Formes modulaires et fonctions zeta p-adiques (proof-free)

Marc Masdeu-Sabaté (copying from Serre's paper)

April 28, 2008

Contents

1 p-adic Modular Forms

1.1 Notation

Let p be a prime. Consider the field p-adic numbers $\mathbb{Q}_p$, with its non-archimedean valuation v_p, normalized such that $v_p(p) = 1$. We say $x \in \mathbb{Q}_p$ is **p-integral** if $v_p(x) \geq 0$.

If $f = \sum a_n q^n \in \mathbb{Q}_p[[q]]$ is a formal power series, we define $v_p(f) \stackrel{\text{def}}{=} \inf v_p(a_n)$. If $v_p(f) \geq m$ we write as well $f \equiv 0 \pmod{p^m}$.

Let (f_i) be a sequence of elements in $\mathbb{Q}_p[[q]]$. We say that $f_i \to f$ if the coefficients of f_i tend uniformly to those of f (that is, if $v_p(f - f_i) \to +\infty$.

For $k \geq 2$ an even integer, we set:

$$G_k \stackrel{\text{def}}{=} -\frac{b_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

$$E_k \stackrel{\text{def}}{=} -\frac{2k}{b_k} G_k = 1 - \frac{2k}{b_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where b_k is the k^{th} Bernoulli number, and $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$. Note that, for $k \geq 4$, the series G_k and E_k are modular forms of weight k (and level 1).

Write also:

$$P \stackrel{\text{def}}{=} E_2 = 1 - 24 \sum \sigma_1(n) q^n$$

$$Q \stackrel{\text{def}}{=} E_2 = 1 + 240 \sum \sigma_3(n) q^n$$

$$R \stackrel{\text{def}}{=} E_2 = 1 - 504 \sum \sigma_5(n) q^n$$

The algebra of modular forms on $SL_2(\mathbb{Z})$ is precisely $\mathbb{C}[Q, R]$.

Lemma 1.1.

- *If* $k' \equiv k \not\equiv 0 \pmod{p-1}$, *then* $G_k \equiv G_{k'} \pmod{p}$.
- *If* $p - 1 | k$, *then* $E_k \equiv 1 \pmod{p-1}$. *In fact, we have:*
  - *If* $p \neq 2$: $E_k \equiv 1 \pmod{p^m}$ *if, and only if,* $k \equiv 0 \pmod{(p-1)p^{m-1}}$.
  - *If* $p = 2$: $E_k \equiv 1 \pmod{2^m}$ *if, and only if,* $k \equiv 0 \pmod{2^{m-2}}$.

1.2 The Algebra of mod-p Modular Forms

For $k \in \mathbb{Z}$, write M_k for the seet of modular forms of weight k, with coefficients in $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$. One can reduce these forms modulo p, and we write $\tilde{M}_k \subseteq \mathbb{F}_p[[q]]$ for the reduction of M_k. Write as well $\tilde{M} \stackrel{\text{def}}{=} \sum_{k \in \mathbb{Z}} \tilde{M}_k$.

Theorem 1.2 ($p \geq 5$). *Define, for* $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$*:*

$$\tilde{M}^{\alpha} \stackrel{\textit{def}}{=} \cup_{k \in \alpha} \tilde{M}_k$$

where one sends M_k *to* M_{k+p-1} *by multiplying by* E_{p-1}*. Then:*

$$\tilde{M} = \oplus_{\alpha} \tilde{M}^{\alpha}$$

Theorem 1.3 ($p = 2, 3$)**.** *One then has:*

$$\tilde{M} = \mathbb{F}_p[\tilde{\Delta}]$$

where $\tilde{\Delta}$ is the mod-p reduction of the weight-12 cusp form Δ.

1.3 Congruences mod-p^m between Modular Forms

Theorem 1.4. *Let f and f' be two modular forms with rational coefficients, of respective weights k and k'. Assume also that $f \neq 0$ and that:*

$$v_p(f - f') \geq v_p(f) + m \text{ for some integer } m \geq 0$$

Then:

$$\begin{aligned} k' &\equiv k \pmod{(p-1)p^{m-1}} && \text{if } p \geq 3 \\ k' &\equiv k \pmod{2^{m-2}} && \text{if } p = 2 \end{aligned}$$

1.4 p-adic Modular Forms

Definition 1.5. Let X_m be defined, for $m \geq 1$, as:

$$X_m \stackrel{\text{def}}{=} \begin{cases} \mathbb{Z}/(p-1)p^{m-1}\mathbb{Z} & \text{if } p \neq 2 \\ \mathbb{Z}/2^{m-2}\mathbb{Z} & \text{if } p = 2 \end{cases}$$

The **group of weights** is defined as:

$$X \stackrel{\text{def}}{=} \varprojlim_m X_m = \begin{cases} \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } p \neq 2 \\ \mathbb{Z}_2 & \text{if } p = 2 \end{cases}$$

Note that $\mathbb{Z}$ can be viewed as a dense subgroup of X.

Definition 1.6. A **p-adic modular form** is a formal series with coefficients in $\mathbb{Q}_p$ which is the limit of classical modular forms of weights k_i.

