ACTA ARITHMETICA
XCVIII.1 (2001)

# Units and norm residue symbol

by

BRUNO ANGLÈS (Caen)

Let $p$ be an odd prime number, $p \geq 5$. Let $\zeta_p$ be a primitive $p$th root of unity and consider the following equation:

$$(*) \quad a, b \in \mathbb{Z},\ ab \neq 0,\ \gcd(a,b)=1,\ (a-b\zeta_p)\mathbb{Z}[\zeta_p] = I^p,\ I \text{ ideal of } \mathbb{Z}[\zeta_p].$$

Then one can show that the $ABC$ conjecture implies that the above equation has a finite number of solutions, and, if $p$ is large enough, $(*)$ has only the trivial solutions, i.e. $a=1$, $b=-1$, and $a=-1$, $b=1$.

When studying the first case of $(*)$ (i.e. $ab(a+b) \not\equiv 0 \pmod p$), G. Terjanian was led to conjecture that the Kummer system of congruences has only the trivial solutions (see [8] and Section 5). In this paper we prove that Eichler's Theorem applies to Terjanian's conjecture (Corollary 5.5). More precisely, we prove that if $i(p) < \sqrt{p} - 2$ then Terjanian's conjecture is true for the prime $p$, where $i(p)$ is the index of irregularity of $p$.

Let $F$ be a real subfield of $\mathbb{Q}(\zeta_p)$ and let $E_F$ be the group of units of $F$. Our aim is to study the *Kummer subgroup* of $E_F$:

$$E_F^{\mathrm{Kum}} = \{\varepsilon \in E_F : \exists a \in \mathbb{Z},\ \varepsilon \equiv a \pmod p\}.$$

We show that there exists a duality between $E_F/E_F^{\mathrm{Kum}}$ and the orthogonal of $E_F$ for the norm residue symbol (see Theorem 4.4). A natural problem arises: do we have an equivalence in Kummer's Lemma (see Section 3)? We show that this question is connected to a class number congruence obtained by T. Metsänkylä (see [4] and Section 6). In particular, we are led to investigate the orthogonal of the group of units of $\mathbb{Q}(\zeta_p)$ for the norm residue symbol and, thus, this leads us to Terjanian's conjecture.

Finally, we would like to mention the following question which we call the "weak Kummer–Vandiver conjecture": let $E$ be the group of units of $\mathbb{Q}(\zeta_p)$ and let $C$ be the group of cyclotomic units of $\mathbb{Q}(\zeta_p)$; do we have $E^{\perp} = C^{\perp}$ (see Section 4)?

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

**1. Notations.** Let $p$ be an odd prime number. Let $\mathbb{Z}_p$ be the ring of $p$-adic integers, $\mathbb{Q}_p$ the field of $p$-adic numbers, and $\mathbb{C}_p$ a completion of an algebraic closure of $\mathbb{Q}_p$. All the finite extensions of $\mathbb{Q}_p$ considered in this paper are contained in $\mathbb{C}_p$.

Let $L/\mathbb{Q}_p$ be a finite extension. We set:

- $O_L$ — the integral closure of $\mathbb{Z}_p$ in $L$,
- $\mathfrak{p}_L$ — the maximal ideal of $O_L$,
- $v_L$ — the normalized discrete valuation on $L$ associated with $\mathfrak{p}_L$,
- $U_L$ — the group of units of $O_L$ and for $n \geq 1$, $U_L^{(n)} = 1 + \mathfrak{p}_L^n$.

Let $L/\mathbb{Q}_p$ be a finite extension and let $L'/L$ be a finite abelian extension. We denote the local Artin map associated with $L'/L$ by $(\cdot, L'/L)$.

Let $\zeta_p$ be a fixed primitive $p$th root of unity in $\mathbb{C}_p$. We set $\lambda_p = \zeta_p - 1$ and $K = \mathbb{Q}_p(\zeta_p)$. For $\alpha, \beta \in K^*$, we define the norm residue symbol $(\alpha, \beta)$ as follows:

$$(\alpha, \beta) = \frac{(\beta, K(\gamma)/K)(\gamma)}{\gamma},$$

where $\gamma \in \mathbb{C}_p$ is such that $\gamma^p = \alpha$.

Let $G = \mathrm{Gal}(K/\mathbb{Q}_p)$. For $a \in \mathbb{Z} \setminus p\mathbb{Z}$ we define $\sigma_a$ to be the element of $G$ such that $\sigma_a(\zeta_p) = \zeta_p^a$. Recall that we have an isomorphism of groups $(\mathbb{Z}/p\mathbb{Z})^* \to G$, $\overline{a} \mapsto \sigma_a$. Let $\widehat{G}$ be the set of group homomorphisms between $G$ and $\mathbb{Z}_p^*$. The *Teichmüller character* $\omega$ is the element $\omega \in \widehat{G}$ such that

$$\omega(\sigma_a) \equiv a \pmod{p}.$$

Recall that $\widehat{G}$ is a cyclic group and that $\omega$ is a generator of $\widehat{G}$.

We view $\mathbb{Q}$ as contained in $\mathbb{Q}_p$. Let $F/\mathbb{Q}$ be a finite extension, $F \subset \mathbb{C}_p$. We set

- $\widehat{F} = F\mathbb{Q}_p$,
- $O_F$ — the ring of integers of $F$,
- $E_F$ — the group of units of $O_F$,
- $\mathfrak{p}_F = \mathfrak{p}_{\widehat{F}} \cap O_F$,
- $h_F$ — the class number of $F$.

If $A$ is a commutative unitary ring, we denote the set of invertible elements of $A$ by $A^*$. Let $n \geq 1$ be an integer. We denote the group of $n$th roots of unity in $\mathbb{C}_p$ by $\mu_n$.

**2. Some results from Lubin–Tate theory.** First, we recall some basic facts from Lubin–Tate theory (see [3], Chapter 8). We consider the following two elements in $\mathbb{Z}_p[[X]]$:

$$T(X) = (1+X)^p - 1 \quad \text{and} \quad L(X) = X^p + pX.$$

Then $T$ and $L$ are Lubin–Tate polynomials. Thus there exist two formal groups $F_T = \mathbb{G}_{\mathrm{m}}$ and $F_L$ in $\mathbb{Z}_p[[X,Y]]$ such that

$$T \circ F_T = F_T \circ T \quad \text{and} \quad L \circ F_L = F_L \circ L.$$

We have two ring homomorphisms: $\mathbb{Z}_p \to \mathrm{End}_{\mathbb{Z}_p}\mathbb{G}_{\mathrm{m}}$, $a \mapsto [a]_T = (1+X)^a - 1$ and $\mathbb{Z}_p \to \mathrm{End}_{\mathbb{Z}_p} F_L$, $a \mapsto [a]_L$. Note that

- $\forall a \in \mathbb{Z}_p,\ [a]_T \equiv [a]_L \equiv aX \pmod{\deg 2}$,
- $F_T(X,Y) = (1+X)(1+Y) - 1$, $F_L(X,Y) \equiv X + Y \pmod{\deg p}$,
- $\forall a \in \mathbb{Z}_p,\ [a]_L \equiv aX \pmod{\deg p}$, $\forall \varepsilon \in \mu_{p-1}$, $[\varepsilon]_L = \varepsilon X$.

We set

$$\mathrm{Log}_T(X) = \lim_{n\ge 1} \frac{1}{p^n}[p^n]_T \in \mathbb{Q}_p[[X]],$$
$$\mathrm{Log}_L(X) = \lim_{n\ge 1} \frac{1}{p^n}[p^n]_L \in \mathbb{Q}_p[[X]].$$

Note that

$$\mathrm{Log}_T(X) = \sum_{n\ge 1} (-1)^{n+1}\frac{X^n}{n} \quad \text{and} \quad \mathrm{Log}_L(X) \equiv X \pmod{\deg p}.$$

We denote the inverses of $\mathrm{Log}_T$ and $\mathrm{Log}_L$ by $\mathrm{Exp}_T$ and $\mathrm{Exp}_L$ respectively.

