ACTA ARITHMETICA
142.3 (2010)

On Jacobi sums in $\mathbb{Q}(\zeta_p)$

by

Bruno Anglès (Caen) and Filippo A. E. Nuccio (Roma)

Let p be a prime number, $p \geq 5$. Iwasawa has shown that the p-adic properties of Jacobi sums for $\mathbb{Q}(\zeta_p)$ are linked to Vandiver's Conjecture (see [5]). In this paper, we follow Iwasawa's ideas and study the p-adic properties of the subgroup J of $\mathbb{Q}(\zeta_p)^*$ generated by Jacobi sums.

Let A be the p-Sylow subgroup of the class group of $\mathbb{Q}(\zeta_p)$. If E denotes the group of units of $\mathbb{Q}(\zeta_p)$, then if Vandiver's Conjecture is true for p, by Kummer theory and class field theory, there is a canonical surjective map

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)(\sqrt[p]{E})/\mathbb{Q}(\zeta_p)) \to A^-/pA^-.$$

Note that J is, for the "minus" part, the analogue of the group of cyclotomic units. We introduce a submodule W of $\mathbb{Q}(\zeta_p)^*$ which was already considered by Iwasawa [6]. This module can be thought of, for the minus part, as the analogue of the group of units. We observe that $J \subset W$ and if the Iwasawa–Leopoldt Conjecture is true for p then $W(\mathbb{Q}(\zeta_p)^*)^p = J(\mathbb{Q}(\zeta_p)^*)^p$. We prove that if $pA^- = \{0\}$ then (Corollary 4.8) there is a canonical surjective map

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)(\sqrt[p]{W})/\mathbb{Q}(\zeta_p)) \to A^+/pA^+.$$

The last part of our paper is devoted to the study of the jacobian of the Fermat curve $X^p + Y^p = 1$ over $\mathbb{F}_\ell$ where ℓ is a prime number, $\ell \neq p$. It is well-known that Jacobi sums play an important role in the study of that jacobian. Following ideas developed by Greenberg [4], we prove that Vandiver's Conjecture is equivalent to some properties of that jacobian (for a precise statement see Corollary 5.3).

1. Notations. Let p be a prime number, $p \geq 5$. Let $\zeta_p \in \mu_p \setminus \{1\}$, and let $L = \mathbb{Q}(\zeta_p)$. Set $\mathcal{O} = \mathbb{Z}[\zeta_p]$ and $E = \mathcal{O}^*$. Let $\Delta = \mathrm{Gal}(L/\mathbb{Q})$ and let $\widehat{\Delta} = \mathrm{Hom}(\Delta, \mathbb{Z}_p^*)$. Let $\mathcal{I}$ be the group of fractional ideals of L which are

2010 *Mathematics Subject Classification*: 11R18, 11R29, 11R23.
Key words and phrases: Jacobi sums, ideal class group, Iwasawa theory, Vandiver's conjecture.

DOI: 10.4064/aa142-3-1

prime to p, and let $\mathcal{P}$ be the group of principal ideals in $\mathcal{I}$. Let A be the p-Sylow subgroup of the ideal class group of L.

Set $\pi = \zeta_p - 1$, $K = \mathbb{Q}_p(\zeta_p)$, $U = 1 + \pi^2\mathbb{Z}_p[\zeta_p]$. Observe that if $\mathcal{A} \in \mathcal{P}$, then there exists $\alpha \in L^* \cap U$ such that $\mathcal{A} = \alpha\mathcal{O}$. If H is a subgroup of U, we will denote the closure of H in U by $\overline{H}$. Let $\omega \in \widehat{\Delta}$ be the Teichmüller character, i.e.

$$\forall \sigma \in \Delta, \quad \sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}.$$

For $\rho \in \widehat{\Delta}$, we set

$$e_\rho = \frac{1}{p-1} \sum_{\delta \in \Delta} \rho^{-1}(\delta)\delta \in \mathbb{Z}_p[\Delta].$$

If M is a $\mathbb{Z}_p[\Delta]$-module, for $\rho \in \widehat{\Delta}$, we set

$$M(\rho) = e_\rho M.$$

For $\psi \in \widehat{\Delta}$, ψ odd, recall that

$$B_{1,\psi} = \frac{1}{p} \sum_{a=1}^{p-1} a\psi(a).$$

Set

$$\theta = \frac{1}{p} \sum_{a=1}^{p-1} a\sigma_a^{-1} \in \mathbb{Q}[\Delta],$$

where $\sigma_a \in \Delta$ is such that $\sigma_a(\zeta_p) = \zeta_p^a$. Observe that we have the following equality in $\mathbb{C}[\Delta]$:

$$\theta = \frac{N}{2} + \sum_{\psi \in \widehat{\Delta},\, \psi \text{ odd}} B_{1,\psi^{-1}} e_\psi,$$

where $N = \sum_{\delta \in \Delta} \delta$.

If M is a $\mathbb{Z}[\Delta]$-module, we set

$$M^- = \{m \in M : \sigma_{-1}(m) = -m\}, \quad M^+ = \{m \in M : \sigma_{-1}(m) = m\}.$$

If M is an abelian group of finite type, we set

$$M[p] = \{m \in M : pm = 0\}, \quad d_p M = \dim_{\mathbb{F}_p} M/pM.$$

2. Background on Jacobi sums. Let $Cl(L)$ be the ideal class group of L. Then $Cl(L) \simeq \mathcal{I}/\mathcal{P}$. Note that we have a natural $\mathbb{Z}[\Delta]$-morphism (see [6, pp. 102–103])

$$\phi : (\mathrm{Ann}_{\mathbb{Z}[\Delta]} Cl(L))^- \to \mathrm{Hom}_{\mathbb{Z}[\Delta]}(Cl(L), E^+/(E^+)^2).$$

For the convenience of the reader, we recall the construction of ϕ. Let $x \in (\mathrm{Ann}_{\mathbb{Z}[\Delta]} Cl(L))^-$ and $\mathcal{A} \in \mathcal{I}$. We have $\mathcal{A}^x = \gamma_a \mathcal{O}$, where $\gamma_a \in L^* \cap U$. Now,

$$\overline{\gamma_a} = \varepsilon_a \gamma_a^{-1}$$

for some $\varepsilon_a \in E^+ \cap U$. One can prove that we obtain a well-defined morphism of $\mathbb{Z}[\Delta]$-modules $\phi(x) : Cl(L) \to E^+/(E^+)^2$, class of $\mathcal{A} \mapsto$ class of ε_a. In this section, we will study the kernel of the morphism ϕ.

Let $\mathcal{W}$ be the set of elements $f \in \mathrm{Hom}_{\mathbb{Z}[\Delta]}(\mathcal{I}, L^*)$ such that:

- $f(\mathcal{I}) \subset U$,
- there exists $\beta(f) \in \mathbb{Z}[\Delta]$ such that $f(\alpha\mathcal{O}) = \alpha^{\beta(f)}$ for all $\alpha \in L^* \cap U$.

One can prove that if $f \in \mathcal{W}$ then $\beta(f)$ is unique, the map $\beta : \mathcal{W} \to \mathbb{Z}[\Delta]$ is an injective $\mathbb{Z}[\Delta]$-morphism and $\beta(\mathcal{W}) \subset \mathrm{Ann}_{\mathbb{Z}[\Delta]}(Cl(L))$ (see [2]). If $\mathcal{B}$ denotes the group of Hecke characters of type (A_0) that have values in $\mathbb{Q}(\zeta_p)$ (see [6]), then one can prove that $\mathcal{B}$ is isomorphic to $\mathcal{W}$.

LEMMA 2.1. $\mathrm{Ker}\,\phi = \beta(\mathcal{W}^-)$.

Proof. We just prove the inclusion $\mathrm{Ker}\,\phi \subset \beta(\mathcal{W}^-)$. Let $x \in \mathrm{Ker}\,\phi$. Let $\mathcal{A} \in \mathcal{I}$. Then there exists a unique $\gamma_a \in L^* \cap U$ such that $\overline{\gamma_a}\gamma_a = 1$ and

$$\mathcal{A}^x = \gamma_a\mathcal{O}.$$

Let $f : \mathcal{I} \to L^*$, $\mathcal{A} \mapsto \gamma_a$. It is not difficult to see that $f \in \mathrm{Hom}_{\mathbb{Z}[\Delta]}(\mathcal{I}, L^*)$ and $f(\mathcal{I}) \subset U$. Now, if $\alpha \in L^* \cap U$, we have

$$f(\alpha\mathcal{O}) = \alpha^x u$$

for some $u \in E$. Since $x \in \mathbb{Z}[\Delta]^-$ and $\alpha, f(\alpha\mathcal{O}) \in U$, we must have $u = 1$. Therefore $f \in \mathcal{W}^-$ and $x = \beta(f)$. ∎

Now, we recall some basic properties of Gauss and Jacobi sums (we refer the reader to [12, Sec. 6.1]).

