ANNALES

DE

L'INSTITUT FOURIER

Bruno ANGLÈS & Gabriele RANIERI

On the linear independence of p-adic L-functions modulo p

Tome 60, n° 5 (2010), p. 1831-1855.

<http://aif.cedram.org/item?id=AIF_2010__60_5_1831_0>

Ann. Inst. Fourier, Grenoble
60, 5 (2010) 1831-1855

ON THE LINEAR INDEPENDENCE OF p-ADIC L-FUNCTIONS MODULO p

by Bruno ANGLÈS & Gabriele RANIERI

ABSTRACT. — Let $p \geqslant 3$ be a prime. Let $n \in \mathbb{N}$ such that $n \geqslant 1$, let $\chi_1, \dots, \chi_n$ be characters of conductor d not divided by p and let ω be the Teichmüller character. For all i between 1 and n, for all j between 0 and $(p-3)/2$, set

$$\theta_{i,j} = \begin{cases} \chi_i \omega^{2j+1} & \text{if } \chi_i \text{ is odd;} \\ \chi_i \omega^{2j} & \text{if } \chi_i \text{ is even.} \end{cases}$$

Let $K = \mathbb{Q}_p(\chi_1, \dots, \chi_n)$ and let π be a prime of the valuation ring $\mathcal{O}_K$ of K. For all i, j let $f(T, \theta_{i,j})$ be the Iwasawa series associated to $\theta_{i,j}$ and $\overline{f(T, \theta_{i,j})}$ its reduction modulo (π). Finally let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$. Our main result is that if the characters χ_i are all distinct modulo (π), then 1 and the series $\overline{f(T, \theta_{i,j})}$ are linearly independent over a certain field Ω that contains $\overline{\mathbb{F}_p}(T)$.

RÉSUMÉ. — Soit $p \geqslant 3$ un nombre premier. Soit $n \in \mathbb{N}$ tel que $n \geqslant 1$, soient $\chi_1, \dots, \chi_n$ des caractères de conducteur d premier à p ; notons ω le caractère de Teichmüller. Pour tout i entre 1 et n et pour tout j entre 0 et $(p-3)/2$, on pose

$$\theta_{i,j} = \begin{cases} \chi_i \omega^{2j+1} & \text{si } \chi_i \text{ est impair ;} \\ \chi_i \omega^{2j} & \text{si } \chi_i \text{ est pair.} \end{cases}$$

Soit $K = \mathbb{Q}_p(\chi_1, \dots, \chi_n)$ et soit π un premier de l'anneau de valuation $\mathcal{O}_K$ de K. Pour tout i, j notons $f(T, \theta_{i,j})$ la série d'Iwasawa associée à $\theta_{i,j}$ et $\overline{f(T, \theta_{i,j})}$ sa réduction modulo (π). Finalement soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Nous montrons que si les caractères χ_i sont distincts modulo (π), alors 1 et les séries $\overline{f(T, \theta_{i,j})}$, sont linéairement indépendantes sur un certain corps Ω qui contient $\overline{\mathbb{F}_p}(T)$.

Keywords: p-adic L-functions, p-adic Leopoldt transform, Iwasawa theory, irrationality.
Math. classification: 11R23, 11R18, 11S80, 11J72.

1. Introduction

Let p be an odd prime. Let $n \in \mathbb{N}$ such that $n \geqslant 1$, let $\chi_1, \dots, \chi_n$ be characters of conductor d not divided by p and let ω be the Teichmüller character. For all i between 1 and n and j such that $0 \leqslant j \leqslant (p-3)/2$, set

$$\theta_{i,j} = \begin{cases} \chi_i \omega^{2j+1} & \text{if } \chi_i \text{ is odd;} \\ \chi_i \omega^{2j} & \text{if } \chi_i \text{ is even.} \end{cases}$$

Observe that, by definition, $\theta_{i,j}$ is an even character for all i, j.

Set $\kappa_0 = 1 + dp$ and $K = \mathbb{Q}_p(\chi_1, \dots, \chi_n)$ (i.e. the extension of $\mathbb{Q}_p$ generated by all the images of χ_i for all i). Let π be a prime of the valuation ring $\mathcal{O}_K$ of K and let $\mathbb{F}_q$ be $\mathcal{O}_K/\pi\mathcal{O}_K$. For all i between 1 and n and j between 0 and $(p-3)/2$, set $f(T, \theta_{i,j})$ the Iwasawa power series attached to the p-adic L-function $L_p(s, \theta_{i,j})$ (see [4, Theorem 7.10]) and $\overline{f(T, \theta_{i,j})}$ its reduction modulo (π).

Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$. For $F(T) \in \overline{\mathbb{F}_p}[[T]]$, we say that $F(T)$ is a pseudo-polynomial if and only if there exist $r \in \mathbb{N}$, $a_1, \dots, a_r \in \mathbb{Z}_p$ and $c_1, \dots, c_r \in \overline{\mathbb{F}_p}$ such that

$$F(T) = \sum_{i=1}^{r} c_i (T+1)^{a_i}.$$

Then the set of the pseudo-polynomials is a ring which we denote by A. Moreover we denote by Ω the quotient field of A. The elements of Ω are called pseudo-rational functions. Anglès (see [1, Theorem 4.5]) shows that for all non-trivial even character of the first kind θ, $\overline{f(T, \theta)}$ is not a pseudo-rational function. We shall prove the following generalisation of this result:

THEOREM 1. — *Suppose that the characters χ_i are all distinct modulo (π) (i.e. for all integer $i \neq j$ there exist $a \in (\mathbb{Z}/d\mathbb{Z})^*$ such that $\chi_i(a) \not\equiv \chi_j(a) \mod (\pi)$). Then the elements of the set*

$$\{1,\ \overline{f(T, \theta_{i,j})},\ 1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant (p-3)/2\}$$

are linearly independent over Ω.

Observe that in the statement of Theorem 1 it is necessary to suppose that the characters χ_i are all distinct modulo (π). Indeed suppose that there exist $i \neq k$ between 1 and n such that χ_i and χ_k are congruent modulo (π). Since p is odd this implies that χ_i and χ_k have the same parity. Then for all $0 \leqslant j \leqslant (p-3)/2$ we have that $\theta_{i,j}$ is congruent to $\theta_{k,j}$ modulo (π), which implies $\overline{f(T, \theta_{i,j})} = \overline{f(T, \theta_{k,j})}$. Thus in this case the series $\overline{f(T, \theta_{i,j})}$ are dependent.

Observe also that if the characters χ_i are distinct modulo (π), then for all i, i' between 1 and n, j, j' between 0 and $(p-3)/2$, $\theta_{i,j}$ is congruent to $\theta_{i',j'}$ modulo (π) if and only if $i = i', j = j'$. It is clear that $i = i'$ implies $j = j'$ and $j = j'$ implies $i = i'$. Then suppose that $i \neq i'$, $j \neq j'$ and that $\theta_{i,j}$ is congruent to $\theta_{i',j'}$ modulo (π). Moreover suppose that χ_i and $\chi_{i'}$ are even (the other case is identical). Hence there exists an integer a such that $\omega^{2j}(a) \not\equiv \omega^{2j'}(a) \mod (\pi)$. Since p does not divide d there exists an integer c such that $1 + cd \equiv a \mod (p)$. Then $\theta_{i,j}(1 + cd) \equiv \omega^{2j}(a) \mod (\pi)$ and $\theta_{i',j'}(1+cd) \equiv \omega^{2j'}(a) \mod (\pi)$. Since $\theta_{i,j}$ and $\theta_{i',j'}$ are equivalent modulo (π), we get $\omega^{2j}(a) \equiv \omega^{2j'}(a) \mod (\pi)$, which is a contradiction.

As in the proof of [1, Theorem 4.5], the main ingredient in the proof of Theorem 1 is a remarkable result due to Sinnott. Before the statement of that result we must define the following equivalence relation: let $a, b \in \mathbb{Z}_p - \{0\}$. We say that a is equivalent to $b \mod (\mathbb{Q}^*)$ ($a \equiv b \mod (\mathbb{Q}^*)$) if and only if there exists $c \in \mathbb{Q}^*$ such that $ab^{-1} = c$.

PROPOSITION 1. — ([3, Proposition 1]) *Let F be a finite field of characteristic p and let $r_1(T), \ldots, r_s(T) \in F(T) \cap F[[T]]$. Let $c_1, \ldots, c_s \in \mathbb{Z}_p - \{0\}$ and suppose that*

$$\sum_{i=1}^{s} r_i((T+1)^{c_i} - 1) = 0.$$

Then for all $a \in \mathbb{Z}_p$,

$$\sum_{c_i \equiv a \mod (\mathbb{Q}^*)} r_i((T+1)^{c_i} - 1) \in F.$$

Let's describe briefly the strategy of the proof of Theorem 1. First (section 2) we recall some properties of the p-adic Leopoldt transform (most of them already proved in [1]) which we will often use.