We set $f_p(X) = \mathrm{Exp}_T \circ \mathrm{Log}_L$ and $g_p(X) = \mathrm{Exp}_L \circ \mathrm{Log}_T$. Then $f_p$ and $g_p$ are elements of $\mathbb{Z}_p[[X]]$ and we have:

- $f_p(X) \equiv g_p(X) \equiv X \pmod{\deg 2}$,
- $\forall a \in \mathbb{Z}_p,\ f_p \circ [a]_L = [a]_T \circ f_p$ and $g_p \circ [a]_T = [a]_L \circ g_p$,
- $f_p \circ F_L = F_T \circ f_p$ and $g_p \circ F_T = F_L \circ g_p$,
- $f_p \circ g_p = g_p \circ f_p = X$.

Let $v_p$ be the $p$-adic valuation on $\mathbb{C}_p$ such that $v_p(p) = 1$. Set $D = \{\alpha \in \mathbb{C}_p : v_p(\alpha) > 0\}$. Then $T$ induces a new structure of $\mathbb{Z}_p$-module for $D$ and we denote this $\mathbb{Z}_p$-module by $D_T$; the same holds for $L$ and we denote $D$ equipped with the structure of $\mathbb{Z}_p$-module induced by $L$ by $D_L$. We have an isomorphism of $\mathbb{Z}_p$-modules $D_T \to D_L$, $\alpha \mapsto g_p(\alpha)$. Set $\Lambda_T = \{\alpha \in \mathbb{C}_p : [p]_T(\alpha) = 0\}$ and $\Lambda_L = \{\alpha \in \mathbb{C}_p : [p]_L(\alpha) = 0\}$. Then $\Lambda_T$ is a $\mathbb{Z}_p$-submodule of $D_T$ and $\Lambda_L$ is a $\mathbb{Z}_p$-submodule of $D_L$. Note that $g_p$ induces an isomorphism of the $\mathbb{Z}_p$-modules $\Lambda_T$ and $\Lambda_L$. We have $\lambda_p \in \Lambda_T$. We set

$$\lambda_L = g_p(\lambda_p).$$

Note that $\lambda_L^{p-1} = -p$ and $K = \mathbb{Q}_p(\lambda_p) = \mathbb{Q}_p(\lambda_L)$.

Lemma 2.1. *We have*

$$g_p(X) \equiv \sum_{n=1}^{p-1} (-1)^{n+1}\frac{X^n}{n} \pmod{X^p\mathbb{Z}_p[[X]]},$$

$$f_p(X) \equiv \sum_{n=1}^{p-1} \frac{X^n}{n!} \pmod{X^p \mathbb{Z}_p[[X]]}.$$

*Proof.* This comes from the fact that $\mathrm{Exp}_L(X) \equiv \mathrm{Log}_L(X) \equiv X \pmod{\deg p}$. ∎

COROLLARY 2.2.

(i) $\lambda_L \equiv \sum_{n=1}^{p-1} (-1)^{n+1} \frac{\lambda_p^n}{n} \pmod{\mathfrak{p}_K^p}$;

(ii) $\lambda_p \equiv \sum_{n=1}^{p-1} \frac{\lambda_L^n}{n!} \pmod{\mathfrak{p}_K^p}$.

LEMMA 2.3. *Let* $\sigma \in G$.

(i) $\sigma(\lambda_p) = [\omega(\sigma)]_T(\lambda_p)$;
(ii) $\sigma(\lambda_L) = \omega(\sigma)\lambda_L$.

*Proof.* The first assertion is obvious. We have

$$\sigma(\lambda_L) = \sigma(g_p(\lambda_p)) = g_p(\sigma(\lambda_p)).$$

Thus $\sigma(\lambda_L) = g_p([\omega(\sigma)]_T(\lambda_p)) = [\omega(\sigma)]_L(g_p(\lambda_p)) = \omega(\sigma)\lambda_L$. ∎

Let $k$ be an integer, $1 \leq k \leq p-1$. We set

$$\eta_k = \sum_{i=1}^{p-1} (i!)^{k-1} \tau(\omega^{-i})^k,$$

where, for $i = 1, \ldots, p-1$,

$$\tau(\omega^{-i}) = -\sum_{\sigma \in G} \omega(\sigma)^{-i} \sigma(\lambda_p) \in \mathfrak{p}_K.$$

Note that $\eta_1 = (1-p)\lambda_p$.

PROPOSITION 2.4. *Let* $k$ *be an integer*, $1 \leq k \leq p-1$.

(i) $\eta_k \equiv f_p(\lambda_L^k) \pmod{\mathfrak{p}_K^p}$;
(ii) $\lambda_L^k \equiv g_p(\eta_k) \pmod{\mathfrak{p}_K^p}$;
(iii) $\forall \sigma \in G,\ \sigma(1+\eta_k) \equiv (1+\eta_k)^{\omega(\sigma)^k} \pmod{\mathfrak{p}_K^p}$.

*Proof.* Let $\sigma \in G$. We have

$$\sigma(\lambda_p) \equiv \sum_{n=1}^{p-1} \omega(\sigma)^n \frac{\lambda_L^n}{n!} \pmod{\mathfrak{p}_K^p}.$$

Thus

$$\tau(\omega^{-i}) \equiv \frac{\lambda_L^i}{i!} \pmod{\mathfrak{p}_K^p}.$$

Therefore we have (i) and (ii). Now, let $\sigma \in G$. Then

$$\sigma(\eta_k) \equiv f_p(\omega(\sigma)^k \lambda_L^k) \equiv [\omega(\sigma)^k]_T(f_p(\lambda_L^k)) \equiv (1+\eta_k)^{\omega(\sigma)^k} - 1 \pmod{\mathfrak{p}_K^p}.$$

Thus we have (iii). ∎

Now, we recall the definition of the Kummer homomorphisms (see [3], Chapter 7). Let $u \in U_K$ and write $u = h(\lambda_L)$ for some $h(X) \in \mathbb{Z}_p[[X]]$. Then $h'(\lambda_L)/u$ is well defined modulo $\mathfrak{p}_K^{p-2}$ and we can write

$$\frac{h'(\lambda_L)}{u} \equiv \sum_{k=1}^{p-2} \varphi_k(u)\lambda_L^{k-1} \pmod{\mathfrak{p}_K^{p-2}},$$

where $\varphi_k(u)$ is in $\mathbb{Z}_p$ modulo $p\mathbb{Z}_p$ for $k = 1, \ldots, p-2$. The map $\varphi_k$ is called the *Kummer homomorphism* of degree $k$.

We have the following basic properties:

- $\varphi_k : U_K \to \mathbb{F}_p$ is a surjective group homomorphism and $\mu_{p-1}U_K^{(k+1)} \subset \ker \varphi_k$;
- $\forall \sigma \in G, \forall u \in U_K,\ \varphi_k(\sigma(u)) \equiv \omega(\sigma)^k \varphi_k(u) \pmod{p}$;
- $\forall u \in U_K^{(1)}, \forall a \in \mathbb{Z}_p,\ \varphi_k(u^a) \equiv a\varphi_k(u) \pmod{p}$;
- $\bigcap_{1 \le k \le p-2} \ker \varphi_k = \mu_{p-1}U_K^{(p-1)}$.

We calculate the values of these homomorphisms for some remarkable elements.

PROPOSITION 2.5.