Theorem 1.7. *Let f be a nonzero p-adic modular form. If (f_i) is a sequence of rational modular forms of weight k_i tending to f, then the k_i tend to an element $k \in X$, which is even.*

Example. *If $p = 5$ (or $p = 2, 3$), then $Q \equiv 1 \pmod p$, so that:*

$$\frac{1}{Q} = \lim_{m \to \infty} Q^{p^m - 1}$$

and hence $\frac{1}{Q}$ is p-adic modular, as well as $1/j = \Delta/Q^3$.

1.5 First Properties of the p-adic Modular Forms

Theorem 1.8 (generalizes Theorem 1.4). *Let f and f' be two p-adic modular forms, of respective weights k and k'. Assume also that $f \neq 0$ and that:*

$$v_p(f - f') \geq v_p(f) + m \text{ for some integer } m \geq 0$$

Then k and k' have the same image in X_m.

Corollary 1.9. *Let $f = a_0 + a_1 q + \cdots + a_n q^n + \cdots$ be a p-adic modular form of weight $k \in X$. Let $m \geq 0$ be an integer such that the image of k in X_{m+1} is nonzero. Then:*

$$v_p(a_0) + m \geq \inf_{n \geq 1} v_p(a_n)$$

(in particular, if the a_n are p-integral for all $n \geq 1$, then the same holds for $p^m a_0$ (interesting case: $p - 1 \nmid k$. Then $m = 0$).

Corollary 1.10. *Let $f^{(i)}$ be a sequence of p-adic modular forms, of weights $k^{(i)}$, such that the $a_n^{(i)}$ tend uniformly to $a_n \in \mathbb{Q}_p$ for all $n \geq 1$, and $k^{(i)}$ tends (in X) to a limit $k \neq 0$. Then the coefficients $a_0^{(i)}$ tend to some $a_0 \in \mathbb{Q}_p$, and the limit series is a p-adic modular form of weight k.*

1.6 An Example: p-adic Eisenstein series

Define, for $k \in X$ and $n \geq 1$:

$$\sigma^*_{k-1}(n) \stackrel{\text{def}}{=} \sum d^{k-1} \in \mathbb{Z}_p$$

where the sum is for all $d \geq 1$, $d \mid n$, such that $p \nmid d$. Then the sequence $G_{k_i} \stackrel{\text{def}}{=} -b_{k_i}/2k_i + \sum_{n \geq 1} \sigma_{k_i - 1}(n) q^n$ has a limit:

$$G^*_k = a_0 + \sum_{n \geq 1} \sigma^*_{k-1}(n) q^n$$

with $a_0 = \frac{1}{2} \lim_{i \to \infty} \zeta(1 - k_i) \stackrel{\text{def}}{=} \frac{1}{2} \zeta^*(1 - k)$.

The function ζ^* is thus defined on the odd elements of $X \setminus \{1\}$, and by a Corollary 1.10 it is continuous.

Theorem 1.11.

- *For $p \neq 2$, and if $(s, u) \neq 1$ is an odd element of $X = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$, then:*

  $$\zeta^*(s, u) = L_p(s; \omega^{1-u})$$

  where $L_p(s; \chi)$ is the p-adic L-function of a character χ, and ω is the Teichmuller character.

- *If $p = 2$ and if $s \neq 1$ is an odd element of $X = \mathbb{Z}_2$, then:*

  $$\zeta^*(s, u) = L_2(s; \chi^0)$$

Note also that, if $k \geq 0$ is an even **integer**, then we have:

$$G^*_k = G_k - p^{k-1} G_k | V$$

Lastly, if $k \equiv 0 \pmod{(p-1)p^{m-1}}$, then $E^*_k \equiv 1 \pmod{p^m}$, and so we set $E^*_0 \stackrel{\text{def}}{=} 1$, as this is the limit of the E^*_k when $k \to 0$.

2 Hecke Operators

2.1 Action of T_l, U, V, θ on the p-adic Modular Forms

Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a formal power series with coefficients in $\mathbb{Q}_p$. Define:

$$f|U \stackrel{\text{def}}{=} \sum_{n=0}^{\infty} a_{pn} q^n \qquad \text{and} \qquad f|V \stackrel{\text{def}}{=} \sum_{n=0}^{\infty} a_n q^{pn}$$

Also, if $l \neq p$ is a prime and $k \in X$, define:

$$f|_k T_l \stackrel{\text{def}}{=} \sum_{n=0}^{\infty} a_{ln} q^n + l^{k-1} \sum_{n=0}^{\infty} a_n q^{ln}$$

$$\theta f \stackrel{\text{def}}{=} q \frac{df}{dq} = \sum_{n=0}^{\infty} n a_n q^n$$

For $h \in X$, define:

$$f|R_h \stackrel{\text{def}}{=} \sum_{(n,p)=1} n^h a_n q^n$$

Theorem 2.1. *The operators U, V and T_l preserve the p-adic modular forms of a given weight k. The operator θ increases the weight by 2. The operator R_h increases the weight by $2h$ (for $h \in X$).*

One can define then the Hecke operators for any m coprime to p, through the usual formulae:

$$\begin{aligned} &T_m T_n = T_n T_m = T_{mn} && \text{if } (m,n) = 1 \\ &T_l T_{l^n} = T_{l^{n+1}} + l^{k-1} T_{l^{n-1}} && \text{if } l \text{ is a prime and } n \geq 1. \end{aligned}$$

Proposition 2.2. *Here there are some formulae:*

$$\begin{aligned} &(\theta f)|U = p\theta(f|U) && f|R_h|U = 0 \\ &\theta(f|V) = p(\theta f)|V && (\theta f)|_{k+2} T_l = l\theta(f|_k T_l) \\ &f|V|R_h = 0 && (f|R_h)|_{k+2h} T_l = l^h (f|_k T_l)|R_h \end{aligned}$$

2.2 A Contraction Property

Definition 2.3. Let $p \geq 5$. The **filtration** of $f \in \tilde{M}^\alpha$ is written $w(f)$ and is the least k such that $f \in \tilde{M}_k$.