Then (section 3) we consider the case $d \geqslant 2$. Some results about the p-adic Leopoldt transform of [1] and Proposition 1 will allow us to reduce the proof of Theorem 1 to the computation of the rank of a certain matrix whose entries depend on the values of the characters χ_i (Lemma 4). After such computation the proof of this case of the theorem will follow by some simple remarks of linear algebra.

In section 4 we study the case $d = 1$. In that case we have to consider a "perturbation" of the functions $f(T, \theta_{i,j})$ to be able to apply Proposition 1. Then the proof is not very different from the proof of the previous case (actually it is simpler since it does not request a result similar to Lemma 4) and some remarks of linear algebra will imply the assumption.

Finally we give a link between Theorem 1 and Ferrero-Washington's heuristic (see [2]). Let i be an integer between 1 and $(p-3)/2$. Write

$$f(T,\omega^{2i}) = \sum_{k=0}^{+\infty} a_k(\omega^{2i})T^k.$$

The λ-invariant of $f(T,\omega^{2i})$, denoted by $\lambda(\omega^{2i})$, is the least k such that $a_k(\omega^{2i}) \not\equiv 0 \mod (p)$. We set

$$\lambda^- = \sum_{i=1}^{(p-3)/2} \lambda(\omega^{2i}).$$

Ferrero and Washington make the following hypothesis to define a heuristic to make previsions about possible bounds for λ^-.

Ferrero-Washington's hypothesis: Every coefficient of $f(T,\omega^{2i})$ is random mod (p) *and independent from the other coefficients.*

Theorem 1 implies that

$$1, \overline{f(T,\omega^0)}, \overline{f(T,\omega^2)}, \dots, \overline{f(T,\omega^{p-3})}$$

are linearly independent over Ω. Thus our result seems to confirm Ferrero-Washington's hypothesis.

2. Preliminaries

In this section we shall list some properties of the p-adic Leopoldt transform that will be very important in the proof of Theorem 1. Let L be a finite extension of $\mathbb{Q}_p$, $\mathcal{O}_L$ its valuation ring and $\mathbb{F}_{q'}$ its residue field. Let κ a topological generator of $1+p\mathbb{Z}_p$ and, for all $a \in \mathbb{Z}_p^*$, set $\omega(a)$ the unique $(p-1)$th root of unity in $\mathbb{Z}_p$ congruent to $a \mod (p)$. Following [1] for all $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$ we define p-adic Leopoldt transform Γ_δ the unique continuous $\mathcal{O}_L$-linear endomorphism of $\mathcal{O}_L[[T]]$ such that for all $a \in \mathbb{Z}_p$,

$$\Gamma_\delta((T+1)^a) = \begin{cases} \omega^\delta(a)(T+1)^{\frac{\log_p(a)}{\log_p(\kappa)}} & \text{if } a \in \mathbb{Z}_p^*; \\ 0 & \text{otherwise} \end{cases}$$

(see [1, Sections 2., 3.] for the proof of the fact that Γ_δ is well-defined and unique). In an obvious way we can define a similar $\mathbb{F}_{q'}$-linear continuous endomorphism of $\mathbb{F}_{q'}[[T]]$ that we denote by $\overline{\Gamma}_\delta$. Observe that if $a \in \mathbb{Z}_p^*$ we have $a \equiv \omega(a) \mod (p)$. Thus, for all $a \in \mathbb{Z}_p^*$, we have

$$\overline{\Gamma}_\delta((T+1)^a) = a^\delta(T+1)^{\frac{\log_p(a)}{\log_p(\kappa)}}.$$

In the proof of Theorem 1 we use other $\mathcal{O}_L$-linear endomorphisms of $\mathcal{O}_L[[T]]$ already introduced by Anglès in [1]. Let us recall their definition. Let $\mu_{p-1} \subseteq \mathbb{Z}_p^*$ be the group of $(p-1)$th roots of unity. For all $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$ and $F(T) \in \mathcal{O}_L[[T]]$, we set

$$\gamma_\delta(F(T)) = \frac{1}{p-1} \sum_{\eta \in \mu_{p-1}} \eta^\delta F((T+1)^\eta - 1).$$

Observe that $\gamma_\delta \gamma_{\delta'} = 0$ for $\delta \neq \delta'$, $\gamma_\delta^2 = \gamma_\delta$ and $\sum_{\delta \in \mathbb{Z}/(p-1)\mathbb{Z}} \gamma_\delta = Id_{\mathcal{O}_L[[T]]}$.

For $F(T) \in \mathcal{O}_L[[T]]$ set

$$D(F(T)) = (T+1)\frac{d}{dT}F(T)$$
$$U(F(T)) = F(T) - \frac{1}{p} \sum_{\zeta \in \mu_p} F(\zeta(T+1) - 1) \in \mathcal{O}_L[[T]].$$

In an obvious way we can define the $\mathbb{F}_{q'}$-linear endomorphism of $\mathbb{F}_{q'}[[T]]$ $\overline{\gamma}_\delta$, $\overline{D}$ and $\overline{U}$. Observe that:

- $U^2 = U$;
- $DU = UD$;
- $\gamma_\delta U = U\gamma_\delta$ for all $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$;
- $D\gamma_\delta = \gamma_{\delta+1} D$ for all $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$;
- $\overline{U} = \overline{D}^{p-1}$.

In the following lemma we shall list some properties of Γ_δ whose we need to prove Theorem 1.

LEMMA 1. — *Let $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$ and $F(T) \in \mathcal{O}_L[[T]]$. Then*

(1) $\Gamma_\delta(F(T)) = \Gamma_\delta \gamma_{-\delta}(F(T)) = \Gamma_\delta \gamma_{-\delta} U F(T)$.

(2) *Suppose that $\Gamma_\delta(F(T))$ is a pseudo-polynomial. Then $\gamma_{-\delta}U(F(T))$ is a pseudo-polynomial.*

(3) $\overline{\Gamma}_{\delta+1}(\overline{F(T)}) = \overline{\Gamma}_\delta \overline{D}(\overline{F(T)})$.

Proof. —

(1) See [1, Proposition 3.2(2)].

(2) The assumption immediately follows from [1, Proposition 3.1].

(3) Since $\overline{\Gamma}_\delta$ is a $\mathbb{F}_{q'}$-linear continuous endomorphism of $\mathbb{F}_{q'}[[T]]$, it suffices to prove that the assumption is true for $F(T) = (T+1)^a$ with $a \in \mathbb{Z}_p$. If p divides a we have

$$0 = \overline{\Gamma}_{\delta+1}((T+1)^a) = \overline{\Gamma}_\delta(\overline{D}((T+1)^a))$$

and the assumption is trivial.

Suppose that p does not divide a. We have

$$\begin{aligned}\overline{\Gamma}_\delta(\overline{D}((T+1)^a)) &= \overline{\Gamma}_\delta(a(T+1)^a)) \\ &= a\overline{\Gamma}_\delta((T+1)^a) \\ &= a^{\delta+1}(T+1)^{\frac{\log_p(a)}{\log_p(\kappa)}} \\ &= \overline{\Gamma}_{\delta+1}((T+1)^a).\end{aligned}$$

□

Let θ be a Dirichlet character of the first kind such that

$$\theta = \chi\omega^{\delta+1},$$

with $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$ and χ a character of conductor d not divided by p. Observe that $\kappa_0 = 1+dp$ is a topological generator of $1+p\mathbb{Z}_p$ and from now on set $\kappa = \kappa_0$. Suppose that $\mathbb{Q}_p(\chi) \subseteq L$. Set

$$F_\chi(T) = \sum_{a=1}^{d} \frac{\chi(a)(T+1)^a}{1-(T+1)^d}$$

and $\overline{F_\chi}(T) \in \mathbb{F}_{q'}(T)$ its reduction modulo the maximal ideal of $\mathcal{O}_L$. In the following lemma we list some properties of $F_\chi(T)$ and we recall the relation between $F_\chi(T)$ and $f(T,\theta)$.

Lemma 2. — *We have:*

(1) *If $d \geqslant 2$, then $F_\chi(T) \in \mathcal{O}_L[[T]]$.*

(2) *If $d = 1$, then $\gamma_\alpha(F_\chi(T)) \in \mathcal{O}_L[[T]]$ for all $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$ and $\alpha \neq 1$.*

(3) *If $d \geqslant 2$, then $F_\chi((T+1)^{-1}-1) = \varepsilon F_\chi(T)$ where $\varepsilon = 1$ if χ is odd and $\varepsilon = -1$ if χ is even.*

(4) *If $d = 1$, then $F_\chi((T+1)^{-1}-1) = -F_\chi(T) - 1$.*

(5) *If d divides a positive integer g we have*

$$F_\chi(T) = \frac{\sum_{a=1}^{g}\chi(a)(T+1)^a}{1-(T+1)^g}.$$

(6) $\Gamma_\delta\gamma_{-\delta}U(F_\chi(T)) = f((T+1)^{-1}-1,\theta)$.

Proof. —
For (1), (2), (3), (4), see [1, Lemma 4.1].

