

p-adic interpolation

- (44) Bernoulli numbers & polynomials (elementary prop's)
- (45) Bernoulli numbers & ζ @ negative odd integers
- (46) p-adic measures from Bernoulli polynomials
- (47) p-adic ζ & L -fns and p-adic Mellin transforms of measures
- (48) Modular parametrization & Manin-Drinfeld revisited.
- (49) p-adic L -fns attached to modular ell. curves
- (50) Birch & Swinnerton-Dyer conjecture (intermezzi, nupfs)
- (51) p-adic measures, moments, and Iwasawa series & fns
- (52) p-adic interpolation of Eisenstein series (cf. Serre-Katz)
- (53) Iwasawa algebra of a profinite group
- (54) Modules over the Iwasawa algebra.
- (55) "Main conjectures" à la Iwasawa (the philosophy)
- (56) Analogy with function fields
- (57) Analogies between analogies

44 Bernoulli numbers & polynomials : elementary properties

(Def) $\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$, $B_k \in \mathbb{Q}$, Bern. #'s So $B_1 = -\frac{1}{2}$ $\sim P$

(Def) Let $B, t, x, \dots$ be variables. Define $\mathbb{Q}[B] \rightarrow \mathbb{Q}$, $\sum a_i B^i \mapsto \sum a_i B_i$ *
 Similarly $\mathbb{Q}[B][t] \rightarrow \mathbb{Q}[t]$, $f = \sum P_i t^i \mapsto \tilde{f} := \sum \tilde{P}_i t^i$ **
 —||— $\mathbb{Q}[B][t, x] \rightarrow \mathbb{Q}[t, x]$, etc.

(Ex) $\frac{t}{e^t - 1} = e^{\tilde{t}B} \in \mathbb{Q}[t]$

(Def) $B_k(x) = (B+x)^k = \sum \binom{k}{i} B_i x^{k-i} = B_k + k B_{k-1} x + \binom{k}{2} B_{k-2} x^2 + \dots = x^k - \frac{k}{2} x^{k-1} + \dots$

(Prop) $\frac{t e^{xt}}{e^t - 1} = \sum_0^{\infty} B_k(x) \frac{t^k}{k!}$ [Pf: $\frac{t e^{xt}}{e^t - 1} = e^{\tilde{B}t} e^{xt} = e^{(B+x)t} = \sum \frac{(B+x)^k}{k!} t^k = \text{RHS}$]

(Prop) $1^k + 2^k + \dots + n^k = \frac{1}{k+1} [B_{k+1}(n+1) - B_{k+1}]$.

Pf. $\sum_{k=0}^{\infty} (1^k + 2^k + \dots + n^k) \frac{t^k}{k!} = e^t + e^{2t} + \dots + e^{nt} = -1 + \frac{e^{(n+1)t}}{e^t - 1} = -1 + \frac{e^{(n+1)t}}{e^t - 1} = -1 + \frac{t}{e^t - 1} e^{(n+1)t}$
 $= -1 + \frac{1}{t} [e^{(n+1+B)t} - e^{\tilde{B}t}] = -1 + (\sum_{k=1}^{\infty} \frac{(B+n+1)^k}{k!} t^{k-1} - \sum \frac{B^k}{k!} t^{k-1})$ etc

(Prop) $B_k(px) = p^{k-1} \sum_{i=0}^{p-1} B_i(x + \frac{i}{p})$

Pf. Want $I = \sum_{k=0}^{\infty} \text{LHS} \cdot \frac{t^k}{k!} = \sum_{k=0}^{\infty} \text{RHS} \cdot \frac{t^k}{k!} = II$. Now $I = \sum (B+px)^k \frac{t^k}{k!} = e^{\tilde{B}t + pxt}$

Also $II = \frac{1}{p} \sum_{i=0}^{p-1} (B+x+\frac{i}{p})^k \frac{p^k t^k}{k!} = \frac{1}{p} (e^{(B+px)t} + e^{(B+px+1)t} + \dots + e^{(B+px+p-1)t})$
 $= \frac{1}{p} e^{pBt + pxt} \frac{e^{pt} - 1}{e^t - 1} = \frac{1}{p} e^{pBt} e^{pxt} \frac{e^{pt} - 1}{pt} \frac{pt}{e^t - 1} = e^{\tilde{B}t + pxt}$ □

(Prop) $B_k(1-x) = (-1)^k B_k(x)$. In particular, for $x=0 \Rightarrow (B+1)^k = (-1)^k B^k$ ($\Rightarrow$ can compute B_k 's induct)

Pf. $\sum B_k(1-x) \frac{t^k}{k!} = \frac{t e^{(1-x)t}}{e^t - 1} = \frac{t e^t e^{-xt}}{e^t - 1} = \frac{t e^{-xt}}{1 - e^{-t}} = \frac{(-t) e^{x(-t)}}{e^{-t} - 1} = \sum B_k(x) \frac{(-t)^k}{k!}$

(Prop) $\lim_{n \rightarrow \infty} \frac{1}{p^n} \sum_{x=0}^{p^n-1} x^k = B_k$

Pf $\frac{1}{p^n} \sum_{x=0}^{p^n-1} x^k = \frac{1}{p^n} \cdot \frac{1}{k+1} (B_{k+1}(p^n) - B_{k+1})$

$$= \frac{1}{p^n} \frac{1}{k+1} (B_{k+1} + \binom{k+1}{1} B_k p^n + \binom{k+1}{2} B_{k-1} p^{2n} + \dots - B_{k+1})$$

$$= B_k + p^n (\dots) \rightarrow B_k$$

(Def) If $f \in \mathbb{Q}_p[B]$ define $\int_{\mathbb{Z}_p} f(B) dB = \lim_{n \rightarrow \infty} \frac{1}{p^n} \sum_{x=0}^{p^n-1} f(x)$ (Volkenborn integral, $\widetilde{f(B)}$)

(it follows by previous prop & actually it's equal to $\widetilde{f(B)}$.)

45

Bernoulli Numbers and ζ at odd neg integers

Def $\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$, $B_k \in \mathbb{Q}$.

Prop $B_k = 0$ for k odd ≥ 3 [Pf. $\frac{t}{2} + \frac{t}{e^t - 1} = \frac{t}{2} \left(\frac{e^t + 1}{e^t - 1} \right)$ is even]

Prop $\left(\frac{\pi}{\sin \pi z} \right)^2 = \sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2}$ (w/ RHS normally convergent ^{*})

Pf. Both LHS & RHS are/mero on $\mathbb{C}$, z their poles are in $\mathbb{Z}$ (double poles w/ princip. part $\frac{1}{(z-n)^2}$, 3) tend to 0 unif w/ $\text{Re } z$ as $|\text{Im } z| \rightarrow \infty$.

So LHS-RHS is holo & bounded so (Liouville) const so 0.

Prop $\pi \cot \pi z = \frac{1}{z} + \sum_{n \neq 0} \left(\frac{1}{z-n} + \frac{1}{n} \right) \stackrel{!}{=} \frac{1}{z} + \sum_{n \geq 1} \frac{2z}{z^2 - n^2}$

Pf. $\frac{d}{dz}(\text{RHS}) = -\frac{1}{z^2} - \sum_{n \neq 0} \frac{1}{(z-n)^2} = -\left(\frac{\pi}{\sin \pi z} \right)^2 = \frac{d}{dz}(\pi \cot \pi z)$

so RHS-LHS = const, But also odd. So = 0.

Th (Euler) $\zeta(k) = -\frac{(2\pi i)^k B_k}{2 \cdot k!}$ for k even, ≥ 2 .

Pf. $\pi \cot \pi z = \frac{1}{z} + \frac{1}{z} \sum_{n \geq 1} \frac{2z^2}{z^2 - n^2} = \frac{1}{z} - \frac{2}{z} \sum_{n \geq 1} \frac{z^2}{n^2 - z^2} = \frac{1}{z} - \frac{2}{z} \sum_{n \geq 1} \frac{z^2/n^2}{1 - z^2/n^2}$
 $= \frac{1}{z} - \frac{2}{z} \sum_{n \geq 1} \sum_{k \geq 1} \frac{z^{2k}}{n^{2k}} = \frac{1}{z} - \frac{2}{z} \sum_{k \geq 1} \zeta(2k) z^{2k}$

$\pi \cot \pi z = \frac{\pi i (e^{i\pi z} + e^{-i\pi z})}{e^{i\pi z} - e^{-i\pi z}} = \pi i \cdot \frac{e^{2\pi i z} + 1}{e^{2\pi i z} - 1} = \pi i + \frac{2\pi i}{e^{2\pi i z} - 1}$
 $= \pi i + \frac{1}{z} \frac{2\pi i z}{e^{2\pi i z} - 1} = \pi i + \frac{1}{z} \sum_{k=0}^{\infty} B_k \frac{(2\pi i z)^k}{k!}$ & compare

uses final eqn for ζ $\rightarrow$ **Cor** $\zeta(1-k) = -\frac{B_k}{k}$ for k even, ≥ 2 .

Pf. Use final eqn for ζ , final eqn for Γ , $\Gamma(\frac{1}{2}) = \sqrt{\pi}$, and prev. Th.

^{*} $\left(\frac{1}{z-n} + \frac{1}{n} \right) + \left(\frac{1}{z+n} - \frac{1}{n} \right) = \frac{2z}{z^2 - n^2}$

^{*} i.e., $\sum_{n=-\infty}^{\infty} = \sum_{n=0}^{\infty} + \sum_{n=-1}^{-\infty}$ & both $\sum$'s abs & unif conv ^{each} comparts after fin many terms removed (depending on the comparts)

45

p-adic measures from Bernoulli polynomials

has p-adic metric $|x-y|_p$.

Recall def $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$.

$B(a, \frac{1}{p^n})$ = ball of rad $\frac{1}{p^n}$.

Def An interval in $\mathbb{Q}_p$ is a set $a + p^n\mathbb{Z}_p$ w/ $a \in \mathbb{Q}_p$.

Prop (triv) $\forall$ compact open in $\mathbb{Q}_p$ is a fin. union of intervals.

Def A $\star$ distribution is a map $\mu : \{ \text{compact open sets of } X \} \rightarrow \mathbb{Q}_p$ s.t. if on a compact open X in $\mathbb{Q}_p$

Def μ is called p-invariant if $\mu(pU) = \mu(U)$ $\forall U$ compact open in X & $U = U_1 \cup \dots \cup U_m$ disj $\Rightarrow \mu(U) = \sum \mu(U_i)$.

Prop (triv) A map $\mu : \{ \text{intervals } \subset X \} \rightarrow \mathbb{Q}_p$ s.t. $\mu(pU) = \mu(U)$ $\forall U$ interval $\subset X$ & $U = U_1 \cup \dots \cup U_m$ disj $\Rightarrow \mu(U) = \sum \mu(U_i)$.

$\mu(a + p^n\mathbb{Z}_p) = \sum_{b=0}^{p-1} \mu(a + bp^n + p^{n+1}\mathbb{Z}_p)$, $\forall a + p^n\mathbb{Z}_p \subset X$

extends uniquely to a distr. on X

Ex 1) $\mu_{\text{Haar}}(a + p^n\mathbb{Z}_p) = \frac{1}{p^n}$ distr on $\mathbb{Z}_p$ (transl. inv.)

2) $\mu_{\text{Dirac}}(U) = \begin{cases} 1 & a \in U \\ 0 & a \notin U \end{cases}$, a fixed $\in \mathbb{Z}_p$

3) $\mu_{\text{Bernoulli}}^k = \mu_{\text{Haar}}^k$, $\mu_{\text{Bernoulli}}^k(a + p^n\mathbb{Z}_p) = p^{n(k-1)} B_k(\langle \frac{a}{p^n} \rangle)$ $\star\star$

$\mu_{\text{Bernoulli}}^1$ is p-invariant

[Checking the latter is a distrib: Enough to take $a \in \{0, 1, \dots, p^n-1\}$ & check $\star\star$]

LHS of $\star\star = p^{n(k-1)} B_k(\frac{a}{p^n}) = p^{n(k-1)} B_k(p \cdot \frac{a}{p^{n+1}}) = p^{n(k-1)} \sum_{b=0}^{p-1} B_k(\frac{a}{p^{n+1}} + \frac{b}{p})$
 $= p^{(n+1)(k-1)} \sum_{b=0}^{p-1} B_k(\frac{a + p^n b}{p^{n+1}}) = \text{RHS of } \star\star$ For $B(pX)$

Def A distrib μ on X is called a measure if $\exists C \forall$ interval $U \subset X$, $|\mu(U)|_p \leq C$

Rem μ_{Haar} & $\mu_{\text{Bernoulli}}$ are not measures!