Lemma 2.4. *Suppose that $p \geq 5$. Then:*

1. *$w(\theta f) \leq w(f) + p + 1$, with equality if, and only if, $p \nmid w(f)$.*
2. *For all $i \geq 1$, one has $w(f^i) = iw(f)$.*
3. *$w(f|U) \leq p + \frac{w(f)-1}{p}$.*
4. *If $w(f) = p - 1$, then $w(f|U) = p - 1$.*

Theorem 2.5.

1. *If $k > p+1$, then $U(\tilde{M}_k) \subseteq \tilde{M}_{k'}$ for some $k' < k$.*

2. *For $k = p-1$, the operator U induces a bijection on $\tilde{M}_{p-1}$.*

Corollary 2.6. *Let $p \geq 5$, and let $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$ be even. Then:*

1. *The space $\tilde{M}^\alpha$ can be uniquely decomposed as $\tilde{M}^\alpha = \tilde{S}^\alpha \oplus \tilde{N}^\alpha$, such that U is bijective on $\tilde{S}^\alpha$, and locally nilpotent on $\tilde{N}^\alpha$. Also, $\tilde{S}^\alpha \subseteq \tilde{M}_j$, where $j \in \alpha$ is such that $4 \leq j \leq p+1$. In particular, $\tilde{S}^\alpha$ is finite-dimensional.*

2. *For $\alpha = 0$, one has $j = p-1$, and $\tilde{S}^0 = \tilde{M}_{p-1}$.*

If $p = 2$ or $p = 3$, then one can also decompose $\tilde{M} = \tilde{S} \oplus \tilde{N}$, with $\tilde{S} = \tilde{M}_0 = \mathbb{F}_p$, and $\tilde{N} = \tilde{\Delta}\tilde{M}$. Then U is the identity on $\tilde{S}$, and it is locally nilpotent on $\tilde{N}$.

2.3 Application: Computing the Constant Term of a p-adic Modular Form

Theorem 2.7. *Let f be a p-adic modular form of weight $k \in X$. Let p be a prime such that $p \leq 7$ or such that $p \geq 11$ and $k \equiv 4, 6, 8, 10, 14 \pmod{p-1}$. Then:*

$$a_0(f) = \frac{1}{2}\zeta^*(1-k) \lim_{n\to\infty} a_{p^n}(f)$$

Theorem 2.8 (case $p-1 \mid k$). *There exists a polynomial $H \in \mathbb{Z}[U, T_l : l \text{ prime}]$ such that, for all $k \in X$ divisible by $p-1$, one has:*

1. *$E_k^*|H = c(k)E_k^*$, wich $c(k) \in \mathbb{Z}_p^\times$.*

2. *$\lim_{n\to\infty} f|H^n = 0$ for any cuspidal p-adic modular form of weight k.*

(note that H doesn't depend on k, but its action on f actually does).

Corollary 2.9. *If f is a p-adic modular form of weight $0 \neq k \equiv 0 \pmod{p-1}$ one has:*

$$a_0(f) = \frac{1}{2}\zeta^*(1-k) \lim_{n\to\infty} c(k)^{-n} a_1\left(f|H^n\right)$$

Note that this allows to compute $a_0(f)$ in terms of the $a_m(f)$'s, as $a_1(f|H^n)$ is a $\mathbb{Z}_p$-linear combination of the $a_m(f)$, for $m \geq 1$.

Examples.

- *For $p \leq 11$, take $H = U$ and $c(k) = 1$.*
- *For $p = 13$, take $H = U(U+5)$ and $c(k) = 6$, or $H = U(T_2 - 2)$ and $c(k) = 2^{k-1} - 1$.*
- *For $p = 17$, take $H = U(T_2 + 5)$ and $c(k) = 2^{k-1} + 6$.*

Theorem 2.10 (case $p-1 \nmid k$). *Let $k \in X$ be such that $p-1 \nmid k$. Then there is a sequence $(\lambda_{m,n})_{m,n\geq 1}$ of elements in $\mathbb{Z}_p$ such that:*

1. *For each n, then $\lambda_{m,n} = 0$ for all m sufficiently large.*

2. *$a_0(f) = \lim_{n\to\infty} u_n(f)$, where $u_n(f) = \sum_{m\geq 1} \lambda_{m,n} a_m(f)$, for each p-adic modular form of weight k.*

(note that the coefficients $\lambda_{m,n}$ DO depend on the weight k.

