ACTA ARITHMETICA
105.1 (2002)

On the Hilbert symbol in cyclotomic fields

by

Charles Helou (Media, PA)

1. Introduction. Let l be a prime number ≥ 5, ζ a primitive lth root of unity in an algebraic closure of the field $\mathbb{Q}_l$ of l-adic numbers, $K = \mathbb{Q}(\zeta)$, $\mathcal{O}_K = \mathbb{Z}[\zeta]$, $\lambda = 1 - \zeta$, $\widehat{K} = \mathbb{Q}_l(\zeta)$, the λ-adic completion of K, and $\mathcal{O}_{\widehat{K}} = \mathbb{Z}_l[\zeta]$, where $\mathbb{Z}_l$ is the ring of l-adic integers. The group of units of a ring $\mathcal{O}$ is denoted by $\mathcal{O}^*$. For $\alpha, \beta \in \widehat{K}^*$, we write

$$(\alpha, \beta)_\lambda = \zeta^{[\alpha,\beta]} \quad \text{with } [\alpha, \beta] \text{ in } \mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}$$

for the Hilbert symbol as defined in [3], inverse of the one in [2]. Namely,

$$(\alpha, \beta)_\lambda = \frac{\psi(\beta)(\alpha^{1/l})}{\alpha^{1/l}},$$

where $\psi : \widehat{K}^* \to \mathrm{Gal}(\widehat{K}(\alpha^{1/l})|\widehat{K})$ is the local Artin map associated with the extension $\widehat{K}(\alpha^{1/l})|\widehat{K}$. This bilinear, skew-symmetric symbol defines an orthogonality relation in $\widehat{K}^*$ by the condition $[\alpha, \beta] = 0$. Let C be the group of cyclotomic units of K, i.e. the subgroup of $\mathcal{O}_K^*$ generated by the special units

$$u_k = \frac{1 - \zeta^k}{1 - \zeta} = \frac{\sigma_k(\lambda)}{\lambda},$$

where σ_k is the element of the Galois group of $\widehat{K}|\mathbb{Q}_l$ defined by $\sigma_k(\zeta) = \zeta^k$ ($k \in \mathbb{Z} \setminus l\mathbb{Z}$). Fix an element $a \in \mathbb{Z} \setminus \{0\}$ and, for $n \in \mathbb{N} \setminus \{0\}$, let $\alpha_n = a^n - \zeta^n$. In 1989, G. Terjanian ([7]) conjectured that

(TC) *If $a \in \mathbb{Z} \setminus l\mathbb{Z}$ and $\alpha_1 = a - \zeta$ is orthogonal to C, then $a \equiv \pm 1 \pmod{l}$.*

He showed that (TC) is true for the regular primes l and for those for which $2^{l-1} \not\equiv 1 \pmod{l^2}$ or the Bernoulli number $B_{l-3} \not\equiv 0 \pmod{l}$. More recently, B. Anglès ([1]) showed that Eichler's condition, $i(l) < \sqrt{l} - 2$, for the index of irregularity $i(l)$ of the prime l ([8]), implies that (TC) is true for l.

2000 *Mathematics Subject Classification*: 11R18, 11S31.

In this paper, we study the following weak form of the conjecture:

(WTC) *If $a \in \mathbb{Z} \setminus l\mathbb{Z}$ and, for all $n \in \mathbb{N} \setminus l\mathbb{N}$, $\alpha_n = a^n - \zeta^n$ is orthogonal to C, then $a \equiv \pm 1 \pmod{l}$.*

We can also state (TC) and (WTC) in an equivalent form using the group μ_{l-1} of $(l-1)$th roots of unity in $\mathbb{Z}_l^*$. Indeed, for any $a \in \mathbb{Z} \setminus l\mathbb{Z}$, there is an $\omega \in \mu_{l-1}$ such that $\omega \equiv a \pmod{l}$, namely $\omega = \lim_{n\to\infty} a^{l^n}$ ([4]). Therefore $\omega \equiv a^l \pmod{l^2}$ and, by the properties of the Hilbert symbol, $[\omega^n - \zeta^n, u] = [a^{ln} - \zeta^n, u]$ for all $u \in \mathbb{Z}_l^*$ and $n \in \mathbb{N} \setminus l\mathbb{N}$. Thus, $\omega^n - \zeta^n$ is orthogonal to C if and only if $a^{ln} - \zeta^n$ is. Moreover, if $a^n - \zeta^n$ is orthogonal to C $(n \in \mathbb{N}\setminus l\mathbb{N})$, then $a^{l-1} \equiv 1 \pmod{l^2}$ ([7]) and $\omega^n - \zeta^n \equiv a^{ln} - \zeta^n \equiv a^n - \zeta^n \pmod{l^2}$, so that $\omega^n - \zeta^n = \sigma_n(\omega^n - \zeta)$ is orthogonal to C, i.e. $\omega^n - \zeta$ is orthogonal to C. Also, since $\omega^{l^k} = \omega$ $(k \in \mathbb{N})$ and $\omega^{-1} = \omega^{l-2}$, we see that, for any $m \in \mathbb{Z} \setminus \{0\}$, $\omega^m - \zeta = \omega^n - \zeta$ for some $n \in \mathbb{N} \setminus l\mathbb{N}$; as to $m = 0$, the element λ is anyway orthogonal to C. Therefore the assumption in (TC) (resp. in (WTC)) entails the orthogonality of $\omega - \zeta$ (resp. of $\omega^m - \zeta$, for all $m \in \mathbb{Z}$) to C. On the other hand, $a \equiv \pm 1 \pmod{l}$ if and only if $\omega \equiv \pm 1 \pmod{l}$, which, by a simple induction argument, amounts to $\omega = \omega^{l^n} \equiv \pm 1 \pmod{l^{n+1}}$ for all $n \geq 1$, i.e. to $\omega = \pm 1$. It follows that (TC) and (WTC) are respectively equivalent to

(TC) *If $\omega \in \mu_{l-1}$ and $\omega - \zeta$ is orthogonal to C, then $\omega^2 = 1$.*

(WTC) *If $\omega \in \mu_{l-1}$ and, for all $n \in \mathbb{Z}$, $\omega^n - \zeta$ is orthogonal to C, then $\omega^2 = 1$.*

In fact, the assumption in (WTC) is equivalent to: $\omega^n - \zeta$ is orthogonal to C for $1 \leq n \leq f-1$, where f is the order of ω.

We first derive some properties of the Hilbert symbol and some explicit expressions obtained via the Artin–Hasse reciprocity law, that we need in what follows. We then establish orthogonality relations between some classes of elements $\omega^m - \zeta$ and $\sigma_k(\omega^n - \zeta)$ and deduce the validity of (WTC) under certain conditions. Thus if (WTC) fails for l then there exists a divisor $f \geq 11$ of $l-1$ such that for any divisor d of f, $d^{l-1} \equiv 1 \pmod{l^2}$. Furthermore, (WTC) is true for every prime l of one of the following forms: $l = 2^n + 1$; or $l = 2^n - 1$; or $l = 2^{h_0}p^h + 1$ with $h_0 \leq 3$, p prime and $h \geq 1$; or $l = 2^{h_0}p_1^{h_1}p_2^{h_2} + 1$ with $h_0 \leq 3$, p_1, p_2 primes and $h_1, h_2 \geq 1$ such that $h_i q(p_i) \not\equiv 1 \pmod{l}$ $(i = 1, 2)$; or $l = 2^{h_0}p_1^{h_1} \ldots p_m^{h_m}$, where the p_i are primes and the $h_i \geq 1$ are such that $\sum_{i=1}^m h_i q(p_i) \not\equiv 1 \pmod{l}$ or $h_0 \leq 3$ and $p_i^{l-1} \not\equiv 1 \pmod{l^2}$ for $1 \leq i \leq m$. Here $q(x) = (x^{l-1} - 1)/l$ is the *Fermat quotient* for $x \in \mathbb{Z}_l^*$.

2. Properties of the Hilbert symbol. The Hilbert symbol has the following fundamental properties (see [2, Ch. 12, §1]).

Lemma 1. *For any $x, y, z \in \widehat{K}^*$, we have*:

(1) $[xy, z] = [x, z] + [y, z]$; $[x^n, y] = [x, y^n] = n[x, y]$ $(n \in \mathbb{Z})$;
$[y, x] = -[x, y]$; $[x, \pm x] = 0$.

