\forall\, u = (u_n) \in U_\infty$, we have $f_u(0) = 1$.

Proof: $f_u((1+T)^p - 1) = \prod_{\zeta \in \mu_p} f_u(\zeta(1+T)-1)$. $\quad \Phi_n = \mathbb{Q}_p(\mu_{p^{n+1}})$

$f_u(0) = N_{\Phi_0|\mathbb{Q}_p}(u_0) = N_{\Phi_n|\mathbb{Q}_p}(u_n) \quad \forall n \geq 1$.

$\mathbb{Q}_p^\times \overset{p^n(p-1)}{\supset} N_{\Phi_n|\mathbb{Q}_p}(\Phi_n^\times) = \mu_{p-1} \times (1 + p^{n+1}\mathbb{Z}_p) \quad \therefore \; \equiv 1 \bmod p^{n+1} \quad \forall n \geq 0.$

$\| \; p^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p)$

p-adic logarithmic derivative.

$u = (u_n) \in U_\infty$. To define the kth p-adic logarithmic derivative of u for all $k \geq 1$:

$f_u(T) \leftrightarrow$. Don't take $(\frac{d}{dT})^k \log f_u(T)$.

Use $T = e^z - 1$, and $\frac{d}{dz}$. Let $D = (1+T)\frac{d}{dT} = \frac{1}{\log'(1+T)} \frac{d}{dT}$.

Key definition: For each $k \geq 1$, $\delta_k(u) = (D^k \log f_u(T))(0) \in \mathbb{Z}_p$.

$\delta_k : U_\infty \to \mathbb{Z}_p$.

Group homomorphism: $f_{u_1 u_2}(T) = f_{u_1}(T) f_{u_2}(T)$

Lemma: For each $k \geq 1$ and each $\sigma \in \mathcal{G}_\infty$, have $\delta_k(\sigma(u)) = \Psi(\sigma)^k \delta_k(u)$.

Proof: $f_{\sigma(u)} = f_u((1+T)^{\Psi(\sigma)} - 1)$

$\delta_k(\sigma(u)) = (D^k \log f_u((1+T)^{\Psi(\sigma)} - 1))(0) = \Psi(\sigma)^k (D^k \log f_u(T))(0)$.

Proposition: For each $u \in U_\infty$ and each integer $k \geq 1$, we have $\int_{\mathcal{G}_\infty} \Psi(\sigma)^k\, d l_\infty(u)(\sigma) = (1 - p^{k-1}) \delta_k(u)$.

Corollary: $j_\infty \cdot l_\infty = 0$.

$\int_{\mathcal{G}_\infty} \Psi(\sigma)\, d l_\infty(u)(\sigma) = (1 - p^0)\delta_1(u) = 0.$

$\int_{\mathcal{G}_\infty} \Psi(\sigma)^k\, d l_\infty(u)(\sigma) = \int_{\mathbb{Z}_p^\times} x^k\, d\mu_{l_u(T)}(x) = \int_{\mathbb{Z}_p} x^k\, d\mu_{l_u(T)}(x) = \underbrace{(D^k \log f_u)(0) - \frac{1}{p}(D^k \log f_u((1+T)^p - 1))(0)}_{\text{from following proposition...}} = (1 - p^{k-1})\delta_k(u).$

Now, $l_u(T) = \log l_u(T) - \frac{1}{p}\log f_u((1+T)^p-1)$.

Proposition: Let $f(T)$ be any element of $\mathbb{Z}_p[[T]]$, and let μ_f be the corresponding measure in $\Lambda(\mathbb{Z}_p)$. For all $k \geq 1$, we have: $\int_{\mathbb{Z}_p} x^k \, d\mu_f(x) = (D^k f)(0)$.

Proof: Let g be any element of $\mathbb{Z}_p[[T]]$, $\mu_g \in \Lambda(\mathbb{Z}_p)$. Define ν by: for $\alpha(x): \mathbb{Z}_p \to \mathbb{C}_p$, let $\int_{\mathbb{Z}_p} \alpha(x)\, d\nu = \int_{\mathbb{Z}_p} \alpha(x) x \, d\mu_g$. What is the power series corresponding to ν?

Claim: $\nu \longleftrightarrow (Dg)(T)$. ie, $(Dg)(T) = \sum_{n=0}^{\infty} T^n \int_{\mathbb{Z}_p} \binom{x}{n} d\nu$.

$g(T) = \sum_{n=0}^{\infty} b_n T^n$, $Dg(T) = \sum_{n=0}^{\infty} (nb_n + (n+1)b_{n+1}) T^n$.

Consider $\sum_{n=0}^{\infty} T^n \int_{\mathbb{Z}_p} x \binom{x}{n} d\mu_g$. Note $x\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n}$, and $b_n = \int_{\mathbb{Z}_p} \binom{x}{n} d\mu_g$

so on substituting, we get the claim.

Apply to: $\int_{\mathbb{Z}_p} d\mu_h = h(0)$, $\Lambda(\mathbb{Z}_p) \xrightarrow{\sim} \mathbb{Z}_p[[T]]$, k times to get result.

Recall we are trying to show $0 \to T_p(\mu) \to U_\infty \xrightarrow{l_\infty} \Lambda(\mathcal{G}_\infty) \xrightarrow{j_\infty} T_p(\mu) \to 0$ is exact.

Must show $j_\infty(\mu) = 0 \Rightarrow \mu = l_\infty(u)$.

$j_\infty(\mu) = 0 \Leftrightarrow \int_{\mathcal{G}_\infty} \psi(\sigma)\, d\mu(\sigma) = 0$, $\psi: \mathcal{G}_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times$

$\mu \longleftrightarrow \nu$.

So $\int_{\mathbb{Z}_p} x \, d\nu(x) = 0$. ν is a measure on $\mathbb{Z}_p$ which is centred on $\mathbb{Z}_p^\times$. $\nu \leftrightarrow h_\nu(T) \in \mathbb{Z}_p[[T]]$

ν centred on $\mathbb{Z}_p^\times \Rightarrow Vh_\nu(T) = h_\nu(T)$.

So hypothesis is: $Dh_\nu(0) = 0 \Leftrightarrow h_\nu'(0) = 0$.

Coleman's Lemma: Let $g(T)$ be any power series in $\mathbb{Z}_p[[T]]$ such that $Dg(0) = 0$, ie, $g'(0) = 0$. Then $\exists$ a power series $f(T)$ in $\mathbb{Z}_p[[T]]$ with $f(0) \equiv 1 \bmod p$ and $g(T) = \log f(T) - \frac{1}{p}\log f((1+T)^p - 1)$

Proof: Maybe later – it's in Proc. A.M.S. 89 (1983), 1-7, and Inventiones 53 (1979), 91-116.

Apply this to $g(T) = h_\nu(T)$. $Vh_\nu(T) = h_\nu(T)$. Recall $Vf(T) = f(T) - \frac{1}{p}\sum_{\zeta \in \mu_p} f(\zeta(1+T)-1)$

Get $Vh_\nu(T) = \log f(T) - \frac{1}{p}\sum_{\zeta \in \mu_p} \log f(\zeta(1+T)-1)$.

$= \log f(T) - \frac{1}{p}\log f((1+T)^p - 1)$

Now, $\log f((1+T)^p - 1) = \sum_{\zeta \in \mu_p} \log f(\zeta(1+T)-1) \Rightarrow \log\left(\frac{f((1+T)^p-1)}{\prod_{\zeta\in\mu_p} f(\zeta(1+T)-1)}\right) = 0 \Rightarrow f((1+T)^p - 1) = \prod_{\zeta\in\mu_p} f(\zeta(1+T)-1)$

Define $u_n = f(\zeta_n - 1)$. $N_{n,n-1}(u_n) = u_{n-1}$. $u = (u_n) \in U_\infty$. So $\mu = l_\infty(u)$, as required.

So we get the exact sequence of $\mathcal{G}_\infty$-modules: $0 \to T_p(\mu) \to U_\infty \to \Lambda(\mathcal{G}_\infty) \to T_p(\mu) \to 0$ $(p \neq 2)$.

Complex conjugation, $c \in \mathcal{G}_\infty$. c acts on A. $A^+ = A^{\langle 1, c\rangle}$. $T_p(\mu)^+ = 0$.

Corollary: l_∞ induces a canonical isomorphism $l_\infty: U_\infty^+ \to \Lambda(\mathcal{G}_\infty)^+$

(i) $F_n = \mathbb{Q}(\mu_{p^{n+1}})$, $K_n = F_n^+$, $G_n = \mathcal{G}_n / \langle 1, c\rangle$

Let $\Phi_n = \mathbb{Q}_p(\mu_{p^{n+1}})$, $\Psi_n = \Phi_n^+$, V_n = units of Ψ_n which are $\equiv 1 \bmod \mathfrak{p}_n$. So $U_n^+ = V_n$.