Def If μ p-ad distrib on X & $f : X \rightarrow \mathbb{Q}_p$ cont, define $S_n := \sum_{a \in a + p^n\mathbb{Z}_p \subset X} f(a) \mu(a + p^n\mathbb{Z}_p)$

Say f int wrt μ if S_n has a limit in $\mathbb{Q}_p$ (call it $\int f d\mu = \int_X f(x) d\mu(x)$).

Prop μ a p-adic meas & f cont $\Rightarrow f$ int wrt μ . Also if μ is α^X distr. & f loc cont then f int wrt μ .

Def Let $\alpha \in \mathbb{Z}_p^\times$. Define $\mu_{\text{Mazur}}^{k, \alpha} = \mu_{\text{Bernoulli}}^{k, \alpha}$, $\mu_{\text{Mazur}}^{k, \alpha}(U) = \mu^k(U) - \alpha^{-k} \mu^k(\alpha U)$ (regularized Bernoulli distrib). Note $\mu^{1, \alpha}$ is p-invariant

L $\mu^{1, \alpha}$ is a measure; actually $\mu^{1, \alpha}$ is $\mathbb{Z}_p$ -valued. $B_1(x) = x - \frac{1}{2}$

Pf. $\mu^{1, \alpha}(a + p^n\mathbb{Z}_p) = B_1(\langle \frac{a}{p^n} \rangle) - \alpha^{-1} B_1(\langle \frac{\alpha a}{p^n} \rangle) = \frac{a}{p^n} - [\frac{a}{p^n}] - \frac{1}{2} - \alpha^{-1} (\frac{\alpha a}{p^n} - [\frac{\alpha a}{p^n}] - \frac{1}{2})$ $\square$ (also for $p=2$)

$\star$ p-adic $\mid \star\star$ For $b \in \mathbb{Q}_p$, $b = b_{-N} p^{-N} + \dots + b_0 + b_1 p + \dots$ set $[b] = b_0 + b_1 p + \dots \in \mathbb{Z}_p$

Intermezzo: characterization of $\mu^1_{\text{Bernoulli}}$

(L) Let μ be a measure on $\mathbb{T}_p$. Assume μ is p -invariant.
Then $\exists!$ a function $B = B : \mathbb{Q} \cap [0, 1) \rightarrow \mathbb{Q}_p$ s.t. $\mu(a + p^n \mathbb{T}_p) = B(\langle \frac{a}{p^n} \rangle)$
for all $a \in \mathbb{T}_p$, $n \geq 0$.

Pf Using expansion to base $p \Rightarrow$ any $x \in \mathbb{Q} \cap [0, 1)$ has the form
 $x = \frac{a}{p^n}$, $a \in \mathbb{T}_p$, $0 \leq a < p^n$. Define $B(x) = \mu(a + p^n \mathbb{T}_p)$; well def by
 p -inv of μ . Now if $a \in \mathbb{T}_p^{(\dagger)}$ then $\mu(a + p^n \mathbb{T}_p) = \mu(a_1 + p^n \mathbb{T}_p) = B(\frac{a_1}{p^n}) = B(\langle \frac{a}{p^n} \rangle)$.
Uniqueness is clear

(L) Let μ be a p -invariant measure on $\mathbb{T}_p$ w/ $B(x) = x - c$, $c \in \mathbb{Q}_p$. Then $c = -\frac{1}{2}$.
(Conversely $B(x) = x - \frac{1}{2}$ corr to a measure, of course).

Pf The distribution prop reads $B(\frac{a}{p^n}) = \sum_{b=0}^{p-1} B(\frac{a + p^n b}{p^{n+1}})$ i.e.
 $\frac{a}{p^n} - c = \left(\sum_{b=0}^{p-1} \frac{a + p^n b}{p^{n+1}} \right) - pc = \frac{a}{p^n} + \frac{1}{p} \sum_{b=0}^{p-1} b - pc = \frac{a}{p^n} + \frac{1}{p} \frac{(p-1)p}{2} - pc$

So $-c = \frac{p-1}{2} - pc$. So $c = -\frac{1}{2} \square$

Intermezzo

Rem f polynomial $\Rightarrow f$ int wnt Haar distr μ_{Haar}
& $\int_{\mathbb{T}_p} f(x) d\mu_{\text{Haar}}(x) = \int_{\mathbb{T}_p} f(B) dB = \widetilde{f(B)}$.

8 for $0 \leq a < p^n$

(+) and $a \equiv a_1 (p^n)$, $a_1 \in \mathbb{T}_p$, $0 \leq a_1 < p^n$

(L) Let D_k be the l.c.m of the denominators of $B_k(x)$. Then, for $k \geq 2$,

$$D_k \cdot \mu^{k, \alpha}(a + p^n \mathbb{Z}_p) \equiv D_k \cdot k \cdot a^{k-1} \mu^{1, \alpha}(a + p^n \mathbb{Z}_p) \pmod{p^n}$$

Pf. $B_k(x) = (x+B)^k = x^k + k B_1 x^{k-1} + \dots = x^k - \frac{k}{2} x^{k-1} + \dots$

So $D_k \cdot \mu^{k, \alpha}(a + p^n \mathbb{Z}_p) = D_k \left\{ p^{n(k-1)} B_k \left(\left\langle \frac{a}{p^n} \right\rangle \right) - \alpha^{-k} p^{n(k-1)} B_k \left(\left\langle \frac{\alpha a}{p^n} \right\rangle \right) \right\}$

$= D_k \cdot p^{n(k-1)} \left\{ \left(\frac{a}{p^n} - \left[\frac{a}{p^n} \right] \right)^k - \frac{k}{2} \left(\frac{a}{p^n} - \left[\frac{a}{p^n} \right] \right)^{k-1} + \dots - \alpha^{-k} \left(\frac{\alpha a}{p^n} - \left[\frac{\alpha a}{p^n} \right] \right)^k + \frac{\alpha^{-k}}{2} \left(\frac{\alpha a}{p^n} - \left[\frac{\alpha a}{p^n} \right] \right)^{k-1} + \dots \right\}$

All terms except those involving x^k, x^{k-1} are div by p^n

$\equiv D_k \cdot p^{n(k-1)} \left\{ \left(\frac{a}{p^n} \right)^k - k \left(\frac{a}{p^n} \right)^{k-1} \left[\frac{a}{p^n} \right] - \frac{k}{2} \left(\frac{a}{p^n} \right)^{k-1} - \alpha^{-k} \left(\frac{\alpha a}{p^n} \right)^k + \alpha^{-k} \left(\frac{\alpha a}{p^n} \right)^{k-1} \left[\frac{\alpha a}{p^n} \right] + \frac{\alpha^{-k}}{2} \left(\frac{\alpha a}{p^n} \right)^{k-1} \right\}$

(can assume $0 \leq a < p^n$ so $\left[\frac{a}{p^n} \right] = 0$)
 $= D_k \left\{ -\frac{k}{2} a^{k-1} + \alpha^{-1} k a^{k-1} \left[\frac{\alpha a}{p^n} \right] + \alpha^{-1} \frac{k}{2} a^{k-1} \right\}$

$= D_k \cdot k \cdot a^{k-1} \mu^{1, \alpha}(a + p^n \mathbb{Z}_p).$

(Cor) $\mu^{k, \alpha}$ are measures

(Cor) $\int_X d\mu^{k, \alpha}(x) = k \int_X x^{k-1} d\mu^{1, \alpha}(x)$ for any X

i.e. $(1-p^{-(k-1)}) \zeta(1-s) = \frac{1}{\alpha^{-s}-1} \int_{\mathbb{Z}_p^\times} x^{s-1} d\mu$
 for $s \in \mathbb{Z}$, even ≥ 2
 (RHS DOESN'T MK SENSE FOR $s \in \mathbb{Z}_p$!
 SEE NEXT! FOR THE w -CORRECTING

(2) (Th) $-(1-p^{k-1}) B_k / k = \frac{1}{\alpha^{-k}-1} \int_{\mathbb{Z}_p^\times} x^{k-1} d\mu^{1, \alpha}(x)$

Pf. $k \int_{\mathbb{Z}_p^\times} x^{k-1} d\mu^{1, \alpha} = \int_{\mathbb{Z}_p^\times} d\mu^{k, \alpha} = \int_{\mathbb{Z}_p^\times} d\mu^{k, \alpha} - \int_{p\mathbb{Z}_p^\times} d\mu^{k, \alpha} = \mu^{k, \alpha}(\mathbb{Z}_p^\times) - \mu^{k, \alpha}(p\mathbb{Z}_p^\times)$
 $= \mu^k(\mathbb{Z}_p) - \alpha^{-k} \mu^k(\alpha \cdot \mathbb{Z}_p) - \mu^k(p\mathbb{Z}_p) - \alpha^{-k} \mu(p\alpha \mathbb{Z}_p)$
 $= B_k - \alpha^{-k} B_k - p^{k-1} B_k + \alpha^{-k} p^{k-1} B_k = (1 - \alpha^{-k})(1 - p^{k-1}) B_k.$

(Cor) (Kummer - Serre) If $i, j \not\equiv 0 \pmod{p-1}$ & $i \equiv j \pmod{\phi(p^n)}$ then $(1-p^{i-1}) \frac{B_i}{i} \equiv (1-p^{j-1}) \frac{B_j}{j} \pmod{p^{n+1}}$
 Pf. Choose α prim root mod p so $\alpha^i \not\equiv 1, \alpha^j \not\equiv 1 \pmod{p}$ so $\alpha^{-i-1} \in \mathbb{Z}_p^\times$.
 Also $x^{i-1} \equiv x^{j-1} \pmod{p^n}$ if $i \equiv j \pmod{\phi(p^n)}$ by Euler $\square$.
 so done b/c $\mu^{1, \alpha}$ is $\mathbb{Z}_p$ -valued.

(Variant) (of th above) (same pf)

$B_k / k = \frac{1}{1 - \alpha^{-k}} \int_{\mathbb{Z}_p^\times} x^{k-1} d\mu^{1, \alpha}$

i.e. difference is in $\mathbb{Z}_p$

(14) (Van Staudt) If $k \equiv 0 \pmod{p-1}$, k even, then

$$B_k \equiv -\frac{1}{p} \pmod{\mathbb{Z}_p} \quad (\text{i.e. difference in } \mathbb{Z}_p)$$

Pf. Set $\alpha = (1+p)^{-1}$. So $\frac{1}{1-\alpha^{-k}} = \frac{1}{1-(1+p)^k} = -\frac{1}{kp+p^2(\dots)} \equiv -\frac{1}{kp} \pmod{\mathbb{Z}_p}$

by variant above

$$\text{So } B_k = \frac{k}{1-\alpha^{-k}} \int_{\mathbb{Z}_p^\times} x^{k-1} d\mu^{1,\alpha} \equiv -\frac{1}{p} \int_{\mathbb{Z}_p^\times} x^{k-1} d\mu^{1,\alpha} \pmod{\mathbb{Z}_p}$$

$$\equiv -\frac{1}{p} \sum_{x=1}^{p-1} x^{k-1} \left(\left\langle \frac{x}{p} \right\rangle - \alpha^{-1} \left\langle \frac{\alpha x}{p} \right\rangle + \frac{\alpha^{-1}-1}{2} \right) \pmod{\mathbb{Z}_p}$$

(b/c $\int_{\mathbb{Z}_p^\times} x^{k-1} d\mu^{1,\alpha} \equiv \sum_{x=1}^{p-1} x^{k-1} \pmod{p\mathbb{Z}_p}$)

$$\equiv \frac{\alpha^{-1}-1}{p^2} \sum_{x=1}^{p-1} x^k - \frac{1}{p} \frac{\alpha^{-1}-1}{2} \sum_{x=1}^{p-1} x^{k-1} \pmod{\mathbb{Z}_p}$$

(b/c $\sum_{x=1}^{p-1} x^k \equiv -1/p \pmod{\mathbb{Z}_p}$)

b/c $x^k \equiv -1 \pmod{p\mathbb{Z}_p}$
b/c $k \equiv 0 \pmod{p-1}$

(47) p -adic ζ & L -funs and Mellin transforms of measures

Let $\omega: \mathbb{F}_p^\times \xrightarrow{\sim} \mu_{p-1} \subset \mathbb{Z}_p^\times$ be the Teichmüller char (by def $\omega(x \bmod p) \equiv x \pmod{p}$), $\exists$ by Hensel

For $\chi: \mathbb{F}_p^\times \rightarrow \mathbb{Z}_p^\times$ character, identify χ w/ $\mathbb{Z}_p^\times \xrightarrow{\text{can}} \mathbb{F}_p^\times \xrightarrow{\chi} \mathbb{Z}_p^\times$.