(2) *If* $x \neq 1$ *then* $[x, 1-x] = 0$. *If* $x \neq -1$ *then* $[x, 1+x] = 0$.

(3) *If* $x \neq -y$ *then* $[x, y] = [x, x+y] + [x+y, y]$.
If $x \neq y$ *then* $[x, y] = [x, x-y] + [x-y, y]$.

Lemma 2. (1) *For* $x, y \in \widehat{K}^*$ *and* $k \in \mathbb{Z} \setminus l\mathbb{Z}$, $[\sigma_k(x), \sigma_k(y)] = k[x, y]$.

(2) *If F is a proper subfield of $\widehat{K}$ and $x, y \in F^*$ then* $[x, y] = 0$.

(3) *The group C of cyclotomic units is invariant under the action of* $\mathrm{Gal}(\widehat{K}|\mathbb{Q}_l)$, *i.e.* $\sigma_k(C) = C$ *for any* $k \in \mathbb{Z} \setminus l\mathbb{Z}$.

We denote by v_λ the normalized λ-adic *valuation* of $\widehat{K}$.

Lemma 3. (1) *If* $\alpha \in \mathcal{O}^*_{\widehat{K}}$ *satisfies* $\alpha^{l-1} \equiv 1 \pmod{\lambda^{l+1}}$, *then α is orthogonal to $\widehat{K}^*$. In particular, any $\omega \in \mu_{l-1}$ is orthogonal to $\widehat{K}^*$.*

(2) *If* $x_1, x_2, y_1, y_2 \in \widehat{K}^*$ *are such that* $v_\lambda(x_1) = v_\lambda(x_2) = h$, $v_\lambda(y_1) = v_\lambda(y_2) = k$, $v_\lambda(x_1 - x_2) \geq l + h + 1$ *and* $v_\lambda(y_1 - y_2) \geq l + k + 1$, *then* $[x_1, y_1] = [x_2, y_2]$.

Proof. (1) By an application of Hensel's lemma, a unit of $\widehat{K}$ which is congruent to an lth power $\pmod{\lambda^{l+1}}$ is an lth power in $\widehat{K}$ ([2, Ch. 12, Lemma 4]). In particular, if $\alpha^{l-1} \equiv 1 \pmod{\lambda^{l+1}}$ then $\alpha^{l-1} = \gamma^l$ for some $\gamma \in \mathcal{O}^*_{\widehat{K}}$ and $[\alpha, y] = -[\alpha^{l-1}, y] = -l[\gamma, y] = 0$.

(2) We have $x_i = \lambda^h \alpha_i$ and $y_i = \lambda^k \beta_i$, with $\alpha_i, \beta_i \in \mathcal{O}^*_{\widehat{K}}$ $(i = 1, 2)$. Moreover, $v_\lambda(\alpha_1 - \alpha_2) = v_\lambda(x_1 - x_2) - h \geq l + 1$, i.e. $\alpha_1 \alpha_2^{-1} \equiv 1 \pmod{\lambda^{l+1}}$; and similarly $\beta_1 \beta_2^{-1} \equiv 1 \pmod{\lambda^{l+1}}$. Then, by (1), $x_1 x_2^{-1} = \alpha_1 \alpha_2^{-1}$ and $y_1 y_2^{-1} = \beta_1 \beta_2^{-1}$ are orthogonal to $\widehat{K}^*$. In particular, $[x_1 x_2^{-1}, y_1] = 0$ and $[x_2, y_1 y_2^{-1}] = 0$, i.e. $[x_1, y_1] = [x_2, y_1]$ and $[x_2, y_1] = [x_2, y_2]$. Hence the result.

Lemma 4. (1) *If* $\alpha, \beta \in \mathcal{O}^*_{\widehat{K}}$ *are such that* $\alpha^{l-1} \equiv 1 \pmod{\lambda^i}$ *and* $\beta^{l-1} \equiv 1 \pmod{\lambda^j}$, *with* $i, j \in \mathbb{N}$, *and* $i + j \geq l + 1$, *then* $[\alpha, \beta] = 0$.

(2) *If* $\alpha \in \mathcal{O}^*_{\widehat{K}}$ *satisfies* $\alpha^{l-1} \equiv 1 \pmod{\lambda^l}$, *then α is orthogonal to* $\mathcal{O}^*_{\widehat{K}}$.

(3) *If* $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathcal{O}^*_{\widehat{K}}$ *are such that* $\alpha_1^{l-1} \equiv \alpha_2^{l-1} \pmod{\lambda^l}$ *and* $\beta_1^{l-1} \equiv \beta_2^{l-1} \pmod{\lambda^l}$, *then* $[\alpha_1, \beta_1] = [\alpha_2, \beta_2]$.

Proof. (1) If $i = 0$ or $j = 0$, the result follows from Lemma 3(1). Moreover, since $[\alpha, \beta] = [\alpha^{l-1}, \beta^{l-1}]$, we may then assume that $\alpha \equiv 1 \pmod{\lambda^i}$ and $\beta \equiv 1 \pmod{\lambda^j}$, with $i, j \geq 1$ and $i + j \geq l + 1$. The proof uses the multiplicative basis $\eta_i = 1 - \lambda^i$ $(i \geq 1)$ of the principal units (i.e. those $\equiv 1$ $\pmod{\lambda}$) of $\widehat{K}$.

Note first that the property holds for the η_i's. Indeed, from the relation $\eta_{i+j} = \eta_j + \lambda^j \eta_i$, we deduce, via Lemma 1, that $[\eta_i, \eta_j] = [\eta_i, \eta_{i+j}] + [\eta_{i+j}, \eta_j] + j[\lambda, \eta_{i+j}]$; and each of the last three symbols is zero, by Lemma 3(1).

Then the property is extended to all the principal units, using a descending induction on $i+j$ and the fact that we can write $\alpha = \eta_i^m \alpha'$ and $\beta = \eta_j^n \beta'$, with $m, n \in \mathbb{Z}$ and $\alpha', \beta' \in \mathcal{O}_{\widehat{K}}$ such that $\alpha' \equiv 1 \pmod{\lambda^{i+1}}$ and $\beta' \equiv 1 \pmod{\lambda^{j+1}}$. Indeed, since by the binomial formula $\eta_i^k \equiv 1 - k\lambda^i \pmod{\lambda^{i+1}}$ (for $k \in \mathbb{Z}$) and since $(1-\alpha)/\lambda^i$ is in $\mathcal{O}_{\widehat{K}}$ and is thus $\equiv m \pmod{\lambda}$ for some $m \in \mathbb{Z}$, it follows that we may take $\alpha' = \alpha\eta_i^{-m}$, as it is $\equiv 1 \pmod{\lambda^{i+1}}$; similarly for β'. Therefore $[\alpha, \beta] = mn[\eta_i, \eta_j] + m[\eta_i, \beta'] + n[\alpha', \eta_j] + [\alpha', \beta']$, where the last three symbols are zero by the induction assumption and the one before them is zero by the property for the η_i's. Hence the result in general.

(2) For $\beta \in \mathcal{O}_{\widehat{K}}^*$, we have $\beta^{l-1} \equiv 1 \pmod{\lambda}$, and since $\alpha^{l-1} \equiv 1 \pmod{\lambda^l}$, (1) shows that $[\alpha, \beta] = 0$.

(3) We have $(\alpha_1\alpha_2^{-1})^{l-1} \equiv 1 \pmod{\lambda^l}$ and thus, by (2), $[\alpha_1\alpha_2^{-1}, \beta_1] = 0$, i.e. $[\alpha_1, \beta_1] = [\alpha_2, \beta_1]$. Similarly, $[\alpha_2, \beta_1\beta_2^{-1}] = 0$, i.e. $[\alpha_2, \beta_1] = [\alpha_2, \beta_2]$. Hence the result.