(5) We have:

$$\begin{aligned}
&\frac{\sum_{a=1}^{g}\chi(a)(T+1)^a}{1-(T+1)^g}\\
&=\sum_{a=1}^{d}\chi(a)\sum_{b\equiv a \mod (d)}\frac{\chi(b)(T+1)^b}{1-(T+1)^g}\\
&=\sum_{a=1}^{d}\chi(a)\frac{(T+1)^a+(T+1)^{a+d}+\ldots+(T+1)^{a+g-d}}{1-(T+1)^g}\\
&=\frac{\sum_{a=1}^{d}\chi(a)(T+1)^a(1-(T+1)^g)}{(1-(T+1)^g)(1-(T+1)^d)}\\
&=F_\chi(T).
\end{aligned}$$

(6) Remember that $U\gamma_{-\delta}=\gamma_{-\delta}U$. Then apply [1, Lemma 4.4]. □

Consider the ring $\mathcal{O}_L[[t]]$. It acts over $\mathcal{O}_L[[T]]$ via:

$$(t+1)F(T)=F((T+1)^{\kappa_0}-1)\in\mathcal{O}_L[[T]],$$

for all $F(T)\in\mathcal{O}_L[[T]]$.

LEMMA 3. — *Let $H(T)\in\mathcal{O}_L[[T]]$. Then for all $F(T)\in\mathcal{O}_L[[T]]$ we have*

$$H(T)\Gamma_\delta(F(T))=\Gamma_\delta(H(t)F(T)).$$

Proof. — Since Γ_δ is $\mathcal{O}_L$-linear and continuous it suffices to prove the assumption in the case $P(T)=(T+1)^a$, where $a\in\mathbb{Z}_p$. By [1, Proposition 3.2(3)] for all $b\in\mathbb{Z}_p^*$ we have

$$\Gamma_\delta(F(T+1)^b-1)=\omega^\delta(b)(T+1)^{\frac{\log_p(b)}{\log_p(\kappa)}}\Gamma_\delta(F(T)).$$

Then we get

$$\begin{aligned}
\Gamma_\delta((t+1)^aF(T))&=\Gamma_\delta(F((T+1)^{\kappa_0^a}-1)\\
&=\omega^\delta(\kappa_0^a)(T+1)^{\frac{\log_p(\kappa_0^a)}{\log_p(\kappa_0)}}\Gamma_\delta(F(T))\\
&=(T+1)^a\Gamma_\delta(F(T)).
\end{aligned}$$

□

3. The case $d\geqslant 2$

The aim of this section is to prove Theorem 1 in the case where the conductor d of the characters χ_i is $\geqslant 2$.

Proof of Theorem 1 in the case $d \geqslant 2$. — Let $\chi_1, \chi_2, \dots, \chi_n$ characters of conductor $d \geqslant 2$ distinct modulo (π). Without loss of generality we can suppose $\chi_1, \dots, \chi_r$ odd and $\chi_{r+1}, \dots, \chi_n$ even for a certain integer $r \leqslant n$. For all i between 1 and n and j between 0 and $(p-3)/2$ set

$$\theta_{i,j} = \begin{cases} \chi_i \omega^{2j+1} & \text{if } 1 \leqslant i \leqslant r; \\ \chi_i \omega^{2j} & \text{otherwise.} \end{cases} \tag{3.1}$$

Suppose that for all $1 \leqslant i \leqslant n$, $0 \leqslant j \leqslant (p-3)/2$, there exist $g_{i,j}(T) \in \Omega$ such that

$$\sum_{i=1}^{n} \sum_{j=0}^{(p-3)/2} g_{i,j}(T) \overline{f(T, \theta_{i,j})} \in \Omega$$

and $g_{i,j}(T) \neq 0$ for some i, j. Set $h_{i,j}(T) = g_{i,j}(1/(T+1) - 1)$ for all i, j. Then we have

$$\sum_{i=1}^{n} \sum_{j=0}^{(p-3)/2} h_{i,j}(T) \overline{f(1/(T+1) - 1, \theta_{i,j})} \in \Omega$$

and $h_{i,j}(T) \neq 0$ for certain i, j. Observe that we can suppose that $h_{i,j} \in A$ for all i, j and that

$$\sum_{i=1}^{n} \sum_{j=0}^{(p-3)/2} h_{i,j}(T) \overline{f(1/(T+1) - 1, \theta_{i,j})} \in A. \tag{3.2}$$

By Lemma 2(6) and (3.1) for all i between 1 and n and j between 0 and $(p-3)/2$, we have:

$$f\left(\frac{1}{T+1} - 1, \theta_{i,j}\right) = \begin{cases} \Gamma_{2j} \gamma_{-2j}(F_{\chi_i}(T)) & \text{if } 1 \leqslant i \leqslant r; \\ \Gamma_{2j-1} \gamma_{-2j+1}(F_{\chi_i}(T)) & \text{otherwise.} \end{cases} \tag{3.3}$$

Moreover by Lemma 1(3), for all $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$ we have

$$\overline{\Gamma}_{\delta+1} \overline{\gamma}_{-\delta-1} = \overline{\Gamma}_{\delta} \overline{\gamma}_{\delta} \overline{D}.$$

Hence we can rewrite relation (3.2) in the following way:

$$\sum_{i=1}^{r} \sum_{j=0}^{(p-3)/2} h_{i,j}(T) \overline{\Gamma}_0 \overline{\gamma}_0 (\overline{D}^{2j} \overline{F}_{\chi_i}(T)) + \sum_{i=r+1}^{n} \sum_{j=0}^{(p-3)/2} h_{i,j}(T) \overline{\Gamma}_0 \overline{\gamma}_0 (\overline{D}^{2j-1} \overline{F}_{\chi_i}(T)) \in A.$$

By Lemma 1(1) this last relation implies that

$$\sum_{i=1}^{r}\sum_{j=0}^{(p-3)/2} h_{i,j}(T)\overline{\Gamma}_0\overline{\gamma}_0\overline{U}(\overline{D}^{2j}\overline{F}_{\chi_i}(T))+ \sum_{i=r+1}^{n}\sum_{j=0}^{(p-3)/2} h_{i,j}(T)\overline{\Gamma}_0\overline{\gamma}_0\overline{U}(\overline{D}^{2j-1}\overline{F}_{\chi_i}(T)) \in A. \tag{3.4}$$

Applying Lemma 3 and 1(2) to (3.4) we get

$$\sum_{i=1}^{r}\sum_{j=0}^{(p-3)/2} h_{i,j}(t)\overline{\gamma}_0\overline{U}(\overline{D}^{2j}\overline{F}_{\chi_i}(T))+ \sum_{i=r+1}^{n}\sum_{j=0}^{(p-3)/2} h_{i,j}(t)\overline{\gamma}_0\overline{U}(\overline{D}^{2j-1}\overline{F}_{\chi_i}(T)) \in A. \tag{3.5}$$

Set for all $1 \leqslant i \leqslant n$, $0 \leqslant j \leqslant (p-3)/2$,

$$F_{i,j}(T) = \begin{cases} \overline{UD}^{2j}(\overline{F}_{\chi_i}(T)) & \text{if } 1 \leqslant i \leqslant r; \\ \overline{UD}^{2j-1}(\overline{F}_{\chi_i}(T)) & \text{otherwise.} \end{cases} \tag{3.6}$$

Then we can rewrite relation (3.5) in the following way:

$$\sum_{i=1}^{n}\sum_{j=0}^{(p-3)/2} h_{i,j}(t)\overline{\gamma}_0(F_{i,j}(T)) \in A. \tag{3.7}$$

Now recall that by Lemma 2(3), we have

$$F_{\chi_i}((T+1)^{-1}-1) = \begin{cases} F_{\chi_i}(T) & \text{if } 1 \leqslant i \leqslant r; \\ -F_{\chi_i}(T) & \text{if } r+1 \leqslant i \leqslant n. \end{cases}$$

Moreover observe that for all $1 \leqslant i \leqslant n$, $0 \leqslant k \leqslant p-2$ we have

$$(\overline{UD}^k\overline{F}_{\chi_i})((T+1)^{-1}-1) = (-1)^k\overline{UD}^k(\overline{F}_{\chi_i}((T+1)^{-1}-1)).$$

Let i be between 1 and r and j be between 0 and $(p-3)/2$. Then

$$\begin{aligned} F_{i,j}((T+1)^{-1}-1) &= (\overline{UD}^{2j}\overline{F}_{\chi_i})((T+1)^{-1}-1)) \\ &= (-1)^{2j}\overline{UD}^{2j}(\overline{F}_{\chi_i}((T+1)^{-1}-1)) \\ &= \overline{UD}^{2j}(\overline{F}_{\chi_i}(T)) \\ &= F_{i,j}(T). \end{aligned}$$