3 Modular forms on $\Gamma_0(p)$

3.1 Review of Classical Definitions

Given f a holomorphic function on $\mathcal{H}$, and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^+$, one defines $f|_k\gamma$, also holomorphic on $\mathcal{H}$, as:

$$f|_k\gamma(z) \stackrel{\text{def}}{=} \det(\gamma)^{k/2}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

Consider also $\Gamma_0(p)$, a subgroup of index $p+1$ in $SL_2(\mathbb{Z})$. Define also the **Fricke** involution W to be the matrix $W \stackrel{\text{def}}{=} \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$.

Definition 3.1. Given $f \in M_k(\Gamma_0(p))$, the **trace** of f is defined to be:

$$\mathrm{Tr}(f) \stackrel{\text{def}}{=} \sum_{j=1}^{p+1} f|_k\gamma_j$$

where $\{\gamma_j\}_{j=1\ldots p+1}$ is a set of coset reps of $\Gamma_0(p)\backslash SL_2(\mathbb{Z})$.

Lemma 3.2. *If $f = \sum a_n q^n$ and $f|_kW = \sum b_n q^n$, then:*

$$\mathrm{Tr}(f) = \sum a_n q^n + p^{1-k/2}\sum b_{pn}q^n = f + p^{1-k/2}(f|_kW)|U$$

Remark. If f is a modular form on $SL_2(\mathbb{Z})$, then:

$$\mathrm{Tr}(f|_kW) = p^{1-k/2} f|_kT_p$$

and so the trace and the Hecke operator are related.

3.2 Passing from $\Gamma_0(p)$ to $SL_2(\mathbb{Z})$

Theorem 3.3. *Let $f = \sum a_n q^n$ be a modular form of weight k on $\Gamma_0(p)$, with rational coefficients. Then f is a p-adic modular form of weight k. In fact, one needs only to require that f is meromorphic at the cusp 0 to get the same result.*

Proof. Define, for $a \geq 4$ an even integer such that $p-1 \mid a$:

$$g \stackrel{\text{def}}{=} E_a - p^{a/2}E_a|_aW = E_a - p^aE_a|V$$

which is a modular form of weight a on $\Gamma_0(p)$.

Lemma 3.4. *We have $g \equiv 1 \pmod{p}$ and $g|_aW \equiv 0 \pmod{p^{1+a/2}}$.*

We have that both f and $f|_kW$ have rational coefficients. For each $m \geq 0$, we have fg^{p^m} is a modular form on $\Gamma_0(p)$, of weight $k_m = k + ap^m$, with rational coefficients as well. Let $f_m \stackrel{\text{def}}{=} \mathrm{Tr}(fg^{p^m})$. We then note that $k_m \to k$, and that $f_m \to f$ (as $m \to \infty$). □

Remark. Consider the following function:

$$j \stackrel{\text{def}}{=} Q^3/\Delta = q^{-1} + \sum_{n=0}^{\infty} c(n)q^n$$

The previous Theorem can be applied to the function $f \stackrel{\text{def}}{=} j|U = \sum c(pn)q^n$, which has a pole of order p at the cusp 0.

3.3 Reduction (mod-p) of weight-2 forms on $\Gamma_0(p)$

Theorem 3.5. *Let $p \geq 3$. Let f be a modular form of weight 2 on $\Gamma_0(p)$, with p-integral rational coefficients. Then:*

1. *$f|_2 W = -f|U$, which is a modular form with p-integral coefficients as well.*
2. *The reduction $\tilde{f} = f \pmod p$ belongs to $\tilde{M}_{p+1}$.*
3. *Conversely, any element of $\tilde{M}_{p+1}$ is the mod-p reduction of some weight-2 modular form on $\Gamma_0(p)$ with p-integral coefficients.*

In other words:

$$M_2(\Gamma_0(p); \mathbb{Z}_{(p)}) \equiv M_{p+1}(SL_2(\mathbb{Z}); \mathbb{Z}_{(p)}) \pmod p$$

Corollary 3.6. *The eigenvalues of U acting on $\tilde{M}_{p+1}$ are ± 1.*

3.4 Forms on $\Gamma_0(p)$ with Nebentypus

Suppose that $p \geq 3$. Let ε be a character mod p. Let $r = \phi(p-1)$, and write $p = \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_r$ the decomposition of p in $\mathbb{Q}(\mu_{p-1})$. Fix one of these prime ideals, which defines an embedding $\sigma\colon \mathbb{Q}(\mu_{p-1}) \hookrightarrow \mathbb{Q}_p$. This in turn induces an isomorphism $\mu_{p-1} \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ (and all isomorphism are obtained in this way). Then $\sigma \circ \varepsilon$ is of the form $x \mapsto x^\alpha$ with some $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$. Then:

Theorem 3.7. *Let $f = \sum a_n q^n$ be a modular form of type (k, ε) on $\Gamma_0(p)$ such that $a_n \in \mathbb{Q}(\mu_{p-1})$ for all n. Then the resulting series $f^\sigma \overset{def}{=} \sum a_n^\sigma q^n$, with coefficients in $\mathbb{Q}_p$ is a p-adic modular form of weight $k + \alpha$ (where α is identified with $(0, \alpha) \in X = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$, and $k + \alpha = (k, k+\alpha)$.*

Proof. For $\varepsilon = 1$ the result has been proven before. So assume $\varepsilon \neq 1$.