(i) $\varphi_1(\zeta_p) = 1$ *and for* $k \ge 2$, $\varphi_k(\zeta_p) = 0$;
(ii) $\varphi_k(\lambda_p/\lambda_L) = (-1)^k B_k/k!$, *where* $B_k$ *is the* $k$*th Bernoulli number*;
(iii) *let* $\sigma \in G$, $\varphi_k(\sigma(\lambda_p)/\lambda_p) = (-1)^k(\omega(\sigma)^k - 1)B_k/k!$;
(iv) $\varphi_k(1+\eta_i) = 0$ *if* $k \ne i$ *and* $\varphi_k(1+\eta_k) = k$;
(v) *let* $a \in \mathbb{Z}$, $a \not\equiv 1 \pmod{p}$, $\varphi_1(a - \zeta_p) = -1/(a-1)$ *and for* $k \ge 2$,

$$\varphi_k(a - \zeta_p) = \frac{(-1)^{k-1}}{(k-1)!(a-1)} M_k(a),$$

*where* $M_k(X) = \sum_{i=1}^{p-1} i^{k-1} X^i$ *is the* $k$*th Mirimanoff polynomial.*

*Proof.* (i) Write $h(X) = \sum_{n=0}^{p-2} X^n/n!$. Then $\zeta_p \equiv h(\lambda_L) \pmod{\mathfrak{p}_K^p}$. Thus $\varphi_k(\zeta_p) = \varphi_k(h(\lambda_L))$. But

$$\frac{h'(\lambda_L)}{h(\lambda_L)} \equiv \zeta_p^{-1} h'(\lambda_L) \equiv \left(\sum_{n=0}^{p-3} (-1)^n \frac{\lambda_L^n}{n!}\right)\left(\sum_{n=0}^{p-3} \frac{\lambda_L^n}{n!}\right) \equiv 1 \pmod{\mathfrak{p}_K^{p-2}}.$$

(ii) Put $h(X) = f_p(X)/X$. Then $\lambda_p/\lambda_L = h(\lambda_L)$. One can show that

$$\frac{h'(X)}{h(X)} \equiv B_1 + 1 + \sum_{k \ge 2} \frac{B_k}{k!} X^{k-1} \pmod{\deg p - 2}.$$

The result follows.

(iii) Let $\sigma \in G$. We have

$$\varphi_k\left(\frac{\sigma(\lambda_p)}{\lambda_p}\right) = \varphi_k\left(\sigma\left(\frac{\lambda_p}{\lambda_L}\right)\right) + \varphi_k\left(\frac{\sigma(\lambda_L)}{\lambda_p}\right) = (\omega(\sigma)^k - 1)\varphi_k\left(\frac{\lambda_p}{\lambda_L}\right).$$

(iv) Set $h(X) = f_p(X^k)+1$. We have $1+\eta_k \equiv h(\lambda_L) \pmod{\mathfrak{p}_K^p}$. Therefore $\varphi_i(1+\eta_k) = \varphi_i(h(\lambda_L))$. But

$$\frac{h'(X)}{h(X)} \equiv kX^{k-1} \ (\operatorname{mod} \deg p - 2),$$

and the result follows.

(v) We have

$$a - \zeta_p \equiv a - 1 - \lambda_L \pmod{\mathfrak{p}_K^2}.$$

Therefore

$$\varphi_1(a - \zeta_p) = \varphi_1(a - 1 - \lambda_L) = \frac{-1}{a-1}.$$

If $a \equiv 0 \pmod p$, then for $k \geq 2$, we have $\varphi_k(a - \zeta_p) = 0$. Now, we suppose that $a \not\equiv 0 \pmod p$. We have

$$D^k \operatorname{Log}(a - \operatorname{Exp}(X))_{X=0} \equiv (k-1)!\varphi_k(a - \zeta_p) \pmod p.$$

But, by [5], Chapter VIII,

$$D^k \operatorname{Log}(a - \operatorname{Exp}(X))_{X=0} \equiv \frac{(-1)^{p-k}}{a-1} M_k(a) \pmod p.$$

The result follows. ■

We recall some basic facts about $\mathbb{F}_p[G]$-modules. For $\chi \in \widehat{G}$, we write

$$e_\chi = \frac{1}{p-1} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \pmod p.$$

We have

- $e_\chi^2 = e_\chi$;
- $e_\chi e_\psi = 0$ if $\chi \neq \psi$;
- $1 = \sum_{\chi \in \widehat{G}} e_\chi$;
- $\forall \sigma \in G,\ \sigma e_\chi = \chi(\sigma) e_\chi$.

Let $A$ be an $\mathbb{F}_p[G]$-module. For $1 \leq i \leq p-1$, we set

$$A(i) = e_{\omega^i} A = \{a \in A : \forall \sigma \in G,\ \sigma(a) = \omega(\sigma)^i a\}.$$

We have

$$A = \bigoplus_{i=1}^{p-1} A(i).$$

We set

$$\mathcal{U} = \frac{U_K}{\mu_{p-1} U_K^{(p)}}.$$

It is clear that $\mathcal{U}$ is a finite $\mathbb{F}_p[G]$-module and that, for $1 \le i \le p-1$, $\mathcal{U}(i)$ is an $\mathbb{F}_p$-vector space of dimension 1. More precisely, let $u \in \mathcal{U}$; then $e_{\omega^i} u$ generates $\mathcal{U}(i)$ if and only if

- $\varphi_i(u) \neq 0$ if $1 \le i \le p-2$;
- $N_{K/\mathbb{Q}_p}(u) \not\equiv 1 \pmod{p^2}$ for $i = p-1$.

In particular, for $1 \le k \le p-1$, $1+\eta_k \in \mathcal{U}(k)$ and $1+\eta_k$ generates $\mathcal{U}(k)$.

PROPOSITION 2.6. *Let $u \in U_K$. Then*

$$\mathrm{Log}_p(u) \equiv \frac{N_{K/\mathbb{Q}_p}(u) - 1}{p} \lambda_L^{p-1} + \sum_{k=2}^{p-2} \frac{1}{k} \varphi_k(u) \lambda_L^k \pmod{\mathfrak{p}_K^p},$$

*where* $\mathrm{Log}_p$ *is the usual $p$-adic logarithm on $\mathbb{C}_p^*$.*

*Proof.* Note that we can suppose $u \in U_K^{(1)}$. We have $\mathrm{Log}_p(u) \in \mathfrak{p}_K$ and, if $u \in U_K^{(p)}$, $\mathrm{Log}_p(u) \in \mathfrak{p}_K^p$. Therefore, $\mathrm{Log}_p$ induces a group homomorphism between $\mathcal{U}$ and $\mathfrak{p}_k/\mathfrak{p}_K^p$. Note that, for $k \ge 2$,

$$\mathrm{Log}_p(1+\eta_k) \equiv g_p(\eta_k) \equiv \lambda_L^k \pmod{\mathfrak{p}_K^p}$$

and

$$\mathrm{Log}_p(1+\eta_1) \equiv \mathrm{Log}_p(\zeta_p) \equiv 0 \pmod{\mathfrak{p}_K^p}.$$

Let $u \in U_K^{(2)}$. We have

$$u \equiv \prod_{k=2}^{p-1} (1+\eta_k)^{a_k} \pmod{U_K^{(p)}},$$

where $a_k \in \mathbb{F}_p$. Thus

$$\mathrm{Log}_p(u) \equiv \sum_{k=2}^{p-1} a_k \lambda_L^k \equiv \sum_{k=2}^{p-2} \frac{1}{k} \varphi_k(u) \lambda_L^k + a_{p-1} \lambda_L^{p-1} \pmod{\mathfrak{p}_K^p}.$$

But

$$e_{\omega^{p-1}} u \equiv (1+\eta_{p-1})^{a_{p-1}} \equiv N_{K/\mathbb{Q}_p}(u)^{-1} \pmod{U_K^{(p)}}.$$

Thus

$$-\mathrm{Log}_p(N_{K/\mathbb{Q}_p}(u)) \equiv -a_{p-1} p \pmod{\mathfrak{p}_K^p}.$$

But

$$\mathrm{Log}_p(N_{K/\mathbb{Q}_p}(u)) \equiv N_{K/\mathbb{Q}_p}(u) - 1 \pmod{p^2}.$$

Therefore we get our result for $u \in U_K^{(2)}$.