So $U_\infty^+ = V_\infty = \varprojlim V_n$

(ii) There is a natural identification of $\Lambda(\mathcal{G}_\infty)^+$ with $\Lambda(G_\infty)$, specifically the canonical surjection $\Lambda(\mathcal{G}_\infty) \to \Lambda(G_\infty)$ maps $\Lambda(\mathcal{G}_\infty)^+$ isomorphically onto $\Lambda(G_\infty)$.

$\mathbb{Z}_p[\mathcal{G}_n] \to \mathbb{Z}_p[G_n]$

$\mathbb{Z}_p[\mathcal{G}_n]^+ \xrightarrow{\sim}$

Saying $c\sum_{\sigma\in\mathcal{G}_n} d(\sigma)\sigma = \sum_{\sigma\in\mathcal{G}_n} d(\sigma)\sigma$ is the same as saying $d(\sigma) = d(c\sigma)$.
So we can rewrite the preceeding corollary as:

Corollary: L_∞ induces a canonical isomorphism $L_\infty : V_\infty \to \Lambda(G_\infty)$

$u = (u_n) \in \varprojlim U_n$. $f_u(T)$.
$N_{n,n-1}(1-\zeta_n) = 1-\zeta_{n-1}$. $f_u(T) = T$. $f(T) = 1-(1+T)^a$

Correction: We had $u = (u_n) \in U_\infty$, $f_u(T)$, claimed $f_u(0) = 1$ – False!
$f_u((1+T)^p - 1) = \prod_{\zeta\in\mu_p} f_u(\zeta(1+T)-1)$. $f_u(0) = (N_{\Phi_0/\mathbb{Q}_p} f_u(\zeta_0)) f_u(0)$.
This doesn't affect earlier though: $f_u(T)^p = f_u((1+T)^p - 1)$, so $f_u(0)^{p-1} = 1$
$\Rightarrow f_u(0) = 1$, as $f_u(0) \equiv 1 \bmod p$.

Classical cyclotomic units of $K_n = \mathbb{Q}(\mu_{p^{n+1}})^+$. ζ_n generator of $\mu_{p^{n+1}}$, $\zeta_n^p = \zeta_{n-1}$ $\forall n \geq 1$.
Definition: The group of cyclotomic units of K_n is the intersection with the unit group of K_n of the subgroup of $F_n^\times$ generated by ζ_n and $1-\zeta_n^\sigma$, where $\sigma \in G(F_n/\mathbb{Q})$.

Notation: J_n will denote any set of representatives in $\mathbb{Z}$ of the classes $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times/\{\pm 1\}$, which are not equal to 1.

$(a,p)=1$. $e_n(a) = \frac{\zeta_n^{-a} - \zeta_n^a}{\zeta_n^{-1} - \zeta_n} \in K_n$. $\zeta_n^{1-a}\left(\frac{1-\zeta_n^{2a}}{1-\zeta_n^2}\right)$. $e_n(a)$ a unit of K_n for every $(a,p)=1$.

Lemma: The cyclotomic units of J_n are generated by -1 and $e_n(a)$ $(a \in J_n)$

Lemma: The group of cyclotomic units of K_n modulo ± 1 is generated by one element over $\mathbb{Z}[G_n]$. Specifically, a generator is given by $e_n(g)$ where g is any primitive root modulo p^{n+1}.
Proof: $(a,p)=1$. $g^r \equiv a \bmod p^{n+1}$
$$e_n(a) = \zeta_n^{1-a}\cdot\left(\frac{1-\zeta_n^{2a}}{1-\zeta_n^2}\right) = \zeta_n^{1-g^r}\cdot\left(\frac{1-\zeta_n^{2g^r}}{1-\zeta_n^2}\right) = \prod_{i=0}^{r-1}\left(\zeta_n^{g^i - g^{i+1}}\right)\cdot\left(\frac{1-\zeta_n^{2g^{i+1}}}{1-\zeta_n^{2g^i}}\right)$$
σ_g: restriction to K_n of automorphism of K_n which acts of $\mu_{p^{n+1}}$ by raising to power g $\Rightarrow$
$$= \prod_{i=0}^{r-1}\left(\zeta_n^{1-g}\cdot\frac{1-\zeta_n^{2g}}{1-\zeta_n^2}\right)^{\sigma_g^i} = \prod_{i=0}^{r-1} e_n(g)^{\sigma_g^i}.$$

Lemma: For each integer a with $(a,p)=1$, and all $m \geq n$, have $N_{m,n}(e_m(a)) = e_n(a)$.
Proof: $m = n+1$. Minimal equation for ζ_{n+1} over F_n is $X^p - \zeta_n = 0$. $N_{n,n+1}(\zeta_{n+1}) = \zeta_n$.
$N_{n,n-1}(1-\zeta_{n+1}^a) = 1-\zeta_n^a$. $e_{n+1}(a) = \zeta_{n+1}^{1-a}\cdot\frac{1-\zeta_{n+1}^{2a}}{1-\zeta_n^a} \Rightarrow N_{n+1,n}(e_{n+1}(a)) = e_n(a)$.

$\#(J_n) = \frac{p^n(p-1)}{2} - 1$. $[K_n:\mathbb{Q}] = \frac{p^n(p-1)}{2}$.

Theorem (see Washington): The units $e_n(a)$, for $a \in J_n$, are multiplicatively independent. Moreover, the index of the subgroup generated by -1 and $e_n(a)$ $(a \in J_n)$ in the full group of units of K_n is precisely the class number of K_n.

Cyclotomic units for all n simultaneously: $(e_n(a)) \in \varprojlim \{\text{Local unit of } \Phi_n\}$. $\Phi_n = \mathbb{Q}_p(\mu_{p^{n+1}})^+$, $(a,p)=1$.

<u>Definition</u>: $\Omega = \{ (n_1,\dots,n_r) \in \mathbb{Z}^r, (a_1,\dots,a_r) \in \mathbb{Z}^r : (i)\ r \geq 1,\ (ii)\ \sum_{i=1}^{r} n_i = 0,\ (iii)\ (a_i,p)=1,\ (iv)\ \prod_{i=1}^{r} a_i^{n_i} \equiv 1 \bmod p \}$.

<u>Definition</u>: If $\alpha \in \Omega$, $f(T,\alpha) = \prod_{i=1}^{r} \left((1+T)^{-a_i} - (1+T)^{a_i}\right)^{n_i}$

<u>Lemma</u>: $f_\alpha(T) \in \mathbb{Z}_p[[T]]$ and $f_\alpha(0) \equiv 1 \bmod p$.
<u>Proof</u>: $(1+T)^{-a_i} - (1+T)^{a_i} = -2a_i T +$ higher powers of T (coefficients in $\mathbb{Z}$).
$= 2a_i T \times (\text{unit in } \mathbb{Z}_p[[T]])$. $= -2a_i T \times h_i(T)$, $h_i(T) \in \mathbb{Z}_p[[T]]$, $h_i(0)=1$
So $f(T,\alpha) = T^{\sum n_i} \times \prod_{i=1}^{r}(-2a_i)^{n_i} \times g(T,\alpha)$, $g(T,\alpha) \in \mathbb{Z}_p[[T]]$, $g(0,\alpha)=1$.
So, $f(0,\alpha) \equiv 1 \bmod p$ because $\prod a_i^{n_i} \equiv 1 \bmod p$.

<u>Lemma</u>: $f_\alpha(\zeta_n - 1)$ is a cyclotomic unit of K_n, which is $\equiv 1 \bmod \mathfrak{p}_n$, and
$N_{n,n-1}(f_\alpha(\zeta_n - 1)) = f_\alpha(\zeta_{n-1} - 1)$.
$\left[f(\zeta_n - 1, \alpha) = \prod_{i=1}^{r} e_n(a_i)^{n_i} \right]$

<u>Definition</u>: C_n = group of cyclotomic units of K_n which $\equiv 1 \bmod \mathfrak{p}_n$, $= \{ f(\zeta_n - 1, \alpha) \cdot \alpha \in \Omega \}$.
$N_{m,n}(C_m) = C_n$. $C_n \subset V_n$, $\overline{C_n} \subset V_n$. $\quad w_\alpha = (w_{\alpha,n})$
$\overline{C_n}$ = $\mathbb{Z}_p$-submodule generated by C_n.

<u>Definition</u>: $\mathcal{L}_n$ = closure of C_n in V_n in the p-adic topology.
= $\mathbb{Z}_p$-submodule generated by the $f(\zeta_n - 1, \alpha)$, $\alpha \in \Omega$.