(Def) For set $L_p(1-s, \chi) := \left(\int_{\mathbb{Z}_p^\times} \left(\frac{x}{\omega(x)} \right)^s \chi(x) x^{-1} d\mu^{1,\alpha}(x) \right) \cdot \frac{1}{\chi(\alpha) \left(\frac{\alpha}{\omega(\alpha)} \right)^{-s-1}}$

any $s \in \mathbb{Z}_p$, $\alpha \in \mathbb{Z}_p^\times$ s.t. $\chi(\alpha) \left(\frac{\alpha}{\omega(\alpha)} \right)^s \neq 1$

(mks sense b/c $\frac{x}{\omega(x)} \in 1+p\mathbb{Z}_p$ can be raised to $s \in \mathbb{Z}_p$)

(a priori depends on α ; a posteriori doesn't!)

$$\zeta_p(1-s) := L_p(1-s, 1) = \frac{1}{\left(\frac{\alpha}{\omega(\alpha)} \right)^{-s-1}} \int_{\mathbb{Z}_p^\times} \left(\frac{x}{\omega(x)} \right)^s x^{-1} d\mu^{1,\alpha}(x)$$

(*) For case $k \not\equiv 0 \pmod{p}$

Let $\zeta^{(p)}(z) = (1-p^{-s})\zeta(s) = \prod_{\ell \neq p} (1-\ell^{-s})^{-1}$ (mero on $\mathbb{C}$)

(Prop) If $k \equiv 0 \pmod{p-1}$, $\zeta_p(1-k) = \zeta^{(p)}(1-k)$ in $\mathbb{Q}$ (LHS $\in \mathbb{Q} \subset \mathbb{Q}_p$, RHS $\in \mathbb{Q} \subset \mathbb{R}$)
In particular ζ_p does not depend on α (B) (C)

Pf. $\zeta_p(1-k) = \frac{1}{\alpha^{-k-1}} \int_{\mathbb{Z}_p^\times} x^{k-1} d\mu^{(1)}(x) = (1-p^{k-1})\zeta(1-k) = \zeta^{(p)}(1-k)$
 $\omega^{p-1}=1$ (3), Th (2), last cor

Rem: ~~not~~ Above not true for $k \not\equiv 0 \pmod{p-1}$.

(Def) A function $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is called rigid analytic (*) if $\exists F \in \mathbb{Z}_p[[x]]$, $F = \sum b_n x^n$, $b_n \rightarrow 0$ s.t. $f(a) = F(a)$, $a \in \mathbb{Z}_p$.
Set $\text{Rig}(\mathbb{Z}_p, \mathbb{Z}_p)$ set of rig. an. fns

(Def) If μ is a $\mathbb{Z}_p$ -valued measure on $\mathbb{Z}_p^\times$ define $M_\mu: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$

by $(M_\mu)(s) = \int_{\mathbb{Z}_p^\times} \left(\frac{x}{\omega(x)}\right)^s x^{-1} d\mu(x)$ [call it $\overset{(p\text{-adic})}{\text{Mellin trans. of } \mu}$] $\nearrow \text{Rig}(\mathbb{Z}_p, \mathbb{Z}_p)$

(a) (Prop) If $\mu \in \text{Meas}(\mathbb{Z}_p, \mathbb{Z}_p)$ then M_μ is rigid analytic (B) So $M: \text{Meas}(\mathbb{Z}_p, \mathbb{Z}_p) \rightarrow \text{Rig}(\mathbb{Z}_p, \mathbb{Z}_p)$

Pf. $(M_\mu)(s) = \sum_{i=1}^{p-1} \int_{i+p\mathbb{Z}_p} \left(\frac{x}{\omega(x)}\right)^s x^{-1} d\mu(x) = \sum_{i=1}^{p-1} \int_{i+p\mathbb{Z}_p} \left(1 + p \frac{z+c}{\omega(c)}\right)^s \frac{1}{x} d\mu(x)$
 $x = i + pz$, $i = \omega(c) + pc$
 $= \sum_{n=0}^{\infty} \frac{p^n}{n!} s(s-1)\dots(s-n+1) \int_{i+p\mathbb{Z}_p} \left(\frac{\frac{x-i}{p} + c}{\omega(c)}\right)^n \frac{1}{x} d\mu(x)$
 $\underbrace{\int_{i+p\mathbb{Z}_p} \left(\frac{\frac{x-i}{p} + c}{\omega(c)}\right)^n \frac{1}{x} d\mu(x)}_{\substack{n \\ \mathbb{Z}_p}} \sum_n s(s-1)\dots(s-n+1) \frac{p^n}{n!} \left(\frac{\frac{x-i}{p} + c}{\omega(c)}\right)^n$ $\square$

(Cor) $L_p(1-s, \chi) = \left(\text{quotient of two rigid analytic fns} \right)$ (B)

(Rem) ζ_p & $\zeta^{(p)}$ coincide on $S_p := \{1-m(p-1) \mid m=1,2,3,\dots\}$.

Note: S_p is p -adically dense in $\mathbb{Z}_p$

(*) A similar pf shows $L_p(1-s, \chi)$ doesn't depend on α

(*) b/c the values of ζ_p on a dense set don't depend on α .

(*) More is true if $p \nmid 10^4$ bis.

(*) as opposed to "locally" analytic meaning $\forall s_0 \in \mathbb{Z}_p \exists$ disk centered at s_0 where f given by a conv. series.

④8 Modular parametrizations of ell curves & Manin-Drinfeld revisited

α Def

Let E be an ell curve / $\mathbb{Q}$. By a modular parametrization we mean a morphism $\varphi: X_0(N) \rightarrow E$ over $\mathbb{Q}$ (for some N) s.t. $\oplus$

- 1) $\varphi^* \omega_E = 2\pi i f dz$, $f = \sum_{n \geq 1} c_n q^n$, $c_1 = 1$, $c_n \in \mathbb{Z}$, ω_E 1-form def_ℓ
- 2) $f \in S_2(\Gamma_0(N))$ $\oplus$ is an eigenform for all Hecke op's $T(n)$, $n \geq 1$
- 3) $L(f, s) = L(E, s)$ up to fin many Euler factors (cf ③7) i.e.

$$c_p = a_p := -\#E(\mathbb{F}_p) + 1 + p \text{ for all } p \text{ prime } \gg 0, \quad \text{one can get = for ALL Euler factors if } L \text{ well defined!}$$

By $\oplus \oplus \Rightarrow L(f, 1) = 2\pi \int_0^1 f(ix) dx = -2\pi i \int_0^1 f(z) dz$

Shim-Taniyama-Weil conj: $\forall E/\mathbb{Q}$ has a mod. par. $\Leftarrow$ proved by Wiles Taylor Taylor et al

Recall (p. 82): for $z_1, z_2 \in \mathbb{H}$ define $\{z_1, z_2\}_{\Gamma_0(N)} = \{z_1, z_2\} : H^0(X_0(N), \Omega^1) \rightarrow \mathbb{C}$

$$\omega \mapsto \int_{z_1}^{z_2} g(z) dz, \quad \pi^* \omega = g(z) dz$$

$$\int_{\pi([z_1, z_2])} \omega =: \langle \{z_1, z_2\}, g \rangle$$

By R-iso $H_1(X_0(N), \mathbb{R}) \xrightarrow{\text{int}} H^0(X_0(N), \mathbb{R})^0$ can think $\{z_1, z_2\} \in H_1(X_0(N), \mathbb{R})$

Th (p. 84: Manin-Drinfeld) If $x, y \in \mathcal{C} := \mathbb{Q} \cup \{\infty\}$ then $\{x, y\} \in H_1(X_0(N), \mathbb{Q})$

Rem Method of pf in p. 84 $\Rightarrow$ more namely $\{x, y\} \in \frac{1}{D} H_1(X_0(N), \mathbb{Z})$, $D \in \mathbb{Z}$ indep of x, y . (Indeed can take $D = \det(T(M)_2^t - sI)$ in p. 85).

β Cor With notations as in Def α let $\gamma^+, \gamma^- \in H_1(E, \mathbb{Z})$ be $\mathbb{Z}$ -lin indep. Then for $\forall x, y \in \mathbb{Q} \cup \{\infty\}$ can write

$$\{x, y\}_f := \langle \{x, y\}, 2\pi i f \rangle = \{x, y\}_f^+ \Omega^+ + \{x, y\}_f^- \Omega^- \text{ where}$$

$$\frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty x^{s-1} f(ix) dx$$

|| p. 63

$$\text{Recall: } L(E, s) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1}, \quad L(f, s) = \prod_{p \nmid N} (1 - c_p p^{-s} + p^{1-2s})^{-1} = \sum c_n n^{-s}$$

if $\bar{\pi}$ denote by $\pi: \mathbb{H} = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\} \rightarrow X_0(N) = \mathbb{H}/\Gamma_0(N)$, $\Gamma_0(N) = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in \Gamma(1) \right\}$ (cf ③4 bis) in Mod fms)

where $\Omega^\pm = \int_{\mathbb{R}^\pm} \omega_E$ and $\{x, y\}_f^\pm \in \mathbb{Q}$ have bounded denominators (i.e. denom. dividing a fixed integer) as x, y vary.

pp. Let $\gamma_1, \gamma_2, \dots \in H_1(X_0(N), \mathbb{Z})$ be a $\mathbb{Z}$ -basis. Then $\varphi_* \gamma_i$ are $\mathbb{Q}$ -lin. comb's of γ^+, γ^- w/ denom's dividing some d . Get $\{x, y\} = \sum \frac{m_i}{D} \gamma_i$, $m_i \in \mathbb{Z}$.
 $\langle \{x, y\}, 2\pi i f \rangle = \sum_i \frac{m_i}{D} \int_{\gamma_i} \varphi^* \omega_E = \sum_i \frac{m_i}{D} \int_{\varphi_* \gamma_i} \omega_E = \left(\sum_i \frac{m_i m'_i}{Dd} \right) \Omega^+ + \left(\sum_i \frac{m_i m''_i}{Dd} \right) \Omega^-$
 $\frac{\varphi^* \omega_E}{dz}$ □

⑦ Def w/ notations as in Cor ③ set $P^\pm(x) = \{\infty, x\}_f^\pm$, $P(x) = P^+(x) + P^-(x)$.
 (Also, usually, one takes $\gamma^\pm$ a generator of $\{\gamma \in H_1(E, \mathbb{Z}) \mid \gamma^c = \pm \gamma\}$ where $c: H_1(E, \mathbb{Z}) \rightarrow H_1(E, \mathbb{Z})$ induced by complex conj., since $\omega_E^c = \omega_E$ get $(\Omega^\pm)^c = \int \omega_E^c = \pm \Omega^\pm$)

⑧ Prop 1) $P(x+1) = P(x)$ for $x \in \mathbb{Q}$
 2) $\sum_{i=0}^{p-1} P\left(\frac{x+i}{p}\right) = c_p P(x) - P(px)$

Proof. Enough to show 1') $\{\infty, x\}_f^\pm = \{\infty, x+1\}_f^\pm$, 2') $\sum_{i=0}^{p-1} \{\infty, \frac{x+i}{p}\}_f^\pm = c_p \{\infty, x\}_f^\pm - \{\infty, px\}_f^\pm$.
 (Hc then same true for $\{\infty, -x\}_f^\pm$ by taking $\text{Re} \pm i\text{Im}$, hence for $\{\infty, x\}_f$.
 Now $T\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$ so by p. 82 $\{\infty, x\} = \{\tau\infty, \tau x\} = \{\infty, x+1\}$.
 Also recall that $T(p)$ acts as $\sum_{i=0}^p [\alpha_i]_2$ on $H^0(X_0(N), \Omega^1)$ $\left(\begin{array}{l} \alpha_i = \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} \text{ for } 0 \leq i \leq p-1 \\ \alpha_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \end{array} \right)$

