# VANDIVER PAPERS ON CYCLOTOMY REVISITED AND FERMAT′S LAST THEOREM

*by*

Georges Gras & Roland Quême

***Abstract.*** — Relying on classical studies of H.S. Vandiver and P. Furtwängler, we intend to lay the foundations of a new global cyclotomic approach to Fermat's Last Theorem (FLT) for $p > 3$ and to a stronger version called *"Strong Fermat's Last Theorem"* (SFLT), by introducing an infinite number of auxiliary cyclotomic fields of the form $\mathbb{Q}(\mu_{q-1})$ for $q \neq p$ a prime.

We show that the existence of nontrivial counterexamples to SFLT implies strong constraints on the arithmetic of the fields $\mathbb{Q}(\mu_{q-1})$ with respect to Čebotarev's density theorem in suitable canonical Abelian $p$-extensions. Further investigations (of an analytic or a geometric nature) would be necessary to lead to a proof of SFLT. Our results imply sufficient conditions for the non-existence of nontrivial solutions of the SFLT equation and suggest various conjectures.

We prove for instance that if there exist infinitely many primes $q$, $q \not\equiv 1 \pmod{p}$, $q^{p-1} \not\equiv 1 \pmod{p^2}$ such that for $\mathfrak{q} \,|\, q$ in $\mathbb{Q}(\mu_{q-1})$, $\mathfrak{q}^{1-c}$ is of the form $\mathfrak{a}^p\,(\alpha)$ for some ideal $\mathfrak{a}$ and some $\alpha \equiv 1 \pmod{p^2}$ (where $c$ is the complex conjugation), then Fermat's Last Theorem holds for $p$.

***Résumé.*** — À partir de travaux classiques de H.S. Vandiver et P. Furtwängler, nous posons les bases d'une nouvelle approche cyclotomique globale du dernier théorème de Fermat pour $p > 3$ et d'une version plus forte appelée *"Strong Fermat's Last Theorem"* (SFLT), en introduisant une infinité de corps cyclotomiques auxiliaires de la forme $\mathbb{Q}(\mu_{q-1})$ pour $q \neq p$ premier.

Nous montrons que l'existence de contre-exemples non triviaux à SFLT implique de fortes contraintes sur l'arithmétique des corps $\mathbb{Q}(\mu_{q-1})$ au niveau du théorème de densité de Čebotarev dans certaines $p$-extensions abéliennes canoniques. Des investigations supplémentaires (analytiques ou géométriques) seraient nécessaires pour conduire à une preuve de SFLT. À partir de là, nous donnons des conditions suffisantes de non existence de solutions non triviales à l'équation associée à SFLT et formulons diverses conjectures.

Nous prouvons par exemple que s'il existe une infinité de nombres premiers $q$, $q \not\equiv 1 \pmod{p}$, $q^{p-1} \not\equiv 1 \pmod{p^2}$, tels que pour $\mathfrak{q} \,|\, q$ dans $\mathbb{Q}(\mu_{q-1})$, on ait $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(\alpha)$ avec $\alpha \equiv 1 \pmod{p^2}$ (où $c$ est la conjugaison complexe), alors le dernier théorème de Fermat est vrai pour $p$.

**2000** ***Mathematics Subject Classification.*** — 11D41, 11R18, 11R44, 11R45.
***Key words and phrases.*** — Fermat's last theorem, cyclotomic fields, cyclotomic units, class field theory, Vandiver's and Furtwängler's theorems, Čebotarev's density theorem.

We would like to thank Jean-Pierre Serre for his interest in the manuscript, some advice and suggestions about the writing, and Jacques Martinet for his contribution in checking and improving on our English.

## 1. Introduction

This paper is devoted to the study of the following phenomenon. Consider the maximal Abelian extension $\overline{\mathbb{Q}}^{\mathrm{nr}}$ of $\mathbb{Q}$, unramified (= non-ramified) at a given prime $p > 2$.

By class field theory we have $\overline{\mathbb{Q}}^{\mathrm{nr}} = \bigcup_{n,\, p\nmid n} \mathbb{Q}(\mu_n)$. Then denote by $H_{\overline{\mathbb{Q}}^{\mathrm{nr}}}[p]$ the maximal $p$-ramified (i.e., unramified outside $p$) $p$-elementary (Abelian) extension of $\overline{\mathbb{Q}}^{\mathrm{nr}}$; this $p$-extension is equal to $\bigcup_{n,\, p\nmid n} H_{\mathbb{Q}(\mu_n)}[p]$ where $H_{\mathbb{Q}(\mu_n)}[p]$ is the maximal $p$-ramified $p$-elementary extension of $\mathbb{Q}(\mu_n)$.

We have found that any nontrivial solution $(u, v)$ of a classical diophantine equation, associated to Fermat's equation for $p > 2$, and called the SFLT equation [(1)], implies some constraints on the law of decomposition, in $H_{\overline{\mathbb{Q}}^{\mathrm{nr}}}[p]/\overline{\mathbb{Q}}^{\mathrm{nr}}$, of every prime $q \neq p$, $q \nmid uv$.

These constraints may be characterized at some finite levels $n$ via the law of decomposition of $q$ in a *canonical* family $\mathcal{F}_n$ of conjugate $p$-cyclic sub-extensions of $H_{\mathbb{Q}(\mu_n)}[p]/\mathbb{Q}(\mu_n)$, where $n \mid q-1$ is the order of $\frac{v}{u}$ modulo $q$; see Theorem 3.3 on the computations of some canonical $p$th power residue symbols. Its interpretation in terms of Frobenius automorphisms in $\mathcal{F}_n$ leads to Theorem 6.6 and a specific use leads to Theorem 5.1 (stated in the abstract).

Some methods needed to prove these connections stem from techniques of Vandiver and Furtwängler, who, using a different viewpoint from ours, try to give a classical cyclotomic proof of Fermat's Last Theorem (FLT). Our perspective is global, in contrast to previous studies of the classical literature that are local at $p$.

Of course the problem is now empty for Fermat's equation, except if we wish to prove FLT in this way; but we shall see that for the SFLT equation, the result is unknown for $p > 3$ (but conjecturally similar) and, moreover, leads to infinitely many solutions for $p = 3$. We shall show that the case $p = 3$ is exceptional and this we shall explain in Subsection 5.3 and in Section 8.

## 2. Generalities on the method – The $\omega$-SFLT equation

**2.1. Prerequisites on Fermat's Last Theorem.** — Let $p$ be an odd prime, and let $a$, $b$, $c$ be pairwise coprime nonzero integers such that

$$a^p + b^p + c^p = 0\,.$$

If $p \mid abc$ (second case of FLT), we assume that $p$ divides $c$.

We can find for instance in **[Gr1]**, **[Ri]**, **[Wa1]** the following easy properties concerning such a speculative counterexample to FLT, where $\zeta$ is a primitive $p$th root of unity, $K := \mathbb{Q}(\zeta)$, $\mathfrak{p} := (\zeta - 1)\mathbb{Z}[\zeta]$, and $\mathrm{N}_{K/\mathbb{Q}}$ is the norm map in $K/\mathbb{Q}$. For a detailed proof, a more complete bibliography, and an analysis of the classical cyclotomic approach to FLT, we refer to **[Gr1]**.

Let $\nu \geq 0$ be the $p$-adic valuation of $c$. We have:

$$a + b = c_0^p \ (\text{resp. } p^{\nu p - 1} c_0^p) \ \text{ and } \ \mathrm{N}_{K/\mathbb{Q}}(a + b\,\zeta) = c_1^p \ (\text{resp. } p\, c_1^p)\,, \ \text{ if } \nu = 0 \ (\text{resp. } \nu > 0)\,,$$

---

(1) Equation in coprime integers $u$, $v$, of the form $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^{\delta}\, \mathfrak{w}_1^p$, where $\zeta := e^{2i\pi/p}$, $\mathfrak{p} := (\zeta - 1)\,\mathbb{Z}[\zeta]$ (see Conjecture 2.4); this formulation is equivalent to $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(u + v\,\zeta) = p^{\delta}\, w_1^p$ with $w_1 = \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\mathfrak{w}_1)$. The important condition g.c.d. $(u, v) = 1$ implies $\delta \in \{0, 1\}$ and $\mathfrak{p} \nmid \mathfrak{w}_1$.

with $-c = c_0\, c_1$ (resp. $p^\nu c_0\, c_1$), and $p \nmid c_0\, c_1$.
By cyclic permutation, since $p \nmid ab$, we have the following analogous relations

$$\begin{aligned} b + c &= a_0^p, \quad \mathrm{N}_{K/\mathbb{Q}}(b + c\,\zeta) = a_1^p, \ \text{ with } \ -a = a_0\, a_1,\\ c + a &= b_0^p, \quad \mathrm{N}_{K/\mathbb{Q}}(c + a\,\zeta) = b_1^p, \ \text{ with } \ -b = b_0\, b_1\,. \end{aligned}$$

We have:

$$(a + b\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{c}_1^p \ (\text{resp. } \mathfrak{p}\,\mathfrak{c}_1^p) \text{ if } \nu = 0 \ (\text{resp. } \nu > 0), \text{ with } \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{c}_1) = c_1\mathbb{Z}\,,$$

where $\mathfrak{c}_1$ is an integer ideal of $K$ prime to $\mathfrak{p}$, and the analogous relations

$$(b + c\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{a}_1^p, \quad \text{with } \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}_1) = a_1\mathbb{Z}\,,$$

$$(c + a\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{b}_1^p, \quad \text{with } \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{b}_1) = b_1\mathbb{Z}\,.$$

All prime divisors of the positive numbers $a_1$, $b_1$, $c_1$ are congruent to 1 modulo $p$.