Let P be a prime ideal in $\mathcal{I}$ and let ℓ be the prime number such that $\ell \in P$. We fix $\zeta_\ell \in \mu_\ell \setminus \{1\}$. Set $\mathbb{F}_P = \mathcal{O}/P$. Let $\chi_P : \mathbb{F}_P^* \to \mu_p$ be such that

$$\forall \alpha \in \mathbb{F}_P^*, \quad \chi_P(\alpha) \equiv \alpha^{(1-NP)/p} \pmod{P},$$

where $NP = |\mathcal{O}/P|$. For $a \in \mathbb{Z}/p\mathbb{Z}$, we set

$$\tau_a(P) = -\sum_{\alpha \in \mathbb{F}_P} \chi_P^a(\alpha)\zeta_\ell^{\mathrm{Tr}_{\mathbb{F}_P/\mathbb{F}_\ell}(\alpha)}.$$

We also set $\tau(P) = \tau_1(P)$. For $a, b \in \mathbb{Z}/p\mathbb{Z}$, we set

$$j_{a,b}(P) = -\sum_{\alpha \in \mathbb{F}_P} \chi_P^a(\alpha)\chi_P^b(1-\alpha).$$

Then:

- if $a + b \equiv 0 \pmod{p}$, we have:
  - (i) if $a \not\equiv 0 \pmod{p}$, then $j_{a,b}(P) = 1$,
  - (ii) if $a \equiv 0 \pmod{p}$, then $j_{a,b}(P) = 2 - NP$,

- if $a+b \not\equiv 0 \pmod p$, we have

$$j_{a,b}(P) = \frac{\tau_a(P)\tau_b(P)}{\tau_{a+b}(P)}.$$

Observe that $\tau(P) \equiv 1 \pmod \pi$, and therefore (see [5, Theorem 1])

$$\forall a, b \in \mathbb{Z}/p\mathbb{Z}, \quad j_{a,b}(P) \in U.$$

Let Ω be the compositum of the fields $\mathbb{Q}(\zeta_\ell)$ where ℓ runs through the prime numbers distinct from p. The map $P \mapsto \tau(P)$ induces by linearity a $\mathbb{Z}[\Delta]$-morphism

$$\tau : \mathcal{I} \to \Omega(\zeta_p)^*.$$

Let $\mathcal{G}$ be the $\mathbb{Z}[\Delta]$-submodule of $\mathrm{Hom}_{\mathbb{Z}[\Delta]}(\mathcal{I}, \Omega(\zeta_p)^*)$ generated by τ. We set

$$\mathcal{J} = \mathcal{G} \cap \mathrm{Hom}_{\mathbb{Z}[\Delta]}(\mathcal{I}, L^*).$$

Let $\mathcal{S}$ be the Stickelberger ideal of L, i.e. $\mathcal{S} = \mathbb{Z}[\Delta]\theta \cap \mathbb{Z}[\Delta]$. Then one can prove the following facts (see [2]):

- $\mathcal{J} \subset \mathcal{W}$,
- the map $\beta : \mathcal{W} \to \mathbb{Z}[\Delta]$ induces an isomorphism $\mathcal{J} \simeq \mathcal{S}$ of $\mathbb{Z}[\Delta]$-modules.

LEMMA 2.2. *Let $\mathcal{N} \in \mathrm{Hom}_{\mathbb{Z}[\Delta]}(I_L, L^*)$ be the ideal norm map. Then, as a $\mathbb{Z}$-module,*

$$\mathcal{J} = \mathcal{N}\mathbb{Z} \oplus \bigoplus_{n=1}^{(p-1)/2} j_{1,n}\mathbb{Z}.$$

Proof. Recall that, for $1 \le n \le p-2$ and a prime P in $\mathcal{I}$, we have

$$j_{1,n}(P) = -\sum_{\alpha \in \mathbb{F}_P} \chi_P(\alpha)\chi_P^n(1-\alpha) = \frac{\tau(P)\tau_n(P)}{\tau_{n+1}(P)}.$$

Thus, for $1 \le n \le p-2$,

$$j_{1,n} = \tau^{1+\sigma_n - \sigma_{1+n}} = \frac{\tau\tau_n}{\tau_{n+1}},$$

where $\tau^{\sigma_a} = \tau_a$ for $a \in \mathbb{F}_p^*$. Observe that

$$\forall a \in \mathbb{F}_p^*, \quad \tau_a\tau_{-a} = \mathcal{N}.$$

Thus $\mathcal{N} \in \mathcal{J}$. Since $\mathcal{J} \simeq \mathcal{S}$, $\mathcal{J}$ is a $\mathbb{Z}$-module of rank $(p+1)/2$. It is not difficult to show that (see [5, Lemma 2])

$$\mathcal{J} = \tau^p\mathbb{Z} \oplus \bigoplus_{a=1}^{(p-1)/2} \tau_{-a}\tau^a\mathbb{Z}.$$

Observe also that, for $2 \le n \le p-2$, we have

$$j_{1,p-n} = j_{1,n-1}.$$

Let V be the $\mathbb{Z}$-submodule of $\mathcal{J}$ generated by $\mathcal{N}$ and the $j_{1,n}$, $1 \le n \le (p-1)/2$. Then $j_{1,n} \in V$ for $1 \le n \le p-2$. Furthermore,

$$\prod_{n=1}^{p-2} j_{1,n} = \frac{\tau^p}{\mathcal{N}}.$$

Therefore $\tau^p \in V$. Since $\tau_{-1}\tau^1 = \mathcal{N}$, $\tau_{-1}\tau^1 \in V$. Now, let $2 \le r \le (p-1)/2$ and assume that we have proved that $\tau_{-(r-1)}\tau^{r-1} \in V$. We have

$$j_{1,r-1} = \frac{\tau\tau_{r-1}}{\tau_r} = \frac{\mathcal{N}\tau\tau_{1-r}^{-1}}{\mathcal{N}\tau_{-r}^{-1}}.$$

Thus

$$\tau_{-r} = j_{1,r-1}^{-1}\tau_{1-r}\tau^{-1} \quad \text{and} \quad \tau_{-r}\tau^r = j_{1,r-1}^{-1}\tau_{-(r-1)}\tau^{r-1}.$$

Hence $\tau_{-r}\tau^r \in V$ and the lemma follows. ∎

LEMMA 2.3. *Let ℓ be a prime number, $\ell \ne p$. Let P be a prime ideal of $\mathcal{O}$ above ℓ and let $a \in \{1, \ldots, p-2\}$. Then $\mathbb{Q}(j_{1,a}(P)) = L$ if and only if $\ell \equiv 1 \pmod p$ and $a^2 + a + 1 \not\equiv 0 \pmod p$ if $p \equiv 1 \pmod 3$.*

Proof. Since $j_{1,a}(P) \equiv 1 \pmod{\pi^2}$ and $j_{1,a}(P)j_{1,a}(P)^{\sigma_{-1}} = \ell^f$ where f is the order of ℓ in $(\mathbb{Z}/p\mathbb{Z})^*$, we have

$$\forall \sigma \in \Delta, \quad j_{1,a}(P)^\sigma = j_{1,a}(P) \ \Leftrightarrow\ j_{1,a}(P)^\sigma\mathcal{O} = j_{1,a}(P)\mathcal{O}.$$

Recall that

$$\forall \sigma \in \Delta, \quad j_{1,a}(P)^\sigma\mathcal{O} = j_{1,a}(P)\mathcal{O} \ \Leftrightarrow\ P^{(\sigma-1)(1+\sigma_a-\sigma_{1+a})\theta} = \mathcal{O}.$$

Since $j_{1,a}(P)^{\sigma_\ell} = j_{1,a}(P)$, we can assume $\ell \equiv 1 \pmod p$. Let $\sigma \in \Delta$. We have to consider the following equation in $\mathbb{C}[\Delta]$:

$$(\sigma - 1)(1 + \sigma_a - \sigma_{1+a})\theta = 0.$$

This is equivalent to

$$\forall \psi \in \widehat{\Delta},\ \psi \text{ odd}, \quad (\psi(\sigma) - 1)(1 + \psi(a) - \psi(1+a)) = 0.$$