Get $\langle \{\infty, x\}, T(p)(2\pi i f) \rangle = c_p \langle \{\infty, x\}, 2\pi i f \rangle = c_p \{\infty, x\}_f$
 $\langle T(p)^t \{\infty, x\}, 2\pi i f \rangle = \langle \sum_{i=0}^p \{\alpha_i \infty, \alpha_i x\}, 2\pi i f \rangle$
 $= \sum_{i=0}^{p-1} \langle \{\infty, \frac{x+i}{p}\}, 2\pi i f \rangle + \langle \{\infty, px\}, 2\pi i f \rangle$
 $= \sum_{i=0}^{p-1} \{\infty, \frac{x+i}{p}\}_f + \{\infty, px\}_f$ □

(49) p -adic L -functions attached to modular elliptic curves
(cf. Manin, Mazur, SwD)

(Def) Assume notations in (48), (2), (8) and assume $c_p \not\equiv 0 \pmod{p}$; for $p \gg 0$ this condition means $a_p \not\equiv 0 \pmod{p}$ i.e. E has ord. reduction @ p . Then by Hensel the eqn $x^2 - c_p x + p = 0$ has a sol $\alpha_p \in \mathbb{Z}_p^\times$ (& one $\beta_p \in p\mathbb{Z}_p^\times$).
For any $a \in \mathbb{Z}$ define μ , for $n \geq 0$
$$\mu^f(a + p^n \mathbb{Z}_p) = \alpha_p^{-n+1} \left(P\left(\frac{a}{p^n}\right) - \alpha_p^{-n} P\left(\frac{a}{p^{n-1}}\right) \right) \in \mathbb{Q}_p$$

(Prop) μ^f defines a measure on $\mathbb{Z}_p$; also $\mu^f(pU) = \alpha_p^{-1} \mu^f(U)$.
Proof
$$\sum_{b=0}^{p-1} \mu^f(a + bp^n + p^{n+1} \mathbb{Z}_p) = \sum_{b=0}^{p-1} \left(\alpha_p^{-n} \left(P\left(\frac{a+bp^n}{p^{n+1}}\right) - \alpha_p^{-n-1} P\left(\frac{a+bp^n}{p^n}\right) \right) \right)$$

$$= \alpha_p^{-n} \sum_{b=0}^{p-1} P\left(\frac{x+b}{p}\right) - \alpha_p^{-n-1} p P(x), \quad \text{with } x = \frac{a}{p^n}$$

$$\stackrel{(102)}{=} \stackrel{(8)}{=} \alpha_p^{-n} (c_p P(x) - P(px)) - \alpha_p^{-n-1} p P(x)$$

$$= \underbrace{\alpha_p^{-n-1} P(x) (\alpha_p c_p - p)}_{\alpha_p^2} - \alpha_p^{-n} P(px) = \mu^f(a + p^n \mathbb{Z}_p)$$

μ_f is a measure b/c $P(x)$ has bounded denom's by (48), (3) $\square$.
So μ_f is a distrib.

(Def) $L_p(E, s) : \mathbb{Z}_p \rightarrow \mathbb{Q}_p$, $L_p(E, s) = (M(\bar{w}_f^{-1})) (s) = \int_{\mathbb{Z}_p^\times} \left(\frac{x}{w(x)}\right)^{s-1} d\mu^f(x)$.

(2) (Prop) $L_p(E, 1) = -(1 - \alpha_p)(1 - \alpha_p^{-1}) \frac{L(f, 1)}{\Omega^+}$

Pf $L_p(E, 1) = \int_{\mathbb{Z}_p^\times} d\mu^f = \mu^f(\mathbb{Z}_p^\times) = \mu^f(\mathbb{Z}_p) - \mu^f(p\mathbb{Z}_p) = \alpha_p P(0) - P(0) - P(0) + \alpha_p^{-1} P(0)$
$$= -(1 - \alpha_p)(1 - \alpha_p^{-1}) P(0) \quad \%$$

$\uparrow$ well defined b/c $P(x+1) = P(x)$, $x \in \mathbb{Q}$

Now $P(0) = \{ \infty, 0 \}_f^+ + \{ \infty, 0 \}_f^-$; $\{ \infty, 0 \}_f^{\textcircled{B} 0} = 2\pi i \int_0^{\infty} f(z) dz = -2\pi i \int_0^{\infty} f(z) dz = L(f, 1)$
 $\in \mathbb{R}$ (b/c $L(f, 1) = 2\pi \int_0^{\infty} f(ix) dx$ & $f(i\mathbb{R}) \subset \mathbb{R}$ cf its series expression).

So $\{ \infty, 0 \}_f = \{ \infty, 0 \}_f^+ \cdot \Omega^+$ and $\{ \infty, 0 \}_f^- = 0$. So

$$P(0) = \frac{L(f, 1)}{\Omega^+} \quad \square$$

(Cor) (of the proof above) 1) $L(f, 1) \in \mathbb{Q} \cdot \Omega^+$

$$2) L(f, 1) = 0 \Leftrightarrow L_p(E, 1) = 0$$

$$3) L(E, 1) \in \mathbb{Q} \cdot \Omega^+$$

Pf 1, 2 clear. 3 follows from 1 + fact that $\forall$ Euler factor @ 1 is in $\mathbb{Q}$.

Rem 3) above is a weak form of the Birch - SwD conjecture.

Rem Formula in Prop has RHS of form $\alpha_p - 1$ times what I found in Darmon & I can't account for this discrepancy.

Rem Prop (2) can be generalized to show that " $L_p(E, \chi) = L(f, \chi)$ " for "finite char's (but NOT for $\chi \in \mathbb{Z}!$)" $\uparrow$

(50) Birch & Swinnerton-Dyer conjecture(s)

(will only state variants that only depend on (E, s) mod finitely many Euler factors)

(Th) (Mordell-Weil) E ell curve / $\#$ field $K \Rightarrow E(K)$ fin. gen. (as ab. group)

(Conj) (Birch-SwD) 1) $\text{ord}_{s=1} L(E, s) = \text{rank } E(\mathbb{Q})$ if E ell curve / $\mathbb{Q}$. $\uparrow$

$$2) L(E, 1) \in \mathbb{Q} \cdot \Omega^+$$

Rem 2) above follows from last (Cor) in (49) + Wiles et al saying E is modular

Rem $\exists$ variant of 2) of form $\frac{d^r L}{ds^r} (1) \in \mathbb{Q} \cdot \Omega^+, \text{Reg}(E)$ w/ $r = \text{rank } E(\mathbb{Q})$

$$\text{Reg}(E) = (\det \langle P_i, P_j \rangle) / t^2 \text{ where } P_i \in E(\mathbb{Q}), [E(\mathbb{Q}) : \sum_{i=1}^r \mathbb{Z} P_i] = t, \cdot$$

$\langle, \rangle \in \mathbb{R}$ "Néron-Tate" pairing (will not define here but note analogy w/ Dirichlet class # formula)

(Th) (Gross-Zagier - Kolyvagin - Wiles...) B-SwD true if $\text{ord}_{s=1} L(E, s) \leq 1$.

$\uparrow$ $\text{ord}_{s=1} L(E, s)$ called analytic rank of E | $\textcircled{B}$ A different kind of interp!

(51) p-adic measures, moments, and Iwasawa series and functi.

Let $X = \text{a compact open set in } \mathbb{Q}_p \text{ (usually } \mathbb{Z}_p)$

$R = \text{any } p\text{-adically complete ring}$

$C(X, R) = \{ \text{cont fctns } X \rightarrow R \}$

(L) $C(X, \mathbb{Z}_p) \hat{\otimes} R \rightarrow C(X, R)$ is an iso

(Def) An R -valued measure on X is an R -lin map $\mu: C(X, R) \rightarrow R$

(equiv. by (L) above a $\mathbb{Z}_p$ -lin map $C(X, \mathbb{Z}_p) \rightarrow R$) [$\text{if } R = \mathbb{Z}_p$,

X compact open in $\mathbb{Q}_p$ this def agrees w/ the one in (46) via $\int_X$]

(call $\text{Meas}(X, R)$ space of all such μ 's. $\longleftrightarrow$ If $X = \mathbb{Z}_p$ call $\mu(x^n)$ the moments of μ)

(2) (Prop) Let $\mu \in \text{Meas}(\mathbb{Z}_p, R)$. Then

$$1) \left(\text{if } k \equiv k' \pmod{(p-1)p^n} \Rightarrow \int_{\mathbb{Z}_p} x^k d\mu \equiv \int_{\mathbb{Z}_p} x^{k'} d\mu \pmod{p^{n+1}} \right)$$

2) Pf. $\int_{\mathbb{Z}_p} x^k d\mu \equiv \int_{\mathbb{Z}_p} x^{k'} d\mu \pmod{p^{n+1}}$ for $x \in \mathbb{Z}_p^*$ b/c $\#(\mathbb{Z}_p^*/p^{n+1}\mathbb{Z}_p^*) = (p-1)p^n$. (hence for $x \in \mathbb{Z}_p$)

$$\text{So } x^k - x^{k'} = p^{n+1} f(x), x \in \mathbb{Z}_p^* \Rightarrow f(x) \text{ cont on } \mathbb{Z}_p^* \Rightarrow \int_{\mathbb{Z}_p} x^k d\mu = \int_{\mathbb{Z}_p} x^{k'} d\mu + p^{n+1} \int_{\mathbb{Z}_p} f(x) d\mu$$

(Def) $\binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!} = \sum_{i=0}^n C_{i,n} x^i \in \mathbb{Q}[x]$

Rem $\binom{x}{n}(\mathbb{Z}) \subset \mathbb{Z}$ so by cont $\binom{x}{n}(\mathbb{Z}_p) \subset \mathbb{Z}_p$ so $\binom{x}{n} \in C(\mathbb{Z}_p, \mathbb{Z}_p)$.

(Th) (Mahler) The map $\{ (a_n)_{n=0,1,2,\dots} \mid a_n \in R, a_n \rightarrow 0 \} \rightarrow C(\mathbb{Z}_p, R), (a_n) \mapsto$

$\mapsto \sum a_n \binom{x}{n}$ is a bijection.

Pf. (For $\mathbb{Z}_p = R$) For surj. Enough to show $\forall f \in C(\mathbb{Z}_p, \mathbb{Z}_p), \forall N \geq 1, \exists f_N \in C(\mathbb{Z}_p, \mathbb{Z}_p)$

s.t. $f = \sum a_n \binom{x}{n} + p^N f_N$. Induction on N . So enough to show $f_N \text{ congr mod } p$

✓) If in odd μ is p -invariant then $(k \equiv k' \pmod{(p-1)p^n}) \Rightarrow (1-p^k) \int_{\mathbb{Z}_p} x^k d\mu \equiv (1-p^{k'}) \int_{\mathbb{Z}_p} x^{k'} d\mu \pmod{p^{n+1}}$

✓) Indeed $\int_{\mathbb{Z}_p^*} x^k d\mu = \int_{\mathbb{Z}_p} x^k d\mu - \int_{p\mathbb{Z}_p} x^k d\mu$; $\int_{\mathbb{Z}_p} x^k d\mu = \lim \sum_i x_i^k \mu(U_i) = p^{-k} \lim \sum_i (px_i)^k \mu(pU_i)$

So $\int_{\mathbb{Z}_p^*} x^k d\mu = (1-p^k) \int_{\mathbb{Z}_p} x^k d\mu$ & then do same proof. $= p^{-k} \int_{p\mathbb{Z}_p} x^k d\mu$

(+) Define then $\mu(U) = \int_U d\mu = \int_X (\text{char fctn of } U) d\mu$. Also set $\int_X f d\mu = \int_X f \cdot \text{char}_X d\mu$

to a a lin comb of $\binom{x}{n}$.