Lemma 5. (1) *If $x, y \in K^*$ are of the form $x = \lambda^h u$ and $y = \lambda^k v$, where $u, v \in \mathcal{O}_K^*$ are global units and $h, k \in \mathbb{Z}$, then $[x, y] = 0$.*

(2) *The $\mathbb{Q}$-conjugates of ζ, of λ and of the elements of C are pairwise orthogonal.*

(3) *If $\omega \in \mu_{l-1}$ has order f, then, for any $n \in \mathbb{Z}$ such that $f \mid 2n$, $\omega^n - \zeta$ is orthogonal to its $\mathbb{Q}_l$-conjugates, to those of λ and to C.*

Proof. (1) By the product formula for the Hilbert symbols over all the primes (finite or infinite) $\mathfrak{p}$ of K ([2, Ch. 12, Theorem 13]), for $x, y \in K^*$, $\prod_{\mathfrak{p}} (x, y)_{\mathfrak{p}} = 1$. Moreover, from the properties of the local Artin maps, if $\mathfrak{p}$ is finite, $\mathfrak{p} \nmid l$ and the $\mathfrak{p}$-adic valuations $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(y) = 0$, then $(x, y)_{\mathfrak{p}} = 1$. Also, for the infinite primes $\mathfrak{p}$, the completion of K at $\mathfrak{p}$ is $\simeq \mathbb{C}$ and thus $(x, y)_{\mathfrak{p}} = 1$. Therefore, for x, y as in the statement, $(x, y)_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \neq (\lambda)$. Thus, the product formula reduces to $(x, y)_\lambda = 1$, i.e. $[x, y] = 0$.

(2) follows immediately from (1).

(3) Since $f \mid 2n$, we see that $\omega^{2n} = 1$, i.e. $\omega^n = \pm 1$. Hence $\omega^n - \zeta = \pm 1 - \zeta = \lambda$ or $= -(1+\zeta) = -\sigma_2(\lambda)/\lambda = -u_2$, which lies in C. Hence the result, by (2).

Lemma 6. (1) *If $\alpha, \beta \in \mathcal{O}_{\widehat{K}}^*$ and $a_0, a_1, b \in \mathbb{Z}_l$ are such that $\alpha \equiv a_0 + a_1\lambda \pmod{\lambda^2}$ and $\beta \equiv b \pmod{\lambda^l}$, then $[\alpha, \beta] = (a_1/a_0)q(b)$.*

(2) *For $u, v, x, y \in \mathbb{Z}_l$ such that $l \nmid (u+v)(x+y)$, we have*

$$[u + v\zeta, x + y\zeta] = \frac{(uy - vx)^l - (u+v)y^l + v^l(x+y)}{l(u+v)(x+y)}.$$

(3) *If $\alpha \in \mathcal{O}^*_{\widehat{K}}$, then $[\alpha, \zeta] = (N(\alpha) - 1)/l$, where N is the norm in $\widehat{K}|\mathbb{Q}_l$.*

(4) *If $a \in \mathbb{Z}_l^*$, then $[a, \lambda] = \frac{1}{2}q(a)$.*

Proof. (1) By Lemma 4, $[\alpha, \beta] = [\alpha, b]$. Then, by [6, Corollary 1 to Theorem 2 and the Remark after Corollary 2],

$$[\alpha, b] = \frac{a_1}{a_0} \cdot \frac{b^{l-1} - 1}{l}.$$

Hence the result.

(2) This results from [6, Theorem 3 and its Corollary 2] by the same calculation that gave the expression for

$$\left(\frac{x + y\zeta}{u + v\zeta}\right)_l \left(\frac{u + v\zeta}{x + y\zeta}\right)_l^{-1} = [u + v\zeta, x + y\zeta],$$

which, in view of the note following that theorem, is valid for $[u+v\zeta, x+y\zeta]$ when $u, v, x, y \in \mathbb{Z}_l$.

(3) This results from [6, Theorem 2 and the Remark after its Corollary 2], since $\zeta = 1 - \lambda$ and $\log \zeta = 0$.

(4) By [2, Ch. 12, Th. 10], whose third part is missing a factor $1/\lambda$ of $\zeta \log \alpha$, and in which the symbol is the opposite of the one in [3], used here, we have

$$[a, \lambda] = -\frac{1}{l} \operatorname{Tr}\left(\frac{\zeta}{\lambda} \log a\right),$$

where Tr is the trace map in $\widehat{K}|\mathbb{Q}_l$. Since $a \in \mathbb{Z}_l^*$, we find that $a^{l-1} \equiv 1 \pmod{l}$ and

$$\log a = \frac{1}{l-1} \log(a^{l-1}) \equiv \frac{1}{l-1}(a^{l-1} - 1) \equiv -(a^{l-1} - 1) \pmod{l^2}.$$

Hence

$$\frac{\zeta}{\lambda} \log a \equiv -\frac{\zeta}{\lambda}(a^{l-1} - 1) \pmod{l^2\mathfrak{D}^{-1}},$$

where $\mathfrak{D} = (\lambda^{l-2})$ is the different ideal of $\widehat{K}|\mathbb{Q}_l$, and therefore

$$\operatorname{Tr}\left(\frac{\zeta}{\lambda} \log a\right) \equiv -(a^{l-1} - 1) \operatorname{Tr}\left(\frac{\zeta}{\lambda}\right) \pmod{l^2}$$

(cf. [5, p. 150]). Moreover, $\operatorname{Tr}(\zeta/\lambda) = \operatorname{Tr}(1/\lambda - 1) = \operatorname{Tr}(1/\lambda) - (l-1)$ and, by [5, p. 173], $\mathrm{Tr}(1/\lambda) = (l-1)/2$. Thus

$$\mathrm{Tr}\left(\frac{\zeta}{\lambda}\log a\right) \equiv \frac{l-1}{2}(a^{l-1}-1) \equiv -\frac{1}{2}(a^{l-1}-1) \pmod{l^2}.$$

The result follows by substitution into the expression of $[a,\lambda]$.

Lemma 7. *Let* $a \in \mathbb{Z}_l^*$.

(1) *If* $a^2 \not\equiv 1 \pmod{l}$ *then*

$$[a-\zeta, a^2-\zeta^2] = \frac{2a}{a^2-1}(q(2)+q(a)).$$

(2) *If* $a^3 \not\equiv 1 \pmod{l}$ *then*

$$[a-\zeta, a^3-\zeta^3] = \frac{3a(a+1)}{2(a^3-1)}(q(3)+2q(a)),$$

where, *for any* $x \in \mathbb{Z}_l^*$, $q(x) = (x^{l-1}-1)/l$.

Proof. We use the notation $\alpha_n = a^n - \zeta^n$.

(1) Since $\alpha_2 = (a+\zeta)\alpha_1$, we see that $[\alpha_1,\alpha_2] = [a-\zeta, a+\zeta]$. By Lemma 6(2),

$$[a-\zeta, a+\zeta] = \frac{(2a)^l - 2a}{l(a^2-1)} = \frac{2a}{a^2-1}\,q(2a).$$

The result follows by noting that $q(2a) \equiv q(2)+q(a) \pmod{l}$ ([5, Lemma 2]).

(2) Since $\alpha_3 = (a^2+a\zeta+\zeta^2)\alpha_1$, we find that $[\alpha_1,\alpha_3] = \frac{1}{2}[\alpha_1^2, a^2+a\zeta+\zeta^2]$. By Lemma 1, $[\alpha_1^2, a^2+a\zeta+\zeta^2] = [\alpha_1^2,\ 3a\zeta] + [3a\zeta, \alpha_3/\alpha_1]$. Hence $[\alpha_1,\alpha_3] = \frac{3}{2}[\alpha_1, 3a\zeta] - \frac{1}{2}[\alpha_3, 3a\zeta]$. For $n = 1$ or 3, we have $[\alpha_n, 3a\zeta] = [\alpha_n, 3a] + [\alpha_n, \zeta]$, and since $\alpha_n = a^n - (1-\lambda)^n \equiv a^n - 1 + n\lambda \pmod{\lambda^2}$, Lemma 6 shows that

$$[\alpha_n, 3a] = \frac{n}{a^n-1}\,q(3a) \quad \text{and} \quad [\alpha_n,\zeta] = \frac{N(\alpha_n)-1}{l}.$$

Moreover, since $N(\alpha_n) = (a^{nl}-1)/(a^n-1)$, it follows that

$$\frac{N(\alpha_n)-1}{l} = \frac{a^{nl}-a^n}{l(a^n-1)} = \frac{a^n}{a^n-1}\,q(a^n).$$

Therefore,

$$[\alpha_n, 3a\zeta] = \frac{n}{a^n-1}(q(3)+(a^n+1)q(a))$$

(using the additivity of $q(x) \pmod{l}$ [5, Lemma 2]). The result now follows by substitution.