Assume that $\omega^3(\sigma) \ne 1$. Then

$$1 + \omega^3(a) - \omega^3(1+a) = 0.$$

This implies $a^2 + a \equiv 0 \pmod p$, which is a contradiction. Thus $\omega^3(\sigma) = 1$. Suppose that $\sigma \ne 1$. We get $1 + \omega(a) = \omega(1+a)$, which is equivalent to

$$a^2 + a + 1 \equiv 0 \pmod p.$$

Conversely, one can see that if $p \equiv 1 \pmod 3$, $a^2 + a + 1 \equiv 0 \pmod p$, and $\omega^3(\sigma) = 1$, then

$$\forall \psi \in \widehat{\Delta},\ \psi \text{ odd}, \quad (\psi(\sigma) - 1)(1 + \psi(a) - \psi(1+a)) = 0.$$

The lemma follows. ∎

For $x \in \mathbb{Z}_p$, let $[x] \in \{0, \dots, p-1\}$ be such that $x \equiv [x] \pmod p$. We set

$$\eta = \Big(\prod_{n=1}^{p-2} j_{1,n}^{[n^{-1}]}\Big)^{1-\sigma_{-1}} \in \mathcal{J}^-.$$

LEMMA 2.4.

(a) *Let $\psi \in \widehat{\Delta}$, $\psi \neq \omega$, ψ odd. Then*

$$e_\psi\Big(\sum_{n=1}^{p-2}(1+\sigma_n - \sigma_{1+n})[n^{-1}]\Big) \in \mathbb{Z}_p^* e_\psi.$$

(b) *We have*

$$\frac{1}{p}\, e_\omega\Big(\sum_{n=1}^{p-2}(1+\sigma_n - \sigma_{1+n})[n^{-1}]\Big) \in \mathbb{Z}_p^* e_\omega.$$

Proof. (a) Write $\psi = \omega^k$, k odd, $k \in \{3, \dots, p-2\}$. We have

$$\sum_{n=2}^{p-2}(1+\psi(n) - \psi(1+n))[n^{-1}] \equiv \sum_{n=1}^{p-1} \frac{1+n^k - (1+n)^k}{n} \equiv k \pmod p.$$

This implies (a).

(b) We have

$$\forall a \in \mathbb{F}_p^*, \qquad \omega(a) \equiv a^p \pmod{p^2}.$$

Thus

$$\frac{1}{p}\sum_{n=1}^{p-2}(1+\omega(n) - \omega(1+n))[n^{-1}] \equiv -\sum_{n=1}^{p-1}\sum_{k=1}^{p-1} \frac{p!}{(p-k)!k!p}\, n^{k-1} \pmod p,$$

and we get

$$\frac{1}{p}\sum_{n=1}^{p-2}(1+\omega(n) - \omega(1+n))[n^{-1}] \equiv -1 \pmod p.$$

This implies (b). ∎

LEMMA 2.5. *Let ℓ be a prime number, $\ell \neq p$. Let V_ℓ be the $\mathbb{Z}[\Delta]$-submodule of $L^*/(L^*)^p$ generated by $\{f(P) : f \in \mathcal{J}\}$ where P is some prime of $\mathcal{I}$ above ℓ. Let $\psi \in \widehat{\Delta}$, ψ odd and $\psi \neq \omega$. Then*

$$V_\ell(\psi) = \mathbb{F}_p e_\psi \eta(P).$$

Proof. Let $E = L(\zeta_\ell)$. Then

$$\frac{L^*}{(L^*)^p}(\psi) \hookrightarrow \frac{E^*}{(E^*)^p}(\psi).$$

Now, in $\frac{E^*}{(E^*)^p}(\psi)$, we have $V_\ell(\psi) = \mathbb{F}_p e_\psi \tau(P)$. It remains to apply Lemma 2.4. ∎

Finally, we record the following lemma:

LEMMA 2.6. *We have*

$$(\mathcal{J}^- : \mathbb{Z}[\Delta]\eta) = 2^{(p-3)/2}\,\frac{1}{p}\prod_{\psi\in\widehat{\Delta},\,\psi\ odd}\Big(\sum_{n=1}^{p-2}(1+\psi(n)-\psi(1+n))[n^{-1}]\Big).$$

Furthermore $(\mathcal{J}^- : \mathbb{Z}[\Delta]\eta) \not\equiv 0 \pmod p$.

Proof. Set $\widetilde{\mathcal{J}}^- = (1-\sigma_{-1})\mathcal{J} \subset \mathcal{J}^-$. Then (see [12, Sec. 6.4]):

$$(\mathcal{J}^- : \widetilde{\mathcal{J}}^-) = 2^{(p-3)/2}.$$

Now, by the same kind of argument as in [12, Sec. 6.4], we get

$$(\widetilde{\mathcal{J}}^- : \mathbb{Z}[\Delta]\eta) = \frac{1}{p}\prod_{\psi\in\widehat{\Delta},\,\psi\ \mathrm{odd}}\Big(\sum_{n=1}^{p-2}(1+\psi(n)-\psi(1+n))[n^{-1}]\Big).$$

It remains to apply Lemma 2.4 to conclude the proof. ∎

3. Jacobi sums and the ideal class group of $\mathbb{Q}(\zeta_p)$. Recall that the Iwasawa–Leopoldt Conjecture ([9, p. 258]) asserts that A is a cyclic $\mathbb{Z}_p[\Delta]$-module. This conjecture is equivalent to:

$$\forall\psi\in\widehat{\Delta},\ \psi\ \mathrm{odd},\ \psi\neq\omega,\qquad A(\psi)\simeq\mathbb{Z}_p/B_{1,\psi^{-1}}\mathbb{Z}_p.$$

It is well-known (see [12, Theorem 10.9]) that

$$\forall\psi\in\widehat{\Delta},\ \psi\ \mathrm{odd},\ \psi\neq\omega,\qquad A(\omega\psi^{-1})=\{0\}\ \Rightarrow\ A(\psi)\simeq\mathbb{Z}_p/B_{1,\psi^{-1}}\mathbb{Z}_p.$$

In this section, we will study the links between Jacobi sums and the structure of A^-.

We fix $\psi\in\widehat{\Delta}$, ψ odd and $\psi\neq\omega$. We set

$$m(\psi)=v_p(B_{1,\psi^{-1}}).$$

Recall that, by [12, Sec. 13.6], we have $|A(\psi)| = p^{m(\psi)}$. Let $p^{k(\psi)}$ be the exponent of the group $A(\psi)$. Then

$$B_{1,\psi^{-1}}\equiv 0 \pmod{p^{k(\psi)}}.$$

LEMMA 3.1. *Let P be a prime ideal in $\mathcal{I}$ above a prime number ℓ. Then*

$$e_\psi\eta(P)\mathcal{O}=0\ \mathit{in}\ \mathcal{I}/\mathcal{I}^p\ \Leftrightarrow\ \psi(\ell)\neq 1\ \mathit{or}\ B_{1,\psi^{-1}}\equiv 0 \pmod p.$$

Proof. First note that, if $\rho\in\widehat{\Delta}$, then $e_\rho P = 0$ in $\mathcal{I}/\mathcal{I}^p$ if and only if $\rho(\ell)\neq 1$. By the Stickelberger Theorem, we have

$$\eta(P)\mathcal{O}=\Big(\sum_{n=1}^{p-2}(1+\sigma_n-\sigma_{1+n})[n^{-1}]\Big)(1-\sigma_{-1})\theta P.$$

Recall that $e_\psi\theta = B_{1,\psi^{-1}}e_\psi$. The lemma follows. ∎

Lemma 3.2. *Let $f \in \mathcal{W}^-$. Then f lies in $\mathcal{W}^p$ if and only if $f(P) \in (L^*)^p$ for all prime ideals $P \in \mathcal{I}$.*

Proof. Let $f \in \mathcal{W}^-$ be such that $f(P) \in (L^*)^p$ for all prime ideals $P \in \mathcal{I}$. Let $\mathcal{A} \in \mathcal{I}$. Then there exists $\gamma_a \in L^* \cap U$ such that $\gamma_a \overline{\gamma_a} = 1$ and $f(\mathcal{A}) = \gamma_a^p$. Observe that $\beta(f) \in p(\mathbb{Z}[\Delta])^-$. Let $g : \mathcal{I} \to L^*$, $\mathcal{A} \mapsto \gamma_a$. Then one can verify that $f = g^p$ and $g \in \mathcal{W}^-$. ∎