<u>Definition</u>: $\mathcal{L}_\infty = \varprojlim \mathcal{L}_n \subset V_\infty$, a $\Lambda(G_\infty)$-submodule.

<u>Aim</u>: Determine the $\Lambda(G_\infty)$-module $V_\infty / \mathcal{L}_\infty$

$\iota_\infty : V_\infty \xrightarrow{\sim} \Lambda(G_\infty)$. $\iota_\infty(\mathcal{L}_\infty) \subset \Lambda(G_\infty)$.
w_α, $\iota_\infty(w_\alpha)$, $\mu \in \Lambda(G_\infty)$, $\int_{G_\infty} \psi(\sigma)^k \, d\mu(\sigma)$, $k = 2,4,6,\dots$
Calculation of $\int_{G_\infty} \psi(\sigma)^k \, d\iota_\infty(w_\alpha)(\sigma)$, $(k = 2,4,6,\dots)$

<u>Proposition</u>: For every $\alpha \in \Omega$, we have $\int_{G_\infty} \psi(\sigma)^k \, d\iota_\infty(w_\alpha)(\sigma) = -\zeta(1-k)(1-p^{k-1}) \times \sum_{j=1}^{r} n_j (2a_j)^k$
for all even integers $k \geq 2$.
<u>Proof</u>: We know that $\int_{G_\infty} \psi(\sigma)^k \, d\iota_\infty(w_\alpha)(\sigma) = (1-p^{k-1}).(D^k \operatorname{Log} f_{w_\alpha})(0)$, $D = (1+T)\frac{d}{dT}$
$f_{w_\alpha}(T) = \prod_{j=1}^{r} \left((1+T)^{-a_j} - (1+T)^{a_j}\right)^{n_j}$.
$1 + T = e^z$, $(1+T)\frac{d}{dT} = \frac{d}{dz}$.
Hence $(D^k \operatorname{Log} f_{w_\alpha}(T))(0) = \left(\left(\frac{d}{dz}\right)^k \operatorname{Log} f_{w_\alpha}(e^z - 1)\right)(0)$, $k = 2,4,\dots$
$f_{w_\alpha}(e^z - 1) = \prod_{j=1}^{r} (e^{-a_j z} - e^{a_j z})^{n_j}$
$\frac{d}{dz} \log f_{w_\alpha}(e^z - 1) = \sum_{j=1}^{r} n_j \cdot \frac{-a_j e^{-a_j z} - a_j e^{a_j z}}{e^{-a_j z} - e^{a_j z}} = \sum_{j=1}^{r} n_j a_j \left(\frac{1}{e^{2a_j z} - 1} - \frac{1}{e^{-2a_j z} - 1} \right)$

$\left[\frac{1}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^{n-1} \right]$, $\quad = \sum_{j=1}^{r} n_j a_j \left(\sum_{k=0}^{\infty} \frac{B_k}{k!} \left((2a_j)^{k-1} - (-2a_j)^{k-1} \right) z^{k-1} \right)$.
$[k=0$ gives nothing as $\sum n_j = 0$. $B_k = 0$ for k odd, $>1]$
$= \sum_{\substack{k=2 \\ \text{even}}}^{\infty} \frac{B_k}{k!} z^{k-1} \times \sum_{j=1}^{r} n_j (2a_j)^k$. So $\left(\frac{d}{dz}\right)^k \log f_{w_\alpha}(e^z - 1)\Big|_{z=0} = \frac{B_k}{k!} \times \sum_{j=1}^{r} n_j (2a_j)^k$, $k = 2,4,6,\dots$
Noting $\zeta(1-k) = \frac{-B_k}{k!}$ gives result.

Leopoldt-Kubota-Iwosawa pseudo-measure μ_B: $(\sigma-1)\mu_B \in \Lambda(G_\infty)$ $\forall\, \sigma \in G_\infty$.

$\int_{G_\infty} \psi^k(\sigma)\, d\mu_B(\sigma) = \zeta(1-k)\,[1-p^{k-1}]$, $k = 2, 4, 6, \ldots$

$\Lambda(G_\infty)_0 = \mathrm{Ker}\,(\Lambda(G_\infty) \to \mathbb{Z}_p)$ = augmentation ideal.

$\lambda \in \Lambda(G_\infty)_0$, then $\lambda\mu_B \in \Lambda(G_\infty)$.

$\int_{G_\infty} \psi^k(\sigma)\, d(\lambda\mu_B)(\sigma) = \underbrace{\left(\int_{G_\infty} \psi^k(\sigma)\, d\mu_B\right)}_{\zeta(1-k)(1-p^{k-1})} \times \left(\int_{G_\infty} \psi(\sigma)^k\, d\lambda\right)$, $k = 2, 4, \ldots$

$u \in \mathbb{Z}_p^\times$, $\sigma_u \in \mathcal{G}_\infty$, $\psi(\sigma_u) = u$.

t_u = image of σ_u in $G_\infty = \mathcal{G}_\infty / \langle 1, c\rangle$.

$\alpha \in \Omega$. $\varphi_\alpha = -\sum_{j=1}^r n_j\, t_{2a_j}$. $\sum_{j=1}^r n_j = 0 \Rightarrow \varphi_\alpha \in \Lambda(G_\infty)_0$.

$\psi^k(\varphi_\alpha) = \sum_{j=1}^r n_j (2a_j)^k$ ($k \in \mathbb{Z}$, k even)

$\overset{\shortparallel}{\int_{G_\infty} \psi^k(\sigma)\, d\varphi_\alpha(\sigma)}$

<u>Conclusion:</u> $\forall\, \alpha \in \Omega$ and all even integers $k \geq 2$, we have $\int_{G_\infty} \psi(\sigma)^k\, d l_\infty(w_\alpha)(\sigma) = \int_{G_\infty} \psi(\sigma)^k\, d(\varphi_\alpha \mu_B)(\sigma)$.

$\Rightarrow l_\infty(w_\alpha) = \varphi_\alpha \mu_B$.

<u>Lemma:</u> We can choose $\alpha \in \Omega$ such that $\{\varphi_\alpha\}$ generate the augmentation ideal.

<u>Iwasawa's Theorem:</u> $V_\infty / \mathcal{L}_\infty \cong \Lambda(G_\infty) / \mu_B \Lambda(G_\infty)_0$ as $\Lambda(G_\infty)$-modules.

$V_\infty / \mathcal{L}_\infty \underset{\Lambda(G_\infty)}{\xrightarrow{\sim}} \Lambda(G_\infty) / \Lambda(G_\infty)_0 \mu_B$?

$\mathbb{Z}_p^\times = \varprojlim (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$.

$G_\infty \cong \mathbb{Z}_p^\times / \{\pm 1\}$.

g primitive root mod $p^2 \Rightarrow g$ primitive root mod p^n, $n \geq 2$.

ρ any fixed topological generator of G_∞.

$\Lambda(G_\infty)_0 = (\rho - 1)\Lambda(G_\infty)$. $V_\infty / \mathcal{L}_\infty \xrightarrow{\sim} \Lambda(G_\infty) / ((\rho-1)\mu_B)$

<u>Lemma:</u> $\exists\, \alpha \in \Omega$ such that φ_α generates $\Lambda(G_\infty)_0$.

$\alpha = (n_1, \ldots, n_r)\ \&\ (a_1, \ldots, a_r)$. $r = 2$, $n_1 = p-1$, $n_2 = -(p-1)$

$a_1 = hg$, $a_2 = +1$.

$\varphi_\alpha = -\sum_{i=1}^r n_i \tau_{2a_i}$

g = primitive root mod p^2

h = inverse of 2 mod p^2.

$a_1 = hg$, $2a_1$ is a primitive root mod $p^2 \Rightarrow 2a_1$ is a primitive root mod p^n, $n \geq 2$.

$\varphi_\alpha = (1-p)\tau_{2a_1} - (1-p)\tau_1$

$(\varphi_\alpha) = (\tau_{2a_1} - 1) = (\rho - 1)$

<u>2. Euler Systems.</u>

$$\begin{array}{l} K_\infty = \mathbb{Q}(\mu_{p^\infty})^+ \text{ — } M_\infty \\ \quad \mid\ G_\infty \\ \quad \mathbb{Q} \end{array}$$

<u>Definition:</u> M_∞ = maximal abelian p-extension of K_∞ which is unramified outside of p.

M_∞ is clearly Galois over $\mathbb{Q}$

$0 \to G(M_\infty/K_\infty) \to G(M_\infty/\mathbb{Q}) \to G_\infty \to 0$.

$z_\sigma \longmapsto \sigma$

We define a continuous action of G_∞ on $G(M_\infty/K_\infty)$ as follows:
$\sigma \in G_\infty$, z_σ a lifting of σ to $G(M_\infty/\mathbb{Q})$, and then we define, for $x \in G(M_\infty/K_\infty)$, $\sigma(x) = z_\sigma \cdot x \cdot z_\sigma^{-1}$.