Lemma 8. *Let* $\omega \in \mu_{l-1}$.

(1) *For any* $n \in \mathbb{Z}$ *and* $k \in \mathbb{Z}\setminus l\mathbb{Z}$, $[\omega^n \pm \zeta^k, \zeta] = 0$.

(2) *For any* $j,m,n \in \mathbb{Z}$ *and* $k \in \mathbb{Z}\setminus l\mathbb{Z}$, $[\omega^{-m}-\zeta^{-j}, \omega^n-\zeta^k] = [\omega^m-\zeta^j, \omega^n-\zeta^k]$.

(3) *For any $j,k,m,n\in\mathbb{Z}$ such that $l\nmid j$,*

$$[\omega^m-\zeta^j,\omega^n-\zeta^k]=[\omega^m-\zeta^j,\omega^{m-n}-\zeta^{j-k}]+[\omega^{m-n}-\zeta^{j-k},\omega^n-\zeta^k].$$

(4) *For any $j,k,m,n\in\mathbb{Z}$ such that $l\nmid j+k$,*

$$[\omega^m-\zeta^j,\omega^n-\zeta^k]=[\omega^m-\zeta^j,\omega^{m+n}-\zeta^{j+k}]+[\omega^{m+n}-\zeta^{j+k},\omega^n-\zeta^k].$$

Proof. (1) By Lemma 1,

$$[\omega^n\pm\zeta^k,\zeta]=\frac{1}{k}[\omega^n\pm\zeta^k,\zeta^k]=\frac{1}{k}([\omega^n\pm\zeta^k,\omega^n]+[\omega^n,\zeta^k]).$$

The last two symbols are zero since, by Lemma 3, ω is orthogonal to $\widehat{K}^*$.

(2) We have $\omega^{-m}-\zeta^{-j}=-\omega^{-m}\zeta^{-j}(\omega^m-\zeta^j)$. Therefore

$$[\omega^{-m}-\zeta^{-j},\omega^n-\zeta^k]=[\omega^m-\zeta^j,\omega^n-\zeta^k]-m[\omega,\omega^n-\zeta^k]-j[\zeta,\omega^n-\zeta^k].$$

The latter symbol is zero by (1) above, and the one before it is zero since ω is orthogonal to $\widehat{K}^*$. Hence the result.

(3) We have $\omega^n-\zeta^k=\omega^{n-m}(\omega^m-\omega^{m-n}\zeta^k)$. Since ω is orthogonal to $\widehat{K}^*$, it follows that $[\omega^m-\zeta^j,\omega^n-\zeta^k]=[\omega^m-\zeta^j,\omega^m-\omega^{m-n}\zeta^k]$. By Lemma 1, we have

$$\begin{aligned}[\omega^m-\zeta^j,\omega^m-\omega^{m-n}\zeta^k]&=[\omega^m-\zeta^j,\omega^{m-n}\zeta^k-\zeta^j]\\&\quad+[\omega^{m-n}\zeta^k-\zeta^j,\omega^m-\omega^{m-n}\zeta^k].\end{aligned}$$

Since $\omega^{m-n}\zeta^k-\zeta^j=\zeta^k(\omega^{m-n}-\zeta^{j-k})$ and, by (1) above, as $l\nmid j$, ζ is orthogonal to $\omega^m-\zeta^j$, we find that $[\omega^m-\zeta^j,\omega^{m-n}\zeta^k-\zeta^j]=[\omega^m-\zeta^j,\omega^{m-n}-\zeta^{j-k}]$. Also, and since ω is orthogonal to $\widehat{K}^*$, we have

$$\begin{aligned}[\omega^{m-n}\zeta^k-\zeta^j,\omega^m-\omega^{m-n}\zeta^k]&=[\zeta^k(\omega^{m-n}-\zeta^{j-k}),\omega^n-\zeta^k]\\&=[\zeta^k,\omega^n-\zeta^k]+[\omega^{m-n}-\zeta^{j-k},\omega^n-\zeta^k]\end{aligned}$$

and $[\zeta^k,\omega^n-\zeta^k]=[\zeta^k,\omega^n]+[\omega^n,\omega^n-\zeta^k]=0$. Therefore

$$[\omega^{m-n}\zeta^k-\zeta^j,\omega^m-\omega^{m-n}\zeta^k]=[\omega^{m-n}-\zeta^{j-k},\omega^n-\zeta^k]$$

and the result follows.

(4) It follows from (3) that

$$[\omega^{m+n}-\zeta^{j+k},\omega^n-\zeta^k]=[\omega^{m+n}-\zeta^{j+k},\omega^m-\zeta^j]+[\omega^m-\zeta^j,\omega^n-\zeta^k].$$

Hence the result.

3. Orthogonality conditions. In what follows, ω will denote an element of μ_{l-1} of order f.

PROPOSITION 1. *Assume that, for some $n\in\mathbb{Z}$, $\omega^n-\zeta$ is orthogonal to C. Then*

(1) *$\omega^n-\zeta$ is orthogonal to its $\mathbb{Q}_l$-conjugates and to those of λ.*

(2) *If* $\omega^{2n} \neq 1$, *then* $(\omega^n - 1)^{l-1} \equiv (\omega^n + 1)^{l-1} \equiv 1 \pmod{l^2}$, *and thus* $\omega^n \pm 1$ *are orthogonal to* $\widehat{K}^*$.

Proof. By the same arguments as in the proof of [5, Proposition 6(b)], applied to ω^n instead of a, since $\omega^n - \zeta$ is orthogonal to C, it is orthogonal to its $\mathbb{Q}_l$-conjugates and to those of λ. In particular, $[\omega^n - \zeta, \lambda] = 0$. But, by Lemma 1,

$$[\omega^n - \zeta, \lambda] = [\omega^n - 1 + \lambda, \lambda] = [\omega^n - 1 + \lambda, \omega^n - 1] + [\omega^n - 1, \lambda].$$

And, by Lemma 6, since $\omega^n \neq 1$, we have

$$[\omega^n - 1 + \lambda, \omega^n - 1] = \frac{1}{\omega^n - 1}\, q(\omega^n - 1) \quad \text{and} \quad [\omega^n - 1, \lambda] = \frac{1}{2}\, q(\omega^n - 1).$$

Thus

$$[\omega^n - \zeta, \lambda] = \frac{\omega^n + 1}{2(\omega^n - 1)}\, q(\omega^n - 1) = 0,$$

and since $\omega^n \neq -1$, this implies that $q(\omega^n - 1) = 0$ in $\mathbb{F}_l$, i.e. $(\omega^n - 1)^{l-1} \equiv 1 \pmod{l^2}$. On the other hand, $\omega^n - \zeta$ is also orthogonal to the cyclotomic unit $u_2 = 1 + \zeta$. Therefore, similarly using Lemmas 1 and 6, we get

$$\begin{aligned}[\omega^n - \zeta, 1 + \zeta] &= [\omega^n - 1 + \lambda, \omega^n + 1] + [\omega^n + 1, 2 - \lambda] \\ &= \frac{1}{\omega^n - 1}\, q(\omega^n + 1) + \frac{1}{2}\, q(\omega^n + 1) \\ &= \frac{\omega^n + 1}{2(\omega^n - 1)}\, q(\omega^n + 1) = 0,\end{aligned}$$

which means that $(\omega^n + 1)^{l-1} \equiv 1 \pmod{l^2}$. We conclude, by Lemma 3, that $\omega^n - 1$ and $\omega^n + 1$ are orthogonal to $\widehat{K}^*$.

Proposition 2. (1) *If* $\omega^n - \zeta$ *is orthogonal to* C *for* $1 \leq n \leq f - 1$, *then* $\omega^n - \zeta$ *is orthogonal to* C *for all* $n \in \mathbb{Z}$.