With exactly the same computation we can prove that

$$F_{i,j}((T+1)^{-1}-1) = F_{i,j}(T)$$

for all i,j, also in the case where $r+1 \leqslant i \leqslant n$. Then

$$F_{i,j}((T+1)^{-1}-1) = F_{i,j}(T),\ \forall i,j. \tag{3.8}$$

We recall that $\mathbb{F}_q$ is, by definition, the residue field of the smallest extension of $\mathbb{Q}_p$ that contains all the images of the characters χ_i. Consider the smallest field that contains $\mathbb{F}_q$ and all the coefficients of $h_{i,j}(T)$ for all i,j. Since $h_{i,j}(T) \in A \subseteq \overline{\mathbb{F}}_p[[T]]$, such field is a finite extension of $\mathbb{F}_q$. Call it $\mathbb{F}_{q_1}$ and write $h_{i,j}(t) = \sum_{b\in\mathbb{Z}_p} c_{i,j,b}(t+1)^b$ with $c_{i,j,b} \in \mathbb{F}_{q_1}$. Moreover observe that since $h_{i,j}(T) \neq 0$ for certain integer i,j, there exist i,j,b such that $c_{i,j,b} \neq 0$. Let

$$G_b(T) = \sum_{i=1}^{n} \sum_{j=0}^{(p-3)/2} c_{i,j,b} F_{i,j}(T).$$

By Lemma 2(1), $G_b(T) \in \mathbb{F}_{q_1}[[T]] \cap \mathbb{F}_{q_1}(T)$. Since

$$(t+1)^b (G_b(T)) = G_b((T+1)^{\kappa_0^b} - 1),$$

by (3.7) we have

$$\overline{\gamma}_0\Big(\sum_{b\in\mathbb{Z}_p} G_b((T+1)^{\kappa_0^b}-1)\Big) \in A. \tag{3.9}$$

Choose a subset of μ_{p-1} whose elements represent all the classes of $\mu_{p-1}/\{-1,1\}$ and call it S. From (3.8) it follows that

$$G_b(T) = G_b((T+1)^{-1}-1) \tag{3.10}$$

for all b. Thus by (3.9) we get

$$\sum_{\eta\in S} \sum_{b\in\mathbb{Z}_p} G_b((T+1)^{\eta\kappa_0^b}-1) \in A.$$

Since $G_b(T) = 0$ for all but finitely many $b \in \mathbb{Z}_p$, there exists a positive integer u such that

$$\sum_{\eta\in S} \sum_{k=1}^{u} G_{b_k}((T+1)^{\eta\kappa_0^{b_k}}-1) \in A.$$

Moreover we set $G_k(T) = G_{b_k}(T)$. By Proposition 1 there exist an integer $l \leqslant u$, $b_1, b_2, \ldots, b_l \in \mathbb{Z}_p$, $b_i \neq b_j$ for $i \neq j$, $\eta_1, \eta_2, \ldots, \eta_l \in \mu_{p-1}$ with $\eta_i \kappa_0^{b_i} \sim_{\mathbb{Q}^*} \eta_j \kappa_0^{b_j}$ for all i, j and $\eta_i \kappa_0^{b_i} \neq \eta_j \kappa_0^{b_j}$ for $i \neq j$ such that

$$\sum_{k=1}^{l} G_k((T+1)^{\eta_k \kappa_0^{b_k}}-1) \in A. \tag{3.11}$$

For all $1 \leqslant k \leqslant l$ write

$$\eta_k \kappa_0^{b_k} = \eta_1 \kappa_0^{b_1} x_k,$$

where $x_k \in \mathbb{Q}^* \cap \mathbb{Z}_p^*$ and $x_i \neq x_j$ if $i \neq j$. Recall that by (3.10), we have $G_k(T) = G_k((T+1)^{-1} - 1)$. Hence we can suppose that $x_k > 0$ for all k. By (3.11) we get

$$\sum_{k=i}^{l} G_k((T+1)^{x_k} - 1) \in A.$$

Therefore there exist some positive integers $N_1, N_2, \ldots, N_l$ not divided by p such that $1 \leqslant N_1 < N_2 < \ldots < N_l$ and

$$\sum_{k=i}^{l} G_k((T+1)^{N_k} - 1) \in A.$$

If we rewrite $G_k(T)$ as a combination of $F_{i,j}(T)$, we get

$$\sum_{k=1}^{l} \sum_{i=1}^{n} \sum_{j=0}^{(p-3)/2} c_{i,j,k} F_{i,j}((T+1)^{N_k} - 1) \in A.$$

By [1, Lemma 3.5] if $H(T) \in \mathbb{F}_{q_1}(T)$, then $H(T) \in A$ if and only if there exists $m \in \mathbb{N}$ such that $(T+1)^m H(T) \in \mathbb{F}_{q_1}[T]$. Since the denominator of $F_{i,j}((T+1)^{N_k} - 1)$ is relatively prime to $(T+1)$ for all i, j, k, we get

$$\sum_{k=1}^{l} \sum_{i=1}^{n} \sum_{j=0}^{(p-3)/2} c_{i,j,k} F_{i,j}((T+1)^{N_k} - 1) \in \mathbb{F}_{q_1}[T]. \tag{3.12}$$

Observe that, by Lemma 2(5), we have

$$F_{\chi_i}(T) = \sum_{a=1}^{dp} \frac{\chi_i(a)(T+1)^a}{1 - (T+1)^{dp}}.$$

Then for all $1 \leqslant i \leqslant n$ and $0 \leqslant j \leqslant (p-3)/2$, we have

$$F_{i,j}(T) = \begin{cases} \sum_{a=1, p\nmid a}^{dp-1} \frac{\chi_i(a) a^{2j} (T+1)^a}{1-(T+1)^{dp}} & \text{if } 1 \leqslant i \leqslant r; \\ \sum_{a=1, p\nmid a}^{dp-1} \frac{\chi_i(a) a^{2j-1} (T+1)^a}{1-(T+1)^{dp}} & \text{otherwise.} \end{cases} \tag{3.13}$$

Then replacing in (3.12) using (3.13), we get

$$\begin{aligned} &\sum_{k=1}^{l} \sum_{i=0}^{r} \sum_{j=0}^{(p-3)/2} c_{i,j,k} \sum_{a=1, p\nmid a}^{dp} \left(\frac{a^{2j} \chi_i(a) (T+1)^{aN_k}}{1 - (T+1)^{dpN_k}} \right) + \\ &+ \sum_{k=1}^{l} \sum_{i=r+1}^{n} \sum_{j=0}^{(p-3)/2} c_{i,j,k} \sum_{a=1, p\nmid a}^{dp} \left(\frac{a^{2j-1} \chi_i(a) (T+1)^{aN_k}}{1 - (T+1)^{dpN_k}} \right) \in \mathbb{F}_{q_1}[T]. \end{aligned} \tag{3.14}$$

To finish the proof we shall prove that (3.14) is satisfied only if $c_{i,j,k} = 0$ for all i, j, k, obtaining a contradiction.

We need the following remark:

REMARK 1. — *Let V be a vector space over a field F and W be a subspace of V. Moreover let ϕ be an endomorphism of V such that $\phi(W) \subseteq W$. We remark that if m is a positive integer and $v_1, v_2, \ldots, v_m \in V$ are eigenvectors of ϕ with non-zero eigen-values $\lambda_1, \lambda_2, \ldots, \lambda_m$ such that $\lambda_i \neq \lambda_j$ if $i \neq j$ and if*

$$v_1 + v_2 + \ldots + v_m \in W,$$

then $v_i \in W$ for all i.

If we apply Remark 1 in the particular case where $F = \mathbb{F}_{q_1}$, $V = \mathbb{F}_{q_1}(T)$, $W = \mathbb{F}_{q_1}[T]$, $m = p-1$, $\phi = \overline{D}$, $\lambda_b = b$ for all $1 \leqslant b \leqslant p-1$ and

$$v_b = V_b(T) = \sum_{k=1}^{l} \sum_{i=0}^{r} \sum_{j=0}^{(p-3)/2} c_{i,j,k} \sum_{aN_k \equiv b \mod (p)} \left(\frac{a^{2j} \chi_i(a) (T+1)^{aN_k}}{1-(T+1)^{dpN_k}} \right) +$$

$$+ \sum_{k=1}^{l} \sum_{i=r+1}^{n} \sum_{j=0}^{(p-3)/2} c_{i,j,k} \sum_{aN_k \equiv b \mod (p)}^{dp} \left(\frac{a^{2j-1} \chi_i(a) (T+1)^{aN_k}}{1-(T+1)^{dpN_k}} \right),$$

by (3.14) we get $V_b(T) \in \mathbb{F}_{q_1}[T]$. Multiply $V_b(T)$ by $1-(T+1)^{dpN_l}$. Then

$$(1-(T+1)^{dpN_l}) V_b(T) \in (1-(T+1)^{dpN_l}) \mathbb{F}_{q_1}[T].$$

Let us recall that p does not divide N_k for all k. Observe that if ζ is a primitive dN_l-th root of unity, then $\zeta - 1$ is a root of $(1-(T+1)^{dpN_l}) V_b(T)$. Since $N_l > N_k$ for all $k < l$, $\zeta - 1$ is a zero of

$$\begin{aligned}
(1-(T+1)^{dpN_l}) & \sum_{k=1}^{l-1} \sum_{i=0}^{r} \sum_{j=0}^{(p-3)/2} c_{i,j,k} \\
& \sum_{aN_k \equiv b \mod (p)} \left(\frac{a^{2j} \chi_i(a) (T+1)^{aN_k}}{1-(T+1)^{dpN_k}} \right) + \\
& + (1-(T+1)^{dpN_l}) \sum_{k=1}^{l-1} \sum_{i=r+1}^{n} \sum_{j=0}^{(p-3)/2} c_{i,j,k} \\
& \sum_{aN_k \equiv b \mod (p)}^{dp} \left(\frac{a^{2j-1} \chi_i(a) (T+1)^{aN_k}}{1-(T+1)^{dpN_k}} \right).
\end{aligned}$$