Lemma 3.8. *Let $k \geq 1$, and assume that $\varepsilon(-1) = (-1)^k$. Then the series:*

$$G_k(\varepsilon) \overset{def}{=} \frac{1}{2} L(1-k, \varepsilon) + \sum_{n=1}^\infty \left(\sum_{d|n} \varepsilon(d) d^{k-1} \right) q^n$$

is a modular form of type (k, ε) on $\Gamma_0(p)$, with coefficients on $\mathbb{Q}(\mu_{p-1})$, and one has:

$$G_k(\varepsilon)^\sigma = G_h^*$$

with $h = k + \alpha$.

□

Remark. One can show that, with the hypotheses of the previous Theorem, $f|_k W$ is of type (k, ε^{-1}), and that $f|_k W^2 = \varepsilon(-1) f$.

4 Analytic Families of p-adic Modular Forms

4.1 The Iwasawa Algebra (for $p \neq 2$)

4.1.1 Notation

For $n \geq 1$, define $U_n \stackrel{\text{def}}{=} \{u \in \mathbb{Z}_p^\times \mid u \equiv 1 \pmod{p^n}\}$, as a subgroup of $\mathbb{Z}_p^\times$. Note that:

$$U_1 \simeq \varprojlim (U_1/U_n) \simeq \mathbb{Z}_p$$

For $u = 1 + pt \in U_1$ and $s \in \mathbb{Z}_p$, one can define $u^s \in \mathbb{Z}_p^\times$ as:

$$u^s = (1+pt)^s = \sum_{n \geq 0} \binom{s}{n} t^n p^n$$

Definition 4.1. Let F be the $\mathbb{Z}_p$-algebra of functions $\mathbb{Z}_p \to \mathbb{Z}_p$, and let $L \subseteq F$ be the subalgebra generated by all the $f_u \stackrel{\text{def}}{=} s \mapsto u^s$ ($u \in U_1$). By independence of characters, the f_u form a basis for L.

Lemma 4.2. *The algebra L is isomorphic to $\mathbb{Z}_p[U_1]$. So any $f \in L$ can be uniquely written as $s \mapsto f(s) = \sum_{u \in U_1} \lambda_u u^s$ with $\lambda_u \in \mathbb{Z}_p$, and almost all of them being 0.*

4.1.2 The algebra $\overline{L}$

Definition 4.3. Let $\overline{L}$ be the adherence of L in F, with respect to the topology given by uniform convergence.

Remark. The elements of L are equicontinuous:

$$s \equiv s' \pmod{p^n} \implies f(s) \equiv f(s') \pmod{p^{n+1}}$$

So the same property holds for $\overline{L}$. Note also that $\overline{L}$ is compact.

4.1.3 The algebra Λ

Definition 4.4. The **Iwasawa algebra** is $\Lambda \stackrel{\text{def}}{=} \mathbb{Z}_p[[U_1]] = \varprojlim \mathbb{Z}_p[U_1/U_n]$.

Claim. *The algebra $\Lambda \simeq \mathbb{Z}_p[[T]]$, through sending $f_u \mapsto 1+T$, if $u = 1+\pi$ is a topological generator of U_1 with $v_p(\pi) = 1$.*

4.1.4 $\overline{L} = \Lambda$

Note that $L = \mathbb{Z}_p[U_1]$ is contained in both $\overline{L}$ and Λ.

Lemma 4.5. *There is a unique isomorphism of topological algebras:*

$$\varepsilon \colon \Lambda \to \overline{L}$$

such that it is the identity on $\mathbb{Z}_p[U_1]$. The isomorphism ε maps $f = \sum a_n T^n$ to:

$$\varepsilon(f) : s \mapsto f(u^s - 1) = \sum a_n (u^s - 1)^n$$

(note that $u^s - 1 \equiv 0 \pmod{p}$).

Remark. In this way, we will go from a power series in T to a function of s, using the "change of variables":

$$T = u^s - 1 = vs + \cdots + v^n s^n/n! + \cdots \quad \text{where } v = \log(u)$$

4.1.5 Zeros of an element of Λ

Lemma 4.6. *Let $f \neq 0$ be an element of $\Lambda = \mathbb{Z}_p[[T]]$. Then f can be uniquely written (Weierstrass decomposition) as:*

$$f = p^\mu(T^\lambda + a_1 T^{\lambda-1} + \cdots + a_\lambda)u(T)$$

with $\lambda, \mu \geq 0$, $v_p(a_i) \geq 1$ and $u \in \Lambda^\times$.

In particular, $f(s)$ has a finite number ($\leq \lambda$) of zeros.

Corollary 4.7. *Let $f_1, \ldots, f_n, \ldots$ be a sequence in Λ, converging pointwise for all $s \in S$, where $S \subseteq \mathbb{Z}_p$ is infinite. Then the sequence f_n converges uniformly on $\mathbb{Z}_p$, to a function $f \in \Lambda$.*

4.2 The Iwasawa Algebra (for $p = 2$)

Basically everything extends, with minor changes. Define U_n in the same way as before. Then:

$$\mathbb{Z}_p^\times = U_1 = \{\pm 1\} \times U_2$$

and $U_2 \simeq \mathbb{Z}_2$. For $u \in U_1$, let $\omega(u)$ denote his sign (the component in $\{\pm 1\}$, and let $< u >$ his component in U_2. We will define L and Λ using U_2 instead of U_1.