Remarks: (i) Well-defined because $G(M_\infty/K_\infty)$ is abelian.
(ii) Chosen for compatibility with the Artin map (Thm. 11.5, p. 199 of Tate's article).

Hence $G(M_\infty/K_\infty)$ has a natural $\Lambda(G_\infty)$-module structure.

$$\begin{array}{l} \qquad\quad M_\infty \\ \quad\ L_\infty \\ K_\infty \\ \ \mid\ )\,G_\infty \\ \mathbb{Q} \end{array}$$

Definition: L_∞ = maximal abelian p-extension of K_∞ which is unramified everywhere.

G_∞ acts on $G(L_\infty/K_\infty)$ in an entirely analogous manner. $G(L_\infty/K_\infty)$ is a $\Lambda(G_\infty)$-module.
$0 \to G(M_\infty/L_\infty) \to G(M_\infty/K_\infty) \to G(L_\infty/K_\infty) \to 0.$

E_n = group of all global units of K_n which are $\equiv 1 \bmod \wp_n$.
$\cup$
C_n.

$C_n \subset E_n \subset V_n$.
$\cap$
$\mathcal{C}_n \subset \mathcal{E}_n \subset V_n$.

Definition: $\mathcal{E}_n$ = closure of E_n in V_n
= $\mathbb{Z}_p$-submodule generated by E_n.
Define $\mathcal{E}_\infty = \varprojlim \mathcal{E}_n$ (w.r.t. norm maps).

Theorem (See Washington - full force of global class field theory for K_n $\forall n$).
The Artin map defines a canonical $\Lambda(G_\infty)$-isomorphism, $V_\infty/\mathcal{E}_\infty \xrightarrow{\sim} G(M_\infty/L_\infty)$.

Motivation: for main conjecture (case treated first for Iwasawa).
Assume that the class number of $K_0 = \mathbb{Q}(\mu_p)^+$ is prime to p (Vandiver conjecture: true for $p \leq 128000$).
Easy algebraic argument $\Rightarrow$ class number of K_n is prime to p $\forall n \geq 0$.
$\Rightarrow G(L_\infty/K_\infty) = 0$. Also, $\Rightarrow [E_n \cdot C_n]$ is prime to p $\forall n$. $\Rightarrow \mathcal{E}_n = \mathcal{C}_n$ $\forall n$.

Theorem: If the class number of $\mathbb{Q}(\mu_p)^+ = K_0$ is prime to p, then there is a canonical $\Lambda(G_\infty)$-isomorphism $G(M_\infty/K_\infty) \xrightarrow{\sim} \Lambda(G_\infty)/((\varrho-1)\mu_B)$

$$\begin{array}{l} 0 \to \mathcal{E}_\infty/\mathcal{C}_\infty \to V/\mathcal{C}_\infty \to G(M_\infty/K_\infty) \to G(L_\infty/K_\infty) \to 0. \quad \Lambda(G_\infty)\text{-modules.} \\ \qquad\qquad\qquad\quad \parallel \\ \qquad\qquad\quad \Lambda(G_\infty)/((\varrho-1)\mu_B) \end{array}$$

Structure Theory of Finitely Generated Torsion Modules over $\Lambda(G_\infty)$.
Definition: We say a $\Lambda(G_\infty)$-module X is torsion if $\exists\ \alpha \in \Lambda(G_\infty)$, not a divisor of zero, such that $\alpha . X = 0$.

$$\begin{array}{l} K_\infty \\ \mid \\ K_n \quad G_\infty \\ \mid \\ K_0 \\ \mid \\ \mathbb{Q} \end{array}$$

$G_\infty = D \times \Gamma$, $\Gamma = G(K_\infty/K_0) \xrightarrow{\sim} \mathbb{Z}_p$, $D \xrightarrow{\sim} G(K_0/\mathbb{Q})$ under restriction.
Let $A = \mathbb{Z}_p[D]$.
$\Lambda(G_\infty) = \varprojlim A[G(K_n/K_0)] = A[[\Gamma]]$. $\quad \mathbb{Z}_p[G(K_n/\mathbb{Q})] = A[G(K_n/\mathbb{Q})]$.

$\hat{D} = \mathrm{Hom}(D, \mathbb{Z}_p^\times)$. $\quad \chi \in \hat{D}$ Let $e_\chi = \frac{2}{p-1} \cdot \sum_{\delta \in D} \chi^{-1}(\delta)\,\delta \in A$.
$e_\chi^2 = e_\chi$, $\quad e_\chi \cdot e_{\chi'} = 0$ if $\chi \neq \chi'$. $1 = \sum_{\chi \in \hat{D}} e_\chi$.

Lemma: For each $\chi \in \hat{D}$, the map $\alpha \mapsto \chi(\alpha)$ defines an isomorphism from $e_\chi A$ to $\mathbb{Z}_p$.

$$\Lambda(G_\infty) = A[[\Gamma]] = \bigoplus_{\chi \in \hat{D}} \left(e_\chi A[[\Gamma]]\right) \xrightarrow{\sim} \bigoplus_{\chi \in \hat{D}} \mathbb{Z}_p[[\Gamma]]$$
$\alpha = \sum e_\chi \alpha$. $\quad \alpha$ will be a divisor of zero iff $e_\chi \alpha = 0$ for some $\chi \in \hat{D}$.

Structure Theorem: Let X be any f.g. torsion $\Lambda(G_\infty)$-module. Then $\exists\, f_1, \dots, f_r \in \Lambda(G_\infty)$ such that (i) $f_1, \dots, f_r$ are not divisors of zero, and (ii) we have an exact sequence of $\Lambda(G_\infty)$-modules $\quad 0 \to \bigoplus_{i=1}^r \Lambda(G_\infty)/(f_i) \to X \to H \to 0$, where H is finite.
Moreover, $(f_1 \dots f_r)$ in $\Lambda(G_\infty)$ is uniquely determined by X.

Definition: $c(X) =$ char. ideal of $X = (f_1 \dots f_r) \subset \Lambda(G_\infty)$.

Proof: $X = \bigoplus_{\chi \in \hat{D}} X^{(\chi)}$. $\quad X^{(\chi)} = e_\chi X =$ largest A-submodule of X on which D acts via χ.
$X^{(\chi)}$ is a $\Lambda(\Gamma)$-module, f.g. torsion $\Lambda(\Gamma)$-module. $\Lambda(\Gamma) \cong \mathbb{Z}_p[[T]]$, $\mathfrak{m} = (p, T)$.
$0 \to \bigoplus_{i=1}^r \Lambda(\Gamma)/(g_{i,\chi}) \to X^{(\chi)} \to H_\chi \to 0$, $\quad g_{i,\chi} \neq 0$, H_χ finite.
$g_{i,\chi} \in \mathbb{Z}_p[[\Gamma]] \xrightarrow{\sim} g'_{i,\chi} \in e_\chi A[[\Gamma]]$. $\quad$ Let $f_i = \sum_{\chi \in \hat{D}} g_{i,\chi} \in A[[\Gamma]]$
$\Lambda(G_\infty)/(f_i) \cong \bigoplus_{\chi \in \hat{D}} \mathbb{Z}_p[[\Gamma]]/(g_{i,\chi})$.

Return to Main Conjecture.

$$\begin{array}{l} - M_\infty \\ - L_\infty \\ K_\infty \\ \big|\,\big)\, G_\infty \\ \mathbb{Q} \end{array}$$

$$0 \to G(M_\infty/L_\infty) \to G(M_\infty/K_\infty) \to G(L_\infty/K_\infty) \to 0$$
$$\overset{\shortparallel}{V_\infty/\mathcal{E}_\infty}$$
Had: $\quad 0 \to \mathcal{E}_\infty/\mathcal{I}_\infty \to V_\infty/\mathcal{I}_\infty \to G(M_\infty/K_\infty) \to G(L_\infty/K_\infty) \to 0.$
$$\begin{array}{c} \wr\Vert \text{ - as } \Lambda(G_\infty)\text{-modules.} \\ \Lambda(G_\infty)/((p-1)\mu_B) \end{array}$$

Lemma: $(p-1)\mu_B$ is not a zero divisor in $\Lambda(G_\infty)$
Proof: $\psi^k((p-1)\mu_B) = \int_{G_\infty} \psi^k \, d((p-1)\mu_B) = \{\psi^k(\gamma) - 1\}\, \zeta(1-k)\, (1 - p^{k-1})$, k even integer ≥ 2.
$\zeta(1-k) \neq 0$ as k even. $\psi(\gamma)$ is not a root of unity, as it is a topological generator.
$\psi^k|D$ - all characters in $\hat{D}$.