Then we get

$$\sum_{i=1}^{r}\sum_{j=0}^{(p-3)/2} c_{i,j,l} \sum_{aN_l\equiv b \mod (p)} a^{2j}\chi_i(a)\zeta^{aN_l} + \sum_{i=r+1}^{n}\sum_{j=0}^{(p-3)/2} c_{i,j,l} \sum_{aN_l\equiv b \mod (p)} a^{2j-1}\chi_i(a)\zeta^{aN_l} = 0. \tag{3.15}$$

Observe that since p does not divide d, $\{a, p+a, \dots, p(d-1)+a\}$ is a set of representatives of all the classes modulo d. Moreover observe that, since ζ is a primitive dN_l-th root of unity, $\zeta' = \zeta^{N_l}$ is a primitive d-th root of unity. Let $k \in \mathbb{Z}/p\mathbb{Z}$ such that $kN_l \equiv b \mod (p)$. We can rewrite (3.15) as

$$\sum_{i=1}^{r}\sum_{j=0}^{(p-3)/2} c_{i,j,l}k^{2j}\sum_{h=0}^{d-1}\chi_i(h)\zeta'^h + \sum_{i=r+1}^{n}\sum_{j=0}^{(p-3)/2} c_{i,j,l}k^{2j-1}\sum_{h=0}^{d-1}\chi_i(h)\zeta'^h = 0. \tag{3.16}$$

Then for all primitive d-th root of unity, (3.16) must be satisfied.

Set

$$x_{i,k} = \begin{cases} \sum_{j=0}^{(p-3)/2} c_{i,j,l}k^{2j}, & \text{if } 1 \leqslant i \leqslant r; \\ \sum_{j=0}^{(p-3)/2} c_{i,j,l}k^{2j-1} & \text{otherwise} \end{cases}$$

and let

$$\{\zeta_1, \zeta_2, \dots, \zeta_{\phi(d)}\}$$

be the set of primitive d-th roots of unity in $\overline{\mathbb{F}_p}$ (recall that p does not divide d). Then by (3.16) we have

$$\sum_{i=1}^{n} x_{i,k}\sum_{h=0}^{d-1}\chi_i(h)\zeta_c^h = 0 \tag{3.17}$$

for all $1 \leqslant c \leqslant \phi(d)$. Hence we have a system of n unknows $(x_{1,k}, \dots, x_{n,k})$ and $\phi(d)$ equations (one for all primitive d-th root of unity). Observe that $n < \phi(d)$. Indeed by definition n is less than the number of the characters of conductor $d \geqslant 2$ distinct $\mod (\pi)$. Since we have only $\phi(d)$ characters whose conductor divides d and since the trivial character has conductor $1 \neq d$, we have $n \leqslant \phi(d)-1$. Thus the number of equations of the system is greater then the number of its unknowns. We shall prove that the system has the unique solution $(0, 0, \dots, 0)$.

Let B be the matrix associated to the system (3.17). Then

$$B = \begin{pmatrix} \sum_{h=0}^{d-1} \chi_1(h)\zeta_1^h & \sum_{h=0}^{d-1} \chi_2(h)\zeta_1^h & \cdots & \sum_{h=0}^{d-1} \chi_n(h)\zeta_1^h \\ \sum_{h=0}^{d-1} \chi_1(h)\zeta_2^h & \sum_{h=0}^{d-1} \chi_2(h)\zeta_2^h & \cdots & \sum_{h=0}^{d-1} \chi_n(h)\zeta_2^h \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{h=0}^{d-1} \chi_1(h)\zeta_{\phi(d)}^h & \sum_{h=0}^{d-1} \chi_2(h)\zeta_{\phi(d)}^h & \cdots & \sum_{h=0}^{d-1} \chi_n(h)\zeta_{\phi(d)}^h \end{pmatrix}.$$

Observe that $B = CE$, where

$$C = \begin{pmatrix} 1 & \zeta_1 & \cdots & \zeta_1^{d-1} \\ 1 & \zeta_2 & \cdots & \zeta_2^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_{\phi(d)} & \cdots & \zeta_{\phi(d)}^{d-1} \end{pmatrix},$$

$$E = \begin{pmatrix} \chi_1(0) & \chi_2(0) & \cdots & \chi_n(0) \\ \chi_1(1) & \chi_2(1) & \cdots & \chi_n(1) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_1(d-1) & \chi_2(d-1) & \cdots & \chi_n(d-1) \end{pmatrix}.$$

In the following lemma we will prove that $\ker(B)$ is equals to $\{(0, 0, \ldots, 0)\}$, which implies $x_{1,k} = x_{2,k} = \ldots = x_{n,k} = 0$.

Lemma 4. — *We have:*

(1) *The rank of C is $\phi(d)$.*

(2) *The set*

$$\mathcal{B} = \{(1, \zeta, \ldots, \zeta^{d-1}),\ \zeta \in \mu_d,\ \zeta \text{ not primitive}\}$$

is a basis of $\ker(C)$.

(3) $\ker(B) = \{(0, 0, \ldots, 0)\}$.

Proof. — (1) Let C' be the matrix whose columns coincide with the first $\phi(d)$ columns of the matrix C. Then C' is a square matrix equals to

$$C' = \begin{pmatrix} 1 & \zeta_1 & \cdots & \zeta_1^{\phi(d)-1} \\ 1 & \zeta_2 & \cdots & \zeta_2^{\phi(d)-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_{\phi(d)} & \cdots & \zeta_{\phi(d)}^{\phi(d)-1} \end{pmatrix}.$$

Observe that C' is a Vandermonde matrix. Thus its determinant is equals to

$$\prod_{1\leqslant r<s\leqslant\phi(d)}(\zeta_r-\zeta_s).$$

Since p does not divide d, we have

$$\zeta_r\neq\zeta_s.$$

Thus the determinant of C' is non-zero. Therefore C has rank $\phi(d)$, since its square $\phi(d)\times\phi(d)$ sub-matrix C' has non-zero determinant.

(2) Since C has rank $\phi(d)$, the dimension of $\ker(C)$ is $d-\phi(d)$. Observe that $\mathcal{B}$ has $d-\phi(d)$ elements. Hence $\mathcal{B}$ is a basis of $\ker(C)$ if and only if $\mathcal{B}\subseteq\ker(C)$ and the elements of $\mathcal{B}$ are linearly independent.

First let us prove that $\mathcal{B}\subseteq\ker(C)$. Let $\zeta\in\mu_d$ be a d-th root of unity that is not primitive. Observe that $(1,\zeta,\dots,\zeta^{d-1})\in\ker(C)$ if and only if

$$\sum_{h=0}^{d-1}\zeta_i^h\zeta^h=0$$

for all i. Since

$$\zeta_i\zeta\sum_{h=0}^{d-1}\zeta_i^h\zeta^h=\sum_{h=0}^{d-1}\zeta_i^h\zeta^h$$

and $\zeta_i\zeta\neq1$ because p does not divide d, it follows that

$$\sum_{h=0}^{d-1}\zeta_i^h\zeta^h=0.$$

Thus $(1,\zeta,\dots,\zeta^{d-1})\in\ker(C)$ for all non primitive d-th root of unity ζ. Then $\mathcal{B}\subseteq\ker(C)$.

Denote still by ζ an element of μ_d whose order is different from d. Set $\beta_\zeta\colon\mathbb{Z}/d\mathbb{Z}\to\mu_d$ the character that sends $i\in\mathbb{Z}/d\mathbb{Z}$ to ζ^i. Observe that if $\zeta'\in\mu_d$ and $\zeta\neq\zeta'$,

$$\beta_\zeta(1)=\zeta\neq\zeta'=\beta_{\zeta'}(1),$$

since p does not divide d. Thus the characters β_ζ are all distinct. Hence the theorem of the linear independence of characters imply that β_ζ are linearly independent over $\overline{\mathbb{F}_p}$. From this fact it follows that the vectors $(1,\zeta,\dots,\zeta^{d-1})$ are linearly independent for all non primitive d-th root of unity ζ. Hence $\mathcal{B}$ is a basis of $\ker(C)$.