Now, if $u \in U_K^{(1)}$, there exists an integer $a_1$ such that $u(1+\eta_1)^{a_1} \in U_K^{(2)}$. But

$$\mathrm{Log}_p(u(1+\eta_1)^{a_1}) \equiv \mathrm{Log}_p(u) \pmod{\mathfrak{p}_K^p},$$
$$N_{K/\mathbb{Q}_p}(u(1+\eta_1)^{a_1}) \equiv N_{K/\mathbb{Q}_p}(u) \pmod{p^2}.$$

For $k \geq 2$,

$$\varphi_k(u(1+\eta_1)^{a_1}) = \varphi_k(u).$$

The proposition follows. ■

We recall the definition of the local Kummer symbol relative to $L$ (see [3], Chapter 8). Let $z \in \mathfrak{p}_K$ and let $\alpha \in K^*$. Let $t \in \mathbb{C}_p$ be such that $[p]_L(t) = z$. We set

$$\langle z, \alpha \rangle_L = F_L((\alpha, K(t)/K)(t), -t) \in \Lambda_L.$$

This symbol is connected to the norm residue symbol as follows: let $u \in U_K^{(1)}$ and let $\alpha \in K^*$; then

$$(u, \alpha) - 1 = f_p(\langle g_p(u-1), \alpha \rangle_L).$$

Furthermore, we have the following explicit reciprocity law for $\langle \cdot, \cdot \rangle_L$:

THEOREM 2.7. *Let* $z \in \mathfrak{p}_K$ *and let* $u \in U_K$. *Write* $z \equiv \sum_{i=1}^{p-1} a_i \lambda_L^i \pmod{\mathfrak{p}_K^p}$, *where* $a_i \in \mathbb{F}_p$. *Then*

$$\langle z, u \rangle_L = \left[ a_1 \frac{N_{K/\mathbb{Q}_p}(u^{-1}) - 1}{p} + \sum_{i=2}^{p-1} a_i \varphi_{p-i}(u) \right]_L (\lambda_L).$$

*Proof.* See [3], Chapter 9. ■

**3. Kummer subgroups of units.** Recall that $\mathcal{U} = U_K/(\mu_{p-1}U_K^{(p)})$. Set

$$V = \mathbb{Q}(\zeta_p) \cap U_K, \quad V^{\mathrm{Kum}} = V \cap \mu_{p-1}U_K^{(p)}, \quad \mathcal{V} = V/V^{\mathrm{Kum}}.$$

Then we have an isomorphism of the $\mathbb{F}_p[G]$-modules $\mathcal{V}$ and $\mathcal{U}$.

Let $B$ be a subgroup of $V$. We define the *Kummer subgroup* of $B$ to be

$$B^{\mathrm{Kum}} = B \cap V^{\mathrm{Kum}} = B \cap \mu_{p-1}U_K^{(p)}.$$

Note that

$$B^{\mathrm{Kum}} \subset \{\alpha \in B : \exists a \in \mathbb{Z},\ \alpha \equiv a \pmod{\mathfrak{p}_K^p}\}.$$

Let $F$ be a real subfield of $\mathbb{Q}(\zeta_p)$. The *group of cyclotomic units* of $F$ is the subgroup of $E_F$ generated by $-1$ and $N_{\mathbb{Q}(\zeta_p)^+/F}(\zeta_p^{(1-a)/2}(\zeta_p^a - 1)/(\zeta_p - 1))$, for $2 \leq a \leq (p-1)/2$; we denote this group by $\mathrm{Cyc}_F$. Recall that

$$(E_F : \mathrm{Cyc}_F) = h_F.$$

In this section, our aim is to study the $\mathbb{F}_p[G]$-module $\mathrm{Cyc}_F / \mathrm{Cyc}_F^{\mathrm{Kum}}$. In particular, Theorem 3.2 will generalize a result of Vostokov (see [9], Theorem 1) and we will obtain Kummer's Lemma (see [10], Theorem 5.36) as a corollary.

Now, let $F$ be a real subfield of $\mathbb{Q}(\zeta_p)$ and set $l = [F : \mathbb{Q}]$. We suppose that $l \geq 2$.

Lemma 3.1. *We have*

$$E_F^{\mathrm{Kum}} = \{\alpha \in E_F : \exists a \in \mathbb{Z},\ \alpha \equiv a \pmod p\} = E_F \cap (K^*)^p,$$
$$E_F^{\mathrm{Kum}} = \{\alpha \in E_F : \mathrm{Log}_p(\alpha) \equiv 0 \pmod{\mathfrak{p}_K^p}\}.$$

*Proof.* By [10], page 80,

$$\{\alpha \in E_F : \exists a \in \mathbb{Z},\ \alpha \equiv a \pmod p\} = E_F \cap (K^*)^p.$$

As already noticed, $E_F^{\mathrm{Kum}}$ is a subgroup of this latter group. Now, let $\alpha \in E_F$ be such that $\alpha \equiv a \pmod p$ for some integer $a$. Then there exists $\epsilon \in \mu_{p-1}$ such that $\alpha\epsilon \in U_K^{(p-1)}$. But $N_{K/\mathbb{Q}_p}(\alpha\epsilon) = 1$. Therefore $\alpha\epsilon \in U_K^{(p)}$. Thus $\alpha \in E_F^{\mathrm{Kum}}$.

Now, recall that $(U_K)^p = \mu_{p-1}U_K^{(p+1)}$. Thus

$$E_F^{\mathrm{Kum}} \subset \{\alpha \in E_F : \mathrm{Log}_p(\alpha) \equiv 0 \pmod{\mathfrak{p}_K^p}\}.$$

Let $\alpha$ be in the right side group. Then, by Proposition 2.6, $\varphi_k(\alpha) = 0$ for $k = 1, \ldots, p-2$. Therefore $\alpha \in \mu_{p-1}U_K^{(p-1)}$. But $N_{K/\mathbb{Q}_p}(\alpha) = 1$, thus $\alpha \in \mu_{p-1}U_K^{(p)}$, i.e. $\alpha \in E_F^{\mathrm{Kum}}$. ■

We define the *index of regularity* of $F$ to be

$$r(F) = |\{i : 1 \le i \le l-1,\ B_{i(p-1)/l} \not\equiv 0 \pmod p\}|.$$

The *index of irregularity* of $F$ is then

$$i(F) = l - 1 - r(F).$$

We call $F$ *regular* if $i(F) = 0$. Note that, in this case, $p$ does not divide $h_F$ (see [10], Theorem 5.24).

If $F = \mathbb{Q}(\zeta_p)^+$, then $i(F) = i(p)$, the index of irregularity of $p$.

Theorem 3.2. *Let $F$ be a real subfield of $\mathbb{Q}(\zeta_p)$ with $[F:\mathbb{Q}] = l \ge 2$.*

(i) *If $i = p-1$ or if $i \not\equiv 0 \pmod{(p-1)/l}$, then*

$$\frac{\mathrm{Cyc}_F}{\mathrm{Cyc}_F^{\mathrm{Kum}}}(i) = 0.$$

(ii) *For $j = 1, \ldots, l-1$,*

$$\frac{\mathrm{Cyc}_F}{\mathrm{Cyc}_F^{\mathrm{Kum}}}\left(j\frac{(p-1)}{l}\right) = 0 \ \Leftrightarrow\ B_{j(p-1)/l} \equiv 0 \pmod p.$$

(iii) *We have*

$$\dim_{\mathbb{F}_p} \frac{\mathrm{Cyc}_F}{\mathrm{Cyc}_F^{\mathrm{Kum}}} = r(F).$$

*Proof.* We view $\mathrm{Cyc}_F/\mathrm{Cyc}_F^{\mathrm{Kum}}$ as an $\mathbb{F}_p[G]$-submodule of $\mathcal{U}$. Since $N_{K/\mathbb{Q}_p}(E_F)=\{1\}$, we have

$$\frac{\mathrm{Cyc}_F}{\mathrm{Cyc}_F^{\mathrm{Kum}}}(p-1)=0.$$

Now, suppose that there exists $\epsilon\in E_F$ such that $\varphi_i(\epsilon)\neq 0$. Then

$$\varphi_i(\epsilon^{(p-1)/l})=\varphi_i(N_{K/\widehat{F}}(\epsilon))\neq 0.$$

But $\mathrm{Gal}(K/\widehat{F})=G^l$, thus

$$\varphi_i(N_{K/\widehat{F}}(\epsilon))=\frac{1}{l}\Big(\sum_{\sigma\in G}\omega(\sigma)^{il}\Big)\varphi_i(\epsilon).$$

Thus $il\equiv 0 \pmod{p-1}$ and we get (i).