***Remark 2.1.*** — If $\nu \geq 1$, then $\alpha := \frac{a+c\,\zeta}{a+c\,\zeta^{-1}}$ is a pseudo-unit (i.e., $(\alpha)$ is the $p$th power of an ideal), congruent to 1 modulo $\mathfrak{p}^p$. Hence from **[Gr1]**, Theorem 2.2, Remark 2.3 (ii), $\alpha$ is locally a $p$th power in $K$, which implies $\alpha \equiv 1 \pmod{\mathfrak{p}^{p+1}}$, then $\frac{c\,(\zeta-\zeta^{-1})}{a+c\,\zeta^{-1}} \equiv 0 \pmod{\mathfrak{p}^{p+1}}$, whence $c \equiv 0 \pmod{p^2}$. This applies to the equation $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{w}_1^p$ of Conjecture 2.4 when $p \,|\, u$ with $\alpha = \frac{u\,\zeta^{-1}+v}{u\,\zeta+v}$ (resp. $p \,|\, v$ with $\alpha = \frac{u+v\,\zeta}{u+v\,\zeta^{-1}}$) and shows that $p^2 \,|\, u$ (resp. $p^2 \,|\, v$).

***Lemma 2.2.*** — *We can find a permutation $(x, y, z)$ of $(a, b, c)$ such that the following congruences hold:*
*(i) First case of FLT, $p > 3$,*

$$\begin{aligned} x - y &\not\equiv 0, & x + y &\not\equiv 0 \pmod{p},\\ y - z &\not\equiv 0, & y + z &\not\equiv 0 \pmod{p},\\ & & z + x &\not\equiv 0 \pmod{p}\,. \end{aligned}$$

*(ii) First case of FLT, $p = 3$,*

$$\begin{aligned} x - y \equiv y - z \equiv z - x &\equiv 0 \pmod{3},\\ x + y \equiv y + z \equiv z + x &\equiv \pm 1 \pmod{3}\,. \end{aligned}$$

*(iii) Second case of FLT, $p \geq 3$ ($y \equiv 0 \pmod{p}$),*

$$\begin{aligned} x - y &\not\equiv 0, & x + y &\not\equiv 0 \pmod{p},\\ y - z &\not\equiv 0, & y + z &\not\equiv 0 \pmod{p},\\ z - x &\not\equiv 0, & z + x &\equiv 0 \pmod{p}\,. \end{aligned}$$

*Proof.* — Consider the differences $a - b$, $b - c$, $c - a$ in the first case of FLT. If two of them are divisible by $p$, we obtain $a \equiv b \equiv c \not\equiv 0 \pmod{p}$, then since $a^p + b^p + c^p = 0$ implies $a + b + c \equiv 0 \pmod{p}$, we get $3\,a \equiv 0 \pmod{p}$ which leads to $p = 3$. So, if $p > 3$, there exist two differences having the first required property, say, $x - y$, $y - z$.

The second condition is satisfied for any sum and any $p \geq 3$.

The case $p = 3$ in the first case of FLT is obvious since $a \equiv b \equiv c \equiv \pm 1 \pmod{3}$.

In the second case of FLT, we take $y = c \equiv 0 \pmod p$ so that all conditions in (iii) are satisfied. Then $x + y\,\zeta$ and $z + y\,\zeta$ are $p$-primary pseudo-units with $p^2 \,|\, y$. □

***Remark 2.3.*** — For $p \geq 3$ in the first case, the condition $z - x \equiv 0 \pmod p$ implies $2^{p-1} \equiv 1 \pmod{p^2}$ since $x^p + y^p + z^p = 0$ implies $y^p + 2\,z^p \equiv 0 \pmod{p^2}$.

**2.2. Statement of a conjecture stronger than FLT.** — We have stated in **[Gr1]** a conjecture which implies FLT and which does not follow from Wiles's proof; we recall here its statement, which will be called the *Strong Fermat's Last Theorem* (SFLT).

***Conjecture 2.4.*** — *Let $p$ be an odd prime, let $\zeta$ be a primitive* $p$th *root of unity, and set $K = \mathbb{Q}(\zeta)$ and $\mathfrak{p} = (\zeta - 1)\,\mathbb{Z}[\zeta]$. Then the equation*

$$(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^{\delta}\,\mathfrak{w}_1^p$$

*in coprime integers $u$, $v$, where $\delta$ is any integer $\geq 0$ and $\mathfrak{w}_1$ is any integral ideal of $K$, has no solution for $p > 3$ except the trivial ones for which $u + v\,\zeta = \pm 1$, $\pm\zeta$, $\pm(1+\zeta)$, or $\pm(1-\zeta)$.*

We note that necessarily $\delta \in \{0, 1\}$ (depending on whether $u + v$ is prime to $p$ or not) and that $\mathfrak{w}_1$ is necessarily prime to $\mathfrak{p}$.

This SFLT equation is equivalent to the equation

$$\mathrm{N}_{K/\mathbb{Q}}(u + v\,\zeta) = p^{\delta}\,w_1^p\,,$$

with $\delta \in \{0, 1\}$ and $w_1 \in 1 + p\,\mathbb{Z}$, for which we have the relation $w_1\,\mathbb{Z} = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{w}_1)$. This is classical and a detailed proof will be given in the proof of Lemma 2.17 (Subsection 2.6), where we also give another equivalent equation.

The difference between FLT and SFLT is as follows. A solution $(u, v, w)$ of Fermat's equation $u^p + v^p + w^p = 0$ comes from a solution of $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^{\delta}\,\mathfrak{w}_1^p$ (with the same $u, v$) if and only if there exists $w_0 \in \mathbb{Z}$ such that $u + v = w_0^p$ (resp. $p^{\nu p - 1}\,w_0^p$) if $\delta = 0$ (resp. $\delta = 1$), since $\mathrm{N}_{K/\mathbb{Q}}(u + v\,\zeta) = p^{\delta}\,w_1^p$, giving $w := -w_0 w_1$ (resp. $-p^{\nu} w_0 w_1$) for a solution of Fermat's equation.

As for FLT, we can speak of the *first case* of the conjecture or of the equation when

$$u\,v\,(u + v) \not\equiv 0 \pmod p$$

and of the *second case* when

$$u\,v \equiv 0 \pmod p$$

(which implies $u$ or $v \equiv 0 \pmod{p^2}$ as in the case of the Fermat equation); then the case

$$u + v \equiv 0 \pmod p$$

will be called the *special case* of SFLT (it corresponds to the equation with $\delta = 1$).

In the first case of SFLT for $p > 3$, we do not necessarily have $u - v \not\equiv 0 \pmod p$; for $p = 3$, $u\,v\,(u + v) \not\equiv 0 \pmod 3$ implies $u \equiv v \equiv \pm 1 \pmod 3$, hence $u - v \equiv 0 \pmod 3$; see Remark 2.6 below.

***Remark 2.5.*** — If $u-v \equiv 0 \pmod{p}$, then $\alpha := \frac{u\zeta+v}{u+v\zeta}$ is a pseudo-unit congruent to 1 modulo $\mathfrak{p}^p$; so, from **[Gr1]**, Theorem 2.2, Remark 2.3 (ii), $\alpha$ is locally a $p$th power, which implies first $\alpha \equiv 1 \pmod{\mathfrak{p}^{p+1}}$, and next $\frac{(u-v)(\zeta-1)}{u+v\zeta} \equiv 0 \pmod{\mathfrak{p}^{p+1}}$, hence $u - v \equiv 0 \pmod{p^2}$. This is valid in the Fermat case if $z - x \equiv 0 \pmod{p}$ (under the necessary condition $2^{p-1} \equiv 1 \pmod{p^2}$), and we then have $z - x \equiv 0 \pmod{p^2}$.