Theorem: $G(L_\infty/K_\infty)$ is f.g. and $\Lambda(G_\infty)$-torsion

Corollary: $G(M_\infty/K_\infty)$ is f.g. and $\Lambda(G_\infty)$-torsion

Main Conjecture (= Theorem of Iwasawa-Mazur-Wiles): $c(G(M_\infty/K_\infty)) = ((p-1)\mu_B)$

Lemma (see Washington): If we have an exact sequence of f.g. torsion $\Lambda(G_\infty)$-modules $0 \to X \to Y \to Z \to 0$, then $c(Y) = c(X)\,c(Z)$.

Reduction 1: Main Conjecture holds $\Leftrightarrow c(V_\infty/\mathcal{I}_\infty) = c(G(L_\infty/K_\infty))$

Proposition: Main Conjecture is true $\Leftrightarrow c(G(L_\infty/K_\infty)) \supset c(\mathcal{E}_\infty/\mathcal{I}_\infty)$

Proof: Counting argument based on the fact that $\forall n$, the p-part index of C_n in E_n is equal to the p-part of the class number of K_n.

Let $\mathcal{D}_\infty$ be any $\Lambda(G_\infty)$ submodule of $\mathcal{E}_\infty$ such that $\mathcal{E}_0 \supset \mathcal{D}_\infty \supset \mathcal{I}_\infty$.

Proposition: If $c(G(L_\infty/K_\infty)) \supset c(\mathcal{E}_\infty/\mathcal{D}_\infty)$ $-(*)$ then the M.C. is true and $\mathcal{D}_\infty/\mathcal{I}_\infty$ is finite.

Proof: Note $c(\mathcal{E}_\infty/\mathcal{D}_\infty) \supset c(\mathcal{E}_\infty/\mathcal{I}_\infty)$. Hence $(*) \Rightarrow MC$ by previous proposition

$\Rightarrow c(G(L_\infty/K_\infty)) = c(\mathcal{E}_\infty/\mathcal{I}_\infty) \Rightarrow c(\mathcal{E}_\infty/\mathcal{D}_\infty) = c(\mathcal{E}_\infty/\mathcal{I}_\infty) \Rightarrow c(\mathcal{D}_\infty/\mathcal{I}_\infty) = \Lambda(G_\infty) \Rightarrow \mathcal{D}_\infty/\mathcal{I}_\infty$ is finite.

Euler Systems for K_n.

S = finite set of finite primes in $\mathbb{Q}$ (with $2 \in S$ always)

$m \geq 1$. μ_m = mth roots of 1 in $\bar{\mathbb{Q}}$.

$W_S = \bigcup_{(m,S)=1} \mu_m$

Definition: An Euler system is a function $\varphi: W_S \to \bar{\mathbb{Q}}^\times$ (S as above) satisfying:

(E1): $\varphi(\zeta^\sigma) = \varphi(\zeta)^\sigma \quad \forall \sigma \in G(\bar{\mathbb{Q}}/\mathbb{Q}) \quad (\Rightarrow \varphi(\zeta) \in \mathbb{Q}(\zeta) \Rightarrow \varphi(\zeta) \in \mathbb{Q}(\zeta)^+)$.

$\varphi(\zeta^{-1}) = \varphi(\zeta)$

(E2): If p is any prime not in S, we have $\prod_{\rho\in\mu_p} \varphi(\zeta\rho) = \varphi(\zeta^p) \ \forall \zeta \in W_S$.

(E3): Let p be any prime not in S. Then for all $\zeta \in W_S$ of order prime to p, we have $\varphi(\zeta\rho) \equiv \varphi(\zeta)$ mod all $\mathfrak{P}|p$, for all $\rho \in \mu_p$.

Basic Example of an Euler System.

$a_1, \dots, a_r$ non-zero integers, $n_1, \dots, n_r$, $\sum_{i=1}^r n_i = 0$.

Define $\lambda(T) = \prod_{j=1}^r (T^{-a_j} - T^{a_j})^{n_j} \in \mathbb{Q}(T)$.

Take S to be 2 and the set of all primes dividing any of $a_1, \dots, a_r$. Define $\varphi: W_S \to \bar{\mathbb{Q}}^\times$ by $\varphi(\zeta) = \lambda(\zeta) \quad \forall 1 \neq \zeta \in W_S$, and $\varphi(1) = \lim_{T\to 1} \varphi(T) = \prod_{j=1}^r a_j^{n_j}$.

Claim: φ_S is an Euler System.

(E1): obvious.

(E2): (i) $\zeta \in \mu_p$. $E2 \Leftrightarrow \prod_{1\neq\eta\in\mu_p} \lambda(\eta) = 1$. $\prod_{1\neq\eta\in\mu_p} \lambda(\eta) = \prod_{j=1}^r \Big(\prod_{\substack{\eta\in\mu_p \\ \eta\neq 1}} (\eta^{-a_j} - \eta^{a_j})\Big)^{n_j}$. $\prod_{1\neq\eta\in\mu_p} \eta^{-a_j} = 1$.

$$= \prod_{j=1}^r \Big(\prod_\eta (1 - \eta^{2a_j})\Big)^{n_j} \quad . \ (X^{p-1} + \dots + 1 = \prod_\eta (X - \eta)).$$

$$= \prod_{j=1}^r p^{n_j} = 1 \text{ because } \sum n_j = 0.$$

(ii) $\zeta \notin \mu_p$. $\prod_{\rho\in\mu_p} \lambda(\zeta\rho) = \prod_{j=1}^r \prod_{\rho\in\mu_p} ((\zeta\rho)^{-a_j} - (\zeta\rho)^{a_j})^{n_j}$

$$= \prod_{j=1}^r \prod_{\rho\in\mu_p} (\zeta^{-a_j} - \rho^{2a_j}\zeta^{a_j})^{n_j} = \prod_{j=1}^r (\zeta^{-pa_j} - \zeta^{pa_j})^{n_j}$$

(E3). $p \notin S \Rightarrow a_j$ are all prime to p. $\lambda(T) = \prod_{j=1}^r a_j^{n_j} + c_1(T-1) + c_2(T-1)^2 + \cdots$, $c_i \in \mathbb{Z}_p$.

$T_1 = \rho\zeta$, $T_2 = \zeta$. $T_1 - 1 - (T_2 - 1) = \zeta(\rho - 1)$. $\lambda(\rho\zeta) - \lambda(\zeta) = \zeta(\rho-1) \times \beta$, β integral at all primes above p.

$\equiv 0$ mod all $\mathfrak{P}|p$.

$\varphi(1)$ is not in general a unit of $\mathbb{Z}$.
$\varphi(\zeta)$ is a unit in $\mathbb{Q}(\zeta)^+$ $\forall$ $\zeta \neq 1$ in W_S.

$(m,n)=1$. $\mathbb{Q}(\mu_m)\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{mn})$. $\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$.
$H_m = \mathbb{Q}(\mu_m)^+$. Not true that $H_m H_n = H_{mn}$. We know $H_m \cap H_n = \mathbb{Q}$.

$$\begin{tikzcd} H_{mn} \arrow[r, dash, "2"] \arrow[d, dash] & \mathbb{Q}(\mu_{mn}) = H_{mn}\mathbb{Q}(\mu_n) \arrow[d, dash] \\ H_n \arrow[r, dash, "2"] & \mathbb{Q}(\mu_n) \end{tikzcd}$$

$\leftarrow$ claim this

claim Galois groups (under restriction) are isomorphic.

Note $\mathbb{Q}(\mu_n) \cap H_{mn} = H_n$.

$\varphi : W_S = \bigcup_{(m,S)=1} \mu_m \to \overline{\mathbb{Q}}^\times$. $H_m = \mathbb{Q}(\mu_m)^+$.
If p is a prime with $(p,m)=1$, we write Frob_p for the <u>Frobenius element</u> of p in $G(H_m/\mathbb{Q})$.
$\mathrm{Frob}_p(\zeta) = \zeta^p$ $\forall$ $\zeta \in \mu_m$
$\varphi(\zeta) \in H_m$ when $\zeta \in \mu_m$.

<u>Lemma</u>: Let ζ be any element of μ_m with $(m,S)=1$. Let p be any prime with $(p,m)=(p,S)=1$.
Then we have $N_{H_{mp}|H_m} \varphi(\zeta\rho) = \varphi(\zeta)^{\mathrm{Frob}_p - 1}$ $\forall \rho \neq 1$ in μ_m.