Since $f_N: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ unif cont

the map $\mathbb{Z}_p \xrightarrow{f_N} \mathbb{Z}_p \rightarrow \mathbb{F}_p$ factors through $\mathbb{Z}/p^m\mathbb{Z} \rightarrow \mathbb{F}_p$ for some m

Claim $\mathbb{Z}_p \xrightarrow{\binom{x}{k}} \mathbb{Z}_p \rightarrow \mathbb{F}_p$ also factors through $\mathbb{Z}/p^m\mathbb{Z} \rightarrow \mathbb{F}_p$ if $0 \leq k \leq p^m$

So I'm reduced to show bijectivity of

$$\{(\bar{a}_0, \dots, \bar{a}_{p^m-1}) \mid \bar{a}_i \in \mathbb{F}_p\} \rightarrow \text{Maps}(\mathbb{Z}/p^m\mathbb{Z}, \mathbb{F}_p), (\bar{a}_n) \mapsto \sum_{n=0}^{p^m-1} \bar{a}_n \binom{x}{n}$$

Both LHS & RHS have $\mathbb{F}_p$ -dim p^m . So injectivity enough. Injectiv

follows b/c if $\sum_{n=0}^{p^m-1} \bar{a}_n \binom{x}{n} = 0$ for all $x \in \mathbb{F}_p$ then $\underbrace{\varphi(x+1) - \varphi(x)}_{=0} = 0$

Ing of map in the statement follows as ing here.

$$\sum \bar{a}_n \binom{x}{n-1} \text{ \& induct}$$

(Cor1) The map $\{(b_n)_{n=0,1,2,\dots} \mid b_n \in R\} \rightarrow \text{Meas}(\mathbb{Z}_p, R)$,

$\mathbb{B} = (b_n) \mapsto \mu_{\mathbb{B}}, \mu_{\mathbb{B}}(\sum a_n \binom{x}{n}) = \sum a_n b_n$ is a bijection. Identify $\mathbb{B}$ w/ series

$f(x) = \sum b_n x^n \in R[[x]]$. Call it the Iwasawa series (or transform of μ), set $\mu_f = \mu_{\mathbb{B}}$.

(Cor2) A sequence $(m_n)_{n=0,1,2,\dots}, m_n \in R$ is the sequence of moments of some $\mu \in \text{Meas}(\mathbb{Z}_p, R)$ iff $\sum_{i=0}^n C_{i,n} m_i \in R$ for all n .

Pf If $m_n = \int_{\mathbb{Z}_p} x^n d\mu$ then $\sum_{i=0}^n C_{i,n} m_i = \int_{\mathbb{Z}_p} (\sum_{i=0}^n C_{i,n} x^i) d\mu = \int_{\mathbb{Z}_p} \binom{x}{n} d\mu \in R$.

Conversely if $b_n := \sum_{i=0}^n C_{i,n} m_i \in R$ for all n then by prev. coroll can define $\mu_{\mathbb{B}}$ & $\mu_{\mathbb{B}}(\binom{x}{n}) = b_n$ i.e. $\int_{\mathbb{Z}_p} \binom{x}{n} d\mu = b_n$ i.e. $\sum_{i=0}^n C_{i,n} \int_{\mathbb{Z}_p} x^i d\mu = b_n$. Since the system $\{\sum_{i=0}^n C_{i,n} X_i = b_n \mid n=0,1,2,\dots\}$ has a unique sol $\Rightarrow \int_{\mathbb{Z}_p} x^n d\mu = m_n$.

(Cor3) Assume $(m_n)_{n=0,1,2,\dots}, m_n \in R$ is a sequence s.t. $\sum_{i=0}^n C_{i,n} m_i \in R, \text{ all } n$. Then for all $k, k' \geq n+1, k \equiv k' \pmod{(p-1)p^n}$ we have $m_k \equiv m_{k'} \pmod{p^{n+1}}$.

Pf. (Cor2) + (Prop 2). } (Rem: This doesn't seem to imply $\exists f: \mathbb{Z}_p \rightarrow R^{\text{cont}}$ s.t. $f(k) = m_k$ b/c of the cond. $k, k' \geq n+1$)

(+) Need $\binom{x+p^m}{k} \equiv \binom{x}{k} \pmod{p}$ if $k < p^m$. But $(1+T)^{x+p^m} = (1+T)^x (1+T)^{p^m} \equiv (1+T)^x (1+T^{p^m})$ & compare coeff of T^k . Note that for $\forall s \in R$ $(P\mu)(ps) = \int_{\mathbb{Z}_p} (1+ps)^x d\mu(x)$

I want to strengthen prop ② in ④7

Def A fcn $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is called an Iwasawa fcn if $\exists \kappa \in 1+p\mathbb{Z}_p$ a topol. generator $\oplus$ & $\exists F \in \mathbb{Z}_p[[x]]$ s.t. $f(s) = F(\kappa^s - 1)$, $s \in \mathbb{Z}_p$ $\oplus$
(Then $\forall$ other top gen $\kappa' \exists F'$ s.t. $f(s) = F'((\kappa')^s - 1)$, $s \in \mathbb{Z}_p$).

Call $I(\mathbb{Z}_p, \mathbb{Z}_p)$ the ring of Iwasawa fcn's; $I(\mathbb{Z}_p, \mathbb{Z}_p) \subset \text{Rig}(\mathbb{Z}_p, \mathbb{Z}_p)$

Rem $\mathbb{Z}_p$ acts on $I(\mathbb{Z}_p, \mathbb{Z}_p)$ by translation: for $c \in \mathbb{Z}_p$, $f \in I(\mathbb{Z}_p, \mathbb{Z}_p)$, $(T_c f)(s) = f(s+c)$ rig. an. fcn.
is in $I(\mathbb{Z}_p, \mathbb{Z}_p)$. (Pf easy)

Prop Let μ be a $\mathbb{Z}_p$ -valued measure on $\mathbb{Z}_p$. Then, M_μ , its Mellin transform belongs to $I(\mathbb{Z}_p, \mathbb{Z}_p)$, i.e. is an Iwasawa fcn.
So we have $M: \text{Meas}(\mathbb{Z}_p, \mathbb{Z}_p) \rightarrow I(\mathbb{Z}_p, \mathbb{Z}_p)$.

Pf. For $\delta \in \mathbb{F}_p^\times$ define a measure μ_δ on $1+p\mathbb{Z}_p$ by $\mu_\delta(U) = \frac{\mu(w(\delta)U)}{w(\delta)}$. Then (easy) $(M_\mu)(s) = \sum_{\delta \in \mathbb{F}_p^\times} \int_{1+p\mathbb{Z}_p} x^{s-1} d\mu_\delta(x)$.

Now if $\kappa \in 1+p\mathbb{Z}_p$ is a top. gen I have an iso $\mathbb{Z}_p \rightarrow 1+p\mathbb{Z}_p, x \mapsto \kappa^x$

Let ν_δ be the measure on $\mathbb{Z}_p$ corr to $x^{-1} \mu_\delta|_{1+p\mathbb{Z}_p}$. Then

$$\int_{1+p\mathbb{Z}_p} x^{s-1} d\mu_\delta(x) = \int_{1+p\mathbb{Z}_p} x^s (x^{-1} d\mu_\delta(x)) = \int_{\mathbb{Z}_p} \kappa^{xs} d\nu_\delta(x) = \int_{\mathbb{Z}_p} (1+(\kappa^s-1))^x d\nu_\delta(x) = P_{\nu_\delta}(\kappa^s-1)$$

$$\text{So } (M_\mu)(s) = \left(\sum_{\delta \in \mathbb{F}_p^\times} P_{\nu_\delta} \right) (\kappa^s - 1) \quad \square.$$

$\leftarrow$ Rem: P_{ν_δ} & P_μ are NOT easily related!

(Cor) $L_p(1-s, \chi)$ is an Iwasawa fcn of s for $\chi \neq 1$. $L_p(1-s, 1) = \zeta_p(s)$

Pf. By ③ & by the fact that, if $\chi \neq 1$, one can choose $\alpha \in \mathbb{Z}_p^\times$, $\chi(\alpha) \neq 1$, $\alpha \neq w(\alpha)$ & let $\kappa \in 1+p\mathbb{Z}_p$ be a top gens. t $\oplus$
is defined for all $s \neq 0$ and is a quot of 2 Iw. fcn's. ~~then~~

$$\frac{1}{\chi(\alpha)^{-1} \left(\frac{\alpha}{w(\alpha)} \right)^{-s} - 1} = \frac{1}{c\kappa^{ms} - 1} = \frac{1}{c(1+(\kappa^s-1))^m - 1} = \frac{1}{(c-1) + \text{pol in } (\kappa^s-1)} = \text{series in } (\kappa^s-1)$$

$\&$ Say F represents f rel to κ . $\square$

$\oplus$ i.e. κ is the image of 1 under an iso $\mathbb{Z}_p \xrightarrow{\sim} 1+p\mathbb{Z}_p$

$\&$ $(\alpha/w(\alpha))^{-1} = \kappa^m$, $m \in \mathbb{Z}_p$. Also let $c = \chi(\alpha)^{-1}$ so $c-1 \in \mathbb{Z}_p^\times$

(γ) Prop The moments of $\mu^{1,\alpha}$ are $\int_{\mathbb{Z}_p} x^k d\mu^{1,\alpha} = (1 - \alpha^{-k-1}) \frac{B_{k+1}}{k+1}$

Pf. $\int_{\mathbb{Z}_p} x^k d\mu^{1,\alpha} \stackrel{\text{BPP 106}}{=} \stackrel{\text{blc } \mu^{1,\alpha} \text{ is } p\text{-inv.}}{(1 - p^k)^{-1}} \int_{\mathbb{Z}_p^x} x^k d\mu^{1,\alpha} \stackrel{\text{Th (2)}}{=} (1 - \alpha^{-k-1}) \frac{B_{k+1}}{k+1}$

(β) Cor $\sum_{i=0}^n C_{i,n} (1 - \alpha^{-i-1}) \frac{B_{i+1}}{i+1} \in \mathbb{Z}_p$ for all n. $(1 - p^k \alpha_p^{-1})$

Prop With notations as in (49) the moments of $\mu^{\frac{1}{p}}$ are $\int_{\mathbb{Z}_p} x^k d\mu^{\frac{1}{p}} = L_p(E, k+1)$ if $k \equiv 0 \pmod{p-1}$ (same pf)

(52) p-adic interpolation of Eisenstein series

Recall: one has the (non-normalized ^{*}) Eisenstein series

$$G_{k+1}(q) = -\frac{B_{k+1}}{k+1} + 2 \sum_{n \geq 1} \left(\sum_{d|n} d^k \right) q^n, \quad G_k = 0 \text{ for } k \geq 1, k \text{ odd.}$$

View $G_k \in \mathbb{Q}[[q]]$. Let $\mathbb{V} \subset \mathbb{Z}_p[[q]]$ be any subring s.t. $\frac{1}{p} G_k \in \mathbb{V} \forall k$.

1) $\mathbb{Z}_p \subset \mathbb{V}$ & $\mathbb{V}$ is p-adically complete,

2) $\mathbb{V}[\frac{1}{p}] \cap \mathbb{Z}_p[[q]] = \mathbb{V}$ (in $\mathbb{Q}_p[[q]]$).

Call such a $\mathbb{V}$ a Katz ring (non-standard!) E.g. $\mathbb{V} = \mathbb{Z}_p[[q]]$

(α) (Th) (Katz, Serre) For any $\alpha \in \mathbb{Z}_p^x$ there $\exists$ a $\mathbb{V}$ -valued measure $\mu^\alpha = \mu_{\text{Eisenstein}}^\alpha$ on $\mathbb{Z}_p$ whose moments are

$$\int_{\mathbb{Z}_p} x^k d\mu^\alpha = (1 - \alpha^{-k-1}) G_{k+1}$$

Note RHS $\in \mathbb{V}$. Indeed enough RHS $\in \mathbb{Z}_p[[q]]$ This foll from (8) in (51)

Pf. Need to show (cf (51) Cor 2) $\tilde{G}_n := \sum_{i=0}^n C_{i,n} (1 - \alpha^{-i-1}) G_{i+1} \in \mathbb{V}$ for all n.

Enough to show $\tilde{G}_n \in \mathbb{Z}_p[[q]]$ (by property 2) above). Now

$$\tilde{G}_n = \underbrace{-\sum_{i=0}^n C_{i,n} (1 - \alpha^{-i-1}) \frac{B_{i+1}}{i+1}}_{\substack{\in \mathbb{Z}_p \\ \text{(51) (β)}}} + 2 \sum_{n \geq 1} \underbrace{\left(\sum_{d|n} \left[\sum_{i=0}^n C_{i,n} (1 - \alpha^{-i-1}) d^i \right] \right) q^n}_{\substack{\in \mathbb{Z}_p \\ \left(\binom{d}{n} - \alpha^{-1} \binom{\alpha d}{n} \right)}} \in \mathbb{Z}_p[[q]]$$

☺ →

☺

□

* The normalized ones, E_k , start w/ 1 + ...