In the sequel we shall assume, for a hypothetical solution $(x,\, y,\, z)$ of Fermat's equation, that the conditions of Lemma 2.2 are satisfied (i.e., $x - y$ and $y - z$ are prime to $p$ when $p > 3$, and $p \,|\, y$ in the second case).

In this case we have two similar counterexamples to the above SFLT conjecture:

$$(x + y\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{z}_1^p, \quad (y + z\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{x}_1^p$$

(first or second case of SFLT). A third counterexample to SFLT is:

$$(z + x\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{y}_1^p \ \ \text{(first case if } p \nmid y), \ \ (z + x\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}\,\mathfrak{y}_1^p \ \ \text{(special case if } p \,|\, y) \ .$$

More precisely, for $p > 3$, the first case of SFLT implies the first case of FLT, both the second and the special case of SFLT imply the second case of FLT, and FLT holds as soon as the first and second case, or the first and special case of SFLT, hold.

***Remark 2.6.*** — Conjecture 2.4 is false for $p = 3$ since for $\zeta = j$ of order 3 we have the six families of parametric formulas which exhaust the solutions:

$$u + v\,j = j^h\,(j-1)^\delta\,(s+t\,j)^3, \ \ s,\, t \in \mathbb{Z}, \ \ s + t \not\equiv 0 \pmod{3}, \ \text{g.c.d.}\,(s,t) = 1,$$

and $0 \le h < 3$, $\delta \in \{0, 1\}$. These solutions concern all the cases: [(2)]

– first case (for which $u - v \equiv 0 \pmod{9}$):

- $(u, v) = (-s^3 - t^3 + 3s^2t, -s^3 - t^3 + 3st^2)$, from $u + v\,j = j^2\,(s + t\,j)^3$;

– second case (for which $u$ or $v \equiv 0 \pmod{9}$):

- $(u, v) = (3st^2 - 3s^2t, s^3 + t^3 - 3s^2t)$, from $u + v\,j = j\,(s + t\,j)^3$;
- $(u, v) = (s^3 + t^3 - 3st^2, 3s^2t - 3st^2)$, from $u + v\,j = (s + t\,j)^3$;

– special cases (for which $u + v \equiv 0 \pmod{3}$):

- $(u, v) = (-s^3 - t^3 - 3s^2t + 6st^2, s^3 + t^3 - 6s^2t + 3st^2)$, from $u + v\,j = (j - 1)\,(s + t\,j)^3$;
- $(u, v) = (-s^3 - t^3 + 6s^2t - 3st^2, -2s^3 - 2t^3 + 3s^2t + 3st^2)$, from $u + v\,j = j\,(j - 1)\,(s + t\,j)^3$;
- $(u, v) = (2s^3 + 2t^3 - 3s^2t - 3st^2, s^3 + t^3 + 3s^2t - 6st^2)$, from $u + v\,j = j^2\,(j - 1)\,(s + t\,j)^3$.

The special cases are not similar since we have $u + v \equiv 0 \pmod{9}$ for the first solution and $u + v \equiv \pm 3(s^3 + t^3) \equiv \pm 3(s + t) \equiv \pm 3 \pmod{9}$ for the others.

When $p = 3$ we call trivial the solutions $(u, v)$ obtained with $s\,t\,(s - t) = 0$, which leads to the elements $u + v\,j = \pm 1$, $\pm j$, $\pm(1 + j)$, $\pm(1 - j)$, $\pm(1 + 2\,j)$, $\pm(2 + j)$.

[(2)] Since the parameters $(s', t')$ in the expression $s' + t'j = (-j)^r(s + t\,j)$, $0 \le r < 6$, give again the solution $(u(s,t), v(s,t))$ and its opposite, we can consider $(s,t)$ up to the automorphism $T'$ of order 6 defined on $\mathbb{Z} \times \mathbb{Z}$ by $T'(s,t) = (t, t - s)$ since for $r = 1$, $(s', t') = (t, t - s)$.

***Remark 2.7.*** — By contrast with the case of Fermat's equation, we shall not take into account the obvious symmetries of the solutions $(u,v)$ for $p=3$. This will be important in Section 8 where we shall use the action of an automorphism $T$ of order 6 on the set of solutions. Similarly, for any $p \geq 3$ the automorphism $T_0$ of order 2 defined by $T_0(u,v) := (v,u)$ acts on the set of solutions.

However, to simplify, for any $p \geq 3$ a solution $(u,v)$ will be considered up to the sign.

The considerations above indicate that to obtain a proof of SFLT, one must eliminate in a somewhat natural way the case $p=3$, which is an obstruction to the relevance of the method developed here. We shall explain in Subsection 5.3 and in Section 8 the reasons why this case is exceptional and finally does not matter, a priori, for the general theory; we are obliged to differ this justification because we first need some general material.

Meanwhile, for a more comprehensive information, we shall not systematically assume $p > 3$ in the development of the first parts of our study.

**2.3. The cyclotomic field $\mathbb{Q}(\zeta)$ and the character $\omega$.** — We first recall some properties of the cyclotomic field $K = \mathbb{Q}(\zeta)$, $\zeta$ of order a prime $p > 2$.

***Definition 2.8.*** — (i) Let $g := \mathrm{Gal}\,(K/\mathbb{Q})$ and let $\omega$ be the Teichmüller character of $g$, i.e., the character with values in $\mu_{p-1}(\mathbb{Q}_p)$ such that for $s_k \in g$ defined by $s_k(\zeta) = \zeta^k$, $k \not\equiv 0 \pmod p$, $\omega(s_k)$ (also denoted by $\omega(k)$) is the unique $(p-1)$th root of unity in $\mathbb{Q}_p$ congruent to $k$ modulo $p$. This is the character of the $g$-module $\langle\, \zeta \,\rangle$.

(ii) The idempotent corresponding to the character $\omega$ is

$$\mathcal{E}_\omega := \tfrac{1}{p-1} \sum_{s \in g} \omega^{-1}(s)\, s = \tfrac{1}{p-1} \sum_{k=1}^{p-1} \omega^{-1}(k)\, s_k \,\in \mathbb{Z}_p[g]\,.$$

(iii) We denote by $e_\omega$ a representative in $\mathbb{Z}[g]$ of $\mathcal{E}_\omega$ modulo $p\,\mathbb{Z}_p[g]$. We then have $e_\omega\, s_k \equiv k\, e_\omega \pmod{p\,\mathbb{Z}[g]}$ and $e_\omega\,(1 - e_\omega) \in p\,\mathbb{Z}[g]$. Put $e_\omega = \sum_{k=1}^{p-1} u_k\, s_k$, $u_k \in \mathbb{Z}$, $u_k \equiv \frac{k^{-1}}{p-1} \pmod p$.

We have $\omega^{-1}(s_{p-k}) = -\omega^{-1}(s_k)$ since $\omega(s_{-1}) = -1$; thus we may assume that $u_{p-k} = -u_k$ for $1 \leq k \leq \frac{p-1}{2}$, so that $e_\omega = (1 - s_{-1})\, e_\omega^\circ$ with $e_\omega^\circ = \sum_{k=1}^{\frac{p-1}{2}} u_k\, s_k$.
In some circumstances we shall use the representative $e'_\omega := \sum_{k=1}^{p-1} u'_k\, s_k \in \mathbb{Z}[g]$, $u'_k \equiv \frac{k^{-1}}{p-1} \pmod p$, with the conditions $0 < u'_k \leq p-1$.

***Example 2.9.*** — For $p=3$ we have $\mathcal{E}_\omega = \frac{1}{2}(1-s)$, with $s = s_{-1}$. We may thus choose $e_\omega = s - 1$ as a representative with integral coefficients. Then $e'_\omega = s + 2$.

For $p=5$, we may choose $e_\omega = -1 + 2\,s_2 - 2\,s_3 + s_4 = -1 + 2\,s + s^2 - 2\,s^3 = (1 - s^2)\,(2\,s - 1)$ with $s = s_2$. Then $e'_\omega = 4 + 2\,s + s^2 + 3\,s^3$.

***Remark 2.10.*** — Recall that the group of units $E$ of $K$ is the direct product $\langle\, \zeta \,\rangle \times E^+$, where $E^+$ is the group of units of the maximal real subfield $K^+$ of $K$; see **[Wa1]**, Prop. 1.5. Thus if $\varepsilon = \zeta^h\, \varepsilon^+$, $\varepsilon^+ \in E^+$, we get $\varepsilon^{e_\omega} = \zeta^h$, since $\zeta^{e_\omega} = \zeta$ for any representative $e_\omega$.