By Proposition 2.5, for $k\geq 2$, we have

$$\varphi_k\left(\frac{\sigma_a(\lambda_p)}{\lambda_p}\right)=(-1)^k(\omega(\sigma_a)^k-1)\frac{B_k}{k!}.$$

Therefore we get (ii) and (iii). ∎

We recover Kummer's Lemma:

Corollary 3.3. *Suppose that $F$ is regular. Then $E_F^{\mathrm{Kum}}=(E_F)^p$.*

*Proof.* In this case, we have

$$\dim_{\mathbb{F}_p}\frac{\mathrm{Cyc}_F}{\mathrm{Cyc}_F^{\mathrm{Kum}}}=l-1.$$

But $\mathrm{Cyc}_F\cap E_F^{\mathrm{Kum}}=\mathrm{Cyc}_F^{\mathrm{Kum}}$, thus

$$\dim_{\mathbb{F}_p}\frac{E_F}{E_F^{\mathrm{Kum}}}\geq l-1.$$

Note that $(E_F)^p\subset E_F^{\mathrm{Kum}}$ and

$$\dim_{\mathbb{F}_p}\frac{E_F}{(E_F)^p}=l-1.$$

Therefore we get the desired result. ∎

A natural problem arises: do we have an equivalence in Kummer's Lemma? It is not difficult to show that if $p$ does not divide $h_F$, then $E_F^{\mathrm{Kum}}=(E_F)^p$ implies that $F$ is regular. In fact, we have

Proposition 3.4. *Let $F$ be a real subfield of $\mathbb{Q}(\zeta_p)$. Suppose that $p^{\max(i(F),1)}$ does not divide $h_F$. Then $E_F^{\mathrm{Kum}}=(E_F)^p$ implies $i(F)=0$.*

*Proof.* If $E_F^{\mathrm{Kum}}=(E_F)^p$, then

$$\dim_{\mathbb{F}_p}\frac{E_F}{\mathrm{Cyc}_F\,E_F^{\mathrm{Kum}}}=i(F).$$

Since $h_F=(E_F:\mathrm{Cyc}_F)$, $p^{i(F)}$ divides $h_F$. ∎

**4. The orthogonal of local units.** Recall that

$$\mathcal{V} = \frac{\mathbb{Q}(\zeta_p) \cap U_K}{\mathbb{Q}(\zeta_p) \cap \mu_{p-1} U_K^{(p)}}$$

is an $\mathbb{F}_p[G]$-module which is isomorphic to $\mathcal{U} = U_K/(\mu_{p-1}U_K^{(p)})$. Let $\alpha \in \mathbb{Q}(\zeta_p) \cap \mu_{p-1}U_K^{(p)}$. Then for every $\beta \in \mathbb{Q}(\zeta_p) \cap U_K$, we have $(\beta, \alpha) = 1$. Therefore, if $B$ is a subgroup of $\mathcal{V}$, we set

$$B^{\perp} = \{\alpha \in V : \forall b \in B,\ (b, \alpha) = (\alpha, b) = 1\}.$$

Via our isomorphism $\phi : \mathcal{V} \to \mathcal{U}$, we have an isomorphism

$$B^{\perp} \equiv \{\alpha \in \mathcal{U} : \forall b \in B,\ (\alpha, \phi(b)) = 1\}.$$

Note that, if $B$ is an $\mathbb{F}_p[G]$-submodule of $\mathcal{V}$, the above isomorphism is an isomorphism of $\mathbb{F}_p[G]$-modules.

Now, $\mathfrak{p}_K$ can be viewed as a $\mathbb{Z}_p$-submodule of $(D)_L$ (see Section 2). Since $[p]_L(\mathfrak{p}_k) \subset \mathfrak{p}_K^p$ and, for all $a \in \mathbb{Z}_p$, $[a]_L(\mathfrak{p}_K^p) \subset \mathfrak{p}_K^p$, it follows that $(\mathfrak{p}_K)_L/(\mathfrak{p}_K^p)_L$ is an $\mathbb{F}_p$-vector space. Furthermore, since $F_L(X,Y) \equiv X + Y \pmod{\deg p}$ and $[a]_L \equiv aX \pmod{\deg p}$ for all $a \in \mathbb{Z}_p$, $(\mathfrak{p}_K)_L/(\mathfrak{p}_K^p)_L$ is the same as the usual $\mathbb{F}_p$-vector space $\mathfrak{p}_K/\mathfrak{p}_K^p$. Therefore we have an isomorphism of $\mathbb{F}_p[G]$-modules $\psi : \mathcal{U} \to \mathfrak{p}_K/\mathfrak{p}_K^p$, $u \mapsto g_p(u-1)$. But recall that

$$\forall u \in U_K^{(1)},\ \forall \alpha \in K^*, \qquad f_p(\langle g_p(u-1), \alpha\rangle_L) = (u, \alpha) - 1.$$

We deduce from the above discussion that $B^{\perp}$ is isomorphic to the $\mathbb{F}_p$-vector space

$$\{z \in \mathfrak{p}_K/\mathfrak{p}_K^p : \langle z, B\rangle_L = 0\}.$$

THEOREM 4.1. *Let $B$ be an $\mathbb{F}_p[G]$-submodule of $\mathcal{V}$. Then, for $1 \le i \le p-1$, we have*

$$\dim_{\mathbb{F}_p} B^{\perp}(i) + \dim_{\mathbb{F}_p} B(p-i) = 1.$$

*Proof.* First note that $B^{\perp}$ is an $\mathbb{F}_p[G]$-submodule of $\mathcal{V}$. Now, we identify $B^{\perp}$ and $\{z \in \mathfrak{p}_K/\mathfrak{p}_K^p : \langle z, B\rangle_L = 0\}$ which is an $\mathbb{F}_p[G]$-submodule of $\mathfrak{p}_K/\mathfrak{p}_K^p$. Note that $\mathfrak{p}_K/\mathfrak{p}_K^p$ is an $\mathbb{F}_p$-vector space of dimension $p-1$ with $\{\lambda_L, \ldots, \lambda_L^{p-1}\}$ as a base over $\mathbb{F}_p$.

For simplification, we set $e_i = e_{\omega^i}$ for $i = 1, \ldots, p-1$. Let $j$ be an integer, $1 \le j \le p-1$. We have:

- $e_i \lambda_L^j = 0$ if $j \ne i$,
- $e_i \lambda_L^j = \lambda_L^j$ if $j = i$.

Therefore

$$\frac{\mathfrak{p}_K}{\mathfrak{p}_K^p}(i) = \mathbb{F}_p \lambda_L^i.$$

This implies that

$$B^{\perp}(i) \ne 0 \ \Leftrightarrow\ \lambda_L^i \in B^{\perp}.$$

Now, let $2 \le j \le p-1$, $1 \le i \le p-1$. Let $b \in B$. By Theorem 2.7, we have

$$\langle \lambda_L^j, e_i b\rangle_L = [\varphi_{p-j}(e_i b)]_L(\lambda_L).$$

But $\varphi_{p-j}(e_i b) = 0$ if $p-j \neq i$ and $\varphi_{p-j}(e_i b) = \varphi_i(b)$ if $i = p-j$. Now, note that

$$\lambda_L^j \in B^\perp \;\Leftrightarrow\; \forall i, 1 \le i \le p-1,\; \langle \lambda_L^j, B(i)\rangle_L = 0.$$

Furthermore

$$\forall b \in B, \qquad \langle \lambda_L, b\rangle_L = \left[\frac{N_{K/\mathbb{Q}_p}(u^{-1}) - 1}{p}\right]_L (\lambda_L).$$