Let $m \geq 1$ be such that $p^m > |A|$. Set $n = |Cl(L)|/|A|$. Let $e_m(\psi) \in \mathbb{Z}[\Delta]^-$ be such that

$$e_m(\psi) \equiv e_\psi \pmod{p^m}.$$

Set

$$\beta_\psi = 2np^{k(\psi)} e_m(\psi) \in \mathbb{Z}[\Delta]^-.$$

Since $np^{k(\psi)} e_m(\psi) \in (\mathrm{Ann}_{\mathbb{Z}[\Delta]} Cl(L))^-$, by Lemma 2.1 there exists a unique element $f_\psi \in \mathcal{W}^-$ such that $\beta(f_\psi) = \beta_\psi$. Recall that

$$(\mathrm{Ann}_{\mathbb{Z}_p[\Delta]} A)(\psi) = p^{k(\psi)} \mathbb{Z}_p e_\psi.$$

Therefore, for $0 \leq k \leq m$, $\frac{\mathcal{W}^-}{(\mathcal{W}^-)^{p^k}}(\psi)$ is cyclic of order p^k generated by the image of f_ψ. We set

$$W = \{f(\mathcal{A}) : \mathcal{A} \in \mathcal{I},\, f \in \mathcal{W}\}, \qquad J = \{f(\mathcal{A}) : \mathcal{A} \in \mathcal{I}, f \in \mathcal{J}\}.$$

Observe that J is a $\mathbb{Z}[\Delta]$-submodule of W, and it is called the *module of Jacobi sums* of $\mathbb{Q}(\zeta_p)$. Note that, by Lemma 3.2 and the fact that $\frac{\mathcal{W}}{\mathcal{W}^p}(\psi) \neq \{0\}$ (recall that ψ is odd and $\psi \neq \omega$), we have

$$\frac{W(L^*)^p}{(L^*)^p}(\psi) \neq \{0\}.$$

Theorem 3.3. *The map f_ψ induces an isomorphism of groups*

$$A(\psi) \simeq \frac{W(L^*)^{p^{k(\psi)}}}{(L^*)^{p^{k(\psi)}}}(\psi).$$

Proof. First observe that $m \geq k(\psi) + 1$. Let P be a prime in $\mathcal{I}$. Then

$$f_\psi(P)\mathcal{O} = P^{\beta_\psi}.$$

Let $\rho \in \widehat{\Delta}$, $\rho \neq \psi$. Then

$$e_m(\rho) e_m(\psi) \equiv 0 \pmod{p^m}.$$

Therefore, there exists $\gamma \in L^* \cap U$ such that:

$$P^{(1-\sigma_{-1}) n e_m(\rho) e_m(\psi)} = \left(\frac{\gamma}{\sigma_{-1}(\gamma)}\right)^p \mathcal{O}.$$

But $(1 - \sigma_{-1}) e_m(\psi) = 2e_m(\psi)$. Thus, there exists $\alpha \in L^* \cap U$, $\alpha\sigma_{-1}(\alpha) = 1$, and

$$f_\psi(P)^{e_m(\rho)} = \alpha^{p^{k(\psi)+1}}.$$

Therefore, $e_\rho f_\psi(\mathcal{I}) = 0$ in $L^*/(L^*)^{p^{k(\psi)+1}}$. It is clear that f_ψ induces a morphism

$$\frac{\mathcal{I}}{(\mathcal{I})^{p^m}\mathcal{P}}(\psi) \to \frac{L^*}{(L^*)^{p^{k(\psi)}}}(\psi).$$

Now, let P be a prime in $\mathcal{I}$ such that $e_\psi f_\psi(P) = 0$ in $\frac{L^*}{(L^*)^{p^{k(\psi)}}}(\psi)$. Then, by the above remark, we get $f_\psi(P) = 0$ in $L^*/(L^*)^{p^{k(\psi)}}$. Thus, there exists $\gamma \in L^* \cap U$ such that

$$P^{\beta_\psi} = \gamma^{p^{k(\psi)}}\mathcal{O}.$$

Thus $P^{2ne_m(\psi)} = \gamma\mathcal{O}$. This implies

$$e_\psi P = 0 \quad \text{in } \frac{\mathcal{I}}{(\mathcal{I})^{p^m}\mathcal{P}}(\psi).$$

Thus our map is injective. Now, observe that the image of the map induced by f_ψ is $\frac{W(L^*)^{p^{k(\psi)}}}{(L^*)^{p^{k(\psi)}}}(\psi)$ and that $A(\psi) \simeq \frac{\mathcal{I}}{(\mathcal{I})^{p^m}\mathcal{P}}(\psi)$. The theorem follows. ∎

Recall that

$$\eta = \Big(\prod_{n=1}^{p-2} j_{1,n}^{[n^{-1}]}\Big)^{1-\sigma_{-1}} \in \mathcal{J}^-.$$

Set

$$z = (1-\sigma_{-1})\sum_{n=1}^{p-2}(1+\sigma_n - \sigma_{1+n})[n^{-1}] \in \mathbb{Z}[\Delta]^-.$$

We have $\beta(\eta) = z\theta$.

COROLLARY 3.4.

(1) *The map* η *induces an isomorphism of groups*

$$A(\psi) \simeq \frac{J(L^*)^{p^{m(\psi)}}}{(L^*)^{p^{m(\psi)}}}(\psi).$$

(2) $\frac{J(L^*)^p}{(L^*)^p}(\psi) \neq \{0\}$ *if and only if* $A(\psi)$ *is* $\mathbb{Z}_p$*-cyclic.*

Proof. (1) Let P be a prime in $\mathcal{I}$. Then one can show that

$$f_\psi(P)^{z\theta} = \eta(P)^{2np^{k(\psi)}e_m(\psi)}.$$

The first assertion follows from Theorem 3.3.

(2) Note that $A(\psi)$ is $\mathbb{Z}_p$-cyclic $\Leftrightarrow m(\psi) = k(\psi)$. Thus, if $A(\psi)$ is $\mathbb{Z}_p$-cyclic, then

$$\frac{J(L^*)^p}{(L^*)^p}(\psi) = \frac{W(L^*)^p}{(L^*)^p}(\psi) \neq \{0\}.$$

By the proof of (1), if $k(\psi) < m(\psi)$ and if P is a prime in $\mathcal{I}$, then $\eta(P)^{e_m(\psi)} \in (L^*)^p$. Therefore, we get (2). ∎

4. The p-adic behavior of Jacobi sums. Let M be a subgroup of $L^*/(L^*)^p$. We say that M is *unramified* if $L(\sqrt[p]{M})/L$ is an unramified extension. Note that Kummer's Lemma asserts that ([12, Theorem 5.36])

$$\forall \rho \in \widehat{\Delta},\ \rho \text{ even},\ \rho \neq 1, \qquad \frac{E}{E^p}(\rho) \text{ is unramified } \Rightarrow B_{1,\rho\omega^{-1}} \equiv 0 \pmod{p}.$$

It is natural to ask if this implication is in fact an equivalence (see [1], [3]). We will say that the *converse of Kummer's Lemma is true* for the character ρ if

$$\frac{E}{E^p}(\rho) \text{ is unramified } \Leftrightarrow\ B_{1,\rho\omega^{-1}} \equiv 0 \pmod{p}.$$

In this section, we will study this question with the help of Jacobi sums.

Let F/L be the maximal abelian p-extension of L which is unramified outside p. Set $\mathcal{X} = \mathrm{Gal}(F/L)$. We have an exact sequence of $\mathbb{Z}_p[\Delta]$-modules ([12, Corollary 13.6])

$$0 \to U/\overline{E} \to \mathcal{X} \to A \to 0.$$

Let $\rho \in \widehat{\Delta}$ and observe that:

- if $\rho = 1, \omega$ then $\mathcal{X}(\rho) \simeq \mathbb{Z}_p$,
- if ρ is even, $\rho \neq 1$, then $\mathcal{X}(\rho) \simeq \mathrm{Tor}_{\mathbb{Z}_p} \mathcal{X}(\rho)$,
- if ρ is odd, $\rho \neq \omega$, then $\mathcal{X}(\rho) \simeq \mathbb{Z}_p \oplus \mathrm{Tor}_{\mathbb{Z}_p} \mathcal{X}(\rho)$.