<u>Proof</u>: (i) $m>1 \Rightarrow m>2$, because $(m,S)=1$.

$$\begin{tikzcd} H_{mp} \arrow[r, dash, "2"] \arrow[d, dash, "p-1"'] & \mathbb{Q}(\mu_{mp}) = H_{mp}\mathbb{Q}(\mu_m) \arrow[d, dash, "p-1"] \\ H_m \arrow[r, dash, "2"'] & \mathbb{Q}(\mu_m). \end{tikzcd}$$

$G(\mathbb{Q}(\mu_{mp})/\mathbb{Q}(\mu_m))$ operates transitively on $\mu_p \setminus \{1\}$.

$$N_{H_{mp}|H_m} \varphi(\zeta\rho) = \prod_{\sigma \in G(\mathbb{Q}(\mu_{mp})/\mathbb{Q}(\mu_m))} \varphi(\zeta\rho^\sigma)$$

$$= \prod_{\rho \in \mu_p - \{1\}} \varphi(\zeta\rho) = \frac{\varphi(\zeta^{\mathrm{Frob}_p})}{\varphi(\zeta)} = \frac{\varphi(\zeta)^{\mathrm{Frob}_p}}{\varphi(\zeta)}$$

(ii) $m=1$. $\left(N_{H_p/\mathbb{Q}}(\varphi(\rho))\right)^2 = \prod_{\sigma \in G(\mathbb{Q}(\mu_p)/\mathbb{Q})} \varphi(\rho)^\sigma = \prod_{\substack{\rho \in \mu_p \\ \rho \neq 1}} \varphi(\rho) = 1.$

Frob_p acts on $\varprojlim \mu_{l^n}$, $l \neq p$, by p.

<u>Lemma</u>: Let ζ be any element of μ_m with $(m,S)=1$. Let p be any prime with $(p,S)=(p,m)=1$. Then, for all $n \geq 1$, we have $N_{H_{mp^{n+1}}|H_{mp^n}} \varphi(\zeta\rho) = \varphi(\zeta^{\mathrm{Frob}_p} \cdot \rho^p)$, ρ any primitive p^{n+1}-th root of 1.

$$\begin{tikzcd} H_{mp^{n+1}} \arrow[r, dash, "2"] \arrow[d, dash, "p"'] & \mathbb{Q}(\mu_{mp^{n+1}}) \arrow[d, dash, "p"] \\ H_{mp^n} \arrow[r, dash, "2"'] & \mathbb{Q}(\mu_{mp^n}) \end{tikzcd}$$

$\{\rho^\sigma\}$, $\sigma \in G(\mathbb{Q}(\mu_{mp^{n+1}})/\mathbb{Q}(\mu_{mp^n}))$
$\overset{\shortparallel}{\{\rho\eta\}}$, $\eta \in \mu_p$.
$N\varphi(\zeta\rho) = \prod_{\eta \in \mu_p} \varphi(\zeta\rho\eta) = \varphi(\zeta^p \rho^p)$.

ρ_n a primitive p^{n+1}-th root of 1. $\rho_{n+1}^p = \rho_n$. $\zeta \in \mu_m$ with $(m,p)=(m,S)=1$.

<u>Corollary</u>: The sequence $\varphi(\rho_n \zeta^{\mathrm{Frob}_p^{-n}})$, $n=0,1,2,\dots$ is norm compatible in the tower $H_{mp^\infty}|H_{mp}$.

<u>Lemma</u>: Let p be any prime and F any finite extension of $\mathbb{Q}$. Let $\alpha \neq 0$ in F be a norm from every finite extension of F contained in $FH_{p^\infty} = FK_\infty$. Then every prime occurring in the factorisation of α must divide p.

<u>Proof</u>:
$$\begin{array}{ccc} FH_{p^\infty} & & \\ | & \searrow & H_{p^\infty} \\ F & - & \mathbb{Q} \end{array}$$

(i) Each prime of F not above is unramified in FH_{p^∞}.
(ii) Above each finite prime of F, there are only finitely many primes of FH_{p^∞}.

$q \neq p$, order of q in $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ as $n \to \infty$. $p^{n-t} \mid r_{q,n}$ t fixed as $n \to \infty$.

$\wp$ of F, $\wp \nmid p$.

$$\begin{array}{ccc} FH_{p^\infty} & & \\ | & L & k_L \\ | & L' & k_L' \\ F & & \end{array}$$

$N_{L/L'} \wp_L = \wp_{L'}^{[L:L']}$

<u>Lemma</u>: Assume $1 \neq \zeta \in W_S$. Then $\varphi(\zeta)$ is a unit in $\mathbb{Q}(\zeta)^+$. r = exact order of ζ. p a prime dividing r. $r = p^{m+1} r_1$, $m \geq 0$, $(r_1, p) = 1$.

$\zeta = \rho_m \theta^{\mathrm{Frob}_p^{-m}}$ for some $\theta \in \mu_{r_1}$.
ρ_m: primitive p^{m+1}-th root of 1

[Previous lemma
$\Rightarrow \varphi(\zeta)$ is a norm from $H_{r_1 p^{n+1}}$ for all $n \geq m \Rightarrow$ all $\wp$ occurring in fact of $\varphi(\zeta)$ dividing p.]

So $r_1 > 1$ okay. Let $r_1 = 1$.

$N_{H_{p^{m+1}}/H_p} \varphi(\zeta) = \varphi(\rho_0)$. $\rho_0 = p^m \rho_m$. $\varphi(\zeta)$ is a unit $\Leftrightarrow \varphi(\rho_0)$ is a unit.

$N_{H_p/\mathbb{Q}} \varphi(\rho_0) = \pm 1$.

<u>Factorisation</u>: $\varphi(\rho \zeta_{q_1} \cdots \zeta_{q_r})$, ρ a fixed primitive p^{m+1}-th root of 1 $(m \geq 0)$.

$q_1, \ldots, q_r$ distinct primes $\neq p$. ζ_{q_i} - primitive q_i-th root of 1.

$FH_{p^{m+1}}$.

$(*)$ $\varphi(\rho \zeta_{q_1} \cdots \zeta_{q_r}) \in F(\mu_{q_1 \cdots q_r})^+$

Look at $F(\mu_{q_1 \cdots q_r})^{+\times} / F(\mu_{q_1 \cdots q_r})^M$. Act on it by an element of the group ring to make $(*)$ invariant under $G(F(\mu_{q_1 \cdots q_r})^+/F)$.

$F^\times / F^{\times M}$

<u>Factorisation Theorem</u>

$\varphi: W_S \to \overline{\mathbb{Q}}^\times$, $p \notin S$. Fix $F = \mathbb{Q}(\mu_{p^{m+1}})^+$, $q_1, \ldots, q_r$ distinct primes, not in S, $\neq p$.

ρ = primitive p^{m+1}-th root of 1, ζ_{q_i} = primitive q_i-th root of 1.

$\varphi(\rho \zeta_{q_1} \cdots \zeta_{q_r})$ unit in $F(b) = F(\mu_b)^+$, $b = q_1 \cdots q_r$. Fix $M = p^a$, $a \geq m+1$. $G_b = G(F(b)/F)$

<u>Lemma</u>: The natural map from $F^\times / F^{\times M} \to \left(F(b)^\times / F(b)^{\times M}\right)^{G_b}$ is an isomorphism.

Kummer: $F^\times / F^{\times M} \xrightarrow{\sim} H^1(F, \mu_M)$

$$\begin{tikzcd}
 & H^2(G_b, \mu_M(F(b))) = 0 \\
(F(b)^\times / F(b)^{\times M})^{G_b} \arrow[r, "\sim"] & H^1(F(b), \mu_M)^{G_b} \arrow[u] \\
F^\times / F^{\times M} \arrow[u] \arrow[r, "\sim"] & H^1(F, \mu_M) \arrow[u] \\
 & H^1(G_b, \mu_M(F(b))) = 0 \arrow[u] \\
 & 0 \arrow[u]
\end{tikzcd}$$

$\mu_M(F(b)) = 1$ since $F(b)$ is real and $p \neq 2$.

Seek $\Omega \in \mathbb{Z}[G_b]$. $\varphi(\rho \zeta_{q_1} \cdots \zeta_{q_r})^{\Omega} \bmod F(b)^{\times M}$ is fixed by G_b.

Lemma: (i) The ramification index of each prime of F dividing q_i in $F(b)$ is $q_i - 1$

(ii) $F(\mu_{q_i})^+ \cap F(b/q_i) = F \quad (i = 1, \ldots, r)$

Corollary: $G_b \xrightarrow{\sim} G_{q_1} \times \cdots \times G_{q_r}$. $\quad G_{q_i} = G(F(\mu_{q_i})/F) = G(F(b)/F(b/q_i))$.