Thus $\lambda_L \in B^\perp \Leftrightarrow B(p-1) = 0$. The theorem follows. ∎

Corollary 4.2. *Let $B$ be an $\mathbb{F}_p[G]$-submodule of $\mathcal{V}$. Then*

$$\dim_{\mathbb{F}_p} B^\perp + \dim_{\mathbb{F}_p} B = p-1.$$

Corollary 4.3. *Let $B$ be an $\mathbb{F}_p[G]$-submodule of $\mathcal{V}$. Then*

$$(B^\perp)^\perp = B.$$

*Proof.* Note that $B^\perp$ is an $\mathbb{F}_p[G]$-submodule of $\mathcal{V}$. Thus, by Corollary 4.2,

$$\dim_{\mathbb{F}_p} (B^\perp)^\perp + \dim_{\mathbb{F}_p} B^\perp = p-1.$$

But $B \subset (B^\perp)^\perp$, and by Corollary 4.2,

$$\dim_{\mathbb{F}_p} B + \dim_{\mathbb{F}_p} B^\perp = p-1.$$

Thus $B = (B^\perp)^\perp$. ∎

Now, let $F$ be a real subfield of $\mathbb{Q}(\zeta_p)$ with $[F:\mathbb{Q}] = l \ge 2$. If we apply Theorems 3.2 and 4.1, we get

Theorem 4.4. (i) *Let $i$ be an integer*, $1 \le i \le p-1$. *Then*

$$\dim_{\mathbb{F}_p} \mathrm{Cyc}_F^\perp(i) + \dim_{\mathbb{F}_p} \frac{\mathrm{Cyc}_F}{\mathrm{Cyc}_F^{\mathrm{Kum}}}(p-i) = 1.$$

*Thus* $\mathrm{Cyc}_F^\perp \neq 0$ *if and only if* $i \not\equiv 1 \pmod{(p-1)/l}$, $i = p-1$, *or* $i \equiv 1 \pmod{(p-1)/l}$ *and* $B_{p-i} \equiv 0 \pmod p$. *In particular*,

$$\dim_{\mathbb{F}_p} \mathrm{Cyc}_F^\perp = p-1-r(F).$$

(ii) *Let $i$ be an integer*, $1 \le i \le p-1$. *Then*

$$\dim_{\mathbb{F}_p} \frac{\mathrm{Cyc}_F^\perp}{E_F^\perp}(i) = \dim_{\mathbb{F}_p} \frac{E_F}{\mathrm{Cyc}_F\, E_F^{\mathrm{Kum}}}(p-i).$$

Let $I$ be the Stickelberger ideal (see [10], Chapter 6) and let $\mathcal{I}$ be its image in $\mathbb{F}_p[G]$. Let $F = \mathbb{Q}(\zeta_p)^+$. Then, by Theorem 4.4 and [10], Section 6.3, there exists a surjective morphism of $\mathbb{F}_p[G]$-modules

$$\frac{\mathbb{F}_p[G]^-}{\mathcal{I}^-} \to \frac{\mathrm{Cyc}_F^\perp}{E_F^\perp}.$$

Since $\dim_{\mathbb{F}_p} \mathbb{F}_p[G]^-/\mathcal{I}^- = i(p)$, this morphism is an isomorphism if and only if $E_F^{\mathrm{Kum}} = (E_F)^p$.

**5. Mirimanoff's polynomials.** In his attempt to prove the first case of Fermat's Last Theorem, D. Mirimanoff introduced the polynomials

$$M_k(X) = \sum_{i=1}^{p-1} i^{k-1} X^i \in \mathbb{F}_p[X], \qquad k \ge 1 \text{ an integer.}$$

Note that $(X-1)M_1(X) = X^p - X$. Let $\Gamma = X\frac{d}{dX}$. Then, for $k \ge 1$, we have

$$\Gamma^k M_1 = M_{k+1}.$$

From this relation, we deduce immediately that, for $2 \le k \le p-1$, we have

$$M_k(X) = X(X-1)^{p-k} P_k(X),$$

where $P_k(X) \in \mathbb{F}_p[X]$ is of degree $k-2$ and $P_k(0) \not\equiv 0 \pmod p$, $P_k(1) \not\equiv 0 \pmod p$.

Note that, if $k$ is odd, $3 \le k \le p-2$, we have (see [5], Chapter 8):

$$M_k(X) = (-1)^k X(X+1)(X-1)^{p-k} L_k(-X),$$

where $L_k(X) \in \mathbb{F}_p[X]$ is of degree $k-3$. The first polynomials $L_k(X)$ are:

$$\begin{aligned}
&L_3(X) = 1,\\
&L_5(X) = X^2 - 10X + 1,\\
&L_7(X) = X^4 - 56X^3 + 246X^2 - 56X + 1,\\
&L_9(X) = X^6 - 246X^5 + 4047X^4 - 11572X^3 + 4047X^2 - 246X + 1.
\end{aligned}$$

In this section, we will relate the study of the non-trivial zeros in $\mathbb{F}_p^*$ of the polynomials $M_k(X)$, $k$ odd, to the orthogonal of cyclotomic units.

Note that the number of $k$ even, $2 \le k \le p-3$, such that $-1 \in \mathbb{F}_p^*$ is a root of $M_k(X)$ is connected to $i(p)$:

LEMMA 5.1. (i) *Let $k$ be an even integer*, $2 \le k \le p-3$. *Then*

$$M_k(-1) \equiv 2(2^k - 1)\frac{B_k}{k} \pmod p.$$

(ii) $M_{p-1}(-1) \equiv \frac{2^p - 2}{p} \pmod p$.

*Proof.* (i) is a consequence of Proposition 2.5; for (ii) see [5], Chapter 8. ∎

Recall that we identify $\mathcal{V}$ and $\mathcal{U}$. Set

$$\varepsilon_+ = \sum_{i\equiv 0\,(\mathrm{mod}\,2)} e_{\omega^i} \in \mathbb{F}_p[G] \quad \text{and} \quad \varepsilon_- = \sum_{i\equiv 1\,(\mathrm{mod}\,2)} e_{\omega^i} \in \mathbb{F}_p[G].$$

Then $\varepsilon_+\varepsilon_- = 0$, $\varepsilon_+^2 = \varepsilon_+$, $\varepsilon_-^2 = \varepsilon_-$, $1 = \varepsilon_+ + \varepsilon_-$, $\sigma_{-1}\varepsilon_+ = \varepsilon_+$ and $\sigma_{-1}\varepsilon_- = -\varepsilon_-$. We set $\mathcal{V}^+ = \varepsilon_+\mathcal{V}$ and $\mathcal{V}^- = \varepsilon_-\mathcal{V}$. Then

$$\mathcal{V}^+ = \bigoplus_{i\equiv 0\,(\mathrm{mod}\,2)} \mathcal{V}(i), \qquad \mathcal{V}^- = \bigoplus_{i\equiv 1\,(\mathrm{mod}\,2)} \mathcal{V}(i).$$

Furthermore

$$\dim_{\mathbb{F}_p} \mathcal{V}^+ = \dim_{\mathbb{F}_p} \mathcal{V}^- = (p-1)/2.$$

Note also that

$$\mathcal{V}^+ = \frac{\mathbb{Q}(\zeta_p)^+ \cap U_K}{\mathbb{Q}(\zeta_p)^+ \cap \mu_{p-1}U_K^{(p)}}.$$

Let $\epsilon \in \mu_{p-1}$. We set

$$\varrho_\epsilon = \frac{\epsilon - \zeta_p}{\epsilon - \zeta_p^{-1}}.$$

Then $\varrho_\epsilon \in \mathcal{V}^-$. In this section, we suppose that $p \geq 5$.