LEMMA 4.1. *Let $\psi \in \widehat{\Delta}$, ψ odd, $\psi \neq \omega$. Then*

$$d_p \, \mathrm{Tor}_{\mathbb{Z}_p} \mathcal{X}(\psi) = d_p A(\omega\psi^{-1}).$$

Proof. This is a consequence of the proof of Leopoldt's reflection theorem ([12, Theorem 10.9]). For the convenience of the reader, we give the proof.

Let H be the Galois group of the maximal abelian extension of L which is unramified outside p and of exponent p. Then H is a $\mathbb{Z}_p[\Delta]$-module and we have:

- $H(1) \simeq \mathbb{F}_p$ and corresponds to $L(\zeta_{p^2})/L$,
- $H(\omega) \simeq \mathbb{F}_p$ and corresponds to $L(\sqrt[p]{p})/L$,
- if ρ is even, $\rho \neq 1$, then $d_p H(\rho) = d_p \mathrm{Tor}_{\mathbb{Z}_p} \mathcal{X}(\rho)$,
- if ρ is odd, $\rho \neq \omega$, then $d_p H(\rho) = 1 + d_p \mathrm{Tor}_{\mathbb{Z}_p} \mathcal{X}(\rho)$.

Let V be the $\mathbb{Z}[\Delta]$-submodule of $L^*/(L^*)^p$ which corresponds to H, i.e. $H = \mathrm{Gal}(L(\sqrt[p]{V})/L)$. Let M be the $\mathbb{Z}[\Delta]$-submodule of $L^*/(L^*)^p$ generated by E and $1 - \zeta_p$. We have an exact sequence

$$0 \to M \to V \to A[p] \to 0.$$

Let $\psi \in \widehat{\Delta}$, ψ odd, $\psi \neq \omega$. By Kummer theory we have

$$1 + d_p \, \mathrm{Tor}_{\mathbb{Z}_p} \mathcal{X}(\psi) = d_p V(\omega\psi^{-1}),$$

and, by the above exact sequence,

$$d_pV(\omega\psi^{-1}) = 1 + d_pA(\omega\psi^{-1}).$$

The lemma follows. ∎

LEMMA 4.2. *Let* $\rho \in \widehat{\Delta}$, ρ *even and* $\rho \neq 1$. *If* $\frac{E}{E^p}(\rho)$ *is ramified then* $d_pA(\rho) = d_pA(\omega\rho^{-1})$.

Proof. We keep the notations of the proof of Lemma 4.1. Let $V^{\mathrm{unr}} \subset V$ correspond via Kummer theory to A/pA. Then

$$V^{\mathrm{unr}}(\rho) \simeq \frac{A}{pA}(\omega\rho^{-1}).$$

But $\frac{E}{E^p}(\rho)$ is ramified if and only if $V^{\mathrm{unr}}(\rho) \hookrightarrow A[p](\rho)$. Now recall that $d_pA(\rho) \le d_pA(\omega\rho^{-1})$. The lemma follows. ∎

LEMMA 4.3. *There exists a unique* $\mathbb{Z}[\Delta]$*-morphism* $\varphi : K^* \to \mathbb{Z}_p[\Delta]$ *such that*

$$\forall x \in K^*, \qquad \varphi(x)\zeta_p = \mathrm{Log}_p(x).$$

Furthermore,

$$\mathrm{Im}\,\varphi = \bigoplus_{\rho=1,\omega} p\mathbb{Z}_p e_\rho \oplus \bigoplus_{\rho\neq 1,\omega} \mathbb{Z}_p e_\rho.$$

Proof. Let $\lambda \in K^*$ be such that $\lambda^{p-1} = -p$. Then

$$K^* = \lambda^{\mathbb{Z}} \times \mu_{p-1} \times \mu_p \times U.$$

Recall that:

- the kernel of Log_p on K^* is equal to $\lambda^{\mathbb{Z}} \times \mu_{p-1} \times \mu_p$,
- $\mathrm{Log}_p(U) = \pi^2\mathbb{Z}_p[\zeta_p]$.

For $\rho \in \widehat{\Delta}$, set

$$\tau(\rho) = \sum_{a=1}^{p-1} \rho(a)\zeta_p \in \mathbb{Z}_p[\zeta_p].$$

Then $e_\rho\zeta_p = \tau(\rho^{-1})$. But recall that $\mathbb{Z}_p[\zeta_p] = \mathbb{Z}_p[\Delta]\zeta_p$. Thus

$$e_\rho\mathbb{Z}_p[\zeta_p] = \mathbb{Z}_p\tau(\rho^{-1}).$$

If $\rho = \omega^k$, $k \in \{0, \ldots, p-2\}$, we have

$$v_p(\tau(\rho^{-1})) = \frac{k}{p-1}.$$

Therefore

$$\pi^2\mathbb{Z}_p[\zeta_p] = \bigoplus_{\rho=1,\omega} p\mathbb{Z}_p\tau(\rho^{-1}) \oplus \bigoplus_{\rho\neq 1,\omega} \mathbb{Z}_p\tau(\rho^{-1}).$$

The lemma follows. ∎

Let P be a prime in $\mathcal{I}$. We fix a generator $r_P \in \mathbb{F}_P^*$ such that

$$\chi_P(r_P) = \zeta_p.$$

For $x \in \mathbb{F}_P^*$, let $\operatorname{Ind}(P,x) \in \{0,\dots,NP-2\}$ be such that

$$x = r_P^{\operatorname{Ind}(P,x)}.$$

We recall the following theorem (see also [10] for a statement similar but weaker than part (2) below):

THEOREM 4.4.

(1) $\varphi(1-\zeta_p) = \sum_{\rho\in\widehat{\Delta},\,\rho\neq 1,\,\rho\ even} -(p-1)^{-1}L_p(1,\rho)e_\rho$.

(2) *Let $\psi \in \widehat{\Delta}$, ψ odd, $\psi \neq \omega$. Write $\psi = \omega^k$, $k \in \{2,\dots,p-2\}$. Then*

$$e_\psi\varphi(\eta(P)) \equiv 2k\operatorname{Ind}\biggl(P,\prod_{a=1}^{p-1}\biggl(\frac{1-\zeta_p^{-a}}{1-\zeta_p}\biggr)^{a^{k-1}}\biggr)e_\psi \pmod p.$$

Proof. (1) Let $\rho \in \widehat{\Delta}$, ρ even, $\rho \neq 1$. By [12, Theorem 5.18], we have

$$L_p(1,\rho)\tau(\rho^{-1}) = -(p-1)e_\rho\operatorname{Log}_p(1-\zeta_p).$$

Thus the first assertion follows.

(2) Let $\psi \in \widehat{\Delta}$, ψ odd, $\psi \neq \omega$. By a beautiful result of Uehara ([11, Theorem 1]), we have

$$e_\psi\operatorname{Log}_p(\eta(P)) \equiv 2k\operatorname{Ind}\biggl(P,\prod_{a=1}^{p-1}\biggl(\frac{1-\zeta_p^{-a}}{1-\zeta_p}\biggr)^{a^{k-1}}\biggr)\tau(\psi^{-1}) \pmod p.$$

This implies the second assertion. ∎

THEOREM 4.5. *Let $\psi \in \widehat{\Delta}$, $\psi \neq \omega$, ψ odd. We have exact sequences*

$$0 \to \operatorname{Tor}_{\mathbb{Z}_p}\mathcal{X}(\psi) \to A(\psi) \to \overline{W}(\psi)/U^{p^{k(\psi)}}(\psi) \to 0,$$
$$0 \to \operatorname{Tor}_{\mathbb{Z}_p}\mathcal{X}(\psi) \to A(\psi) \to \overline{J}(\psi)/U^{p^{m(\psi)}}(\psi) \to 0.$$

Proof. This is a consequence of the method developed by Iwasawa [5]. We briefly recall it.