(2) *If* $[\omega^m - \zeta, \sigma_k(\omega^n - \zeta)] = 0$ *for* $1 \leq m, n \leq f - 1$, $1 \leq k \leq l - 1$, *then* $\omega^n - \zeta$ *is orthogonal to* C *and* $[\omega^m - \zeta, \sigma_k(\omega^n - \zeta)] = 0$ *for all* $m, n \in \mathbb{Z}$, $k \in \mathbb{Z} \setminus l\mathbb{Z}$.

Proof. (1) For any $n \in \mathbb{Z}$, if $f \nmid n$, then there is some $1 \leq r \leq f - 1$ such that $n \equiv r \pmod{f}$. Then $\omega^n - \zeta = \omega^r - \zeta$ is, by assumption, orthogonal to C. While if $f \mid n$, then $\omega^n - \zeta = \lambda$ is, by Lemma 5, orthogonal to C.

(2) For $1 \leq n \leq f - 1$ and $2 \leq k \leq l - 1$, we have

$$\omega^n - \zeta - \sigma_k(\omega^n - \zeta) = -\zeta\sigma_{k-1}(\lambda)$$

and thus, by Lemma 1 and the assumption,

$$[\omega^n - \zeta, \sigma_k(\omega^n - \zeta)] = [\omega^n - \zeta, -\zeta\sigma_{k-1}(\lambda)] + [-\zeta\sigma_{k-1}(\lambda), \sigma_k(\omega^n - \zeta)] = 0.$$

Moreover, by Lemma 8, $[\omega^n - \zeta, \zeta] = [\zeta, \sigma_k(\omega^n - \zeta)] = 0$. Hence $[\omega^n - \zeta, \sigma_{k-1}(\lambda)] = [\sigma_k(\omega^n - \zeta), \sigma_{k-1}(\lambda)]$. Letting h denote the inverse of $(k - 1)$

$(\mathrm{mod}\, l)$ lying between 1 and $l-1$, we deduce, using Lemma 2, that

$$[\sigma_h(\omega^n-\zeta),\lambda]=[\sigma_{h+1}(\omega^n-\zeta),\lambda] \quad \text{for } 1\le h\le l-2.$$

Thus $[\sigma_k(\omega^n-\zeta),\lambda]=[\omega^n-\zeta,\lambda]$ for $1\le k\le l-1$; and therefore

$$[N(\omega^n-\zeta),\lambda]=\sum_{k=1}^{l-1}[\sigma_k(\omega^n-\zeta),\lambda]=(l-1)[\omega^n-\zeta,\lambda],$$

where N is the norm map in $\widehat{K}|\mathbb{Q}_l$. Moreover,

$$N(\omega^n-\zeta)=\frac{\omega^{nl}-1}{\omega^n-1}=1.$$

Hence $[\sigma_k(\omega^n-\zeta),\lambda]=-[N(\omega^n-\zeta),\lambda]=0$ for $1\le k\le l-1$. Therefore, by Lemma 2, $\omega^n-\zeta$ is orthogonal to the $\mathbb{Q}$-conjugates of λ, and thus to C. This holds for $1\le n\le f-1$, and thus, by (1), for all $n\in\mathbb{Z}$.

Now, for any $m,n\in\mathbb{Z}$, if $f\nmid m$ and $f\nmid n$, then $m\equiv r \pmod f$ and $n\equiv s \pmod f$, for some $1\le r,s\le f-1$, so that $\omega^m-\zeta=\omega^r-\zeta$ and $\sigma_k(\omega^n-\zeta)=\sigma_k(\omega^s-\zeta)$ are, by assumption, orthogonal (for $1\le k\le l-1$). While if $f\mid n$, then the $\mathbb{Q}_l$-conjugates of $\omega^n-\zeta=\lambda$ are, by Proposition 1, orthogonal to $\omega^m-\zeta$ and, by Lemma 5, to those of λ. A similar conclusion is reached if $f\mid m$. Hence $[\omega^m-\zeta,\sigma_k(\omega^n-\zeta)]=0$ in all cases.

In what follows we make the following assumption:

(A) *For all $n\in\mathbb{Z}$, $\omega^n-\zeta$ is orthogonal to C.*

PROPOSITION 3. *Under assumption* (A), *we have*:

(1) *For any $n\in\mathbb{Z}$ such that $f\nmid 2n$, we have* $(\omega^n-1)^{l-1}\equiv(\omega^n+1)^{l-1}\equiv 1$ $(\mathrm{mod}\, l^2)$, *and thus $\omega^n\pm 1$ are orthogonal to $\widehat{K}^*$.*

(2) *For any $m,n\in\mathbb{Z}$ with* $2m\not\equiv 2n \pmod f$, *we have* $(\omega^m-\omega^n)^{l-1}\equiv(\omega^m+\omega^n)^{l-1}\equiv 1 \pmod{l^2}$, *and thus $\omega^m\pm\omega^n$ are orthogonal to $\widehat{K}^*$.*

(3) *For any $n\in\mathbb{Z}$, the $\mathbb{Q}_l$-conjugates of the elements λ, $\omega^n-\zeta$, $\omega^{-n}-\zeta$ are pairwise orthogonal.*

Proof. (1) This follows from Proposition 1.

(2) This follows from (1) since $\omega^m\pm\omega^n=\omega^n(\omega^{m-n}\pm 1)$ and $f\nmid 2(m-n)$.

(3) By Proposition 1 and Lemma 5, the $\mathbb{Q}_l$-conjugates of λ and $\omega^n-\zeta$ (resp. of λ and $\omega^{-n}-\zeta$) are pairwise orthogonal. Moreover, for $k\in\mathbb{Z}\setminus l\mathbb{Z}$, $\sigma_k(\omega^{-n}-\zeta)=-\omega^{-n}\zeta^k\sigma_{-k}(\omega^n-\zeta)$ is a product of elements which are orthogonal to $\omega^n-\zeta$ and its conjugates. Thus the conjugates of $\omega^{-n}-\zeta$ are orthogonal to those of $\omega^n-\zeta$.

PROPOSITION 4. *Under assumption* (A), *we have, for $m,n\in\mathbb{Z}$ and $k\in\mathbb{Z}\setminus l\mathbb{Z}$*:

(1) *If $f\mid 2m$ or $f\mid 2n$, then $[\omega^m-\zeta,\sigma_k(\omega^n-\zeta)]=0$.*

(2) *If* $m \equiv \pm 2n \pmod f$ *or* $n \equiv \pm 2m \pmod f$, *then*

$$[\omega^m - \zeta, \sigma_k(\omega^n - \zeta)] = 0.$$

Proof. By the skew-symmetry of the symbol and Lemma 2, it is enough to only consider one of the two conditions in each case.

(1) Assume that $f \mid 2n$. Then $\omega^n = \pm 1$ and $\omega^n - \zeta = \pm 1 - \zeta = \lambda$ or $= -(1+\zeta) = -u_2$, which lies in C. Therefore, by assumption (A) and Proposition 1, $\omega^m - \zeta$ is orthogonal to the $\mathbb{Q}_l$-conjugates of $\omega^n - \zeta$.