(3) Using the previous notation for all non primitive d-th root of unity ζ, let β_ζ be the function that sends $j\in\mathbb{Z}/d\mathbb{Z}$ to ζ^j. Observe that every non trivial linear combination of the vectors $(\chi_i(0),\chi_i(1),\dots,\chi_i(d-1))$ for $1\leqslant i\leqslant n$ is not in $\ker(C)$ if and only if the functions χ_i and β_ζ for

$1 \leqslant i \leqslant n$ and non primitive d-th root of unity ζ are linealry independent over $\overline{\mathbb{F}_p}$ (here χ_i is considered as a function of $\mathbb{Z}/d\mathbb{Z}$ over $\mathbb{F}_q \subseteq \overline{\mathbb{F}_p}$). Suppose that such functions are dependent. Then we can choose a minimal r, non-zero λ_i and μ_ζ in $\overline{\mathbb{F}_p}$ such that

$$\sum_{i=1}^{r} \lambda_i \chi_i + \sum_{\zeta \text{ not primitive}} \mu_\zeta \beta_\zeta = 0. \tag{3.18}$$

First observe that $r \geqslant 2$. Indeed if $r = 0$ then (3.18) would imply the linear dependence of the elements of $\mathcal{B}$ against (2). Moreover if $r = 1$ then there would exist a character χ_i of conductor d that would satisfy the relation $(\chi_i(0), \chi_i(1), \ldots, \chi_i(d-1)) \in \ker(C)$. Then we would have

$$\sum_{h=0}^{d-1} \zeta_j^h \chi_i(h) = 0$$

for all primitive d-th root of unity ζ_j, which contradicts [4, Lemma 4.8].

Let $b \in (\mathbb{Z}/d\mathbb{Z})^*$ such that $\chi_1(b) \neq \chi_2(b)$ (such b exists because recall that, by hypothesis, χ_1 is different from χ_2 modulo (π)). Hence by (3.18), for all $z \in \mathbb{Z}/d\mathbb{Z}$ we have

$$\sum_{i=1}^{r} \lambda_i \chi_i(bz) + \sum_{\zeta \text{ not primitive}} \mu_\zeta \beta_\zeta(bz) = 0. \tag{3.19}$$

Observe that the function that sends $z \in \mathbb{Z}/d\mathbb{Z}$ to $\beta_\zeta(bz)$ coincides with the function β_{ζ^b}. Hence we can rewrite (3.19) as

$$\sum_{i=1}^{r} \lambda_i \chi_1(b) \chi_i(z) + \sum_{\zeta \text{ not primitive}} \chi_1(b) \mu_\zeta \beta_{\zeta^b}(z) = 0. \tag{3.20}$$

If we multiply (3.18) by $\chi_1(b)$ and we subtract it to (3.20),we get a non trivial relation with less than r characters χ_i and it is impossible by the minimality of r.

Finally consider the matrix B. Let $v = (\lambda_1, \lambda_2, \ldots, \lambda_n) \in \ker(B)$. Since $B = CE$, then $E(v) \in \ker(C)$. This fact implies that

$$\sum_{i=1}^{n} \lambda_i (\chi_i(0), \chi_i(1), \ldots, \chi_i(d-1)) \in \ker(C).$$

But we have previously proved that this relation is possible only if $\lambda_i = 0$ for all i. Thus $v = (0, 0, \ldots, 0)$. □

By the previous lemma we immediately get $x_{i,k} = 0$ for all $1 \leqslant i \leqslant n$ and for all $1 \leqslant k \leqslant p-1$. Remember that, by definition,

$$x_{i,k} = \begin{cases} \sum_{j=0}^{(p-3)/2} c_{i,j,l} k^{2j}, & \text{if } 1 \leqslant i \leqslant r; \\ \sum_{j=0}^{(p-3)/2} c_{i,j,l} k^{2j-1} & \text{otherwise.} \end{cases}$$

We shall prove that the relation $x_{i,k} = 0$ for all i, k implies $c_{i,j,l} = 0$ for all i, j. We just consider the case $i \leqslant r$ (the proof in the other case is very similar). Let i be an integer between 1 and r and set $c_{i,j,l} = y_j$. Since $x_{i,k} = 0$ for all k between 1 and $p-1$, we have the following relations:

$$\sum_{j=0}^{(p-3)/2} y_j k^{2j} = 0. \tag{3.21}$$

The matrix M associated to the first $(p-1)/2$ equations of the system (3.21) is given by:

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 4 & \cdots & 4^{(p-3)/2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \frac{(p-1)^2}{4} & \cdots & \left(\frac{(p-1)^2}{4}\right)^{(p-3)/2} \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{(p-3)/2} \\ 1 & \alpha_2 & \cdots & \alpha_2^{(p-3)/2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{(p-1)/2} & \cdots & \alpha_{(p-1)/2}^{(p-3)/2} \end{pmatrix}.$$

So M is a Vandermonde matrix and its determinant is equals to:

$$\det(M) = \prod_{1 \leqslant r < s \leqslant (p-1)/2} (\alpha_r - \alpha_s) \neq 0.$$

It follows that the only solution of the system (3.21) is $y_j = 0$ for all j.

Then we have proved that the coefficients $c_{i,j,l} = 0$ for all i and j. Since $N_{l-1} > N_k$ for all $k < l-1$, if we replace l with $l-1$ with the same procedure we can prove that the coefficients $c_{i,j,l-1} = 0$ for all i, j and so on. Thus $c_{i,j,k} = 0$ for all i, j, k, which is a contradiction.

4. The case $d = 1$

The aim of this section is to prove Theorem 1 in the case where $d = 1$. In other words, let χ the trivial character. We shall prove that

$$\dim_\Omega(\Omega + \Omega\overline{f(T,\chi\omega^0)} + \Omega\overline{f(T,\chi\omega^2)} + \ldots + \Omega\overline{f(T,\chi\omega^{p-3})}) = \frac{p+1}{2}.$$

As we have already remarked is Section 1 we shall modify the proof of the case $d \geqslant 2$. Let us give a preliminar reason for this. Let $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$ be odd. Then by Lemma 2(6) we have

$$f((T+1)^{-1} - 1, \chi\omega^{\delta+1}) = \Gamma_\delta \gamma_{-\delta} U((F_\chi(T)).$$

Since χ is the trivial character we have

$$F_\chi(T) = \sum_{a=0}^{p-1} \frac{(T+1)^a}{1-(T+1)^p} - 1 = -\frac{1}{T} - 1. \tag{4.1}$$

Thus $\overline{F_\chi}(T) \notin \mathbb{F}_p[[T]]$ and we shall see that this fact does not allow us to apply Proposition 1 (observe that if χ' is not the trivial character then $\overline{F_{\chi'}}(T) \in \mathbb{F}_q[[T]]$ and see also Remark 2). The following lemma explains how we can solve this problem.

Lemma 5. — *Let*

$$\widetilde{F_\chi}(T) = (p+1)F_\chi((T+1)^{p+1} - 1) - F_\chi(T).$$

Then $\widetilde{F_\chi}(T) \in \mathbb{Z}_p[[T]]$.

Moreover

$$T\overline{f((T+1)^{-1} - 1, \chi\omega^{\delta+1})} = \overline{\Gamma}_\delta \overline{\gamma}_{-\delta} \overline{U}(\widetilde{\overline{F_\chi}}(T))$$

for all odd $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$.

Finally $1, T\overline{f((T+1)^{-1} - 1, \chi\omega^0)}, \ldots, T\overline{f((T+1)^{-1} - 1, \chi\omega^{p-3})}$ *are independent over* Ω *if and only if* $1, \overline{f(T,\chi\omega^0)}, \ldots, \overline{f(T,\chi\omega^{p-3})}$ *are independent over* Ω.

Proof. — Observe that

$$\begin{aligned}
\widetilde{F_\chi}(T) &= (p+1)F_\chi((T+1)^{p+1} - 1) - F_\chi(T) \\
&= -\frac{(p+1)}{(T+1)^{p+1} - 1} + \frac{1}{T} - p \\
&= \frac{(T+1)^{p+1} - (p+1)T - 1}{T((T+1)^{p+1} - 1)} - p.
\end{aligned}$$

We remark that T^2 exactly divides $T((T+1)^{p+1} - 1)$. Moreover T^2 divides $(T+1)^{p+1} - (p+1)T - 1$. Then we immediately get $\widetilde{F_\chi}(T) \in \mathbb{Z}_p[[T]]$.