Let $f \in \mathcal{W}$. For $n \geq 2$, set $\mathcal{P}_n = \{\alpha\mathcal{O} : \alpha \equiv 1 \pmod{\pi^n}\}$. Observe that

$$f(\mathcal{P}_n) \subset 1 + \pi^n\mathbb{Z}_p[\zeta_p].$$

Let

$$\widetilde{\mathcal{X}} = \varprojlim \mathcal{I}/\mathcal{P}_n.$$

If $\widetilde{F}$ is the maximal abelian extension of L which is unramified outside p, then, by class field theory,

$$\widetilde{\mathcal{X}} \simeq \operatorname{Gal}(\widetilde{F}/L).$$

By [12, Theorem 13.4], the natural surjective map $\widetilde{\mathcal{X}} \to \mathcal{X}$ has a finite kernel of order prime to p. Thus f induces a map

$$\bar{f} : \mathcal{X} \to U.$$

Furthermore,

$$\bar{f}(U) = U^{\beta(f)} \subset \bar{f}(\mathcal{X}).$$

Now let $\psi \in \widehat{\Delta}$, ψ odd, $\psi \neq \omega$. We have a map

$$\bar{f} : \mathcal{X}(\psi) \to U(\psi).$$

But

$$\mathcal{X}(\psi) \simeq \mathbb{Z}_p \oplus \operatorname{Tor}_{\mathbb{Z}_p} \mathcal{X}(\psi) \quad \text{and} \quad U(\psi) \simeq \mathbb{Z}_p.$$

Thus, if $e_\psi \beta(f) \neq 0$, we get

$$\operatorname{Ker}(\bar{f} : \mathcal{X}(\psi) \to U(\psi)) = \operatorname{Tor}_{\mathbb{Z}_p} \mathcal{X}(\psi).$$

Therefore, if $e_\psi \beta(f) \neq 0$, we get the following exact sequence induced by f:

$$0 \to \operatorname{Tor}_{\mathbb{Z}_p} \mathcal{X}(\psi) \to A(\psi) \to \bar{f}(\mathcal{X})(\psi)/U^{\beta(f)}(\psi) \to 0.$$

It remains to apply this construction to f_ψ and η to get the desired exact sequences. ∎

Corollary 4.6.

(1) *Let $\psi \in \widehat{\Delta}$, ψ odd, $\psi \neq \omega$. Then*

$$d_p A(\psi) = 1 + d_p A(\omega\psi^{-1}) \ \Leftrightarrow\ B_{1,\psi^{-1}} \equiv 0 \pmod{p} \text{ and } \overline{W}(\psi) = U(\psi).$$

(2) *Let $\rho \in \widehat{\Delta}$, ρ even and $\rho \neq 1$. Assume that $B_{1,\rho\omega^{-1}} \equiv 0 \pmod{p}$ and that $\overline{W}(\omega\rho^{-1}) = U(\omega\rho^{-1})$. Then the converse of Kummer's Lemma is true for the character ρ.*

Proof. (1) We apply Theorem 4.5. We identify $\operatorname{Tor}_{\mathbb{Z}_p} \mathcal{X}(\psi)$ with its image in $A(\psi)$. We can write $A(\psi) = B \oplus C$, where C is cyclic of order $p^{k(\psi)}$ and $B \subset \operatorname{Tor}_{\mathbb{Z}_p} \mathcal{X}(\psi)$. Now,

$$(C : C \cap \operatorname{Tor}_{\mathbb{Z}_p} \mathcal{X}(\psi)) = (\overline{W}(\psi) : U^{p^{k(\psi)}}(\psi)).$$

It remains to apply Lemma 4.1 to get the desired result.

(2) We apply the first assertion and Lemma 4.1 to deduce that $d_p A(\rho) = d_p A(\omega\rho^{-1}) - 1$. It remains to apply Lemma 4.2. ∎

We set

$$W^{\mathrm{unr}} = \{\alpha \in W : \alpha \in U^p\}.$$

Let $\psi \in \widehat{\Delta}$, ψ odd, $\psi \neq \omega$. We assume that $B_{1,\psi^{-1}} \equiv 0 \pmod{p}$. Write

$$A(\psi) = \mathbb{Z}/p^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{e_t}\mathbb{Z},$$

where $t = d_p A(\psi)$ and $1 \leq e_1 \leq \cdots \leq e_t = k(\psi)$. Set

$$n(\psi) = |\{i \in \{1, \ldots, t\} : e_i = k(\psi)\}|.$$

Corollary 4.7. *We have*

$$n(\psi)-1\le \dim_{\mathbb{F}_p} W^{\mathrm{unr}}(L^*)^p/(L^*)^p\le n(\psi).$$

Furthermore,

$$\dim_{\mathbb{F}_p} W^{\mathrm{unr}}(L^*)^p/(L^*)^p = n(\psi) \;\Leftrightarrow\; \overline{W}(\psi)\neq U(\psi).$$

Proof. By Theorems 4.5 and 3.3, we have

$$W^{\mathrm{unr}}(L^*)^{p^{k(\psi)}}/(L^*)^{p^{k(\psi)}}\simeq \mathrm{Ker}(A(\psi)\to \overline{W}(\psi)/U^{p^{k(\psi)}}(\psi)).$$

The corollary follows. ∎

Corollary 4.8. *Assume that $pA^-=\{0\}$. Then we have an isomorphism of groups*

$$\mathrm{Gal}(L(\sqrt[p]{W^{\mathrm{unr}}})/L)\simeq A^+/pA^+.$$

Proof. This is a consequence of Kummer theory, Corollary 4.7 and Corollary 4.6. ∎

Note that the above results lead to the following problem (which is a restatement of the converse of Kummer's Lemma): do we have $\varphi(\overline{W}^-)=(\mathrm{Im}\,\varphi)^-$? Observe that $e_\omega\varphi(\overline{W}^-)=e_\omega(\mathrm{Im}\,\varphi)^-$, and since $K_4(\mathbb{Z})=\{0\}$, we have $A(\omega^{-2})=\{0\}$ (see [7]) and therefore $e_{\omega^3}\varphi(\overline{W}^-)=e_{\omega^3}(\mathrm{Im}\,\varphi)^-$.

5. Remarks on the jacobian of the Fermat curve over a finite field. First we fix some notations and recall some basic facts about global function fields.

Let $\mathbb{F}_q$ be a finite field having q elements. Let ℓ be the characteristic of $\mathbb{F}_q$, $\ell\neq p$. Let $\overline{\mathbb{F}_q}$ be a fixed algebraic closure of $\mathbb{F}_q$ and let $\widetilde{\mathbb{F}_q}=\bigcup_{n\ge 1,\,n\not\equiv 0\,(\mathrm{mod}\,p)}\mathbb{F}_{q^n}\subset\overline{\mathbb{F}_q}$. Let $k/\mathbb{F}_q$ be a global function field such that $\mathbb{F}_q$ is algebraically closed in k. We set:

- D_k: the group of divisors of k,
- D_k^0: the group of divisors of degree zero of k,
- P_k: the group of principal divisors of k,
- J_k: the jacobian of k; note that

$$\forall n\ge 1,\qquad J_k(\mathbb{F}_{q^n})\simeq D^0_{\mathbb{F}_{q^n}k}/P_{\mathbb{F}_{q^n}k},$$

- g_k: the genus of k,
- $L_k(Z)\in\mathbb{Z}[Z]$: the numerator of the zeta function of k; we recall that

$$\frac{L_k(Z)}{(1-Z)(1-qZ)}=\prod_{v\text{ place of }k}(1-Z^{\deg v})^{-1},$$

  furthermore $\deg_Z L_k(Z)=2g_k$ and $L_k(1)=|J_k(\mathbb{F}_q)|$,
- $C_k(\mathbb{F}_{q^n})=J_k(\mathbb{F}_{q^n})\otimes_{\mathbb{Z}}\mathbb{Z}_p$,

- $\widetilde{d}_p J_k = d_p C_k(\widetilde{\mathbb{F}_q})$; observe that there exists an integer $m \not\equiv 0 \pmod p$ such that $C_k(\widetilde{\mathbb{F}_q}) = C_k(\mathbb{F}_{q^m})$.

Write

$$L_k(Z) = \prod_{i=1}^{2g_k}(1 - \alpha_i Z).$$

For simplicity, we assume that $v_p(\alpha_i - 1) > 0$ for $i = 1, \ldots, 2g_k$. In this case,

$$C_k(\widetilde{\mathbb{F}_q}) = C_k(\mathbb{F}_q).$$

Set $P_k(Z) = \prod_{i=1}^{2g_k}(Z - (\alpha_i - 1))$. Let γ be the Frobenius of $\mathbb{F}_q$, and set

$$C_n(k) = C_k(\mathbb{F}_{q^{p^n}}).$$

Let $C_\infty(k) = \bigcup_{n\ge 0} C_n(k)$, and set

$$M_k = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, C_\infty(k)).$$

Then M_k is isomorphic to the p-adic Tate module of J_k. Set $\Lambda = \mathbb{Z}_p[[Z]]$ where Z corresponds to $\gamma - 1$. Then it is well-known that:

- M_k is a Λ-module of finite type and of torsion,
- as a $\mathbb{Z}_p$-module, M_k is isomorphic to $\mathbb{Z}_p^{2g_k}$,
- $M_k/\omega_n M_k \simeq C_n(k)$, where $\omega_n = (1+Z)^{p^n} - 1$,
- $\mathrm{Char}_\Lambda M_k = P_k(Z)\Lambda$,
- the action of Z on M_k is semisimple, i.e. the minimal polynomial of the action of Z on M_k has only simple roots.