(2) Since, by Lemmas 8 and 2,

$$[\omega^{-m} - \zeta, \omega^n - \zeta^k] = [\omega^m - \zeta^{-1}, \omega^n - \zeta^k] = -[\omega^m - \zeta, \omega^n - \zeta^{-k}],$$

we may just assume $m \equiv 2n \pmod f$ and, in view of (1), $f \nmid 2n$. Then $\omega^m = \omega^{2n}$ and $\omega^m - \zeta = (\omega^n - \zeta^h)(\omega^n + \zeta^h)$, where $h = (l+1)/2$. Hence $[\omega^m - \zeta, \omega^n - \zeta^k] = [\omega^n - \zeta^h, \omega^n - \zeta^k] + [\omega^n + \zeta^h, \omega^n - \zeta^k]$. By Proposition 1, $[\omega^n - \zeta^h, \omega^n - \zeta^k] = 0$. Thus, Lemma 1 yields

$$\begin{aligned}[\omega^m - \zeta, \omega^n - \zeta^k] &= [\omega^n + \zeta^h, \omega^n - \zeta^k] \\ &= [\omega^n + \zeta^h, \zeta^k(1 + \zeta^{h-k})] + [\zeta^k(1 + \zeta^{h-k}), \omega^n - \zeta^k].\end{aligned}$$

For $k \neq h$, $1 \leq k \leq l-1$, the element $1 + \zeta^{h-k} = u_{2(h-k)}/u_{h-k}$ is the quotient of two cyclotomic units, so that $\zeta^k(1+\zeta^{h-k})$ lies in C. By assumption (A), $\omega^n - \zeta$ and $\omega^{2n} - \zeta$ are orthogonal to C, and thus, by Lemma 2, their $\mathbb{Q}_l$-conjugates are also orthogonal to C. Therefore $\omega^n - \zeta^k = \sigma_k(\omega^n - \zeta)$ and $\omega^n + \zeta^h = (\omega^{2n} - \zeta)/(\sigma_h(\omega^n - \zeta))$ are orthogonal to $\zeta^k(1+\zeta^{h-k})$. It follows that $[\omega^m - \zeta, \omega^n - \zeta^k] = 0$ for $1 \leq k \leq l-1$, $k \neq h$. Moreover, since $f \nmid n$, the norm $N(\omega^n - \zeta)$ is 1 and thus $\sum_{k=1}^{l-1} [\omega^m - \zeta, \omega^n - \zeta^k] = [\omega^m - \zeta, N(\omega^n - \zeta)] = 0$. It follows that also $[\omega^m - \zeta, \omega^n - \zeta^h] = 0$. Hence $[\omega^m - \zeta, \sigma_k(\omega^n - \zeta)] = 0$ for $1 \leq k \leq l-1$.

Proposition 5. *Under assumption* (A), *we have*, *for* $m, n \in \mathbb{Z}$ *and* $k \in \mathbb{Z} \setminus l\mathbb{Z}$,

$$[\omega^m - \zeta^k, \omega^n - \zeta^k] = [\omega^m - \zeta^k, \omega^n - \zeta^{-k}] = 0.$$

Proof. Since, by Lemma 8, $[\omega^m - \zeta^k, \omega^n - \zeta^{-k}] = [\omega^m - \zeta^k, \omega^{-n} - \zeta^k]$, it is enough to get $[\omega^m - \zeta^k, \omega^n - \zeta^k] = 0$ for all m, n, k $(l \nmid k)$. If $2m \equiv 2n \pmod f$, then either $\omega^m = \omega^n$ and the result is trivially true; or $\omega^m = -\omega^n$, in which case $\omega^m - \zeta^k = -(\omega^{2n} - \zeta^{2k})/(\omega^n - \zeta^k)$, so that

$$[\omega^m - \zeta^k, \omega^n - \zeta^k] = [\omega^{2n} - \zeta^{2k}, \omega^n - \zeta^k] = k[\sigma_2(\omega^{2n} - \zeta), \omega^n - \zeta] = 0,$$

by Proposition 4. Assume now that $2m \not\equiv 2n \pmod f$. Then, by Lemma 1,

$$[\omega^m - \zeta^k, \omega^n - \zeta^k] = [\omega^m - \zeta^k, \omega^m - \omega^n] + [\omega^m - \omega^n, \omega^n - \zeta^k],$$

and by Proposition 3, $\omega^m - \omega^n$ is orthogonal to $\widehat{K}^*$. Hence $[\omega^m - \zeta^k, \omega^n - \zeta^k] = 0$.

Proposition 6. *Under assumption* (A), *for* $m, n \in \mathbb{Z}$ *and* $k \in \mathbb{Z} \setminus l\mathbb{Z}$, *if* $2m \equiv \pm 2n \pmod f$, *then* $[\omega^m - \zeta, \sigma_k(\omega^n - \zeta)] = 0$.

Proof. In view of Lemma 8, we may just assume that $2m \equiv 2n \pmod f$, so that $\omega^m = \pm\omega^n$. If $\omega^m = \omega^n$, the result follows from Proposition 1. If $\omega^m = -\omega^n$, then $\omega^m - \zeta = -(\omega^{2n} - \zeta^2)/(\omega^n - \zeta)$ and, by Proposition 1, $\omega^n - \zeta$ is orthogonal to its $\mathbb{Q}_l$-conjugates, so that $[\omega^m - \zeta, \sigma_k(\omega^n - \zeta)] = [\omega^{2n} - \zeta^2, \sigma_k(\omega^n - \zeta)]$. The latter symbol is, by Lemma 2, equal to $2[\omega^{2n} - \zeta, \sigma_{k(l+1)/2}(\omega^n - \zeta)]$, which, by Proposition 4, is equal to 0. Hence the result.

4. Conclusions

Theorem 1. *Let* $\omega \in \mu_{l-1}$, *of order* f, *satisfy the assumption*

(A) *For all* $n \in \mathbb{Z}$, $\omega^n - \zeta$ *is orthogonal to* C.

If $\omega^2 \neq 1$, *i.e. if* $f > 2$, *then*:

(1) $2^{l-1} \equiv 1 \pmod{l^2}$.

(2) *For any divisor* d *of* f *in* $\mathbb{N}$, $d^{l-1} \equiv 1 \pmod{l^2}$.

Proof. (1) Since $\omega^2 \neq 1$, we have $\omega^2 \not\equiv 1 \pmod l$. Indeed the congruence $\omega^2 \equiv 1 \pmod l$ implies, by induction, $\omega^2 = \omega^{2l^n} \equiv 1 \pmod{l^{n+1}}$ for all $n \in \mathbb{N}$, which implies $\omega^2 = 1$. Therefore, by Lemma 7, we have

$$[\omega - \zeta, \omega^2 - \zeta^2] = \frac{2\omega}{\omega^2 - 1}\, q(2),$$

since $q(\omega) = 0$. On the other hand, by Proposition 4(2), $[\omega - \zeta, \omega^2 - \zeta^2] = 0$. It follows that $q(2) = 0$ in $\mathbb{F}_l$, i.e. $2^{l-1} \equiv 1 \pmod{l^2}$.

(2) We may assume $d > 1$. Let $e = f/d$ and $\gamma = \omega^e$. Then γ is a primitive dth root of unity in $\mathbb{Z}_l^*$. Hence $X^d - 1 = \prod_{j=0}^{d-1}(X - \gamma^j)$. Dividing by $X - 1$, we get $\sum_{j=0}^{d-1} X^j = \prod_{j=1}^{d-1}(X - \gamma^j)$. Substituting $X = 1$, we deduce that $d = \prod_{j=1}^{d-1}(1 - \gamma^j) = \prod_{j=1}^{d-1}(1 - \omega^{ej})$. For $1 \leq j \leq d-1$, we have $1 \leq ej < ed = f$, so that $f \nmid ej$. If furthermore $f \nmid 2ej$ then, by Proposition 3, $(1 - \omega^{ej})^{l-1} \equiv 1 \pmod{l^2}$. If however $f \mid 2ej$ then, since $f \nmid ej$, we have $\omega^{ej} = -1$, so that $(1 - \omega^{ej})^{l-1} = 2^{l-1} \equiv 1 \pmod{l^2}$, by (1) above. Thus, for all $1 \leq j \leq d-1$, we have $(1 - \omega^{ej})^{l-1} \equiv 1 \pmod{l^2}$, and therefore $d^{l-1} = \prod_{j=1}^{d-1}(1 - \omega^{ej})^{l-1} \equiv 1 \pmod{l^2}$.

Corollary 1. *Under assumption* (A), *we have*:

(1) *If* l *is not of the form* $2^n + 1$ *then there exists an odd prime factor* p *of* $l - 1$ *which does not divide* f.

(2) *If* $l = 2^n \pm 1$, *for some positive integer* n, *then* $f = 1$ *or* 2.

(3) *If* $l \geq 7$ *then* $f \leq (l-1)/3$.

Proof. (1) By assumption, $l-1$ has at least one odd prime factor. If f is divisible by every odd prime factor p of $l-1$, then $f>2$ and, by Theorem 1, $p^{l-1}\equiv 1 \pmod{l^2}$ for all such p, as well as for $p=2$. Therefore $l-1$, which is a product of powers of those primes, also satisfies $(l-1)^{l-1}\equiv 1 \pmod{l^2}$. But, by the binomial formula, $(l-1)^{l-1}\equiv 1+l\not\equiv 1 \pmod{l^2}$, a contradiction. Hence the result.