**2.4. The principles of the method – The fundamental relation.** — The aim of this article is to examine some properties of the arithmetic of the fields $\mathbb{Q}(\mu_n) \subseteq \mathbb{Q}(\mu_{q-1})$, $n \,|\, q-1$, in relation with a nontrivial solution in coprime integers $u, v$ of the SFLT equation

$$(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^{\delta}\,\mathfrak{w}_1^{p},$$

(see Conjecture 2.4) for all primes $q$ such that $q \nmid u\,v$ and $\frac{v}{u}$ modulo $q$ is of order $n$ prime to $p$. The cases where $n \leq 2$ (i.e., $q \,|\, u^2 - v^2$) are particular, especially when $(u, v)$ is part of a solution $(x, y, z)$ of Fermat's equation, and give Furtwängler's theorems [**Fur**]; see Corollaries 2.15 and 2.16 to Lemma 2.14 for a generalization of Furtwängler's theorems to the SFLT equation, and Remark 3.5 for the classical case of Fermat's equation; see also [**Mih1**] in the context of a Nagell–Ljunggren equation, which is the particular case of the SFLT equation with $v = 1$.

The cases where $n$ is divisible by $p$ give technical complications and are of a different nature. Some complements in this direction are developed in [**Que**] where similar studies are carried out.

***Lemma 2.11.*** — *Let $u$, $v$ be arbitrary coprime integers; put* $\Phi_n(u, v) := \prod_{\xi' \text{ of order } n} (u\,\xi' - v)$, $n \geq 1$, *which is equal to* $\mathrm{N}_{\mathbb{Q}(\mu_n)/\mathbb{Q}}(u\,\xi - v)$ *for any fixed primitive* $n$th *root of unity* $\xi$.
*Let $q$ be a prime. Then the following three properties are equivalent:*
*(i)* $q \,|\, \Phi_n(u, v)$ & $q \nmid n$;
*(ii)* $q \nmid u\,v$ & $\frac{v}{u}$ *is of order $n$ modulo $q$;*
*(iii)* $(q, u\,\xi - v)$ *is a prime ideal of* $\mathbb{Q}(\mu_n)$ & $q \equiv 1 \pmod{n}$.

*Proof.* — Suppose that $q \,|\, \Phi_n(u, v)$ and $q \nmid n$. Then $q \nmid u\,v$ since $\Phi_n(u, v)$ is a homogeneous form $u^{\phi(n)} \pm \cdots \pm v^{\phi(n)}$ in coprime integers $u$, $v$ ($\phi(n)$ is the Euler totient function).
For fixed $\xi$ of order $n$, the ideal $(q, u\,\xi - v)$ of the field $\mathbb{Q}(\mu_n)$ is a prime ideal lying above $q$; indeed, the relation $q \,|\, \Phi_n(u, v) = \prod_{\xi' \text{ of order } n} (u\,\xi' - v)$ shows that $u\,\xi - v \in \mathfrak{q}$ for a prime ideal $\mathfrak{q} \,|\, q$, of degree 1, unramified in $\mathbb{Q}(\mu_n)/\mathbb{Q}$ (since $q \nmid n$). So $(q, u\,\xi - v) = \mathfrak{q}$; thus $q$ is congruent to 1 modulo $n$ and $\frac{v}{u}$ is of order $n$ modulo $q$. This proves (i) $\Rightarrow$ (ii) and (i) $\Rightarrow$ (iii).
If $q \nmid u\,v$ and $\frac{v}{u}$ is of order $n$ modulo $q$, then $u^n - v^n \equiv 0 \pmod{q}$. From the equality $u^n - v^n = \prod_{d \,|\, n} \Phi_d(u, v)$ we deduce that there exists $m \,|\, n$ such that $q \,|\, \Phi_m(u, v)$, which implies $q \,|\, u^m - v^m$, hence $m = n$ by definition of the order; since we have $(\frac{v}{u})^q \equiv \frac{v}{u} \pmod{q}$, it is clear that $n$ cannot be divisible by $q$, proving (ii) $\Rightarrow$ (i). The implication (iii) $\Rightarrow$ (i) is immediate. □

***Corollary 2.12.*** — *For given coprime integers $u$, $v$, consider the set* $\{\Phi_n(u, v),\ n \in \mathbb{N}\backslash\{0\}\}$.
*(i) A given prime $q$ divides one of the numbers* $\Phi_n(u, v)$, $n \not\equiv 0 \pmod{q}$, *if and only if* $q \nmid u\,v$. *When the conditions* $q \,|\, \Phi_n(u, v)$ & $q \nmid n$ *are satisfied, then* $n \,|\, q - 1$ *and $n$ is unique.*
*(ii) For fixed* $n > 2$, *we have* $q \,|\, \Phi_n(u, v)$ & $q \nmid n$ *if and only if* $q \equiv 1 \pmod{n}$ & $q \nmid u\,v\,(u^2 - v^2)$ & $\frac{v}{u}$ *is of order $n$ modulo $q$.* (3)

(3) For $n > 2$, using for $u\,v \neq 0$ the inequalities $(|u| - |v|)^2 < (u\,\xi - v)(u\,\xi^{-1} - v) < (|u| + |v|)^2$, we see that $u\,\xi - v$ is a *global* unit (equivalent to $\Phi_n(u, v) = 1$) if and only if $u\,\xi - v \in \{\pm 1, \pm\xi, \pm(\xi + 1), \pm(\xi - 1)\}$, except

***Definition 2.13***. — Let $q \neq p$ be a prime. Recall that $K = \mathbb{Q}(\mu_p)$.
(i) *Fermat quotients*. Let $f$ be the residue degree of $q$ in $K/\mathbb{Q}$ and let $\kappa = \frac{q^f-1}{p}$. Since $f \mid p-1$, we have $\kappa \equiv 0 \pmod p$ if and only if $q^{p-1} \equiv 1 \pmod{p^2}$.
The integer $\overline{\kappa} := \frac{q^{p-1}-1}{p}$ is called the *Fermat quotient of* $q$. We have $\overline{\kappa} \equiv \frac{p-1}{f}\,\kappa \equiv -\frac{1}{p}\log(q) \pmod p$, where log is the $p$-adic logarithm.
(ii) *Power residue symbols*. Let us recall the definition and properties of the $p$th power residue symbols $\left(\frac{\bullet}{\bullet}\right)$ in $K$ and $M := \mathbb{Q}(\mu_n)K$, $n \mid q-1$, with values in $\mu_p$.

Let $\mathfrak{q}$ be a prime ideal lying above $q$ in $\mathbb{Q}(\mu_n)$ (also denoted by $\mathfrak{q} \mid q$).

If $\alpha \in M$ is prime to $\mathfrak{Q} \mid \mathfrak{q}$ in $M$, then let $\overline{\alpha}$ be the image of $\alpha$ in the residue field $Z_M/\mathfrak{Q} \simeq Z_K/\mathfrak{q}_K \simeq \mathbb{F}_{q^f}$ for $\mathfrak{q}_K = Z_K \cap \mathfrak{Q}$ (indeed, $q$ totally splits in $M/K$); since $Z_M$ contains a primitive $p$th root of unity $\zeta$, the image $\overline{\zeta}$ of $\zeta$ is of order $p$ (since $\zeta \not\equiv 1 \pmod{\mathfrak{Q}}$) and we can put $\overline{\alpha}^{\kappa} = \overline{\zeta}^{\,r}$, $r \in \mathbb{Z}/p\mathbb{Z}$, which defines the $p$th *power residue symbol* $\left(\frac{\alpha}{\mathfrak{Q}}\right)_M := \zeta^r$.

This symbol is trivial if and only if $\alpha$ is a local $p$th power at $\mathfrak{Q}$ (see e.g. **[Gr2]**, I.3.2.1, Ex. 1).

With this definition, for any automorphism $\tau \in \mathrm{Gal}(M/\mathbb{Q})$, from $\alpha^{\kappa} \equiv \zeta^{\,r} \pmod{\mathfrak{Q}}$ one obtains $\tau\alpha^{\kappa} \equiv \tau\zeta^{\,r} \pmod{\tau\mathfrak{Q}}$, thus, considering $\omega$ as a character of $\mathrm{Gal}(M/\mathbb{Q})$ trivial on $\mathrm{Gal}(M/K)$, we have $\left(\frac{\tau\alpha}{\tau\mathfrak{Q}}\right)_M = \tau\left(\frac{\alpha}{\mathfrak{Q}}\right)_M = \zeta^{r\,\omega(\tau)} = \left(\frac{\alpha}{\mathfrak{Q}}\right)_M^{\omega(\tau)}$. So, $\left(\frac{\alpha}{\tau\mathfrak{Q}}\right)_M = \left(\frac{\tau^{-1}\alpha}{\mathfrak{Q}}\right)_M^{\omega(\tau)}$.