Let then L the algebra generated by the functions f_u, with $u \in U_2$. Then again:

$$\overline{L} \simeq \Lambda \stackrel{\text{def}}{=} \mathbb{Z}_2[[U_2]] = \varprojlim \mathbb{Z}_2[U_2/U_n] \simeq \mathbb{Z}_2[[T]]$$

The remaining is the same.

4.3 Char'n of elements in Λ by their expansions

Define the integers c_{in}, for $1 \leq i \leq n$, through the identity:

$$\sum_{i=1}^{n} c_{in} Y^i = Y(Y-1)(Y-2)\cdots(Y-n+1) = n!\binom{Y}{n}$$

Theorem 4.8. *A function $f \in F$ belongs to Λ if, and only if, there exists a sequence of p-adic integers $(b_n)_{n\geq 0}$ such that:*

1. *$f(s) = \sum_{n\geq 0} b_n p^n s^n/n!$ for all $s \in \mathbb{Z}_p$.*
2. *$v_p(\sum_{i=1}^n c_{in} b_i) \geq v_p(n!)$ for all $n \geq 1$.*

(if $p = 2$, one has to replace p^n by 4^n).

Corollary 4.9. *Let $f \in \Lambda$, and let b_n the corresponding coefficients. Then, for all $n \geq 1$:*

$$b_n \equiv b_{n+p-1} \pmod{p}$$

4.4 Char'n of elements in Λ by interpolation properties

Let $s_0, s_1 \in \mathbb{Z}_p$, and let $f \in F$ (that is, a function $\mathbb{Z}_p \to \mathbb{Z}_p$). Define the coefficients $a_n = a_n(f) = f(s_0 + ns_1)$, and let $\delta_0, \delta_1, \ldots$ be the successive differences of the sequence (a_n) (starting with $\delta_0 = a_0$). Let also:

$$h \overset{\text{def}}{=} \begin{cases} 1 + v_p(s_1) & p \neq 2 \\ 2 + v_2(s_1) & p = 2 \end{cases}$$

We have:

Theorem 4.10. *If $f \in \Lambda$, then:*

1. $\delta_n \equiv 0 \pmod{p^{nh}}$ *for all* $n \geq 0$.
2. $v_p\left(\sum_{i=1}^{n} c_{in}\delta_i p^{-ih}\right) \geq v_p(n!)$ *for all* $n \geq 1$.

Corollary 4.11. *Let* $e_n \overset{\text{def}}{=} \delta_n p^{-nh}$. *Then* $e_n \equiv e_{n+p-1} \pmod{p}$ *for all* $n \geq 1$.

In fact, there is a converse to the previous theorem. Let $s_0 = 0$ and $s_1 = 1$, so that $a_n = f(n)$. One can then write (Mahler criterion) for all $s \in \mathbb{Z}_p$:

$$f(s) = \sum_{n \geq 0} \delta_n \binom{s}{n}$$

Theorem 4.12. *Let $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ be a continuous function, and let $\delta_n \overset{\text{def}}{=} \sum (-1)^i \binom{n}{i} f(n-i)$ be its interpolation coefficients. Then $f \in \Lambda$ if, and only if:*

1. $\delta_n \equiv 0 \pmod{p^n}$ *for all* $n \geq 0$.
2. $v_p\left(\sum_{i=1}^{n} c_{in}\delta_i p^{-i}\right) \geq v_p(n!)$ *for all* $n \geq 1$.

(if $p = 2$, one needs to replace p^n by 4^n, and p^{-i} by 4^{-i}).

4.5 Example: Coefficients of the p-adic Eisenstein Series

Write $k = (s, u) \in \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} = X$, for k even and nonzero.

Claim. *The form $G_k^* = G_{s,u}^*$ has coefficients:*

$$a_0(G_{s,u}^*) = \frac{1}{2}\zeta^*(1-s, 1-u)$$
$$a_n(G_{s,u}^*) = \sum d^{-1}\omega(d)^u < d >^s$$

Theorem 4.13. *Consider the function $(s, u) \mapsto G_k^*$. Fix u and n, and consider the function $s \mapsto a_n(G_{s,u}^*)$. Then:*

1. *For $n \geq 1$, this belongs to L (and hence to $\Lambda = \overline{L}$).*
2. *For $n = 0$ and $u \neq 0$ even, this function belongs to Λ.*
3. *For $n = 0$ and $u = 0$, this function is of the form $T^{-1}g(T)$, with $g(T)$ invertible in Λ.*

4.6 Families of p-adic Modular Forms (weight not divisible by $p-1$)

Let f_s be a p-adic modular form, depending on a parameter $s \in \mathbb{Z}_p$, of weight $k(s) \in 2X$. Assume that $k(s) = (rs, u)$ with $r \in \mathbb{Z}, u \in \mathbb{Z}/(p-1)\mathbb{Z}$ independents of s. Suppose further that $u \neq 0$.