Proof of lemma:

$d_i = \frac{b}{q_i} p^{m+1}$.

$$\begin{tikzcd}
 & & \mathbb{Q}(\mu_{d_i q_i}) = \mathbb{Q}(\mu_{d_i}) F(b) \arrow[dd, dash, "q_i - 1" ', "\text{- totally ramified of degree } q_i - 1"] \\
F(b) = \mathbb{Q}(\mu_{d_i q_i})^+ \arrow[urr, dash, "\text{unramified}", "2" '] \arrow[dr, dash, "\text{totally ramified.}" ', "q_i - 1"] & & \\
 & \mathbb{Q}(\mu_{d_i})^+ \arrow[r, dash, "2", "\text{unramified.}" '] & \mathbb{Q}(\mu_{d_i})
\end{tikzcd}$$

$G_{q_i} = G(F(\mu_{q_i})^+/F) \xrightarrow{\sim} (\mathbb{Z}/q_i\mathbb{Z})^\times$. Fix a generator $\tau(q_i)$ of G_{q_i}.

$\mathbb{Z}[G_{q_i}] \subset \mathbb{Z}[G_b]$. $\quad N(q_i) = \sum_{k=0}^{q_i-2} \tau(q_i)^k$, $\quad D(q_i) = \sum_{k=0}^{q_i-2} k\,\tau(q_i)^k$

Lemma: $(\tau(q_i) - 1) D(q_i) = \sum_{k=0}^{q_i-3} k\,\tau(q_i)^{k+1} - \sum_{k=0}^{q_i-2} k\,\tau(q_i)^k + q_i - 2 \quad = q_i - 1 - N(q_i)$.

So $(\tau(q_i) - 1) D(q_i) = q_i - 1 - N(q_i)$

For $b = q_1 \cdots q_r$, let $D(b) = D(q_1) \cdots D(q_r)$ in $\mathbb{Z}[G]$.

$\Omega = D(b)$. Now assume $q_i \equiv 1 \bmod M$ for $i = 1, \ldots, r$.

Lemma: Assume $q_i \equiv 1 \bmod M$ $(i = 1, \ldots, r)$. Then $\varphi(\rho \zeta_{q_1} \cdots \zeta_{q_r})^{D(b)} \bmod F(b)^{\times M}$ is fixed by G_b.

Proof: By induction on $r = \#\{q_i\}$.

$r = 1$: $G_b = G_{q_i}$ generated by $\tau(q_i)$. $\quad \varphi(\rho \zeta_{q_i})^{(\tau(q_i)-1)D(q_i)} \in F(q_i)^{\times M}$

$\varphi(\rho \zeta_{q_i})^{(\tau(q_i)-1)D(q_i)} = \varphi(\rho \zeta_{q_i})^{q_i - 1 - N(q_i)}$

$\varphi(\rho \zeta_{q_i})^{N(q_i)} = \varphi(\rho)^{\mathrm{Frob}_{q_i} - 1} = 1$, $\quad \mathrm{Frob}_{q_i} \in G(F/\mathbb{Q})$.

$r > 1$: $\varphi(\rho \zeta_{q_1} \cdots \zeta_{q_r})^{(\sigma - 1)D(b)}$, $\quad \sigma = \tau(q_i) \quad (i = 1, \ldots, r)$

$(\sigma - 1) D(b) = (\tau(q_i) - 1) D(q_i) . D(b/q_i)$.

So $= \varphi(\rho \zeta_{q_1} \cdots \zeta_{q_r})^{(q_i - 1 - N(q_i)) D(b/q_i)} = \varphi(\rho \zeta_{q_1} \cdots \zeta_{q_r})^{-N(q_i) D(b/q_i)}$

$= \varphi(\rho \zeta_{q_1} \cdots \widehat{\zeta_{q_i}} \cdots \zeta_{q_r})^{(1 - \mathrm{Frob}_{q_i}) D(b/q_i)}$

Definition: $\Phi_M(\rho\zeta_{q_1}\cdots\zeta_{q_r}) \in F^\times/F^{\times M} \longrightarrow F(b)^\times/F(b)^{\times M}$ — only primes dividing $q_1 \cdots q_r$ ramify.
$\longleftrightarrow \varphi(\rho\zeta_{q_1}\cdots\zeta_{q_r})^{D(b)}$

$(\Phi_M(\rho\zeta_{q_1}\cdots\zeta_{q_r})) \in I/MI.$ I = group of fractional ideals of F

$F = \mathbb{Q}(\mu_{p^{m+1}})^+$. $M = p^a$, $a \geq m+1$.
I: free abelian group on all prime ideals of F
I_q = ———— " ———— dividing q.

$$I/MI = \bigoplus_q I_q/MI_q$$
$(x) \mapsto (x)_q \qquad x \in F^\times/F^{\times M}, \ x = \sum_q (x)_q.$

Lemma: Assume q is a prime with $q \equiv 1 \bmod M$. Then there is a canonical $G(F|\mathbb{Q})$-homomorphism $\lambda_{q,M} : (\mathcal{O}_F/q\mathcal{O}_F)^\times \to I_q/MI_q$ which is surjective, and whose kernel is precisely the group of M-th powers in $(\mathcal{O}_F/q\mathcal{O}_F)^\times$.

Proof: q splits completely in $F \Rightarrow (\mathcal{O}_F/q\mathcal{O}_F)^\times \cong \prod_{\mathfrak{q}|q} (\mathcal{O}_F/\mathfrak{q})^\times$.

$F(\mu_q)^+$
$G_q \Big| \ q-1$ - totally ramified.
F

Let $\pi(\mathfrak{q})$ be any local parameter at unique prime above $\mathfrak{q}$.

$G_q \xrightarrow{\sim} k_{\mathfrak{q}}^\times$ Fix $G_q = \langle \tau(q) \rangle$.

$\sigma \longmapsto \dfrac{\sigma(\pi(\mathfrak{q}))}{\pi(\mathfrak{q})} \bmod \mathfrak{q}$.

$\tau(q) \longmapsto \gamma_{\mathfrak{q}}$, by way of definition. Ie, $\gamma_q = \dfrac{\tau(q)(\pi(\mathfrak{q}))}{\pi(\mathfrak{q})}$

$\alpha \in \mathcal{O}_F$, $(\alpha, q) = 1$. $\alpha \bmod \mathfrak{q} = \gamma(\mathfrak{q})^{a(\mathfrak{q})}$, $a(\mathfrak{q}) \in \mathbb{Z}/(q-1)\mathbb{Z}$.
$\lambda_{q,M}(\alpha \bmod q\mathcal{O}_F) = \sum_{\mathfrak{q}|q} (a(\mathfrak{q}) \bmod M)\,\mathfrak{q}$

$\varphi : W_S \to \bar{\mathbb{Q}}^\times$, ρ - primitive p^{m+1}-th root of 1. $q_1, \ldots, q_r \equiv 1 \bmod M$. Let $b = q_1 \cdots q_r$.
$F(b) := F(\mu_b)^+$, $G_b = G(F(b)/F)$. $\zeta_{q_i} \neq 1$. Write $\zeta_b = \zeta_{q_1} \cdots \zeta_{q_r}$.
$D(b) \in \mathbb{Z}[G_b]$.
$\varphi(\rho\zeta_b)^{D(b)} \bmod F(b)^{\times M} \in (F(b)^\times/F(b)^{\times M})^{G_b}$

$I/MI \hookleftarrow \Phi_M(\rho\zeta_b) \in F^\times/F^{\times M}$

Factorisation Theorem: (i) $(\Phi_M(\rho\zeta_b))_q = 0$ for $q \neq q_1, \ldots, q_r$.
(ii) $(\Phi_M(\rho\zeta_b))_{q_i} = \lambda_{q_i,M}(\Phi_M(\rho\zeta_{b/q_i}))$ $(i = 1, \ldots, r)$

Notation: Frob_{q_i} = Frobenius automorphism attached to q_i in $G(F(b/q_i)^+/\mathbb{Q})$. (in $G(F(b/q_i)^+/F)$)
We will use: (i) In $F(b)$, M-th roots are unique since $p \neq 2$.
(ii) axiom E3.