Now, let ℓ be a prime number, $\ell \ne p$. We fix a prime P of $\mathcal{O}$ above ℓ and we view $\mathcal{O}/P$ as a subfield of $\overline{\mathbb{F}_\ell}$, thus $\mathbb{F}_q = \mathcal{O}/P \subset \widetilde{\mathbb{F}_\ell}$. We identify ζ_p with its image in $\mathbb{F}_q$. Let X be an indeterminate over $\mathbb{F}_q$. We set $k = \mathbb{F}_\ell(X, Y)$ where $X^p + Y^p = 1$, and we set $T = X^p$. For $a, b \in \mathbb{Z}$, let $\tau_{a,b} \in \mathrm{Gal}(\overline{\mathbb{F}_\ell}k/\overline{\mathbb{F}_\ell}(T))$ be such that

$$\tau_{a,b}(X) = \zeta_p^a X \quad \text{and} \quad \tau_{a,b}(Y) = \zeta_p^b Y.$$

Let $a \in \{1, \ldots, p-2\}$. Let H_a be the subgroup of $\mathrm{Gal}(\overline{\mathbb{F}_\ell}k/\overline{\mathbb{F}_\ell}(T))$ generated by $\tau_{1,[-a^{-1}]}$. Set

$$E_a = \mathbb{F}_\ell(T, XY^a).$$

If we set $U = T$ and $V = XY^a$, then $V^p - U(1-U)^a = 0$ and of course $E_a = \mathbb{F}_\ell(U, V)$. We set

$$E = \mathbb{F}_q E_a, \qquad F = \mathbb{F}_q k,$$

and observe that $\widetilde{\mathbb{F}_\ell} = \widetilde{\mathbb{F}_q}$. It is clear that $F^{H_a} = E$. Finally, we set

$$G = \mathrm{Gal}(E/\mathbb{F}_q(T)).$$

Note that $g_E = (p-1)/2$.

Lemma 5.1. *We have*

$$L_E(Z) = \prod_{\sigma\in\Delta}(1 - j_{1,a}(P)^\sigma Z).$$

Proof. Let $\chi \in \widehat{G}$ be such that $\chi(g) = \zeta_p^{-1}$, where $g \in G$ is such that $g(XY^a) = \zeta_p XY^a$. Note that

$$L_E(Z) = \prod_{\sigma\in\Delta} L(Z,\chi^\sigma), \quad \text{where} \quad L(Z,\chi) = \prod_{v \text{ place of } \mathbb{F}_q(T)} (1-\chi(v)Z^{\deg v})^{-1}.$$

Since $2g_e = p-1$, we get $\deg_Z L(Z,\chi) = 1$.

For $b \in \mathbb{F}_q \setminus \{0,1\}$, we denote the Frobenius of $T-b$ in $E/\mathbb{F}_q(T)$ by Frob_b. We have

$$\mathrm{Frob}_b(XY^a) = (b(1-b)^a)^{(q-1)/p} XY^a.$$

But

$$L(Z,\chi) \equiv 1 + \Big(\sum_{b\in\mathbb{F}_q\setminus\{0,1\}} \chi(\mathrm{Frob}_b)\Big) X \pmod{X^2}.$$

Thus

$$L(Z,\chi) = 1 + \Big(\sum_{b\in\mathbb{F}_q\setminus\{0,1\}} \chi(\mathrm{Frob}_b)\Big) X.$$

But we can write

$$j_{1,a}(P) = -\sum_{i=0}^{p-1} N_i \zeta_p^{-i},$$

where $N_i = |\{\alpha \in \mathbb{F}_q\setminus\{0,1\} : (\alpha(1-\alpha)^a)^{(q-1)/p} \equiv \zeta_p^{-i} \pmod{P}\}|$. Therefore

$$j_{1,a}(P) = -\sum_{b\in\mathbb{F}_q\setminus\{0,1\}} \chi(\mathrm{Frob}_b).$$

The lemma follows. ∎

Theorem 5.2. *Let n be the smallest integer (if it exists) such that $3 \le n \le p-2$, n is odd and $e_{\omega^n} j_{1,a}(P) \notin U^p$. Then*

$$J_k(\widetilde{\mathbb{F}_\ell})^{H_a} \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq (\mathbb{Z}/p\mathbb{Z})^n.$$

If such an integer does not exist then:

(1) $\widetilde{d}_p J_k^{H_a} = p-1$,

(2) *we have*

$$J_k(\widetilde{\mathbb{F}_\ell})^{H_a} \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq (\mathbb{Z}/p\mathbb{Z})^{p-1} \;\Leftrightarrow\; \ell^{p-1} \not\equiv 1 \pmod{p^2}.$$

Proof. The proof is based on ideas developed by Greenberg [4]. Write $H = H_a$. Let P_0 be the prime of E above T, P_1 the prime of E above $T-1$

and P_∞ the prime of E above $1/T$. Recall that in D_E we have

$$p(P_0 - P_\infty) = (T),$$
$$p(P_1 - P_\infty) = (T-1),$$
$$P_0 - P_\infty + a(P_1 - P_\infty) = (XY^a).$$

Thus, by [4, Sec. 2],

$$J_E(\mathbb{F}_q)^G \simeq \mathbb{Z}/p\mathbb{Z},$$

and $J_E(\mathbb{F}_q)^G$ is generated by the class of $P_0 - P_\infty$. Observe also that F/E is unramified and cyclic of order p. Let us start with the exact sequence

$$0 \to \mathbb{F}_q^* \to F^* \to P_F \to 0.$$

We get

$$P_F^H/P_E \simeq \mathbb{Z}/p\mathbb{Z},$$

and P_F^H/P_E is generated by the image of $P_0 - P_\infty$ in D_F. In particular,

$$P_F^H/P_E \simeq J_E(\mathbb{F}_q)^G.$$

Note that we also have

$$0 \to H^1(H, P_F) \to H^2(H, \mathbb{F}_q^*) \to H^2(H, F^*).$$

But F/E is unramified and cyclic, therefore every element of $\mathbb{F}_q^*$ is a norm in the extension F/E. Thus

$$H^1(H, P_F) \simeq \mathbb{Z}/p\mathbb{Z}.$$

Now, we look at the exact sequence

$$0 \to P_F \to D_F^0 \to J_F(\mathbb{F}_q) \to 0.$$

Since F/E is unramified,

$$H^1(H, D_F^0) = \{0\}.$$

Therefore, we have obtained the following exact sequence:

$$0 \to J_E(\mathbb{F}_q)^G \to J_E(\mathbb{F}_q) \to J_F(\mathbb{F}_q)^H \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

Now, it is not difficult to deduce that, for all $n \geq 1$, we have the exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to J_E(\mathbb{F}_{q^n}) \to J_F(\mathbb{F}_{q^n})^H \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

From this, we get the following exact sequence of $\mathbb{Z}_p[G]$-modules and Λ-modules:

$$0 \to M_E \to M_F^H \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

Recall that in our situation, by Lemma 5.1,

$$P_E(Z) = \prod_{\sigma \in \Delta} (Z - (j_{1,a}(P)^\sigma - 1)).$$

Furthermore the actions of G and Z commute on M_F^H. Now, we have:

- $\mathrm{Char}_\Lambda M_F^H = \mathrm{Char}_\Lambda M_E = P_E(Z)\Lambda$,
- $M_F^H \simeq \mathbb{Z}_p^{p-1}$ as $\mathbb{Z}_p$-modules,
- $M_F^H/\omega_n \simeq C_n(F)^H$.