For $\alpha \in K$ and any $\mathfrak{q}_K \mid q$ in $K$, we have $\left(\frac{\alpha}{\mathfrak{q}_K}\right)_K = \left(\frac{\alpha}{\mathfrak{Q}}\right)_M$ for any $\mathfrak{Q} \mid \mathfrak{q}_K$ in $M$.

These relations imply $\left(\frac{\zeta}{\mathfrak{q}_K}\right)_K = \zeta^{\kappa}$, which does not depend on the choice of $\mathfrak{q}_K \mid q$.

We return to the context of the SFLT equation $(u + v\,\zeta)\mathbb{Z}[\zeta] = \mathfrak{p}^{\delta}\,\mathfrak{w}_1^p$ in coprime integers $u, v$. For a solution $(u, v)$ of the above equation, set

$$\gamma_\omega := (u + v\,\zeta)^{e_\omega}\,.$$

With evident notations, in the context of a solution $(x, y, z)$ of Fermat's equation (see Subsection 2.1) we will have analogous calculations with $\gamma_\omega := (x + y\,\zeta)^{e_\omega}$ satisfying the relation $(x + y\,\zeta)\mathbb{Z}[\zeta] = \mathfrak{z}_1^p$, and with $\gamma'_\omega := (y + z\,\zeta)^{e_\omega}$ satisfying the relation $(y + z\,\zeta)\mathbb{Z}[\zeta] = \mathfrak{x}_1^p$ (non-special cases of the SFLT equation). Then in the first case ($p \nmid y$), $\gamma''_\omega := (z + x\,\zeta)^{e_\omega}$ with the relation $(z + x\,\zeta)\mathbb{Z}[\zeta] = \mathfrak{y}_1^p$ can be used, but $z - x$ may be divisible by $p$. In the second case ($p \mid y$), $\gamma''_\omega$ is of $\mathfrak{p}$-valuation 1 since $(z + x\,\zeta)\mathbb{Z}[\zeta] = \mathfrak{p}\,\mathfrak{y}_1^p$ and this gives a special case of the SFLT equation.

By Stickelberger's theorem, the $\omega$-component of the $p$-class group of $K$ is trivial (it is also a consequence of the reflection theorem, see **[Gr2]**, II.5.4.6.3). Hence the ideal class $c\ell(\mathfrak{w}_1)^{e_\omega}$ is trivial (since $c\ell(\mathfrak{w}_1)^p = 1$, this does not depend on the choice of the representative $e_\omega$ in $\mathbb{Z}[g]$).

---

if $\xi$ (resp. $-\xi$) is of order $\ell^e$, $\ell$ a prime, $e \geq 1$, in which case $\xi - 1$ (resp. $\xi + 1$) is a uniformizing parameter at $\ell$; but if so, necessarily $q = \ell$, $(q, u\,\xi - v) = (\xi \mp 1) \mid \ell$, $n = \ell^e$ (resp. $2\,\ell^e$), hence $q \mid n$, which is not allowed. These units correspond to the trivial solutions $(u, v) = \pm(0, 1), \pm(1, 0), \pm(1, 1), \pm(1, -1)$ of the SFLT equation which are precisely characterized by the relation $u\,v\,(u^2 - v^2) = 0$, in which case such primes $q$ do not exist. This observation, obtained in two different ways, has perhaps a significant meaning for our study.

Write $\mathfrak{w}_1^{e_\omega} = \mu_\omega\, \mathbb{Z}[\zeta],\ \ \mu_\omega \in K^\times$. Then we have

$$\gamma_\omega = \varepsilon_\omega\, \mu_\omega^p \ \text{ or } \ \gamma_\omega = (\zeta - 1)^{e_\omega} \varepsilon_\omega\, \mu_\omega^p$$

(depending on whether $\delta = 0$ or 1), where $\varepsilon_\omega \in E$. Set $\pi := \zeta - 1$.

***Lemma 2.14* (The fundamental relation)**. — *Let $(u, v)$, with g.c.d. $(u, v) = 1$, be a solution of the SFLT equation $(u + v\,\zeta)\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\, \mathfrak{w}_1^p$, and let $\gamma_\omega = (u + v\,\zeta)^{e_\omega}$.*
*Then there exists $h \in \mathbb{Z}/p\mathbb{Z}$ such that $\gamma_\omega \in \zeta^h \cdot K^{\times p}$. More precisely:*[4]
*(i) In the nonspecial cases ($u + v \not\equiv 0 \pmod p$) for $p \geq 3$, we have*

$$\gamma_\omega = \big(1 + \frac{v}{u+v}\,\pi\big)^{e_\omega} \in \zeta^{\frac{v}{u+v}} \cdot K^{\times p}\,.$$

*(ii) In the special case ($u + v \equiv 0 \pmod p$) for $p > 3$, we have*

$$\gamma_\omega = (\frac{u}{v} + \zeta)^{e_\omega} = (1 + \frac{v}{u}\,\zeta)^{e_\omega} \in \zeta^{\frac{1}{2}} \cdot K^{\times p}\,.$$

*(iii) In the special case ($u + v \equiv 0 \pmod 3$) for $p = 3$, we have*

$$\gamma_\omega = (\frac{u}{v} + \zeta)^{e_\omega} = (1 + \frac{v}{u}\,\zeta)^{e_\omega} \in \zeta^{\frac{1}{2}+\frac{1}{2}\,\frac{u+v}{3\,v}} \cdot K^{\times 3}\,.$$

*Proof.* — (i) We have $(u + v\,\zeta)^{e_\omega} = \gamma_\omega = \varepsilon_\omega\, \mu_\omega^p$ with $\varepsilon_\omega = \zeta^h \varepsilon^+$, $\varepsilon^+ \in E^+$, for some $h$; then applying again $e_\omega$ we obtain $(u + v\,\zeta)^{e_\omega^2} = \gamma_\omega^{e_\omega} = \varepsilon_\omega^{e_\omega}\, \mu_\omega^{e_\omega p} \in \zeta^h \cdot K^{\times p}$. Since $e_\omega^2 \equiv e_\omega \pmod{p\,\mathbb{Z}[g]}$, we get $(u + v\,\zeta)^{e_\omega} = \gamma_\omega \in \zeta^h \cdot K^{\times p}$.
Since $u + v\,\zeta = (u + v)\,\big(1 + \frac{v}{u+v}\,\pi\big)$, $(u + v\,\zeta)^{e_\omega} \in \zeta^h \cdot K^{\times p}$ is equivalent to

$$(1 + \tfrac{v}{u+v}\,\pi)^{e_\omega} \ \in \zeta^h \cdot K^{\times p}\,.$$

Using **[Gr1]**, Remark 3.4, we see that $\big(1+\frac{v}{u+v}\,\pi\big)^{e_\omega} \equiv 1+\frac{v}{u+v}\,\pi \pmod{\pi^2}$, and we immediately obtain $h \equiv \frac{v}{u+v} \pmod p$. This proves (i).
(ii) Suppose that $u + v \equiv 0 \pmod p$. Put $\frac{u}{v} = -1 + \lambda\, p$, then $\frac{u}{v} + \zeta = \pi + \lambda\, p = \pi\, \alpha$, where $\alpha := 1 + \frac{\lambda p}{\pi} \equiv 1 \pmod{\pi^{p-2}}$.
We have $\gamma_\omega := (u + v\,\zeta)^{e_\omega} = (1 + \frac{v}{u}\,\zeta)^{e_\omega} = (\frac{u}{v} + \zeta)^{e_\omega} = \pi^{e_\omega}\, \alpha^{e_\omega}$.
From the relation $(u+v\,\zeta)\,\mathbb{Z}[\zeta] = (\pi)\,\mathfrak{w}_1^p$, we obtain $(u+v\zeta)^{e_\omega} \in \pi^{e_\omega}\, \zeta^h \cdot K^{\times p}$ for some $h$, thus $\alpha^{e_\omega} \in \zeta^h \cdot K^{\times p}$, hence $h \equiv 0 \pmod p$ in this case since $p > 3$. Then $\big(1 + \frac{v}{u}\,\zeta\big)^{e_\omega} \in \pi^{e_\omega} \cdot K^{\times p}$.
Put $\alpha \sim \beta$ in $K^\times$ if $\alpha\,\beta^{-1} \in K^{\times p}$. From $(\zeta - 1)\,(\zeta + 1) = \zeta^2 - 1$, we obtain

$$(\zeta - 1)^{e_\omega}\,(\zeta + 1)^{e_\omega} = (\zeta^2 - 1)^{e_\omega} = (\zeta - 1)^{s_2 e_\omega} \sim (\zeta - 1)^{2e_\omega}\,,$$

hence $(\zeta + 1)^{e_\omega} \sim (\zeta - 1)^{e_\omega}$. Since $\zeta + 1 = \zeta^{\frac{1}{2}}(\zeta^{\frac{1}{2}} + \zeta^{-\frac{1}{2}})$ and $\zeta^{\frac{1}{2}} + \zeta^{-\frac{1}{2}} \in K^+$, we have $(\zeta + 1)^{e_\omega} \sim \zeta^{\frac{1}{2}}$, hence $(\zeta - 1)^{e_\omega} \sim (\zeta + 1)^{e_\omega} \sim \zeta^{\frac{1}{2}}$. This proves (ii).