Lemma 5.2. *$\mathcal{V}^-$ is generated as $\mathbb{F}_p[G]$-module by the $\varrho_\epsilon$, $\epsilon \in \mu_{p-1} \setminus \{1,-1\}$.*

*Proof.* Let $\epsilon \in \mu_{p-1}$, $\epsilon \neq 1$. Then, by Proposition 2.5, we have $\varphi_1(\varrho_\epsilon) \neq 0$. Thus

$$\mathcal{V}^-(1) = \mathbb{F}_p e_\omega \varrho_\epsilon.$$

Let $k$ be an odd integer, $3 \leq k \leq p-2$. By Proposition 2.5, we have

$$\mathcal{V}^-(k) = \mathbb{F}_p e_{\omega^k}\varrho_\epsilon \;\Leftrightarrow\; \varphi_k(\varrho_\epsilon) \neq 0 \;\Leftrightarrow\; M_k(\epsilon) \not\equiv 0 \pmod p.$$

But there exists $\epsilon \in \mu_{p-1}\setminus\{1,-1\}$ such that $M_k(\epsilon) \not\equiv 0 \pmod p$. The lemma follows. ∎

Lemma 5.3. *Let $F$ be a real subfield of $\mathbb{Q}(\zeta_p)$ with $[F:\mathbb{Q}] = l \geq 2$. Then $\varrho_\epsilon \in \mathrm{Cyc}_F^\perp$ if and only if for $j = 1,\ldots,l-1$,*

$$B_{j(p-1)/l} M_{p-j(p-1)/l}(\epsilon) \equiv 0 \pmod p.$$

*Proof.* By the proof of Proposition 2.6, we have

$$g_p(\varrho_\epsilon - 1) \equiv \sum_{k=1}^{p-2} \frac{1}{k}\varphi_k(\varrho_\epsilon)\lambda_L^k \pmod{\mathfrak{p}_K^p}.$$

Thus, by Theorem 2.7, Proposition 2.5 and Theorem 3.2, if

$$B_{j(p-1)/l} M_{p-i(p-1)/l}(\epsilon) \equiv 0 \pmod p \qquad \text{for } j = 1,\ldots,l-1,$$

then $\varrho_\epsilon \in \mathrm{Cyc}_F^\perp$.

Conversely, assume that $\varrho_\epsilon \in \mathrm{Cyc}_F^\perp$. Let $B$ be the $\mathbb{F}_p[G]$-submodule of $\mathcal{V}^-$ generated by $\varrho_\epsilon$. By Theorem 4.1, we have

$$\dim_{\mathbb{F}_p} B(i) + \dim_{\mathbb{F}_p} \frac{\mathrm{Cyc}_F}{\mathrm{Cyc}_F^{\mathrm{Kum}}}(p-1) \le 1.$$

It remains to apply Proposition 2.5 and Theorem 3.2. ■

G. Terjanian has conjectured (see [8]) that for every odd prime number, $\varrho_\epsilon \in \mathrm{Cyc}_F^\perp \;\Rightarrow\; \epsilon = 1$ or $\epsilon = -1$, where $F = \mathbb{Q}(\zeta_p)^+$. By Lemma 5.3, Terjanian's conjecture is equivalent to the statement that the Kummer system of congruences

$$B_{2j} M_{p-2j} \equiv 0 \pmod{p}, \qquad 1 \le j \le (p-3)/2,$$

has only the trivial solutions, i.e. $0, 1$ and $-1$. L. Skula has proved (see [7]) that if Terjanian's conjecture is false for a prime $p$ then $i(p) \ge [\sqrt[3]{p/2}]$.

Theorem 5.4. *Let $x, y \in \mathbb{Z}$ be such that $xy(x^2-y^2) \not\equiv 0 \pmod{p}$. Let $B$ be the $\mathbb{F}_p[G]$-submodule of $\mathcal{V}$ generated by $x + y\zeta_p$. Then*

$$\dim_{\mathbb{F}_p} B^- \ge \sqrt{p} - 1.$$

*Proof.* Suppose that $\dim_{\mathbb{F}_p} B^- < \sqrt{p} - 1$. Set $r = [\sqrt{p}] - 1$. Note that $\zeta_p \in B^-$. Consider the set of all products

$$\zeta_p^{b_0} \prod_{i=1}^{r} (x + y\zeta_p^i)^{b_i},$$

where $0 \le b_i < p$ for $i = 0, \ldots, r$. The number of such products is $p^{r+1} > |B^-|$. Therefore, two of them must agree in their $B^-$-components, so we may divide and obtain

$$\prod_{i=1}^{r} (x + y\zeta_p^i)^{a_i} \equiv \zeta_p^{\nu} \delta \pmod{p},$$

where $-p < a_i < p$ and some $a_i$ are non-zero (because a non-trivial power of $\zeta_p$ is not congruent to a real number modulo $p$), $\delta \in \mathbb{Q}(\zeta_p)^+$ and $\nu \ge 0$. Thus, we get

$$\prod_{i=1}^{r} \frac{(x + y\zeta_p^i)^{a_i}}{(y + x\zeta_p^i)^{a_i}} \equiv \zeta_p^{v} \pmod{p}$$

for some $v \ge 0$. But, by the proof of Eichler's Theorem (see [10], Theorem 6.23), this implies that $xy(x^2-y^2) \equiv 0 \pmod{p}$, a contradiction. ■

Corollary 5.5. *Let $p \ge 5$ be a prime number. If Terjanian's conjecture is false for the prime $p$, then*:

(i) $2^{p-1} \equiv 1 \pmod{p^2}$;
(ii) $B_{p-3} \equiv 0 \pmod{p}$;
(iii) $i(p) \ge \sqrt{p} - 2$.

*Proof.* Let $C$ be the group of cyclotomic units of $\mathbb{Q}(\zeta_p)$ and let $F = \mathbb{Q}(\zeta_p)^+$. Then $\epsilon - \zeta_p$ is orthogonal to $C$ for the norm residue symbol if and only if $\varrho_\epsilon \in \mathrm{Cyc}_F^\perp$ (see [2]). Therefore (i) and (ii) are a consequence of [8], Enoncé 8. Now, (iii) is a consequence of Theorem 5.4, Lemma 5.3 and Proposition 2.5. ∎

Note that the *ABC* conjecture implies that Terjanian's conjecture is true for infinitely many primes $p$ (see [6]). It would be interesting to find analogues of Terjanian's conjecture for real subfields of $\mathbb{Q}(\zeta_p)$ (see [1]).

**6. $p$-adic regulators and Kummer subgroups of units.** Let $F$ be a real subfield of $\mathbb{Q}(\zeta_p)$ with $[F:\mathbb{Q}] = l$, $l \geq 2$. We set $G_F = \mathrm{Gal}(\widehat{F}/\mathbb{Q}_p)$ and $\chi = \omega^{(p-1)/l}$. Then

$$\widehat{G}_F = \langle \chi \rangle.$$

We denote the $p$-adic regulator of $F$ by $R_p(F)$ and the discriminant of $F$ by $d(F)$. Let $\varepsilon \in E_F$; we denote by $A_\varepsilon$ the subgroup of $E_F$ generated by $-1$ and $\sigma(\varepsilon)$, $\sigma \in G_F$. We say that $\varepsilon$ is a *Minkowski unit* if $A_\varepsilon$ is of finite index in $E_F$.

PROPOSITION 6.1. *Let $\varepsilon \in E_F$ be a Minkowski unit. Then*

$$(E_F : A_\varepsilon)\frac{R_p(F)}{\sqrt{d(F)}} \equiv \pm \frac{l^{2(l-1)}}{(l-1)!}\prod_{k=1}^{l-1} \varphi_{k(p-1)/l}(\varepsilon) \pmod p.$$

*Proof.* Let $\varepsilon$ be a Minkowski unit. Set

$$R_p(A_\varepsilon) = \det(\mathrm{Log}_p(\sigma\tau(\varepsilon)))_{\sigma,\tau\in G_F\setminus\{1\}}.$$

Then $R_p(A_\varepsilon) \neq 0$ and (see [10], Lemma 4.15)

$$(E_F : A_\varepsilon) = \pm \frac{R_p(A_\varepsilon)}{R_p(F)}.$$

But, from [10], Lemma 5.26,

$$R_p(A_\varepsilon) = \prod_{j=1}^{l-1}\Big(\sum_{\sigma\in G_F} \chi(\sigma)^{-j}\,\mathrm{Log}_p(\sigma(\varepsilon))\Big).$$

Now, by Proposition 2.6,

$$\mathrm{Log}_p(\sigma(\varepsilon)) \equiv \sum_{j=1}^{l-1} \frac{1}{j(p-1)/l}\chi(\sigma)^{-j}\varphi_{j(p-1)/l}(\varepsilon)\lambda_L^{j(p-1)/l} \pmod{\mathfrak{p}_K^p}.$$

Thus, we have

$$\sum_{\sigma\in G_F} \chi(\sigma)^{-k}\,\mathrm{Log}_p(\sigma(\varepsilon)) \equiv \frac{l^2}{k(p-1)}\varphi_{k(p-1)/l}(\varepsilon)\lambda_L^{k(p-1)/l} \pmod{\mathfrak{p}_K^p}.$$