Observe that

$$C_0(F)^H = J_k(\widetilde{\mathbb{F}_\ell})^{H_a} \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Note also that the minimal polynomial of the action of Z on M_F^H is

$$\mathrm{Irr}(j_{1,a}(P) - 1, \mathbb{Q}_p; Z) := G(Z).$$

Set $N = \sum_{\delta \in G} \delta$. Then one can see that

$$NM_E = NM_F^H = \{0\}.$$

Thus M_F^H is a $\mathbb{Z}_p[G]/N\mathbb{Z}_p[G]$-module. Now, we identify $\mathbb{Z}_p[G]/N\mathbb{Z}_p[G]$ with $\mathbb{Z}_p[\zeta_p]$. Since $M_F^H \simeq \mathbb{Z}_p^{p-1}$, there exists $m \in M_F^H$ such that

$$M_F^H \simeq \mathbb{Z}_p[\zeta_p].m,$$

i.e. M_F^H is a free $\mathbb{Z}_p[\zeta_p]$-module of rank one. Therefore there exists an element $x \in \mathbb{Z}_p[\zeta_p]$ such that $Zm = xm$. Now set

$$D(Z) = \prod_{\sigma \in \Delta} (Z - x^\sigma) \in \Lambda.$$

Then $D(Z)M_F^H = \{0\}$. Therefore $G(Z)$ divides $D(Z)$ in Λ. Thus there exists $\sigma \in \Delta$ such that

$$x^\sigma = j_{1,a}(P) - 1.$$

But

$$C_0(F)^H \simeq M_F^H/ZM_F^H \simeq \mathbb{Z}_p[\zeta_p]/x\mathbb{Z}_p[\zeta_p].$$

Therefore, we get

$$J_k(\widetilde{\mathbb{F}_\ell})^{H_a} \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \mathbb{Z}_p[\zeta_p]/(j_{1,a}(P) - 1)\mathbb{Z}_p[\zeta_p].$$

Recall that $j_{1,a}(P) \equiv 1 \pmod{\pi^2}$. Thus

$$v_p(j_{1,a}(P) - 1) = v_p(\mathrm{Log}_p(j_{1,a}(P))).$$

Now

$$\mathrm{Log}_p(j_{1,a}(P)) = \frac{1}{2} f \,\mathrm{Log}_p(\ell) + \sum_{\psi \in \widehat{\Delta},\, \psi\, \mathrm{odd}} e_\psi \,\mathrm{Log}_p(j_{1,a}(P)),$$

where f is the order of ℓ in $(\mathbb{Z}/p\mathbb{Z})^*$. Let $\psi \in \widehat{\Delta}$, $\psi = \omega^n$, n odd. If $e_\psi \,\mathrm{Log}_p(j_{1,a}(P)) \neq 0$, then

$$v_p(e_\psi \,\mathrm{Log}_p(j_{1,a}(P))) \equiv \frac{n}{p-1} \pmod{\mathbb{Z}},$$

and furthermore

$$v_p(e_\psi \,\mathrm{Log}_p(j_{1,a}(P))) > \frac{n}{p-1} \;\Leftrightarrow\; e_\psi j_{1,a}(P) \in U^p.$$

Note also that

$$v_p(e_\omega \operatorname{Log}_p(j_{1,a}(P))) > \frac{1}{p-1}.$$

The theorem follows. ∎

Observe that the proof of the above theorem implies that we have an isomorphism of $\mathbb{Z}[G]$-modules

$$J_{E_a}(\widetilde{\mathbb{F}_\ell}) \simeq J_k(\widetilde{\mathbb{F}_\ell})^{H_a}.$$

COROLLARY 5.3. *Let* $n \in \{3, \ldots, p-2\}$, *n odd. Let* $a \in \{1, \ldots, p-2\}$ *be such that* $1 + a^n - (1+a)^n \not\equiv 0 \pmod{p}$. *The following assertions are equivalent:*

(1) $A(\omega^{1-n}) = \{0\}$,

(2) *there exists a prime number* $\ell \neq p$ *such that* $\widetilde{d}_p J_{E_a} = n$, *where* $E_a = \mathbb{F}_\ell(U, V)$ *and* $V^p - U(1-U)^a = 0$.

Proof. Observe that (2) implies (1) by Theorems 5.2 and 4.5. Write $\psi = \omega^n$. Let ℓ be a prime number, $\ell \neq p$. Write

$$\mathbb{F}_{(\ell)} = \mathcal{O}/\ell\mathcal{O} \quad \text{and} \quad D_\ell = \mathbb{F}_{(\ell)}^*/(\mathbb{F}_{(\ell)}^*)^p.$$

Observe that D_ℓ is a $\mathbb{Z}_p[\Delta]$-module. Let Cyc be the group of cyclotomic units of L. We denote the image of Cyc in D_ℓ by $\overline{\mathrm{Cyc}}^\ell$. Then Theorem 4.4 asserts that $e_\psi \overline{\mathrm{Cyc}}^\ell = \{1\}$ in D_ℓ if and only if $e_\psi j_{1,a}(P) \in U^p$, where P is a prime of $\mathcal{O}$ above ℓ. Let

$$B = L(\sqrt[p]{\mathrm{Cyc}}).$$

We assume that (1) holds. By the Chebotarev density theorem applied to the extension B/L, there exist infinitely many primes ℓ such that:

- $e_\rho \overline{\mathrm{Cyc}}^\ell = \{1\}$ for $\rho \neq \psi$,
- $e_\psi \overline{\mathrm{Cyc}}^\ell \neq \{1\}$.

It remains to apply Theorem 5.2 and the above remarks to get (2). ∎

Now, let ℓ be a prime number. Let p be an odd prime number, $p \neq \ell$. Let T be an indeterminate over $\mathbb{F}_\ell$ and let $E_p/\mathbb{F}_\ell(T)$ be the imaginary quadratic extension defined by

$$E_p = \mathbb{F}_\ell(T, X) \quad \text{where} \quad X^2 - X + T^p = 0.$$

Let n be an odd integer, $n \geq 3$. Let $S_n(\ell)$ denote the set of primes p such that $\widetilde{d}_p J_{E_p} = n$. By our results above, if $p \in S_n(\ell)$ then $A(\omega^{1-n}) = \{0\}$. Observe that if $\ell^n \not\equiv 1 \pmod{p}$ then $p \notin S_n(\ell)$, and therefore $S_n(\ell)$ is a finite set. Set $S(\ell) = \bigcup_n S_n(\ell)$, where n runs through the odd integers. Observe that if the order of ℓ modulo p is even then $p \notin S(\ell)$. Therefore, by a classical result of Hasse (see [8]) there exist infinitely many primes p not in $S(\ell)$ (in fact at least "2/3 of the prime numbers" are not in $S(\ell)$). Thus, we ask the following question: is $S(\ell)$ infinite?

Acknowledgments. The authors thank Cornelius Greither for interesting discussions on the converse of Kummer's Lemma which led us to the study of the analogous statement for the odd part. The second author thanks the mathematicians of the Laboratoire de Mathématiques Nicolas Oresme for their hospitality during his stay at Caen.

References

[1] B. Anglès, *Units and norm residue symbol*, Acta Arith. 98 (2001), 33–51.
[2] B. Anglès and T. Beliaeva, *On Weil numbers in cyclotomic fields*, Int. J. Number Theory 5 (2009), 871–884.
[3] J. Assim et T. Nguyen Quang Do, *Sur la constante de Kummer–Leopoldt d'un corps de nombres*, Manuscripta Math. 115 (2004), 55–72.
[4] R. Greenberg, *On the jacobian variety of some algebraic curves*, Compos. Math. 42 (1980), 345–359.
[5] K. Iwasawa, *A note on Jacobi sums*, in: Symposia Math. XV, Academic Press, London, 1975, 447–459.
[6] —, *Some remarks on Hecke characters*, in: Algebraic Number Theory (Kyoto, 1976), S. Iyanaga (ed.), Japan Soc. Promotion Sci., Tokyo, 1977, 99–108.
[7] M. Kurihara, *Some remarks on conjectures about cyclotomic fields and K-groups of* $\mathbb{Z}$, Compos. Math. 81 (1992), 223–236.
[8] J. C. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. 118 (1985), 449–461.
[9] S. Lang, *Units and class groups in number theory and algebraic geometry*, Bull. Amer. Math. Soc. 6 (1982), 253–316.
[10] F. Thaine, *On the coefficients of Jacobi sums in prime cyclotomic fields*, Trans. Amer. Math. Soc. 351 (1999), 4769–4790.
[11] T. Uehara, *On a congruence relation between Jacobi sums and cyclotomic units*, J. Reine Angew. Math. 382 (1987), 199–214.
[12] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, 1997.

Bruno Anglès
Université de Caen, CNRS UMR 6139
Campus II, Boulevard Maréchal Juin, B.P. 5186
14032 Caen Cedex, France
E-mail: bruno.angles@math.unicaen.fr

Filippo A. E. Nuccio
Istituto Guido Castelnuovo
Università "La Sapienza"
5, Piazzale Aldo Moro
00186 Roma, Italy
E-mail: nuccio@mat.uniroma1.it

Received on 14.2.2008
and in revised form on 12.5.2009 (5644)