Theorem 4.14. *Suppose that, for all $n \geq 1$, the function $s \mapsto a_n(f_s)$ belongs to the Iwasawa algebra Λ. Then so does the function $s \mapsto a_0(f_s)$.*

4.7 Families of p-adic Modular Forms (weight divisible by $p-1$)

Let f_s be a p-adic modular form, depending on a parameter $s \in \mathbb{Z}_p$, of weight $k(s) \in 2X$. Assume that $k(s) = (rs, 0)$ with $r \in \mathbb{Z} \setminus \{0\}$. Say that a function on $\mathbb{Z}_p \setminus \{0\}$ (resp. on $2\mathbb{Z}_2 \setminus \{0\}$) belongs to Λ if it the restriction of a function of Λ.

Theorem 4.15. *Suppose that, for all $n \geq 1$, the function $s \mapsto a_n(f_s)$ belongs to the Iwasawa algebra Λ. Then so does the function*

$$s \mapsto 2\zeta^*(1-rs, 1)^{-1} a_0(f_s)$$

Corollary 4.16. *The function $s \mapsto a_0(f_s)$ belongs to the fraction field of Λ. Moreover, it can be written as $c(T)/((1+T)^r - 1)$, with $c \in \Lambda$.*

5 p-adic zeta-functions

5.1 Notation

Write K for a totally real number field of degree r. Its ring of integers is written $\mathcal{O}_K$, and its different ideal by $\mathfrak{d}$. We will write $d = \operatorname{disc}(K)$ for its discriminant (so that $d = N\mathfrak{d}$) (we write N for both the absolute norm on ideals and on elements). The trace of an element x is written $\operatorname{Tr}(x) \in \mathbb{Q}$. We say that an element $x \in K$ is **totally positive** if $\sigma(x) > 0$ for each embedding $\sigma \colon K \hookrightarrow \mathbb{R}$. We write then $x \gg 0$. Note that in this case, $\operatorname{Tr}(x) > 0$.

Definition 5.1. The zeta function associtated to K is:

$$\zeta_K(s) \stackrel{\text{def}}{=} \sum N\mathfrak{a}^{-s} = \prod (1 - N\mathfrak{p}^{-s})^{-1}, \quad \Re(s) > 1$$

where $\mathfrak{a}$ runs on the set of nonzero ideals of $\mathcal{O}_K$, and $\mathfrak{p}$ runs on the set of nonzero prime ideals of $\mathcal{O}_K$.

This can be meromorphically extended to all $\mathbb{C}$, with a single simple pole at $s = 1$.

Claim. *The function*

$$d^{s/2} \pi^{-rs/2} \Gamma(\frac{s}{2})^r \zeta_K(s)$$

is invariant under $s \mapsto 1-s$ (functional equation). This implies some vanishing (or non-vanishing) at points of the form $1-n$, for $n \geq 1$, which in any case are rational nombers (Hecke-Siegel's theorem).

5.2 Modular Forms attached to K

Define, for $k \geq 2$ an even integer,

$$g_k \stackrel{\text{def}}{=} \sum_{n \geq 0} a_n(g_k) q^n$$

where:

$$\begin{aligned} a_0(g_k) &\stackrel{\text{def}}{=} 2^{-r}\zeta_K(1-k) \\ a_n(g_k) &\stackrel{\text{def}}{=} \sum_{\substack{x \in \mathfrak{d}^{-1} \\ \mathrm{Tr}(x) = n \\ x \gg 0}} \sum_{\mathfrak{a} | x\mathfrak{d}} (N\mathfrak{a})^{k-1} \end{aligned}$$

Theorem 5.2 (Hecke-Siegel). *Except for* $(r = 1, k = 2)$*, the series* g_k *is a modular form on* $SL_2(\mathbb{Z})$ *of weight* rk*.*

Corollary 5.3.

1. *If* $rk \not\equiv 0 \pmod{p-1}$*, then* $\zeta_K(1-k)$ *is* p*-integral.*
2. *If* $rk \equiv 0 \pmod{p-1}$*, then:*

$$\begin{aligned} v_p(\zeta_K(1-k)) &\geq -1 - v_p(rk) && (p \neq 2) \\ v_p(\zeta_K(1-k)) &\geq r - 2 - v_p(rk) && (p = 2) \end{aligned}$$

Define, for $k \geq 2$ an even integer,

$$g'_k \stackrel{\text{def}}{=} \sum_{n \geq 0} a_n(g'_k) q^n$$

where:

$$\begin{aligned} a_0(g'_k) &\stackrel{\text{def}}{=} 2^{-r}\zeta_{K,S}(1-k) = 2^{-r}\zeta_K(1-k) \prod_{\mathfrak{p} \in S} (1 - N\mathfrak{p}^{k-1}) \\ a_n(g'_k) &\stackrel{\text{def}}{=} \sum_{x, \mathfrak{a}} (N\mathfrak{a})^{k-1} && \text{for } n \geq 1 \end{aligned}$$

Theorem 5.4. *The series* g'_k *is a modular form on* $\Gamma_0(p)$ *of weight* rk*.*

5.3 The p-adic Zeta Function of the Field K

One defines the p-adic series g^*_k, of weight $rk \neq 0$ (for k and element of X):

$$\begin{aligned} a_0(g^*_k) &= 2^{-r}\zeta^*_K(1-k) = 2^{-r} \lim_{i \to \infty} \zeta_K(1-k_i) \\ a_n(g^*_k) &= \sum_{\substack{\mathrm{Tr}(x) = n \\ x \in \mathfrak{d}^{-1} \\ x \gg 0}} \sum_{\substack{\mathfrak{a} | x\mathfrak{d} \\ (\mathfrak{a}, p) = 1}} (N\mathfrak{a})^{k-1} \end{aligned}$$

The function ζ^*_K is called the **p-adic zeta function of** K, and takes values on $\mathbb{Q}_p$.