(iii) If $p = 3$ in the special case, we deduce from the calculations done in the proof of (ii) that $\gamma_\omega = \pi^{e_\omega}\, \alpha^{e_\omega} \in \pi^{e_\omega}\, \zeta^h \cdot K^{\times 3}$ for some $h$, with $\alpha = 1 + \frac{3\lambda}{\pi}$ and $\lambda = \frac{u+v}{3\,v}$.
This shows that $\alpha = 1 + (\zeta^2 - 1)\,\frac{u+v}{3\,v} \equiv 1 - \pi\,\frac{u+v}{3\,v} \pmod{\pi^2}$, whence the congruence $h \equiv -\frac{u+v}{3\,v} \equiv \frac{1}{2}\,\frac{u+v}{3\,v} \pmod 3$ and $\gamma_\omega$ belongs to $\zeta^{\frac{1}{2}+\frac{1}{2}\,\frac{u+v}{3\,v}} \cdot K^{\times 3}$. □

[4] For any rational $r$ prime to $p$, in the writing $\zeta^r$, $r$ is considered as an element of $(\mathbb{Z}/p\mathbb{Z})^\times$.

In the second case of SFLT we have $\gamma_\omega \in K^{\times p}$ (resp. $\zeta\cdot K^{\times p}$) if $p \mid v$ (resp. $p \mid u$) since in this case $\frac{v}{u+v} \equiv 0 \pmod p$ (resp. $\frac{v}{u+v} \equiv 1 \pmod p$).

In the special case, the condition $u+v \equiv 0 \pmod{p^2}$ is satisfied when $(u,v)$ is a part of a solution $(x,y,z)=(u,y,v)$ or $(v,y,u)$ of Fermat's equation when $p \mid y$ (see Subsection 2.1).

***Corollary 2.15*** **(Generalization of the first theorem of Furtwängler)**
*Let $(u,v)$, with g.c.d. $(u,v)=1$, be a nontrivial solution of the SFLT equation $(u+v\,\zeta)\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\, \mathfrak{w}_1^p$, and let $q \neq p$ be a prime divisor of $u\,v$. Set $\kappa := \frac{q^f-1}{p}$ (see Definition 2.13 (i)).*

*(i) For $p \geq 3$ in the nonspecial cases we have $u\,\kappa \equiv 0 \pmod p$ if $q \mid u$ and $v\,\kappa \equiv 0 \pmod p$ if $q \mid v$. Hence in the first case we have $\kappa \equiv 0 \pmod p$.*

*(ii) For $p > 3$ in the special case we have $\kappa \equiv 0 \pmod p$.*

*(iii) For $p=3$ in the special case we have $\frac{u-2v}{3v}\,\kappa \equiv 0 \pmod 3$ if $q \mid u$ and $\frac{2u-v}{3v}\,\kappa \equiv 0 \pmod 3$ if $q \mid v$. Hence if $u+v \equiv 0 \pmod 9$, then $\kappa \equiv 0 \pmod 3$; if $u+v \equiv \pm 3 \pmod 9$, then $\kappa \equiv 0 \pmod 3$ if $q \mid u$ & $\frac{2u-v}{3v} \equiv 0 \pmod 3$, or if $q \mid v$ & $\frac{u-2v}{3v} \equiv 0 \pmod 3$.*

*Proof.* — We have $(u+v\,\zeta)^{e_\omega} \in \zeta^h \cdot K^{\times p}$ with $h \equiv \frac{v}{u+v} \pmod p$ in the nonspecial cases, $p \geq 3$, $h \equiv \frac{1}{2} \pmod p$ in the special case if $p>3$, and $h \equiv \frac12 + \frac12\,\frac{u+v}{3\,v} \pmod 3$ in the special case if $p=3$.

Let $\mathfrak{q}_K$ be any prime ideal of $K$ lying above $q$. We use the $p$th power residue symbol in $K$ (see Definition 2.13 (ii)).

Since $u+v\,\zeta \equiv v\,\zeta \pmod q$ if $q \mid u$ and $u+v\,\zeta \equiv u \pmod q$ if $q \mid v$, we have $\left(\frac{(u+v\,\zeta)^{e_\omega}}{\mathfrak{q}_K}\right)_K = \zeta^\kappa$ if $q \mid u$ and $\left(\frac{(u+v\,\zeta)^{e_\omega}}{\mathfrak{q}_K}\right)_K = 1$ if $q \mid v$. But we have $\left(\frac{\zeta^h}{\mathfrak{q}_K}\right)_K = \zeta^{\frac{v}{u+v}\,\kappa}$ (resp. $\zeta^{\frac12\,\kappa}$, $\zeta^{(\frac12+\frac12\,\frac{u+v}{3\,v})\,\kappa}$) in the nonspecial cases (resp. in the special case $p>3$, $p=3$). In the nonspecial cases for $q \mid u$, this gives $\frac{v}{u+v}\,\kappa \equiv \kappa \pmod p$, which is equivalent to $\frac{u}{u+v}\,\kappa \equiv 0 \pmod p$, hence to $u\,\kappa \equiv 0 \pmod p$; and if $q \mid v$, we have $\frac{v}{u+v}\,\kappa \equiv 0 \pmod p$, hence $v\,\kappa \equiv 0 \pmod p$.
The special case for $p>3$ yields $\frac12\,\kappa \equiv \kappa$ (resp. $\frac12\,\kappa \equiv 0$) $\pmod p$ if $q \mid u$ (resp. $q \mid v$), giving $\kappa \equiv 0 \pmod p$ in any case.

For $p=3$ in the special case we have $(\frac12+\frac12\,\frac{u+v}{3\,v})\,\kappa \equiv \kappa \pmod 3$ if $q \mid u$, $(\frac12+\frac12\,\frac{u+v}{3\,v})\,\kappa \equiv 0 \pmod 3$ if $q \mid v$, hence $\frac{u-2v}{3}\,\kappa \equiv 0 \pmod 3$ and $\frac{2u-v}{3}\,\kappa \equiv 0 \pmod 3$, respectively.

The case $u+v \equiv 0 \pmod 9$ is obvious as well as the case $u+v \equiv \pm 3 \pmod 9$. □

***Corollary 2.16*** **(Generalization of the second theorem of Furtwängler)**
*Let $(u,v)$, with g.c.d. $(u,v)=1$, be a nontrivial solution of the SFLT equation $(u+v\,\zeta)\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\, \mathfrak{w}_1^p$ and let $q \neq p$ be a prime divisor of $u^2-v^2$.*

*(i) For $p \geq 3$ in the nonspecial cases, we have $(u-v)\,\kappa \equiv 0 \pmod p$; hence $\kappa \equiv 0 \pmod p$ as soon as $u-v \not\equiv 0 \pmod p$. In particular, in the second case, $\kappa \equiv 0 \pmod p$.*

*(ii) For $p=3$ in the first case the information is empty since $u \equiv v \equiv \pm 1 \pmod 3$.*

*(iii) For $p>3$ in the special case, the information is empty.*

*(iv) For $p=3$ in the special case we have $\frac{u+v}{3\,v}\,\kappa \equiv 0 \pmod 3$, hence $\kappa \equiv 0 \pmod 3$ as soon as $u+v \not\equiv 0 \pmod 9$.*

*Proof.* — We have $(u+v\,\zeta)^{e_\omega} \in \zeta^h \cdot K^{\times p}$ with $h \equiv \frac{v}{u+v} \pmod p$ in the nonspecial cases, $h \equiv \frac{1}{2} \pmod p$ in the special case if $p>3$, and $h \equiv \frac{1}{2} + \frac{1}{2}\,\frac{u+v}{3\,v} \pmod 3$ in the special case if $p=3$.