Let L be a finite extension of $\mathbb{Q}_p$ and let $\mathcal{O}_L$ be its valuation ring. Let d be an integer not divided by p and set $\kappa_0 = 1 + dp$. Remember that in Section 2 we have defined an action of $\mathcal{O}_L[[t]]$ over $\mathcal{O}_L[[T]]$ such that, for all $a \in \mathbb{Z}_p$ and $F(T) \in \mathcal{O}_L[[T]]$,

$$(t+1)^a F(T) = F((T+1)^{\kappa_0^a} - 1).$$

Set $L = \mathbb{Q}_p$, $d = 1$ and $\kappa_0 = 1 + p$. Then, since

$$\widetilde{F_\chi}(T) = F_\chi((T+1)^{p+1} - 1) - F_\chi(T) + pF_\chi((T+1)^{p+1} - 1),$$

we have

$$\widetilde{F_\chi}(T) \equiv tF_\chi(T) \mod (p).$$

By Lemma 3(2) we get

$$\overline{\Gamma_\delta}\overline{\gamma_{-\delta}}\overline{U}(\overline{\widetilde{F_\chi}}(T)) = \overline{\Gamma_\delta}\overline{\gamma_{-\delta}}\overline{U}(t\overline{F_\chi}(T)) = T\overline{\Gamma_\delta}\overline{\gamma_{-\delta}}\overline{U}(\overline{F_\chi}(T)).$$

Then, by Lemma 2(6), we immediately get

$$T\overline{f((T+1)^{-1} - 1, \chi\omega^{\delta+1})} = \overline{\Gamma}_\delta\overline{\gamma}_{-\delta}\overline{U}(\overline{\widetilde{F_\chi}}(T)).$$

Finally $1, T\overline{f((T+1)^{-1} - 1, \chi\omega^0)}, \dots, T\overline{f((T+1)^{-1} - 1, \chi\omega^{p-3})}$ are independent over Ω if and only if $1, \overline{f(T, \chi\omega^0)}, \dots, \overline{f(T, \chi\omega^{p-3})}$ are independent over Ω, since $T \in \Omega$ and the image of Ω via the endomorphism of $\overline{\mathbb{F}_p}((T))$ that sends $F(T) \in \overline{\mathbb{F}_p}((T))$ in $F((T+1)^{-1} - 1)$ is Ω. □

By the previous lemma to finish the proof of Theorem 1 it suffices to show that $1, T\overline{f((T+1)^{-1} - 1, \chi\omega^0)}, \dots, T\overline{f((T+1)^{-1} - 1, \chi\omega^{p-3})}$ are linearly independent over Ω. Since, always by the previous lemma, for all odd $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$ we have

$$T\overline{f((T+1)^{-1} - 1, \chi\omega^{\delta+1})} = \overline{\Gamma}_\delta\overline{\gamma}_{-\delta}\overline{U}(\overline{\widetilde{F_\chi}}(T))$$

and $\overline{\widetilde{F_\chi}}(T) \in \mathbb{F}_p[[T]]$, to show the linear independence we can easily adapt our proof of Theorem 1 in the case $d \geqslant 2$.

Proof of Theorem 1 in the case $d = 1$. — First observe that by Lemma 5 to prove the assumption it suffices to show that

$$1, T\overline{f((T+1)^{-1} - 1, \chi\omega^0)}, \dots, T\overline{f((T+1)^{-1} - 1, \chi\omega^{p-3})}$$

are linearly independent over Ω. Suppose that this is not the case. Then there exist $h_0(T), \dots, h_{(p-3)/2}(T) \in \Omega$ such that

$$\sum_{j=0}^{(p-3)/2} h_j(T)T\overline{f\left(\frac{1}{T+1} - 1, \omega^{2j}\right)} \in \Omega, \tag{4.2}$$

with $h_j(T) \neq 0$ for a certain j. Observe that without loss of generality we can suppose that $h_j(T) \in A$ for all i and that

$$\sum_{j=0}^{(p-3)/2} h_j(T)T\overline{f\left(\frac{1}{T+1}-1,\omega^{2j}\right)} \in A.$$

By Lemma 5 we get

$$\sum_{j=0}^{(p-3)/2} h_j(T)\overline{\Gamma}_{2j-1}\overline{\gamma}_{-2j+1}\overline{U}(\overline{\widetilde{F_\chi}}(T)) \in A.$$

By Lemma 1(3) and since $\overline{D}\overline{\gamma_\delta} = \overline{\gamma_{\delta+1}}\overline{D}$ for all $\delta \in \mathbb{Z}/(p-1)\mathbb{Z}$, we have

$$\sum_{j=0}^{(p-3)/2} h_j(T)\overline{\Gamma}_{-1}\overline{\gamma}_1\overline{D}^{2j}\overline{U}(\overline{\widetilde{F_\chi}}(T)) \in A.$$

Moreover, applying Lemma 3, we get

$$\sum_{j=0}^{(p-3)/2} \overline{\Gamma}_{-1}\overline{\gamma}_1\overline{D}^{2j}\overline{U}(h_j(t)\overline{\widetilde{F_\chi}}(T)) \in A.$$

From Lemma 1(2) it follows

$$\sum_{j=0}^{(p-3)/2} \overline{\gamma}_1\overline{D}^{2j}\overline{U}(h_j(t)\overline{\widetilde{F_\chi}}(T)) \in A. \tag{4.3}$$

For all j such that $0 \leqslant j \leqslant (p-3)/2$ set

$$F_j(T) = \overline{D}^{2j}\overline{U}(\overline{\widetilde{F_\chi}}(T)).$$

Then we can rewrite (4.3) in the following way:

$$\sum_{j=0}^{(p-3)/2} \overline{\gamma}_1(h_j(t)F_j(T)) \in A. \tag{4.4}$$

By Lemma 2(4) we have

$$F_\chi((T+1)^{-1}-1) = -F_\chi(T) - 1.$$

Then

$$\begin{aligned}\overline{\widetilde{F_\chi}}((T+1)^{-1}-1) &= \overline{F_\chi}((T+1)^{-(p+1)}-1) - \overline{F_\chi}((T+1)^{-1}-1)\\ &= -\overline{F_\chi}((T+1)^{p+1}-1) - 1 + \overline{F_\chi}(T) + 1\\ &= -\overline{\widetilde{F_\chi}}(T).\end{aligned}$$

Moreover observe that for all j between 0 and $(p-3)/2$,

$$(\overline{D}^{2j}\overline{U}(\overline{\widetilde{F_\chi}}))((T+1)^{-1}-1) = \overline{D}^{2j}\overline{U}(\overline{\widetilde{F_\chi}}((T+1)^{-1}-1).$$

Then for all j

$$(\overline{D}^{2j}\overline{U}(\overline{\widetilde{F_\chi}}))((T+1)^{-1}-1) = -\overline{D}^{2j}\overline{U}(\overline{\widetilde{F_\chi}}(T)).$$

It follows that

$$F_j(T) = -F_j((T+1)^{-1}-1) \tag{4.5}$$

for all j.

Consider the smallest field that contains $\mathbb{F}_p$ and all the coefficients of $h_j(T)$ for all j. Since $h_j(T) \in A \subseteq \overline{\mathbb{F}_p}[[T]]$, such field is a finite extension of $\mathbb{F}_p$. Call it $\mathbb{F}_{q_1}$ and write $h_j(t) = \sum_{b\in\mathbb{Z}_p} c_{j,b}(t+1)^b$ with $c_{j,b} \in \mathbb{F}_{q_1}$. Moreover observe that since $h_j(T) \neq 0$ for certain integer j, there exist j, b such that $c_{j,b} \neq 0$. Set

$$G_b(T) = \sum_{j=0}^{(p-3)/2} c_{j,b}F_j(T)$$

and observe that $G_b(T) \in \mathbb{F}_{q_1}[[T]] \cap \mathbb{F}_{q_1}(T)$ for all b. Since

$$(t+1)^b(G_b(T)) = G_b((T+1)^{\kappa_0^b}-1),$$

by (4.4) we have

$$\overline{\gamma}_1\Big(\sum_{b\in\mathbb{Z}_p} G_b((T+1)^{\kappa_0^b}-1)\Big) \in A. \tag{4.6}$$

Choose a subset of μ_{p-1} whose elements represent all the classes of the group $\mu_{p-1}/\{-1,1\}$ and call it S. From (4.5) it follows that

$$G_b(T) = -G_b((T+1)^{-1}-1) \tag{4.7}$$

for all b. Thus by (4.6) we get

$$\sum_{\eta\in S}\sum_{b\in\mathbb{Z}_p} \eta G_b((T+1)^{\eta\kappa_0^b}-1) \in A.$$

Since $G_b(T) = 0$ for all but finitely many $b \in \mathbb{Z}_p$, there exists an integer u such that

$$\sum_{\eta\in S}\sum_{k=1}^{u} \eta G_{b_k}((T+1)^{\eta\kappa_0^{b_k}}-1) \in A.$$

Moreover set $G_k(T) = G_{b_k}(T)$. Since $G_k(T) \in \mathbb{F}_{q_1}[[T]] \cap \mathbb{F}_{q_1}(T)$ for all k, we can apply Proposition 1, obtaining that there exist an integer $l \leqslant u$,

$b_1, b_2, \dots, b_l \in \mathbb{Z}_p$, $b_i \neq b_j$ for $i \neq j$, $\eta_1, \eta_2, \dots, \eta_l \in \mu_{p-1}$ with $\eta_i \kappa_0^{b_i} \sim_{\mathbb{Q}^*} \eta_j \kappa_0^{b_j}$ for all i, j and $\eta_i \kappa_0^{b_i} \neq \eta_j \kappa_0^{b_j}$ for $i \neq j$ such that

$$\sum_{k=1}^{l} \eta_k G_k((T+1)^{\eta_k \kappa_0^{b_k}} - 1) \in A. \tag{4.8}$$

Remark 2. — *We remark that that the fact that for all k, $G_k(T) \in \mathbb{F}_{q_1}[[T]] \cap \mathbb{F}_{q_1}(T)$ is necessary to apply Proposition 1. This relation is verified since for all j, we have $F_j(T) \in \mathbb{F}_p[[T]] \cap \mathbb{F}_p(T)$, which is an immediate consequence of the fact that $\widetilde{F_\chi}(T) \in \mathbb{F}_p[[T]] \cap \mathbb{F}_p(T)$.*

Finally observe that in the case $d \geqslant 2$, for all character χ' of conductor d we have $\overline{F_{\chi'}}(T) \in \mathbb{F}_q[[T]] \cap \mathbb{F}_q(T)$. For this reason it is not necessary "to perturbate" $F_{\chi'}(T)$ to apply Proposition 1.