(3) Rem For any $\mathbb{Z}_p$ -lin map $\varphi: \mathbb{V} \rightarrow \hat{\mathbb{Z}}_p^{ur} \ni \hat{\mathbb{Z}}_p^{ur}$ -val meas on $\mathbb{Z}_p$ s.t. $\int_{\mathbb{Z}_p} x^k d\mu^{\varphi, \alpha} = (1 - \alpha^{-k-1}) \varphi(G_{k+1})$

(e.g. if $\varphi(f) = f(0)$ get $\mu^{\varphi, \alpha} = \mu^{\alpha, 1}$ but $\exists$ other interesting examples of φ)

Rem The above pf used the measure $\mu^{\alpha, 1}$ & its moments. Conversely it is possible to deduce (51), (8) using a suitable $\mathbb{V}$ as follows.

(but this is killing a fly w/ a cannon ball). Katz shows $\exists$ Katz ring $\mathbb{V}$ equipped w/ $\mathbb{Z}_p^x$ -action $\mathbb{Z}_p^x \times \mathbb{V} \rightarrow \mathbb{V}$, $(a, v) \mapsto [a]v$ s.t. $[a]G_k = a^k G_k$ (hard: $\mathbb{V}$ represents "trivialized ell curves" of Katz, Proc Symp Pure Math 29(1975)). Then here is a pf of Th(8) not using (51) (8) (& implying (51) (8) via Rem (3)). Need to show $G_k, \tilde{G}_k \in \mathbb{V}$. Write $G_k = \lambda_k + H_k$, $H_k \in \mathbb{Z}_p[[q]]$, $\lambda_k \in \mathbb{Q}$. Then $H_k \in \mathbb{V}[[1/p]]$.

$$(1 - \alpha^{-k}) G_k = G_k - [\alpha^{-1}] G_k = (\lambda_k + H_k) - (\lambda_k - [\alpha^{-1}] H_k) = H_k - [\alpha^{-1}] H_k \in \mathbb{V}$$

So $(1 - \alpha^{-k}) G_k \in \mathbb{V}$.

Similarly, to show $\tilde{G}_k \in \mathbb{V}$ note $\tilde{G}_k = (\sum C_{ik} G_{i+1}) - [\alpha^{-1}] (\sum C_{ik} G_{i+1})$

Write $\sum C_{ik} G_{i+1} = \tilde{\lambda}_k + \tilde{H}_k$, $\tilde{\lambda}_k \in \mathbb{Q}$, $\tilde{H}_k \in \mathbb{Q}[[q]]$. By (3) $\tilde{H}_k \in \mathbb{Z}_p[[q]]$.

$$\text{So } \tilde{G}_k = (\tilde{\lambda}_k + \tilde{H}_k) - (\tilde{\lambda}_k + [\alpha^{-1}] \tilde{H}_k) = \tilde{H}_k - [\alpha^{-1}] \tilde{H}_k \in \mathbb{V}.$$

But $\tilde{H}_k \in \mathbb{V}[[1/p]]$ so $\tilde{H}_k \in \mathbb{V}$.

$\mathbb{V}$ = ring of "trivialized ell curves", φ = "evaluation" @ a "CM curve".

(53) Iwasawa algebra of a profinite group

$R = p\text{-ad compl. ring}$

For Γ a group set $R[\Gamma] = \sum_{g \in \Gamma} Rg$ the group ring on Γ over R

If $\Gamma = \langle \sigma \rangle$ cyclic of ord N , $R[\Gamma] = R[x]$, $x^N = 1$ so $R[\Gamma] \cong \frac{R[T]}{(T^N - 1)}$

If $\Gamma \rightarrow \Gamma'$ fin gr. homo get $R[\Gamma] \rightarrow R[\Gamma']$ ring homo

If $\Gamma = \varprojlim \Gamma_n$, Γ_n finite, setting $R[[\Gamma]] = \varprojlim R[\Gamma_n]$. Note $\Gamma \subset R[[\Gamma]]$

(a) Prop (Serre) Let $\Gamma = \varprojlim \Gamma_n$ where Γ_n is cyclic of ord p^n (+).

Then, for any topological generator γ of Γ (++) $\exists$ an

iso $i_\gamma: R[[\Gamma]] \cong R[[x]]$ s.t. $i_\gamma(\gamma) = x + 1$.

Pf. $\gamma = (\gamma_n)$ defines isomorphisms $\gamma_n \mapsto \frac{\hat{\gamma}}{p^n} \mapsto \frac{\hat{x}+1}{p^n}$

$$R[\Gamma_n] \xrightarrow{\sim} R[T]/(T^{p^n} - 1) \cong R[x]/((x+1)^{p^n} - 1)$$

$$\uparrow \qquad \qquad \uparrow \qquad \qquad \uparrow$$

$$R[\Gamma_{n+1}] \xrightarrow{\sim} R[T]/(T^{p^{n+1}} - 1) \cong R[x]/((x+1)^{p^{n+1}} - 1)$$

Call $h_n = (x+1)^{p^n} - 1 = x^{p^n} + p(\dots)$. Claim: $R[x]/(h_n) \rightarrow R[[x]]/(h_n)$

is an iso (surj $\heartsuit$; inj follows b/c, by $\heartsuit$ again, both $-$ modules have

rank p^n). So get homo $\varepsilon: R[[x]] \rightarrow \varprojlim R[x]/(h_n)$. Claim:

$h_n \in (p, x)^{n+1}$ (trivial by ind on n). So ε clearly surj (use

$R[[x]]$ is complete wrt (p, x)). Also ε inj (b/c $\cap (p, x)^{n+1} = (h_n)$).

Def Let $\Gamma = \varprojlim \Gamma_n$, Γ_n finite $\Rightarrow \Gamma$ is a top space (the open sets are the preim's of sets via $\Gamma \rightarrow \Gamma_n$) so one can define $\longleftrightarrow R$ -valued measures on Γ

(R any p -ad complete ring). Denote their space by $\text{Meas}(\Gamma, R)$.

If $\Gamma \cong \mathbb{Z}_p$ Each choice of γ gives a bij $j: \text{Meas}(\Gamma, R) \xrightarrow{\sim} \text{Meas}(\mathbb{Z}_p, R)$

P1 One has an obvious notion of integration of cont. fcn's on Γ wrt $\mu: \int_{\Gamma} f(x) d\mu(x)$.

($\heartsuit$) L (Eucd. division) If $h \in R[[x]]$ is s.t then $\forall f \in R[[x]] \exists ! g \in R[[x]]$
 $\& r \in R[x]$, $\deg r < d$ s.t. $f = gh + r$.

[Pf: see (54) below]

$$h = \sum_{i=0}^{\infty} a_i x^i, a_0, \dots, a_d \in pR, a_d \in R^\times$$

(++) I.e $\gamma = (\gamma_1, \gamma_2, \dots)$ s.t γ_n gener of Γ_n

$\heartsuit$ as maps $\{op \& b\} \rightarrow R$
w/finite addit. property.

(+) So Γ is abstractly iso to $\mathbb{Z}_p$

$$G_{\mu}^{\Gamma}$$

(Def) Let $\mu \in \text{Meas}(\Gamma, R)$. One defines an elt. $G_{\mu} \in R[[\Gamma]]$ as follows.
Let $\pi_n: \Gamma \rightarrow \Gamma_n$, $\pi_n^{n+1}: \Gamma_{n+1} \rightarrow \Gamma_n$ be the natural maps. Then set

$$G_{\mu} = \left(\sum_{g \in \Gamma_n} \mu(\pi_n^{-1}(g)) g \right); \text{ well defined b/c}$$

$$\begin{aligned} \pi_n^{n+1} \left(\sum_{h \in \Gamma_{n+1}} \mu(\pi_{n+1}^{-1}(h)) h \right) &= \pi_n^{n+1} \left(\sum_{g \in \Gamma_n} \sum_{\substack{h \in \Gamma_{n+1} \\ \pi_n^{n+1}(h)=g}} \mu(\pi_{n+1}^{-1}(h)) h \right) = \\ &= \sum_{g \in \Gamma_n} \left(\sum_{\substack{h \in \Gamma_{n+1} \\ \pi_n^{n+1}(h)=g}} \mu(\pi_{n+1}^{-1}(h)) \right) g = \sum_{g \in \Gamma_n} \mu(\pi_n^{-1}(g)) g. \end{aligned}$$

(Prop) The map $\text{Meas}(\Gamma, R) \xrightarrow{G} R[[\Gamma]]$, $\mu \mapsto G_{\mu}$ is a bijection
Pf. Trivial. (Notation) : We let $\mu_G \leftarrow G$ be the inverse ∇

(Def) The mult on $\text{Meas}(\Gamma, R)$ induced by G above is called convolution $*$
explicitly $(\mu * \nu)(\pi_n^{-1}(g)) = \sum_{\substack{g_1 g_2 = g \\ g_1, g_2 \in \Gamma_n}} \mu(\pi_n^{-1}(g_1)) \nu(\pi_n^{-1}(g_2))$ for $g \in \Gamma_n$.

(Prop) Let $\Gamma \cong \mathbb{Z}_p$ & $\gamma \in \Gamma$ a topol. generator. Then the diag below is commut;
 $\text{Meas}(\Gamma, R) \xrightarrow{G} R[[\Gamma]]$ (G as in the above prop)

$$\begin{array}{ccc} \text{Meas}(\Gamma, R) & \xrightarrow{G} & R[[\Gamma]] \\ \downarrow j_{\gamma} & & \downarrow i_{\gamma} \\ \text{Meas}(\mathbb{Z}_p, R) & \xrightarrow{P} & R[[X]] \end{array} \quad (P \text{ as in } \textcircled{51})$$

Pf We may ass $\Gamma = \mathbb{Z}_p$, $\gamma = 1$, $j_{\gamma} = \text{id}$. So $G_{\mu} = \left(\sum_{a=0}^{p^n-1} \mu(a+p^n \mathbb{Z}_p) \gamma_n^a \right)$ hence
$$i_{\gamma}(G_{\mu}) = \left(\sum_{a=0}^{p^n-1} \mu(a+p^n \mathbb{Z}_p) (X+1)^a \text{ mod } h_n \right) = \left(\sum_{k \geq 0} \left(\sum_{a=0}^{p^n-1} \binom{a}{k} \mu(a+p^n \mathbb{Z}_p) \right) X^k \text{ mod } h_n \right)$$

$$= \sum_{k \geq 0} \left(\int \binom{a}{k} d\mu(a) \right) X^k = P_{\mu}$$

"clearly" $\mathbb{Z}_p$ □

(the notation is unambiguous)

∇ By def, if $g \in \Gamma$ & μ_g is the Dirac meas $\mu_g(U) = \begin{cases} 0, & g \notin U \\ 1, & g \in U \end{cases}$ then $G_{\mu_g} = g$, so
so $G^{-1}: R[[\Gamma]] \cong \{ R\text{-span of Dirac measures } \} \subset \text{Meas}(\Gamma, R)$.

∇ This shows that the theory of $\text{Meas}(\Gamma, R)$ is more general, invariant version of $\text{Meas}(\mathbb{Z}_p, R)$
 ∇ & same notation for maps $R[[\Gamma]] \rightarrow R[[\Gamma_n]]$, $R[[\Gamma_{n+1}]] \rightarrow R[[\Gamma_n]]$

as a map $\Gamma \rightarrow R$

(Def) Let $X(\Gamma, R^x) = \{ \chi: \Gamma \rightarrow R^x \mid \chi \text{ homo, } \chi \text{ continuous} \}$

Any $\chi \in X(\Gamma, R^x)$ is unif cont so comes from a seq. $\chi_n: \Gamma_{N(n)} \rightarrow \frac{R}{p^n R}$
so induces ring homo $R[\Gamma_{N(n)}] \rightarrow R/p^n R$ so a ring homo $\chi: R[\Gamma] \rightarrow R$

If $\mu \in \text{Meas}(\Gamma, R)$ set $(G_\mu)(\chi) := \chi(G_\mu)$. Similarly set $G(\chi) = \chi(G)$ for $G \in R[\Gamma]$

(γ) (Prop) $(G_\mu)(\chi) = \int_\Gamma \chi(x) d\mu(x)$.

$$\text{Pf.}^{\dagger} (G_\mu)(\chi) = \left(\sum_{g \in \Gamma_n} \mu(\pi_n^{-1}(g)) \chi(g) \text{ mod } p^n \right)$$

$$= \lim_{n \rightarrow \infty} \sum_{g \in \Gamma_n} \mu(\pi_n^{-1}(g)) \chi(g_n) \quad \left(\text{where } g_n \in \Gamma, \pi_n(g_n) = g \right)$$

$$= \int_\Gamma \chi d\mu$$

Rem 1) If $\begin{cases} \Gamma = \mathbb{Z}_p, \delta = 1, \\ R = \mathbb{Z}_p \end{cases}$ the above prop ⑧ gives $(i_x G_\mu^{\mathbb{Z}_p})(ps) = \int_{\mathbb{Z}_p^x} (1+ps)^x d\mu(x)$
 $= (P_\mu)(ps)$ (cf bottom p 107)

$$\text{Hence } \boxed{i_x G_\mu^{\mathbb{Z}_p} = P_\mu}$$

This reproves Prop ③

Rem 2) If $\begin{cases} \Gamma = \mathbb{Z}_p^x, \\ R = \mathbb{Z}_p \end{cases}$, $s \in \mathbb{Z}_p$, $\chi_s(x) = \left(\frac{x}{\omega(x)} \right)^s \cdot x^{-1}$, $x \in \mathbb{Z}_p^x$

then Prop ⑧ gives the full expression for the Mellin transform (p. 101)

$$\boxed{(M_\mu)(s) = (G_\mu^{\mathbb{Z}_p^x})(\chi_s)}$$

So Rem 1 shows that $G_\mu^{\mathbb{Z}_p}$ "gives" the Iwasawa series.