This shows that $(1+\frac{v}{u}\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}} \in \zeta^{\overline{h}} \cdot K^{\times p}$ with $\overline{h} \equiv -\frac{1}{2}\frac{u-v}{u+v} \pmod p$ in the nonspecial cases, $\overline{h} \equiv 0 \pmod p$ in the special case if $p>3$, and $\overline{h} \equiv \frac{1}{2}\,\frac{u+v}{3\,v} \pmod 3$ in the special case if $p=3$.

Let $\mathfrak{q}_K$ be any prime ideal of $K$ lying above $q$. If $q \,|\, u^2-v^2$, then $\frac{v}{u} \equiv \pm 1 \pmod q$ and we get $(1+\frac{v}{u}\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}} \equiv (1\pm\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}} \pmod{\mathfrak{q}_K}$; since $(1\pm\zeta)^{e_\omega} \sim \zeta^{\frac{1}{2}}$ (see proof of Lemma 2.14), we obtain $\overline{h}\,\kappa \equiv 0 \pmod p$ in every case.

The nonspecial cases yield $\frac{u-v}{u+v}\,\kappa \equiv 0 \pmod p$, hence $\kappa \equiv 0 \pmod p$ if $u-v \not\equiv 0 \pmod p$. Thus the case $p=3$ is empty since $u \equiv v \equiv \pm 1 \pmod 3$.

The special case for $p>3$ is empty since $\overline{h} \equiv 0 \pmod p$. The special case for $p=3$ gives $\frac{u+v}{3\,v}\,\kappa \equiv 0 \pmod 3$. □

**2.5. Consequences of Lemma 2.14.** — We make the following comments on the fundamental Lemma 2.14 and its corollaries to introduce suitable *$\omega$-cyclotomic units* and the *$\omega$-SFLT equation.*

*2.5.1. General study of the numbers $(u+v\,\zeta)^{e_\omega}$, $u,v \in \mathbb{Z}$,* g.c.d.$\,(u,v)=1$. — For *arbitrary* coprime integers $u$, $v$, $u\,v\,(u+v) \neq 0$, we still have

$$\gamma_\omega := (u+v\,\zeta)^{e_\omega} = \big(\frac{u}{v}+\zeta\big)^{e_\omega} = \big(1+\frac{v}{u}\,\zeta\big)^{e_\omega} = \big(1+\frac{v}{u+v}\,\pi\big)^{e_\omega}, \quad \pi := \zeta - 1\,,$$

and also the various congruences of Lemma 2.14, $\gamma_\omega \equiv \zeta^h \pmod{\pi^2}$, with $h = \frac{v}{u+v}$ (nonspecial cases, $p \geq 3$), $h = \frac{1}{2}$ (special case, $p>3$), and $h = \frac{1}{2} + \frac{1}{2}\,\frac{u+v}{3\,v}$ (special case, $p=3$).

Then we obtain $\gamma_\omega\,\zeta^{-h} \equiv 1 \pmod{\pi^2}$, which easily implies that $\gamma_\omega\,\zeta^{-h}$ is a $p$-primary number (use **[Gr1]**, Lemma 3.15); but since $(u+v\,\zeta)\,\mathbb{Z}[\zeta]$ is not in general the $p$th power of an ideal this number $\gamma_\omega\,\zeta^{-h}$ is not necessarily a global $p$th power. (5)

By class field theory, there exist infinitely many prime ideals $\mathfrak{q}_K$ of $K$, prime to $u\,v$, such that $\gamma_\omega\,\zeta^{-h} = (1+\frac{v}{u}\,\zeta)^{e_\omega}\,\zeta^{-h}$ is not a local $p$th power at $\mathfrak{q}_K$, except if we have a counterexample $(u,v)$ to SFLT in which case such primes do not exist since $(1+\frac{v}{u}\,\zeta)^{e_\omega}\,\zeta^{-h}$ is then a global $p$th power.

The $p$th power residue symbol (Definition 2.13 (ii)) of $(1+\frac{v}{u}\,\zeta)^{e_\omega}\,\zeta^{-h}$ is invariant by conjugation of $\mathfrak{q}_K$ since

$$\big((1+\frac{v}{u}\,\zeta)\,\zeta^{-h}\big)^{e_\omega\,\kappa} \equiv \zeta' \pmod{\mathfrak{q}_K}$$

implies, by conjugation by $s_k \in g$,

$$\big((1+\frac{v}{u}\,\zeta^k)\,\zeta^{-k\,h}\big)^{e_\omega\,\kappa} \sim \big((1+\frac{v}{u}\,\zeta)\,\zeta^{-h}\big)^{k\,e_\omega\,\kappa} \equiv \zeta'^k \pmod{s_k(\mathfrak{q}_K)}\,,$$

which is equivalent (up to $p$th powers) to

$$\big((1+\frac{v}{u}\,\zeta)\,\zeta^{-h}\big)^{e_\omega\,\kappa} \equiv \zeta' \pmod{s_k(\mathfrak{q}_K)}\,.$$

(5) Recall that a $p$-primary number is not necessarily a local $p$th power; this is true for pseudo-units. In the case where $(u+v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{w}_1^p$, Lemma 2.14 shows that $\gamma_\omega\,\zeta^{-h} \in K^{\times p}$; so in this particular case where $\gamma_\omega\,\zeta^{-h}$ is a pseudo-unit, hence a local $p$th power at $p$, we obtain a necessary and sufficient condition to have a global $p$th power.

So this symbol only depends on $q$, the prime under $\mathfrak{q}_K$, which does not divide $u\,v$.

We suppose $\frac{v}{u}$ of order $n$ modulo $q$ (which is equivalent to $q \,|\, \Phi_n(u,v)$ & $q \equiv 1 \pmod n$ by Lemma 2.11 and Corollary 2.12). Assume that $n$ is prime to $p$.

Let $\mathfrak{q}$ be a prime ideal lying above $q$ in $\mathbb{Q}(\mu_n)$, $\xi$ the $n$th primitive root of unity such that $\xi \equiv \frac{v}{u} \pmod{\mathfrak{q}}$, $\mathfrak{Q}$ a prime ideal lying above $\mathfrak{q}$ in $\mathbb{Q}(\mu_n)K$, and $\mathfrak{q}_K := \mathfrak{Q} \cap \mathbb{Z}[\zeta]$. The $p$th power residue symbols of $(1 + \frac{v}{u}\,\zeta)^{e_\omega}\,\zeta^{-h}$ at $\mathfrak{q}_K$ in $K$ and of the cyclotomic unit

$$\eta_1 := (1 + \xi\,\zeta)^{e_\omega}\,\zeta^{-h}$$

at $\mathfrak{Q}$ in $\mathbb{Q}(\mu_n)K$ are equal (see Definition 3.2 for more information on $\eta_1$).

*2.5.2. Case of a solution of the SFLT equation and consequences for FLT.* — In this case both the $p$th power residue symbols of $(1+\frac{v}{u}\,\zeta)^{e_\omega}\,\zeta^{-h} \in K^{\times p}$ at $\mathfrak{q}_K$ in $K$ and of the cyclotomic unit $\eta_1 = (1 + \xi\,\zeta)^{e_\omega}\,\zeta^{-h}$ at $\mathfrak{Q}$ in $\mathbb{Q}(\mu_n)K$ are trivial. This fact is the starting point of our method.

Of course $h$ is a priori unknown (but constant with respect to $q$) and the local study of $(1 + \xi\,\zeta)^{e_\omega}\,\zeta^{-h}$ is ineffective in general, but we may use some partial information, as the following ones in the context of FLT.

Let $(x, y, z)$ be a solution of Fermat's equation (first or second case).

**a)** *Nonspecial cases of SFLT*. Take for instance $u = x$ and $v = y$, which gives $h = \frac{y}{x+y}$.

- If $\zeta$ is not a local $p$th power at $\mathfrak{q}_K$ (which is equivalent to $\kappa \not\equiv 0 \pmod p$), we consider the $p$th power residue symbol at $\mathfrak{Q}$ of $\eta_1 = (1+\xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}$, which must be that of $\zeta^{\,h-\frac{1}{2}} = \zeta^{-\frac{1}{2}\frac{x-y}{x+y}}$. For FLT we have some informations on the differences such as $x - y$, $y - z$, which are prime to $p$ for $p > 3$ or $p = 3$ in the second case; in these cases a contradiction to the existence of such a solution of Fermat's equation is that the unit $\eta_1$ be a local $p$th power at $\mathfrak{Q}$ or does not give the right symbol.