Therefore, there exists $a_k \in \mathbb{Z}_p$, $a_k \equiv \varphi_{k(p-1)/l}(\varepsilon)$, such that

$$\sum_{\sigma \in G_F} \chi(\sigma)^{-k} \operatorname{Log}_p(\sigma(\varepsilon)) = \lambda_L^{k(p-1)/l}\left(\frac{l^2}{k(p-1)} a_k + u_k\right),$$

where $u_k \in \mathfrak{p}_K^{1+(p-1)/l}$. We get

$$R_p(A_\varepsilon) = \lambda_L^{(p-1)(l-1)/2} \prod_{k=1}^{l-1} \left(\frac{l^2}{k(p-1)} a_k + u_k\right).$$

But $\sqrt{d(F)} = \pm\lambda_L^{(p-1)(l-1)/2}$. Therefore

$$(E_F : A_\varepsilon) \frac{R_p(F)}{\sqrt{d(F)}} \equiv \pm \frac{l^{2(l-1)}}{(l-1)!} \prod_{k=1}^{l-1} \varphi_{k(p-1)/l}(\varepsilon) \pmod{\mathfrak{p}_K^{1+(p-1)/l}}.$$

But, since $R_p(F)/\sqrt{d(F)} \in \mathbb{Z}_p$, this congruence holds modulo $p$. ∎

Corollary 6.2. *Let $\varepsilon$ be a Minkowski unit, $\varepsilon \in E_F$. Then*

$$(2l)^{l-1} h_F \prod_{k=1}^{l-1} \varphi_{k(p-1)/l}(\varepsilon) \equiv \pm(E_F : A_\varepsilon) \prod_{k=1}^{l-1} B_{k(p-1)/l} \pmod{p}.$$

*Proof.* By [10], Theorem 5.24,

$$2^{l-1} h_F \frac{R_p(F)}{\sqrt{d(F)}} = \prod_{j=1}^{l-1} L_p(1, \chi^j).$$

Now

$$L_p(1, \chi^j) \equiv \frac{l}{j} B_{j(p-1)/l} \pmod{p}.$$

Therefore

$$2^{l-1} h_F \frac{R_p(F)}{\sqrt{d(F)}} \equiv \frac{l^{l-1}}{(l-1)!} \prod_{j=1}^{l-1} B_{j(p-1)/l} \pmod{p}.$$

Let $\varepsilon$ be a Minkowski unit. By Proposition 6.1, we have

$$(E_F : A_\varepsilon) \frac{R_p(F)}{\sqrt{d(F)}} \equiv \pm \frac{l^{2(l-1)}}{(l-1)!} \prod_{j=1}^{l-1} \varphi_{j(p-1)/l}(\varepsilon) \pmod{p}.$$

The corollary follows. ∎

Let $\varepsilon_1, \ldots, \varepsilon_{l-1}$ be a system of fundamental units of $F$. We set

$$R_F \equiv \left(\det\left(\frac{1}{j(p-1)/l} \varphi_{j(p-1)/l}(\varepsilon_i)\right)_{1 \le i,j \le l-1}\right)^2 \pmod{p}.$$

Note that $R_F$ modulo $p$ is independent of the choice of $\varepsilon_1, \ldots, \varepsilon_{l-1}$ (see [4]).

LEMMA 6.3. *$R_F \not\equiv 0 \pmod p$ if and only if $E_F^{\mathrm{Kum}} = (E_F)^p$.*

*Proof.* It is clear that if $R_F \not\equiv 0 \pmod p$ then $E_F^{\mathrm{Kum}} = (E_F)^p$.

Conversely, assume that $E_F^{\mathrm{Kum}} = (E_F)^p$. Let $\varepsilon$ be a generator of the cyclic $\mathbb{F}_p[G_F]$-module $E_F/E_F^{\mathrm{Kum}}$. Set

$$B \equiv \left(\det\left(\frac{1}{j(p-1)/l}\varphi_{j(p-1)/l}(\sigma(\varepsilon))\right)_{1\le j\le l-1,\,\sigma\in G_F\setminus\{1\}}\right)^2 \pmod p.$$

The rank of this latter matrix is equal to the rank of

$$(\chi(\sigma)^j)_{1\le j\le l-1,\,\sigma\in G_F\setminus\{1\}}.$$

Therefore $B \not\equiv 0 \pmod p$. By Proposition 2.6 and [4], page 113,

$$B \equiv (E_F : A_\varepsilon)^2 R_F \pmod p.$$

Therefore $R_F \not\equiv 0 \pmod p$. ∎

If we apply Proposition 2.6, by the proof of [4], Theorem 1A, we get

THEOREM 6.4. *Let $g$ be a primitive root modulo $p$. We have*

$$4^{l-1}h_F^2R_F \equiv \frac{l^2}{(l-1)!^2}(\det(g^{(p-1)(i-1)k/l})_{1\le i,k\le l-1})^2\prod_{j=1}^{l-1}\frac{B^2_{j(p-1)/l}}{((j(p-1)/l)!)^2} \pmod p.$$

THEOREM 6.5.

$$E_F^{\mathrm{Kum}} = (E_F)^p \quad \textit{if and only if} \quad \frac{R_p(F)}{\sqrt{d(F)}} \not\equiv 0 \pmod p.$$

*Proof.* Let $\varepsilon_1,\ldots,\varepsilon_{l-1}$ be a system of fundamental units of $F$. Set $\beta_i = \mathrm{Log}_p(\varepsilon_i)$ for $i = 1,\ldots,l-1$ and $\beta_l = 1$ (recall that $l = [F:\mathbb{Q}]$). We have $\widehat{F} = \mathbb{Q}_p(\lambda_L^{(p-1)/l})$. Thus

$$O_{\widehat{F}} = \bigoplus_{j=0}^{l-1}\mathbb{Z}_p\lambda_L^{j(p-1)/l}.$$

Therefore, for $i = 1,\ldots,l$, we can write

$$\beta_i = \sum_{j=0}^{l-1}a_{ij}\lambda_L^{j(p-1)/l},$$

where $a_{ij}\in\mathbb{Z}_p$. But

$$\det(\sigma(\beta_i))_{\sigma\in\mathrm{Gal}(\widehat{F}/\mathbb{Q}_p),\,i=1,\ldots,l} = lR_p(F).$$

Furthermore

$$\det(\sigma(\beta_i)) = \det(a_{ij})\det(\sigma(\lambda_L^{j(p-1)/l})).$$

But, for $i = 1, \ldots, l-1$, we have

$$a_{ij} \equiv -\frac{l}{j}\varphi_{j(p-1)/l}(\varepsilon_i) \pmod p$$

for $j = 1, \ldots, l-1$ and $a_{i0} \equiv 0 \pmod p$. Therefore

$$\det(a_{ij})^2 \equiv R_F \pmod p.$$

The theorem follows. ■

**References**


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

[2] —, *Proof of a conjecture of Terjanian for regular primes*, C. R. Math. Rep. Acad. Sci. Canada 18 (1996), no. 5, 193–198.

[3] S. Lang, *Cyclotomic Fields I and II*, Springer, 1990.

[4] T. Metsänkylä, *A class number congruence for cyclotomic fields and their subfields*, Acta Arith. 23 (1973), 107–116.

[5] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, 1979.

[6] J. Silverman, *Wieferich's Criterion and the ABC conjecture*, J. Number Theory 30 (1988), 226–237.

[7] L. Skula, *The orders of solutions of the Kummer system of congruences*, Trans. Amer. Math. Soc. 343 (1994), 587–607.

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

[9] S. V. Vostokov, *Artin–Hasse exponentials and Bernoulli numbers*, in: Amer. Math. Soc. Transl. (2) 166, Providence, RI, 1995, 149–156.

[10] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1997.



Laboratoire SDAD
Université de Caen
Campus II
BP 5186
Boulevard Maréchal Juin
14032 Caen Cedex, France
E-mail: angles@math.unicaen.fr



*Received on 22.11.1999*
*and in revised form on 9.5.2000* (3713)