—11— 2 ———11—— $G_\mu^{\mathbb{Z}_p^x}$ "gives" Mellin transform M_μ

$\dagger$ relabel Γ_n s.t. $N(n) = n$

called "Iwasawa elt"

(S) Def Let $\psi: \Gamma \rightarrow 1+p\mathbb{Z}_p$ be an iso and $f \in I(\mathbb{Z}_p, \mathbb{Z}_p)$ be an Iwasawa fun. I want to define an elt $G = G_{\psi, f} \in R[[\Gamma]]$ as follows. Pick $\gamma \in \Gamma$ a top. gen so $\kappa = \psi(\gamma)$ is a top gen for $1+p\mathbb{Z}_p$. By def of $I \exists F \in \mathbb{Z}_p[[x]]$ s.t $f(s) = F(\psi(\gamma)^s - 1)$, $s \in \mathbb{Z}_p$. Let $G \in \mathbb{Z}_p[[\Gamma]]$ be def. by $G = F(\gamma - 1) \in R[[\Gamma]]$ (mks sense b/c $R[[\Gamma]]$ is compl in $\gamma - 1$ - top). Note that if $\chi_{\psi, s}: \Gamma \rightarrow \mathbb{Z}_p^\times$, $\chi_{\psi, s}(g) = \psi(g)^s$, for $s \in \mathbb{Z}_p$, then

$$G_{\psi, f}(\chi_{\psi, s}) = f(s)$$

(Since an elt of $R[[\Gamma]]$ is uniquely det by its values on $\chi_{\psi, s}$ (all s) $\Rightarrow G_{\psi, f}$ does not dep on γ)

Say $G_{\psi, f}$ represents f w.r.t ψ .

$$\begin{array}{ccc} \cap & \cap & \cap \\ \mathbb{Z}_p[[\Gamma]] & I(\mathbb{Z}_p, \mathbb{Z}_p) & \text{Hom}(\Gamma, 1+p\mathbb{Z}_p) \end{array}$$

Example let $\Gamma = \text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)) = \varprojlim \text{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}(\zeta_p))$

$$\text{let } \psi: \Gamma \xrightarrow{\sim} 1+p\mathbb{Z}_p, \quad \sigma \zeta_{p^n} = \zeta_{p^n}^{\psi(\sigma)} \quad \Gamma_n$$

$$\text{let } f = f_\chi, \quad f_\chi(s) = L_p(1-s, \chi), \quad 1 \neq \chi \in (\mathbb{Z}/p\mathbb{Z})^\times \hookrightarrow \text{Hom}(\mathbb{Z}_p^\times, \mathbb{Z}_p^\times)$$

Then recall $f_\chi \in I(\mathbb{Z}_p, \mathbb{Z}_p)$ is an Iwasawa fun

so one can consider $G_{\psi, f_\chi} = G_{\chi} = \mu_\chi$, $\mu_\chi \in \text{Meas}(\Gamma, \mathbb{Z}_p)$.

Rem: μ_χ called the χ -Stickelberger measure, G_χ called the χ -Stickelberger elt in $\mathbb{Z}_p[[\Gamma]]$. One can compute it explicitly. Hint: Cor 0 p.113 bis

if $\gamma \in \Gamma$ top gen then
So $G_\chi = F(\gamma - 1) = L_p(1-s, \chi)$
 $\psi(\gamma) = \zeta_p - 1$

(w) (Prop) $G_\psi : I(\mathcal{L}_p, \mathcal{L}_p) \rightarrow \mathcal{L}_p[[\Gamma]]$, $f \mapsto G_{\psi, f}$ is an iso.

The inverse G_ψ^{-1} sends elts $\sum_{i=1}^m \lambda_i g_i$ of $\mathcal{L}_p[[\Gamma]]$ into $(s \mapsto \sum \lambda_i \psi(g_i))$

Pf. clear from def.

(5) Rem The $\mathcal{L}_p$ -action by transl. on $I(\mathcal{L}_p, \mathcal{L}_p)$ corresp to a $\mathcal{L}_p$ -action on $\mathcal{L}_p[[\Gamma]]$ s.t. for $g \in \Gamma$

(8) (Def) Let Γ & ψ be as in (Def) (8). Define a map

$f_\psi : \text{Meas}(\Gamma, \mathcal{L}_p) \rightarrow I(\mathcal{L}_p, \mathcal{L}_p)$ by $\mu \mapsto f_{\psi, \mu} = f_\mu$ where

$$f_\mu(s) = \int_{\Gamma} \psi(x)^s d\mu(x).$$

(7) (Prop) The foll diagr is comm⁺

$$\begin{array}{ccc} \text{Meas}(\Gamma, \mathcal{L}_p) & \xrightarrow{G} & \mathcal{L}_p[[\Gamma]] \\ & \searrow f_\psi & \uparrow G_\psi \\ & & I(\mathcal{L}_p, \mathcal{L}_p) \end{array}$$

Pf Enough to show G & $G_\psi \circ f_\psi$ coincide on Dirac measures $\mu_g, g \in \Gamma$.

Now $G\mu_g = g$ while $f_{\psi, \mu_g}(s) = \int_{\Gamma} \psi(x)^s d\mu_g(x) = \psi(g)^s$

By Prop (w) $G_{\psi, f_{\psi, \mu_g}} = g$.

(9) (Cor) The foll diagram is comm where M is the Mellin transform (p.107 bis) and A is the "average operator"

$$A\mu = A_\psi \mu = \sum_{\delta \in \mathbb{F}_p^\times} \mu_{\delta, \psi}, \quad \mu_{\delta, \psi}(u) = \frac{\mu(\omega(\delta)\psi(u))}{\omega(\delta)}, \quad u \in \Gamma.$$

Pf By (51) (3) p.117 bis $(M\mu)(s) = \sum_{\delta \in \mathbb{F}_p^\times} \int_{\Gamma} \psi(x)^{s-1} d\mu_{\delta, \psi}(x) =$

$= f_{\psi, A\mu}(s-1)$. So $M\mu = T f_{\psi, A\mu}$. So $G_\psi M\mu = T G_{\psi, f_{\psi, A\mu}} = T G_{\psi, A\mu}$

(7) $\square$.

⁺ in partic f_ψ is an iso

54 Modules over the Iwasawa algebra

We look @ $\begin{cases} \Gamma \cong \mathbb{Z}_p \\ R = \mathbb{Z}_p \end{cases}$ so $R[\Gamma] \cong \mathbb{Z}_p[[x]] =: \Lambda$

(Q) (Prop) ("Euclid division") Let $f, g \in \mathbb{Z}_p[[x]]$, $g = \sum_{i=0}^{\infty} a_i x^i$, $a_0, \dots, a_{d-1} \in p\mathbb{Z}_p$, $a_d \in \mathbb{Z}_p^\times$. Then $\exists!$ $q, r \in \mathbb{Z}_p[[x]]$, $f = q \cdot g + r$ s.t. $r \in \mathbb{Z}_p[x]$, $\deg r < d$.
pf. Uniqueness. If $q \cdot g + r = 0 \stackrel{+}{\Rightarrow} \bar{q} \cdot \bar{g} + \bar{r} = 0 \Rightarrow \bar{q} (\sum_{i \geq d} \bar{a}_i x^i) + \bar{r} = 0$
 $\Rightarrow \bar{r} = 0 \Rightarrow \bar{q} = 0 \Rightarrow r = p r_1, q = p q_1 \Rightarrow q_1 g + r_1 = 0 \Rightarrow \dots$ etc $\square$.
Existence. We construct a seq $q_n \in \mathbb{Z}_p[[x]]$, $r_n \in \mathbb{Z}_p[x]$, $\deg r_n < d$,
 $f \equiv q_n \cdot g + r_n \pmod{p^n}$, $q_{n+1} \equiv q_n \pmod{p^n}$, $r_{n+1} \equiv r_n \pmod{p^n}$. Induction.
 For $n=1$ need $\bar{f} = \bar{q}_1 \cdot \bar{g} + \bar{r}_1$ which clearly has a solution b/c
 $\bar{g} = x^d$ (unit in $\mathbb{F}_p[[x]]$). Assume I have q_n, r_n . Seek q_{n+1}, r_{n+1} in
 the form $r_n + p^n R$, $q_n + p^n Q$. Let $f = q_n g + r_n + p^n h$. Want
 $q_n g + r_n + p^n h = q_n g + p^n Q g + r_n + p^n R + p^n h$. Enough to solve
 $\bar{h} = \bar{Q} \bar{g} + \bar{R}$ which again can be done $\square$.

(Def) $P \in \mathbb{Z}_p[x]$ is called distinguished if $P = x^n + a_{n-1} x^{n-1} + \dots + a_0$, $a_i \in p\mathbb{Z}_p$.
 (note almost Eisenstein; I don't ask $p^2 \nmid a_0$)

(B) (Prop) (Weierstrass preparation) Let $g = \sum_{i=0}^{\infty} a_i x^i \in \mathbb{Z}_p[[x]]$, $a_0, \dots, a_{d-1} \in p\mathbb{Z}_p$, $a_d \in \mathbb{Z}_p^\times$. Then one can write uniquely $g = P \cdot U$, $U \in \mathbb{Z}_p[[x]]^\times$, $P \in \mathbb{Z}_p[x]$ distinguished of degree d . (Notation $g = \underline{P}_g \cdot \underline{U}_g$)

pf. By Prop (Q) $x^d = qg + r$, $r \in \mathbb{Z}_p[x]$, $\deg r < d$. Since
 $\bar{r} = x^d - \bar{q} \bar{g} = x^d - \bar{q} (\sum_{i \geq d} \bar{a}_i x^i)$ has order $\geq d$ & $\deg < d \Rightarrow \bar{r} = 0$.
 So $qg = x^d - r = P(x)$ is distinguished. Since $\bar{q} \bar{g} = x^d$ &
 $\bar{g}$ has order $d \Rightarrow \bar{q}$ has order 0 $\Rightarrow q =: U \in \mathbb{Z}_p[[x]]^\times$ $\square$.
 Uniqueness follows from un. in (Q).

$\stackrel{+}{\Rightarrow}$ upper bar means image in $\mathbb{F}_p[[x]]$.

(Cor) Any principal ^(non-zero) ideal in $\mathbb{Z}_p[[x]]$ has the form $(p^v P)$ where $P \in \mathbb{Z}_p[x]$ ^(distinguished) ^{(p^v) or}.

(Cor) Any $g \in \mathbb{Z}_p[[x]]$ has only fin many zeroes in $p\mathbb{Z}_p$.

Pf. Write $g = p^v P \cdot U$, $P \in \mathbb{Z}_p[x]$ distinguished, $U \in \mathbb{Z}_p[[x]]^\times$.
Then $g(pa) = 0 \Leftrightarrow P(pa) = 0$ if $a \in \mathbb{Z}_p$ $\square$.

(Cor) $\mathbb{Z}_p[[x]]$ is factorial.