(2) If $f>2$ then, by Theorem 1, $2^{l-1}\equiv 1 \pmod{l^2}$. Since $l=2^n\pm 1$, it follows that $(l\mp 1)^{l-1}=2^{n(l-1)}\equiv 1 \pmod{l^2}$. But, by the binomial formula, $(l\mp 1)^{l-1}\equiv 1\pm l\not\equiv 1 \pmod{l^2}$, a contradiction. Hence the result.

(3) If $l-1$ is not a power of 2 then, by (1), there is an odd prime factor p of $l-1$ which does not divide f; hence $pf\mid l-1$ and thus $f\le (l-1)/p\le (l-1)/3$. If $l-1$ is a power of 2 then, by (2), $f\le 2$ and, since $l\ge 7$, this gives $f\le (l-1)/3$.

Theorem 2. *Let $\omega\in\mu_{l-1}$, of order f, satisfy the assumption*

(A) *For all $n\in\mathbb{Z}$, $\omega^n-\zeta$ is orthogonal to C.*

If $f\le 10$ then, for all $m,n\in\mathbb{Z}$ and $k\in\mathbb{Z}\setminus l\mathbb{Z}$, $[\omega^m-\zeta,\sigma_k(\omega^n-\zeta)]=0$.

Proof. For any $m,n\in\mathbb{Z}$, there exist integers $0\le r,s\le f/2$ such that $m\equiv\pm r \pmod f$ and $n\equiv\pm s \pmod f$. If one of the integers $2r, 2s, 2(r\pm s)$, $2r\pm s, r\pm 2s$ is divisible by f, then, by Propositions 4 and 6, $[\omega^m-\zeta,\sigma_k(\omega^n-\zeta)]=0$. Taking into account the skew-symmetry of the symbol, we are reduced to considering the pairs (r,s) such that $0\le r\le s\le f/2$. Moreover, if $r=0$ or $s=f/2$ then $f\mid 2r$ or $f\mid 2s$; if $r=s$ or $s=f/2-r$ then $f\mid 2(r\pm s)$; if $s=2r$ or $f-2r$ then $f\mid 2r\pm s$; if $s=(f-r)/2$ then $f\mid r+2s$. In all these cases, as explained above, we have $[\omega^m-\zeta,\sigma_k(\omega^n-\zeta)]=0$.

Thus, it only remains to consider the pairs (r,s) such that $1\le r<s<f/2$ and $s\ne 2r,\ f-2r,\ f/2-r,\ (f-r)/2$. Let E_f be the set of pairs (r,s) of integers satisfying these conditions. It is easy to check that for $1\le f\le 8$, $E_f=\emptyset$ and thus the result is established for these values of f; while $E_9=\{(1,3),(2,3),(3,4)\}$ and $E_{10}=\{(1,3)\}$.

Let $f=9$. Consider first the case $(r,s)=(1,3)$, i.e. $m\equiv\pm 1 \pmod f$ and $n\equiv\pm 3 \pmod f$. As, by Lemma 8(2) and Lemma 2, $[\omega^{\pm m}-\zeta,\sigma_k(\omega^{\pm n}-\zeta)]=\epsilon_1[\omega^m-\zeta,\sigma_{\epsilon_2 k}(\omega^n-\zeta)]$ with $\epsilon_1,\epsilon_2=\pm 1$, we may assume that $m\equiv 1 \pmod f$ and $n\equiv 3 \pmod f$. Since $l\nmid k$, there is a unique integer h such that $1\le h\le l-1$ and $hk\equiv 1 \pmod l$. Then, for $0\le j\le h-1$, we have $l\nmid(1-jk)$ and, by Lemma 8(3),

$$[\omega^{m-jn}-\zeta^{1-jk},\omega^n-\zeta^k]=[\omega^{m-jn}-\zeta^{1-jk},\omega^{m-(j+1)n}-\zeta^{1-(j+1)k}]$$
$$+[\omega^{m-(j+1)n}-\zeta^{1-(j+1)k},\omega^n-\zeta^k].$$

Moreover, $m-jn\equiv 1-3j \pmod f$, $m-(j+1)n\equiv -2-3j \pmod f$ and $-2-3j\equiv -2(1-3j) \pmod f$, so that, by Proposition 4, for $0\le$

$j \le h-2$, we have $[\omega^{m-jn}-\zeta^{1-jk}, \omega^{m-(j+1)n}-\zeta^{1-(j+1)k}] = 0$ and thus $[\omega^{m-jn}-\zeta^{1-jk}, \omega^n-\zeta^k] = [\omega^{m-(j+1)n}-\zeta^{1-(j+1)k}, \omega^n-\zeta^k]$. It follows that $[\omega^m-\zeta, \omega^n-\zeta^k] = [\omega^{m-(h-1)n}-\zeta^{1-(h-1)k}, \omega^n-\zeta^k]$ and, by Lemma 8, this is equal to $[\omega^{m-(h-1)n}-\zeta^{1-(h-1)k}, \omega^{m-hn}-\zeta^{1-hk}]+[\omega^{m-hn}-\zeta^{1-hk}, \omega^n-\zeta^k]$. Since $l \mid (1-hk)$ and $2(m-hn) \equiv 2(1-3h) \not\equiv 0 \pmod f$, Proposition 3 shows that $\omega^{m-hn}-\zeta^{1-hk} = \omega^{m-hn}-1$ is orthogonal to $\widehat{K}^*$. Hence $[\omega^m-\zeta, \omega^n-\zeta^k] = 0$.

The remaining two cases $(r,s) = (2,3)$ or $(3,4)$ now follow from the previous ones. Indeed, we may, as before, assume that $m \equiv 2 \pmod f$ and $n \equiv 3 \pmod f$ (resp. $m \equiv 3 \pmod f$ and $n \equiv 4 \pmod f$). We may also assume that $k \not\equiv 1 \pmod l$, otherwise we conclude by Proposition 5. By Lemma 8,

$$[\omega^m-\zeta, \omega^n-\zeta^k] = [\omega^m-\zeta, \omega^{m-n}-\zeta^{1-k}] + [\omega^{m-n}-\zeta^{1-k}, \omega^n-\zeta^k].$$

Since $m-n \equiv -1 \pmod f$, from the case $(r,s) = (1,3)$ we deduce that $[\omega^{m-n}-\zeta^{1-k}, \omega^n-\zeta^k] = 0$ (resp. $[\omega^m-\zeta, \omega^{m-n}-\zeta^{1-k}] = 0$). Moreover, by Proposition 4, i.e. by the case $r \equiv \pm 2s \pmod f$, we get $[\omega^m-\zeta, \omega^{m-n}-\zeta^{1-k}] = 0$ (resp. $[\omega^{m-n}-\zeta^{1-k}, \omega^n-\zeta^k] = 0$). Hence $[\omega^m-\zeta, \omega^n-\zeta^k] = 0$.

Let $f = 10$ and consider the remaining case $(r,s) = (1,3)$. Then, as before, we may assume that $m \equiv 1 \pmod f$, $n \equiv 3 \pmod f$ and $k \not\equiv 1 \pmod l$. By Lemma 8 again,

$$[\omega^m-\zeta, \omega^n-\zeta^k] = [\omega^m-\zeta, \omega^{m-n}-\zeta^{1-k}] + [\omega^{m-n}-\zeta^{1-k}, \omega^n-\zeta^k].$$

Since $m-n \equiv -2 \pmod f$, we have $m-n \equiv -2m \pmod f$ and $2(m-n) \equiv 2n \pmod f$. Therefore, by Propositions 4 and 6, $[\omega^m-\zeta, \omega^{m-n}-\zeta^{1-k}] = 0$ and $[\omega^{m-n}-\zeta^{1-k}, \omega^n-\zeta^k] = 0$. Hence $[\omega^m-\zeta, \omega^n-\zeta^k] = 0$.

Corollary 2. *Under assumption* (A), *if* $f \le 10$ *then* $\omega^2 = 1$ (*i.e.* $f \le 2$).