For all $1 \leqslant k \leqslant l$ write

$$\eta_k \kappa_0^{b_k} = \eta_1 \kappa_0^{b_1} x_k,$$

where $x_k \in \mathbb{Q}^* \cap \mathbb{Z}_p^*$ and $x_i \neq x_k$ if $i \neq k$. Recall that by (4.7), we have $G_k(T) = -G_k((T+1)^{-1} - 1)$. Hence we can suppose that $x_k > 0$ for all k. By (4.6) we get

$$\sum_{k=1}^{l} \eta_k G_k((T+1)^{x_k} - 1) \in A.$$

Therefore there exist some integers $N_1, N_2, \dots, N_l$ not divided by p, such that $1 \leqslant N_1 < N_2 < \ldots < N_l$ and

$$\sum_{k=1}^{l} \eta_k G_k((T+1)^{N_k} - 1) \in A.$$

By definition of $G_k(T)$ this last relation becomes:

$$\sum_{k=1}^{l} \eta_k \sum_{j=0}^{(p-3)/2} c_{j,k} F_j((T+1)^{N_k} - 1) \in A. \tag{4.9}$$

Now we want to compute $F_j(T)$ for all j. First remember that

$$F_\chi(T) = \sum_{a=0}^{p-1} \frac{(T+1)^a}{1-(T+1)^p} - 1.$$

Then

$$\overline{D}^{2j}(\overline{F_\chi}(T)) = \sum_{a=1}^{p-1} \frac{a^{2i}(T+1)^a}{1-(T+1)^p}$$

for all j between 0 and $(p-1)/2$. Since $\overline{U} = \overline{D}^{p-1}$ we have

$$\overline{D}^{2i}\overline{U}(\overline{F_\chi}(T)) = \sum_{a=1}^{p-1} \frac{a^{2i}(T+1)^a}{1-(T+1)^p}.$$

Remember that

$$\overline{\widetilde{F_\chi}}(T) = \overline{F_\chi}((T+1)^{p+1}-1) - \overline{F_\chi}(T) = t\overline{F_\chi}(T).$$

Then

$$\begin{aligned}\overline{D}^{2j}\overline{U}(\overline{\widetilde{F_\chi}}(T)) &= t\overline{D}^{2j}\overline{U}(\overline{F_\chi}(T)) \\ &= t\biggl(\sum_{a=1}^{p-1} \frac{a^{2i}(T+1)^a}{1-(T+1)^p}\biggr) \\ &= \sum_{a=1}^{p-1} \frac{a^{2i}(T+1)^{a(p+1)}}{1-(T+1)^{p(p+1)}} - \sum_{a=1}^{p-1} \frac{a^{2i}(T+1)^a}{1-(T+1)^p}.\end{aligned}$$

Replacing in (4.9) we get

$$\sum_{k=1}^{l} \eta_k \sum_{j=0}^{(p-3)/2} c_{j,k} \sum_{a=1}^{p-1} \biggl(\frac{a^{2j}(T+1)^{aN_k(p+1)}}{1-(T+1)^{pN_k(p+1)}} - \frac{a^{2j}(T+1)^{aN_k}}{1-(T+1)^{pN_k}} \biggr) \in A.$$

Since by [1, Lemma 3.5] a rational function $H(T) \in A$ if and only if there exists an integer n such that $(T+1)^n H(T)$ is a polynomial, we get

$$\begin{aligned}(4.10)\quad &\sum_{k=1}^{l} \eta_k \sum_{j=0}^{(p-3)/2} c_{j,k} \\ &\qquad \sum_{a=1}^{p-1} \biggl(\frac{a^{2j}(T+1)^{aN_k(p+1)}}{1-(T+1)^{pN_k(p+1)}} - \frac{a^{2j}(T+1)^{aN_k}}{1-(T+1)^{pN_k}} \biggr) \in \mathbb{F}_{q_1}[T]\end{aligned}$$

(recall that, by definition, $\mathbb{F}_{q_1}$ is the extension of $\mathbb{F}_p$ generated by $c_{j,k}$ for all j,k).

We apply Remark 1 in the particular case where $F = F_{q_1}$, $V = \mathbb{F}_{q_1}(T)$, $W = \mathbb{F}_{q_1}[T]$, $m = p-1$, $\phi = \overline{D}$, $\lambda_b = b$ for all $1 \leqslant b \leqslant p-1$ and

$$\begin{aligned}v_b &= V_b(T) \\ &:= \sum_{k=1}^{l} \eta_k \sum_{j=0}^{(p-3)/2} c_{j,k} \biggl(\frac{a_{b,k}^{2j}(T+1)^{a_{b,k}N_k(p+1)}}{1-(T+1)^{pN_k(p+1)}} - \frac{a_{b,k}^{2j}(T+1)^{a_{b,k}N_k}}{1-(T+1)^{pN_k}} \biggr),\end{aligned}$$

where $a_{b,k}$ satisfies the relation $a_{b,k}N_k \equiv b \mod (p)$. Then by Remark 1, $V_b(T) \in \mathbb{F}_{q_1}[T]$. Let us recall that p does not divide N_k for all k between 1 and l. Since p does not divide b, we have $a_{b,k} \in \mathbb{F}_p^*$ for all b,k.

Let ζ be a primitive $(p+1)N_l$th root of unity and multiply $V_b(T)$ by the polynomial $1-(T+1)^{p(p+1)N_l}$. We get

$$Q(T)+\eta_l\sum_{j=0}^{(p-3)/2} c_{j,l}a_{b,l}^{2j}(T+1)^{p(p+1)N_l}=P(T), \tag{4.11}$$

where $Q(T)\in\mathbb{F}_{q_1}(T), P(T)\in\mathbb{F}_{q_1}[T]$, $Q(\zeta-1)=0$ (since $N_l>N_k$ for all $k<l$) and $P(\zeta-1)=0$. Then if (4.11) is satisfied we have

$$\eta_l\zeta^{a_bN_l(p+1)}\sum_{j=0}^{(p-3)/2} c_{j,l}a_{b,l}^{2j}=0$$

for all b between 1 and $p-1$. Since $\eta_l\zeta^{a_bN_l(p+1)}=\eta_l\in\mathbb{F}_p^*$, we have

$$\sum_{j=0}^{(p-3)/2} c_{j,l}a_{b,l}^{2j}=0, \tag{4.12}$$

for all b. Observe that, since $1\leqslant b\leqslant p-1$, $a_{b,l}N_l\equiv b \mod (p)$ and p does not divide N_l, for all $c\in\mathbb{F}_p^*$ there exists b such that $a_{b,l}=c$. Then to find the $c_{j,l}$ satisfying (4.12) is equivalent to find all the solutions of the system

$$\sum_{j=0}^{(p-3)/2} x_jk^{2j}=0, \tag{4.13}$$

where x_j are the unknows of the system and $1\leqslant k\leqslant p-1$. Observe that the system (4.13) is identical to the system (3.21) that we have studied at the end of Section 3. Since we have already remarked that (3.21) has only the solution $(0,\dots,0)$, also (4.13) has the unique solution $(0,\dots,0)$. This fact implies $c_{j,l}=0$ for all j.

Since $N_{l-1}>N_k$ for all $k<l-1$, if we replace l with $l-1$ with the same procedure we can prove that the coefficients $c_{j,l-1}=0$ for all j and so on. Thus $c_{j,k}=0$ for all j,k, which implies $h_j(T)=0$ for all j. Since we have supposed that there exists j such that $h_j(T)\neq 0$, we obtain a contradiction.

BIBLIOGRAPHY

[1] B. Anglès, "On the p-adic Leopoldt transform of a power series", *Acta Arith.* **134** (2008), no. 4, p. 349-367.

[2] S. Lang, *Cyclotomic fields I and II*, second ed., Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990, With an appendix by Karl Rubin, xviii+433 pages.

[3] W. SINNOTT, "On the power series attached to p-adic L-functions", *J. Reine Angew. Math.* **382** (1987), p. 22-34.

[4] L. C. WASHINGTON, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997, xiv+487 pages.

Manuscrit reçu le 21 avril 2009,
accepté le 25 août 2009.

Bruno ANGLÈS
Université de Caen
Laboratoire de mathématiques Nicolas Oresme
CNRS UMR 6139
BP 5186
14032 Caen cedex (France)
bruno.angles@math.unicaen.fr

Gabriele RANIERI
Universität Basel
Departement Matematik
Rheinsprung 21
CH-4051 Basel (Switzerland)
gabriele.ranieri@unibas.ch