Pf. It's Noetherian $\checkmark$ so enough to show $\forall$ irr $f \in \mathbb{Z}_p[[x]]$ is prime. Assume $fh = g_1 g_2$ in $\mathbb{Z}_p[[x]]$. Get (by uniqueness in $\mathbb{Z}_p[x]$)
 $P_f \cdot P_h = P_{g_1} \cdot P_{g_2}$. f irr $\Rightarrow P_f$ irr in $\mathbb{Z}_p[x]$ so P_f irr in $\mathbb{Z}_p[x]$
(indeed $P_f = P' \cdot P'' \Rightarrow P', P'' \in \mathbb{Z}_p[x] \Rightarrow P', P''$ distinguished so non-irr in $\mathbb{Z}_p[x]$)
But $\mathbb{Z}_p[x]$ factorial (Gauss) so $P_f \mid P_{g_1}$ or $P_f \mid P_{g_2}$ in $\mathbb{Z}_p[x]$, hence in $\mathbb{Z}_p[[x]]$.

(Th) (Iwasawa, Serre) Let $\Gamma \cong \mathbb{Z}_p$, $\Lambda := \mathbb{Z}_p[[\Gamma]]$, M a torsion, fin gen Λ -module. Then

1) $\exists$ a Λ -mod homo w/ finite ker & coker

$$M \longrightarrow \left(\bigoplus_{i=1}^s \frac{\Lambda}{(p^{n_i})} \right) \oplus \left(\bigoplus_{j=1}^t \frac{\Lambda}{(G_j)} \right)$$

with $G_j \in \Lambda$.

2) If $s=0$ (i.e. no $\frac{\Lambda}{(p^{n_i})}$ factors) then $\text{char}(M) := (\prod G_j)$ depends only on M (called the char ideal of M) $\square$

Pf. (Cohen) use $\Lambda \cong \mathbb{Z}_p[[x]]$ & an adaptation of the row/column ops on matrices (using "Eucl. div" $\otimes$) Tedious. SKIPPED.

$\heartsuit$ If $\gamma \in \Gamma$ is a top gen & I identify Λ w/ $\mathbb{Z}_p[[x]]$ then $\prod G_j$ corr to a series $g \in \mathbb{Z}_p[[x]]$ so $g = P \cdot U$, P dist, U unit; $P =: \text{char}(\gamma^{-1}, M)$ is called the char pol of γ^{-1} on M .
Justification: $P(\gamma^{-1}) \cdot (M \otimes \mathbb{Q}_p) = 0$

$\oplus$ A Noeth $\Rightarrow A[[x]]$ Noeth.

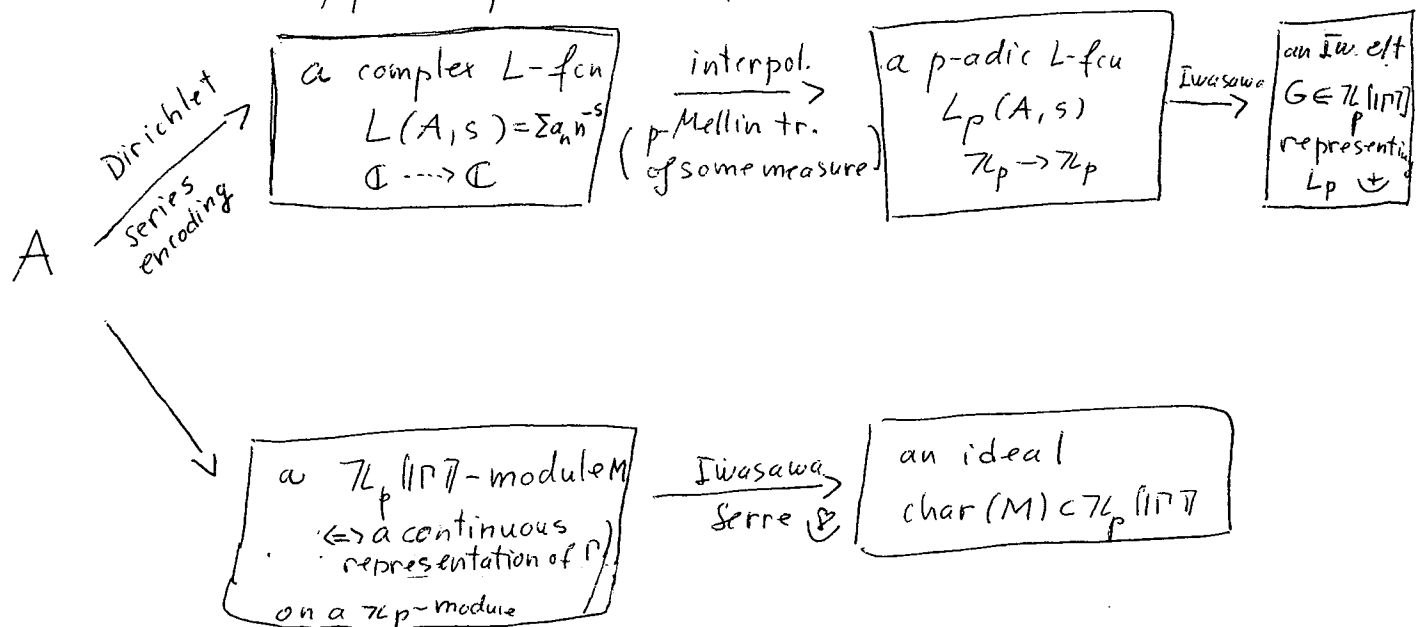
55 "Main conjectures" à la Iwasawa

$$\Gamma := \text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)) (\cong \mathbb{Z}_p)$$

(more generally a Gal group of an ∞ # field ext.)

A = an "arith object"

One attaches, following Iwasawa,



A "main conjecture" states

(Conj) $\text{char}(M) = (G)$.

(Ex1) (for the upper row) p. 113, bottom

(Ex2) (for the bottom row) $M = \varprojlim M_n$ ($\leftarrow$ via norms)

$$M_n = \text{p-primary part of } \text{Cl}(\mathbb{Q}(\zeta_{p^{n+1}}))$$

Rem (Conj) true for appropriate variants of Ex1 & Ex2.

(the Mazur-Wiles Theorem).

Rem $\exists$ elliptic A w/ conj by Mazur.

∇ very technical

∇ the p-primary part of an abgr C is $\{x \in C \mid \exists n, p^n x = 0\}$. Without p-prim parts I have merely

$\&$ one needs M to have no factors $\frac{\Lambda}{p^\nu}$ (Washington-Ferrero) in classical case.

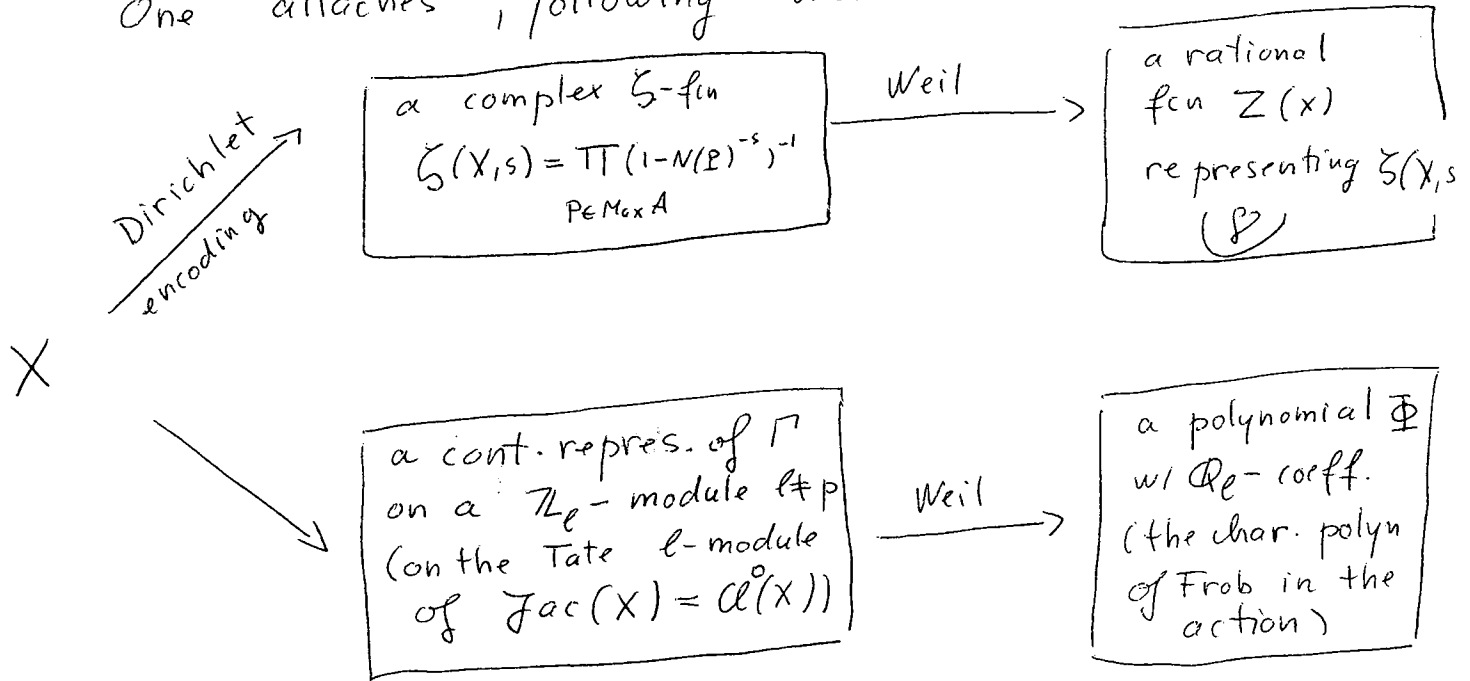
$\oplus$ i.e. $G(\chi_{\gamma,s}) = L_p(A,s)$; if $G = F(\gamma-1)$ this means $L_p(A,s) = F(\gamma(s)-1)$.

56 Analogy with function fields

$$\text{Frob} \in \Gamma = \text{Gal}(\overline{\mathbb{F}_p} / \mathbb{F}_p) (\cong \hat{\mathbb{Z}} = \prod_{\text{all } \ell} \mathbb{Z}_\ell)$$

X = a "curve" over $\mathbb{F}_p$. ($\Leftrightarrow$ ring $A = \mathbb{F}_p[x,y]/(f)$)

One attaches, following Weil



Weil's main thm relates Z & Φ (see my notes on "an intro" to ζ)

He also proves that the zeroes of $\zeta(X,s)$ satisfy $\text{Re } s = \frac{1}{2}$ (as expected for the Riem ζ).

About the structure of these analogies:

(8) i.e. $\zeta(X,s) = Z(p^{-s}) = R(p^{-s}-1)$, $R(x) = Z(x+1)$.

(9) The theory for function fields is due to Weil. This analogy was the main motiv. for Iwasawa.

57 Analogies between analogies

	Weil	Iwasawa	Connes? Denniger?	Dirac et al in Quant.
classical object C	Riemann ζ	Weil $\zeta(X, s)$ Riemann ζ Dirichlet L	$H^1_{\text{et}}(X, \mathbb{Q}_\ell)$ in Weil's th of ζ	Eqn in class phys.
define, by a purely formal analogy a corr non-classical object NC	Weil $\zeta(X, s)$ X a curve/ $\mathbb{F}_p$ (more gen over $\mathbb{F}_q$)	Iwasawa $L_p(s)$ (defined by interpolation which is rather "formal")	Want analogue for Riem ζ (?)	Quantiz of that eqn (b playing a graphical aspect of eq.
conjecture ("predict") that NC behaves in an "expected way"	Weil P conj about the zeroes of his ζ	Iwasawa's Main conj that $L_p(1-s, \chi)$ related to a char pol as in Weil	zeroes of Riem ζ are rel to char (?)	Pred. of new particle
prove conjectures (verify prediction)	Weil Theorem Deligne Theorem	Mazur-Wiles Theorem	(?)	Finding particle experim

Rem

1) Perplexing (vexing!) question

How is it possible that a purely formal analogy (graphical!) leads to correct predictions? Riddle "never to be solved". unless one "believes" in a formal structure of the reality (both mathematical & physical) see more verso (à la Plato)

2) This type of development is a 20-th century business.

Comment on 1): in mathematics this is even more vexing than in physics. Indeed, in physics to verify a theory T by an experiment E one interprets E in the light of T & gets a non-contradiction ($a=a$). So there may be a hidden circularity that "explains" the "miracle". In other words ^(I say) " E validates T ". I mean "adopting D the results of E don't contradict T ". But D is PART of T !
 In math there's no such explanation.

8 i.e. one uses D

9 $T=(D, P)$, D = definitions in $T \in$ physics + math
 P = propositions in $T \in$ math