Proof. By Theorem 2, $[\omega^m-\zeta, \sigma_k(\omega^n-\zeta)] = 0$ for all $m,n \in \mathbb{Z}$ and $k \in \mathbb{Z}\backslash l\mathbb{Z}$. Hence, Lemma 2 yields $[\sigma_j(\omega^m-\zeta), \sigma_k(\omega^n-\zeta)] = 0$ for $j,k \in \mathbb{Z}\backslash l\mathbb{Z}$. Now, let $a \in \mathbb{Z}$ be such that $a \equiv \omega \pmod l$. Then $a^l \equiv \omega^l = \omega \pmod{l^2}$. For $n \in \mathbb{Z} \setminus l\mathbb{Z}$, set $\alpha'_n = \alpha_n(a^l) = a^{ln}-\zeta^n$. Then $\alpha'_n \equiv \omega^n-\zeta^n \pmod{l^2}$, hence $\pmod{\lambda^{l+3}}$. On the other hand, $v_\lambda(\alpha'_n) = v_\lambda(a^{ln}-(1-\lambda)^n) = v_\lambda(a^{ln}-1+n\lambda) \le 1$. It follows, in view of Lemma 3, that, for all $m,n \in \mathbb{Z} \setminus l\mathbb{Z}$, $[\alpha'_m, \alpha'_n] = [\omega^m-\zeta^m, \omega^n-\zeta^n]$, the latter symbol being equal to $[\sigma_m(\omega^m-\zeta), \sigma_n(\omega^n-\zeta)] = 0$, by the above. Thus $[\alpha_m(a^l), \alpha_n(a^l)] = 0$ for all $m,n \in \mathbb{N} \setminus l\mathbb{N}$. Therefore, by [7, Theorem 1], $a^l \equiv \pm 1 \pmod l$, i.e. $\omega^2 \equiv 1 \pmod l$, which, as shown in the proof of Theorem 1, amounts to $\omega^2 = 1$.

Corollary 3. *Under assumption* (A), *we have*:

(1) *If* $2^{l-1} \not\equiv 1 \pmod{l^2}$, *then* $\omega^2 = 1$.

(2) *If* $l = 2^n \pm 1$, *for some positive integer* n, *then* $\omega^2 = 1$.

Further, let $l-1=2^{h_0}p_1^{h_1}\dots p_m^{h_m}$, where $p_1,\dots,p_m$ are distinct odd primes and the h_i are positive integers $(0\le i\le m)$.

(3) *If $h_0\le 3$ and $p_i^{l-1}\not\equiv 1 \pmod{l^2}$ for $1\le i\le m$, then $\omega^2=1$.*

(4) *If $h_0\le 3$ and $m=1$, then $\omega^2=1$.*

(5) *If $\sum_{i=1}^m h_iq(p_i)\not\equiv 1 \pmod{l}$, then $\omega^2=1$.*

(6) *If $h_0\le 3$ and, for any proper subset $S\subsetneq\{1,\dots,m\}$, $\sum_{s\in S}h_sq(p_s)\not\equiv 1 \pmod{l}$, then $\omega^2=1$.*

(7) *If $h_0\le 3$, $m=2$ and $h_iq(p_i)\not\equiv 1 \pmod{l}$ for $i=1,2$, then $\omega^2=1$.*

Proof. (1) If $f>2$ then, by Theorem 1, $2^{l-1}\equiv 1 \pmod{l^2}$, contradicting the assumption. Hence $f\le 2$, i.e. $\omega^2=1$.

(2) This is Corollary 1(2).

(3) If $f>2$ then, by Theorem 1, any p_i dividing f should satisfy $p_i^{l-1}\equiv 1 \pmod{l^2}$, but, in view of the assumption, this cannot occur. Therefore $f\mid 2^{h_0}$, and since $h_0\le 3$, we have $f\le 8$. Hence, by Corollary 2, $\omega^2=1$.

(4) Since f divides $l-1=2^{h_0}p_1^{h_1}$ and since, by Corollary 1(1), the odd prime factor p_1 of $l-1$ does not divide f, we find that f divides 2^{h_0}. Thus $f\le 2^{h_0}\le 8$, and we conclude as in (3) above.

(5) If $f>2$ then, by Theorem 1, $2^{l-1}\equiv 1 \pmod{l^2}$, i.e. $q(2)\equiv 0 \pmod{l}$. Hence, by [5, Lemma 2] and the assumption, $q(l-1)\equiv\sum_{i=1}^m h_iq(p_i)\not\equiv 1 \pmod{l}$. But this contradicts the congruence $(l-1)^{l-1}\equiv 1+l \pmod{l^2}$ (see the proof of Corollary 1), which amounts to $q(l-1)\equiv 1 \pmod{l}$.

(6) If $f>2$ then, by Theorem 1, for any prime p_i dividing f $(1\le i\le m)$, $p_i^{l-1}\equiv 2^{l-1}\equiv 1 \pmod{l^2}$, i.e. $q(p_i)\equiv q(2)\equiv 0 \pmod{l}$. Thus, as in the proof of (5) above, $\sum_{p_i\nmid f}h_iq(p_i)\equiv q(l-1)\equiv 1 \pmod{l}$. But, by assumption, no proper subsum of $\sum_{i=1}^m h_iq(p_i)$ is $\equiv 1 \pmod{l}$. Therefore all $p_i\nmid f$ $(1\le i\le m)$, i.e. $f\mid 2^{h_0}$, so that $f\le 2^{h_0}\le 8$, and we conclude as in (3) above.

(7) This is the special case $m=2$ of (6) above.

Corollary 4. *Let $l-1=2^{h_0}p_1^{h_1}\dots p_m^{h_m}$ be the prime factorization of $l-1$, with $p_1,\dots,p_m$ being distinct odd primes and the h_i positive integers* $(0\le i\le m)$.

The conjecture (WTC) *is true for all primes l which satisfy one of the following conditions*:

(a) $2^{l-1}\not\equiv 1 \pmod{l^2}$.

(b) $l=2^n\pm 1$, *for some positive integer n.*

(c) $h_0\le 3$ *and* $p_i^{l-1}\not\equiv 1 \pmod{l^2}$ *for* $1\le i\le m$.

(d) $h_0\le 3$ *and* $m=1$.

(e) $\sum_{i=1}^m h_iq(p_i)\not\equiv 1 \pmod{l}$.

(f) $h_0\le 3$ *and, for any* $S\subsetneq\{1,\dots,m\}$, $\sum_{s\in S}h_sq(p_s)\not\equiv 1 \pmod{l}$.

(g) $h_0\le 3$, $m=2$ *and* $h_iq(p_i)\not\equiv 1 \pmod{l}$ *for* $i=1,2$.

Acknowledgements. I am grateful for the inspiring friendship, through the years, of Guy Terjanian. In particular, the work on this paper started while I was visiting the University of Toulouse. I would like to thank Guy Terjanian and Bruno Anglès for the gracious hospitality, the stimulating conversations and the congenial atmosphere. I also wish to thank the referee for suggesting substantial simplifications in the paper.

References

[1] B. Anglès, *Units and norm residue symbol*, Acta Arith. 98 (2001), 33–51.

[2] E. Artin and J. Tate, *Class Field Theory*, Benjamin, New York, 1967.

[3] H. Hasse, *Bericht über die neueren Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, *Teil II*: *Reziprozitätsgesetz*, Jahresber. Deutsch. Math.-Verein., Leipzig, 1930.

[4] —, *Number Theory*, Springer, Berlin, 1980.

[5] C. Helou, *Norm residue symbol and cyclotomic units*, Acta Arith. 73 (1995), 147–188.

[6] —, *Power reciprocity for binomial cyclotomic integers*, J. Number Theory 71 (1998), 245–256.

[7] G. Terjanian, *Sur la loi de réciprocité des puissances l-èmes*, Acta Arith. 54 (1989), 87–125.

[8] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, New York, 1997.

Pennsylvania State University
25 Yearsley Mill Road
Media, PA 19063, U.S.A.
E-mail: cxh22@psu.edu

Received on 14.6.2000
and in revised form on 22.11.2001 (3838)