Theorem 5.5. *Let $k \geq 2$ be an even integer. Then:*

$$\zeta_K^*(1-k) = \zeta_{K,S}(1-k) = \zeta_K(1-k)\prod_{\mathfrak{p}\in S}(1 - N\mathfrak{p}^{k-1})$$

where S is the set of primes $\mathfrak{p}$ lying over p.

Note that the theorem implies (because ζ_K^* is continuous) the uniqueness of ζ_K^*, and characterizes it. In fact, ζ_K^* is actually analytic: write $k = (s, u) \in X$, so that the condition $rk \neq 0$ means $s \neq 0$ or $ru \neq 0$. Write $\zeta_K^*(1-k) = \zeta_K^*(1-s, 1-u)$.

Theorem 5.6. *Let $u \in \mathbb{Z}/(p-1)\mathbb{Z}$ be even. Then:*

- *If $p \neq 2$:*
  1. *If $ru \neq 0$, then the function $s \mapsto \zeta_K^*(1-s, 1-u)$ belongs to the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[T]]$.*
  2. *If $ru = 0$, then the function $s \mapsto \zeta_K^*(1-s, 1-u)$ is of the form $h(T)/((1+T)^r - 1)$ with $h \in \Lambda$.*
- *If $p = 2$:*
  The function $s \mapsto \zeta_K^*(1-s)$ is of the form $2^r h(T)/((1+T)^r - 1)$, with $h \in \Lambda$.

Corollary 5.7. *If $ru \neq 0$ and $p \neq 2$, the function $s \mapsto \zeta_K^*(1-s, 1-u)$ is holomorphic in a disk strictly larger than the unit disk.*

Corollary 5.8. *If $ru = 0$, the function $s \mapsto \zeta_K^*(1-s, 1-u)$ is meromorphic in a disk strictly containing the unit disk, and it's holomorphic except for possibly a simple pole at $s = 0$.*

Corollary 5.9. *Let $a, b > 0$ be positive integers. Suppose that $a \geq 2$ is even, $ra \not\equiv 0 \pmod{p-1}$ and $b \equiv 0 \pmod{p-1}$. Then the successive differences δ_n of the sequence $a_n \overset{def}{=} \zeta_{K,S}(1-a-nb)$ satisfy the congruences:*

$$\delta_n \equiv 0 \pmod{p^n} \quad \text{and} \quad \sum_{i=1}^{n} c_{in}\delta_i p^{-i} \equiv 0 \pmod{n!\mathbb{Z}_p}$$

5.4 Computing $\zeta_K^*(1-k, 1-u)$ for $k \geq 1$ integer

Assume here that u is even and that $p \neq 2$. Note that, if $k \equiv u \pmod{p-1}$, then Theorem 5.5 gives us $\zeta_K^*(1-k, 1-u) = \zeta_{K,S}(1-k)$. We want an analogous result for the general case.

Let $\varepsilon\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ be a character such that $\varepsilon(-1) = (-1)^k$. For $\mathfrak{a}$ any ideal coprime to p, let $\varepsilon_K(\mathfrak{a}) \overset{\text{def}}{=} \varepsilon(N\mathfrak{a})$, which gives a character on K, which ramifies on a set $S_\varepsilon \subseteq S$.

Definition 5.10. Define the twisted L-function supported outside S as:

$$L_S(s, \varepsilon_K) \overset{\text{def}}{=} \prod_{\mathfrak{p}\notin S}(1 - \varepsilon_K(\mathfrak{p})N\mathfrak{p}^{-s})^{-1} = L(s, \varepsilon_K)\prod_{\mathfrak{p}\in S\setminus S_\varepsilon}(1 - \varepsilon_K(\mathfrak{p})N\mathfrak{p}^{-s})$$

Fix an embedding $\sigma\colon \mathbb{Q}(\mu_{p-1}) \hookrightarrow \mathbb{Q}_p$, so that ε becomes $x \mapsto x^\alpha$, for some $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$. We have then:

Theorem 5.11.

$$\zeta_K^*(1-k, 1-u) = L_S(1-k, \varepsilon_K)^\sigma$$

5.5 A periodicity property of ζ_K^*

Suppose here that $p \neq 2$. Consider $K(\mu_p)$, the extension of K obtained by adjoining the p^{th} roots of unity, and let $b \stackrel{\text{def}}{=} [K(\mu_p) : K]$. As K is real, we have that b is even and $b \mid p-1$.

Theorem 5.12. *If $u' \equiv u \pmod{b}$, then:*

$$\zeta_K^*(1-s, 1-u) = \zeta_K^*(1-s, 1-u')$$