We know there exists $\beta \in F(b)^\times$ such that $\varphi(\rho\zeta_b)^{D(b)}/\beta^M \in F^\times$.

$$(\Phi_M(\rho\zeta_b))_{q_i} = \sum_{\mathfrak{q}|q_i} \left(\frac{-M}{q_i - 1}\, \mathrm{ord}_{\mathfrak{q}''}(\beta) \bmod M\right)\mathfrak{q}$$

$F(b)$ — $\mathfrak{q}''$
$F(b/q_i)$ — $\mathfrak{q}'$ $\Big\}$ $q_i - 1$ - ramification index.
F — $\mathfrak{q}$
$\mathbb{Q}$ — q

Let $c_{\mathfrak{q}} = \mathrm{ord}_{\mathfrak{q}''}(\beta)$. $\quad \beta = \pi(\mathfrak{q})^{c_{\mathfrak{q}}} \times \alpha_{\mathfrak{q}}$, $\alpha_{\mathfrak{q}}$ a unit at $\mathfrak{q}''$

$\beta^{1-\tau(q_i)} = \gamma(\mathfrak{q})^{c_{\mathfrak{q}}} \times \alpha_{\mathfrak{q}}^{1-\tau(q_i)} \equiv \gamma(\mathfrak{q})^{c_{\mathfrak{q}}} \mod \mathfrak{q}''$

$\varphi(\rho\zeta_b)^{(1-\tau(q_i))D(b)} = \beta^{(1-\tau(q_i))M}$.

$(1-\tau(q_i))D(b) = (N(q_i)+1-q_i)D(b/q_i)$ - from earlier.

$$\varphi(\rho\zeta_b)^{(1-\tau(q_i))D(b)} = \varphi(\rho\zeta_b)^{N(q_i)D(b/q_i)}\left[\varphi(\rho\zeta_b)^{D(b/q_i)\frac{(1-q_i)}{M}}\right]^M$$

$\varphi(\rho\zeta_b)^{N(q_i)} = \varphi(\rho\zeta_{b/q_i})^{\mathrm{Frob}(q_i)-1}$ (from E2).

So $\varphi(\rho\zeta_b)^{(1-\tau(q_i))D(b)} = \beta_i^{(\mathrm{Frob}(q_i)-1)M} \cdot \left[\varphi(\rho\zeta_b)^{D(b/q_i)\frac{(1-q_i)}{M}}\right]^M$

$\Rightarrow \beta^{1-\tau(q_i)} = \beta_i^{(\mathrm{Frob}(q_i)-1)} \times \varphi(\rho\zeta_b)^{D(b/q_i)(1-q_i)/M}$.

We had: $(\Phi_M(\rho\zeta_b))_{q_i} \equiv \sum_{\mathfrak{q}|q_i}\left(\frac{-M}{q_i-1}\mathrm{ord}_{\mathfrak{q}''}(\beta)\,\mathfrak{q}\right)$, $\quad b = q_1 \cdots q_r$, $q_i \equiv 1 \mod M$.

$$\beta^{1-\tau(q_i)} = \beta_i^{(\mathrm{Frob}(q_i)-1)} \times \varphi(\rho\zeta_b)^{\frac{1-q_i}{M}\cdot D(b/q_i)} \mod \mathfrak{q}''$$

$\varphi(\rho\zeta_{b/q_i})^{D(b/q_i)}/\beta_i^M \in F^\times$. $\quad \beta_i \in F(b/q_i)$. $\quad \beta_i^{\mathrm{Frob}(q_i)} \equiv \beta_i^{q_i} \mod \mathfrak{q}'$.

E3: $\varphi(\rho\zeta_b) \equiv \varphi(\rho\zeta_{b/q_i}) \mod \mathfrak{q}''$

$$\beta^{1-\tau(q_i)} \equiv \left(\beta_i^M/\varphi(\rho\zeta_{b/q_i})^{D(b/q_i)}\right)^{\frac{q_i-1}{M}} \mod \mathfrak{q}''$$

$\quad |||\qquad\qquad\qquad ||$

$\gamma(\mathfrak{q})^{c(\mathfrak{q})} \qquad\quad \gamma(\mathfrak{q})^{a(\mathfrak{q})}$

$c(\mathfrak{q}) = \mathrm{ord}_{\mathfrak{q}''}(\beta)$

$c_{\mathfrak{q}} \equiv \left(\frac{-(q_i-1)}{M}a(\mathfrak{q})\right) \mod (q_i-1)$.

$K_\infty = \mathbb{Q}(\mu_{p^\infty})^+$, $G_\infty = G(K_\infty/\mathbb{Q}) = \Delta \times \Gamma$.

V_n = Local units of K_n at $\mathfrak{p}_n|p$, which are congruent to $1 \mod \mathfrak{p}_n$. $\quad V_\infty = \varprojlim V_n$

$i_\infty : V_\infty \xrightarrow{\sim} \Lambda(G_\infty)$

$\mathcal{L}_\infty = \varprojlim \mathcal{L}_n$, $\mathcal{L}_n$ = closure of V_n in cyclotomic units C_n.

$i_\infty(\mathcal{L}_\infty) = ((\rho-1)\mu_B)$ where ρ is any topological generator of G_∞.

$\mathcal{E}_\infty = \varprojlim \mathcal{E}_n$, $\mathcal{E}_n$ = closure of V_n in the group of all units of K_n which are $\equiv 1 \mod \mathfrak{p}_n$.

Question 1: What is $i_\infty(\mathcal{E}_\infty)$ as an ideal of $\Lambda(G_\infty)$.

Theorem: $i_\infty(\mathcal{E}_\infty)$ is a principal ideal of $\Lambda(G_\infty)$, say $i_\infty(\mathcal{E}_\infty) = e_\infty\Lambda(G_\infty)$, some $e_\infty \in \Lambda(G_\infty)$.

Let $\quad$ = group of all Euler Systems $\varphi : W_S \to \overline{\mathbb{Q}}^\times$ with $p \notin S$.

ζ_n = primitive p^{n+1}-th root of 1 : $\zeta_n^p = \zeta_{n-1}$ $\forall n \geq 1$.

Note: $N_{K_{n+1}|K_n}\varphi(\zeta_{n+1}) = \varphi(\zeta_n)$.

$B_n = \{\varphi(\zeta_n) : \varphi \in H(p),\ \varphi(\zeta_n) \equiv 1 \mod \mathfrak{p}_n\} \supset C_n$.

Remark: $\varphi(\zeta_n) \equiv 1 \mod \mathfrak{p}_n$ $\forall n \geq 0 \iff \varphi(\zeta_n) \equiv 1 \mod \mathfrak{p}_n$ for at least one n.

$\mathcal{B}_n$ = closure of B_n in V_n. $\quad \mathcal{B}_\infty = \varprojlim \mathcal{B}_n$. $\quad \mathcal{L}_\infty \subset \mathcal{B}_\infty \subset \mathcal{E}_\infty$.

Question 2: What is $\iota_\infty(\mathcal{B}_\infty)$?

Theorem: $\iota_\infty(\mathcal{B}_\infty)$ is a principal ideal of $\Lambda(G_\infty)$.

X, a finitely generated $\Lambda(G_\infty)$-module. $X = \bigoplus_{\chi \in \mathrm{Hom}(D, \mathbb{Z}_p^\times)} X^{(\chi)}$, $X^{(\chi)} = e_\chi X$.

Lemma: $X \xrightarrow{\sim} \Lambda(G_\infty) \iff \forall \chi \in \mathrm{Hom}(D, \mathbb{Z}_p^\times)$ and all $n \geq 0$, we have $(X^{(\chi)})_{\Gamma_n}$ is a free $\mathbb{Z}_p$-module of rank p^n.

$G_\infty = D \times \Gamma$, $\Gamma_n \underset{p^n}{\subset} \Gamma$. $(\Lambda(G_\infty))_{\Gamma_n} = \mathbb{Z}_p[G_n]$, $G_n = G(K_n/\mathbb{Q})$.

$(\mathcal{E}_\infty)_{\Gamma_n} \twoheadrightarrow \mathcal{E}_n^*$

$(\mathcal{B}_\infty)_{\Gamma_n} \twoheadrightarrow \mathcal{B}_n$.
$\qquad\qquad\qquad \cup$
$\qquad\qquad\qquad \mathcal{I}_n$

L_∞ = maximal unramified p-extension of K_∞.

$$\begin{array}{l} \quad L_\infty \\ \ \ / \\ K_\infty \\ \ |\ G_\infty \\ \mathbb{Q} \end{array}$$

Goal: $c(G(L_\infty/K_\infty)) \supset c(\mathcal{E}_\infty/\mathcal{B}_\infty)$

$G(L_\infty/K_\infty)$ as a $\Lambda(G_\infty)$-module.

$\iota_\infty(\mathcal{E}_\infty) = e_\infty \Lambda(G_\infty)$

$\iota_\infty(\mathcal{B}_\infty) = e_\infty g_\infty \Lambda(G_\infty)$

$\mathcal{E}_\infty/\mathcal{B}_\infty \cong \Lambda(G_\infty)/(g_\infty)$

$c(\mathcal{E}_\infty/\mathcal{B}_\infty) = (g_\infty)$

$$0 \to \bigoplus_{i=1}^{k} \Lambda(G_\infty)/(f_{i,\infty}) \to G(L_\infty/K_\infty) \to D \to 0 \qquad \text{- } D \text{ finite.}$$