For $p = 3$ in the first case, we know that $x \equiv y \equiv z \equiv \pm 1 \pmod 3$; so we have a contradiction if this unit is not a local third power at $\mathfrak{Q}$.

- If $\zeta$ is a local $p$th power at $\mathfrak{q}_K$ (which is equivalent to $\kappa \equiv 0 \pmod p$), we contradict the existence of such a solution of Fermat's equation if the unit $\eta_1$ is not a local $p$th power at $\mathfrak{Q}$.

**b)** *Special case of SFLT*. In the second case of FLT ($p \,|\, y$) with $u = z$, $v = x$, we use a different argument (but of a similar nature), relying on the fact that $h - \frac{1}{2} \equiv 0 \pmod p$ (Lemma 2.14 for $p \geq 3$, since $z + x \equiv 0 \pmod 9$ when $p = 3$).

**c)** *Conclusion*. Our hope in this attempt is that, since the arithmetical properties of the fields $\mathbb{Q}(\mu_n) \subseteq \mathbb{Q}(\mu_{q-1})$ are *a priori* independent of the SFLT problem, they may give valuable indications on the local properties of $\eta_1$, especially in an analytic point of view. In some sense the fields $\mathbb{Q}(\mu_{q-1})$ will play the role of auxiliary fields. Indeed, under a solution of the SFLT equation, the $p$th power residue symbol over $\mathfrak{q}$ of $\eta_1$ is, *independently of the choice of* $q$, equal to the $p$th power residue symbol of a *constant power of* $\zeta$, which may be absurd.

In Section 4 we shall interpret these properties in terms of Frobenius automorphisms in suitable *canonical* $p$-ramified Abelian $p$-extensions of the fields $\mathbb{Q}(\mu_n)$, which will be more suitable for analytic investigations.

*2.5.3. Historical remarks.* — The cyclotomic fields, like $\mathbb{Q}(\mu_{q-1})$ for primes $q$, have been introduced by Vandiver in some papers, such as [**Van1**], [**Van2**], [**Van3**], to generalize some congruences giving Furtwängler's theorems and Wieferich's criteria.

To this end Vandiver considers some of the relations of Lemma 2.14. The $p$th power residue symbol of cyclotomic units, constructed using the cyclotomic unit $\eta$, occurs in congruence relations modulo $p$. The calculations essentially depend on the Stickelberger element

$$S := \frac{1}{p} \sum_{k=1}^{p-1} k\, s_k^{-1} ,$$

related to generalized Bernoulli numbers and the annihilation of the $p$-class group of $K$, and on the idempotents of the group algebra $\mathbb{F}_p[g]$.

Note that Vandiver does not make use of class field theoretical interpretations, nor of analytic results like the Čebotarev density theorem, and, a priori, no conclusion could be deduced from his purely local calculations at $p$.

Our present work is mainly global and does not take precisely into account the arithmetic of $K$ as in the historical researches.

For a recent critical history on FLT see [**Co**]. For some complements on the cyclotomic techniques, see [**He1**], [**He2**], [**Mih1**], [**Mih2**], [**Ter**], [**Ri**], [**Si**]. For similar arguments using auxiliary primes $q$, see [**D**], [**Kr**], and also [**A–H**] and [**Fo**], which make use of results on the distribution of primes.

**2.6. Another equivalent equation.** — We have the following result, the statement of which makes use of the representative $e_\omega = (1 - s_{-1})\, e_\omega^+$ defined in Definition 2.8 (iii).

***Lemma 2.17* (The $\omega$-SFLT equation).** — *The equation $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\, \mathfrak{w}_1^p$ in coprime integers $u$, $v$ (see Conjecture 2.4) is equivalent to the equation in coprime integers $u$, $v$ of the form $(u + v\,\zeta)^{e_\omega} = \zeta'\, \mu_\omega^p$, where $\zeta'$ is any* $p$th *root of unity and $\mu_\omega$ any element of $K^\times$.*

*For a solution $(u, v)$ of this second equation, necessarily $\zeta' = \zeta^h$, where $h \equiv \frac{v}{u+v} \pmod p$ in the nonspecial cases, $h \equiv \frac{1}{2} \pmod p$ in the special case, $p > 3$, and $h \equiv \frac{1}{2} + \frac{1}{2}\, \frac{u+v}{3\,v} \pmod 3$ in the special case, $p = 3$; then $\mu_\omega$ is necessarily prime to $p$.*

*Proof.* — One direction has yet been proved (Lemma 2.14). In the other direction, consider a solution $(u, v)$, g.c.d. $(u, v) = 1$, of the second equation. The prime ideals $\mathfrak{l} \neq \mathfrak{p}$ dividing the ideal $(u + v\,\zeta)\,\mathbb{Z}[\zeta]$ are of degree 1 since $\zeta$ is congruent to a rational modulo $\mathfrak{l}$; thus the prime $\ell$ under $\mathfrak{l}$ splits completely in $K/\mathbb{Q}$.

For each $\ell$, there is a unique $\mathfrak{l}$ lying above $\ell$ dividing $(u + v\,\zeta)\,\mathbb{Z}[\zeta]$ (otherwise, using appropriate conjugates of the congruence $u + v\,\zeta \equiv 0 \pmod{\mathfrak{l}}$, we would have $u \equiv v \equiv 0 \pmod{\mathfrak{l}}$, a contradiction). This implies $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^\delta \prod_\ell \mathfrak{l}^{\alpha_\ell}$, $\delta = 0$ or $1$, $\alpha_\ell \geq 1$, for distinct primes $\ell \neq p$.

For a prime ideal $\mathfrak{l} \neq \mathfrak{p}$ of degree 1 of $K$, the representation $\langle\, \mathfrak{l}^s \,\rangle_{s \in g} / \langle\, \mathfrak{l}^s \,\rangle_{s \in g}^p$ of $g$ is isomorphic to $\mathbb{F}_p[g]$. Hence, since $\mathfrak{p}^{e_\omega} = \mathbb{Z}[\zeta]$ and since $(u + v\,\zeta)^{e_\omega}\,\mathbb{Z}[\zeta] = \prod_\ell \mathfrak{l}^{e_\omega\, \alpha_\ell}$ is a $p$th power by assumption, we have $\alpha_\ell \equiv 0 \pmod p$ for all $\ell$, which implies $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\, \mathfrak{w}_1^p$. □

***Remark 2.18.*** — (i) Using the norm from the equality $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^{\delta} \prod_{\ell} \mathfrak{l}^{\alpha_\ell}$, we obtain the equivalence of the SFLT equation with the equation $\mathrm{N}_{K/\mathbb{Q}}(u + v\,\zeta) = p^{\delta}\, w_1^p$ mentioned in Subsection 2.2.

(ii) We call *$\omega$-SFLT equation* the new equation in coprime integers $u$, $v$. The corresponding form of the SFLT conjecture for $p > 3$ seems reasonable as soon as $p$ is sufficiently large since it asserts (for $u\,v\,(u^2 - v^2) \neq 0$) that there exists $\sum_{k=1}^{p-1} \lambda_k\, \zeta^k \in K$, $\lambda_k \in \mathbb{Q}$, the $p$th power of which is of the form $(u\,\zeta^{-\frac{v}{u+v}} + v\,\zeta^{\frac{u}{u+v}})^{e_\omega}$ in the nonspecial cases and of the form $(u\,\zeta^{-\frac{1}{2}} + v\,\zeta^{\frac{1}{2}})^{e_\omega})$ in the special case, depending on two coefficients $u$, $v$ instead of $p-1$ in general.

(iii) From a relation of the form $(u' + v'\,\zeta)^{e_\omega} = \zeta'\,\mu_\omega^p$, $u', v' \in \mathbb{Q}$, we deduce the solution in coprime integers $(u, v) := \frac{1}{\text{g.c.d.}\,(u',v')}\,(u', v')$ of the equation $(u + v\,\zeta)^{e_\omega} = \zeta'\,\mu_\omega^p$ or of the SFLT equation. This is this unique solution modulo $\mathbb{Q}^\times$ that we consider for the $\omega$-SFLT equation.

Recall that for $p > 3$, SFLT implies FLT; if necessary we can restrict ourselves to the nonspecial cases of SFLT to get the two cases of FLT. So in this paper we mainly focus on SFLT, using the simpler $\omega$-SFLT context which does not involve in an essential way the arithmetic of $K$, the crucial point in the lack of success of the classical theory that we have analyzed in **[Gr1]**.

## 3. Utilization of the auxiliary fields $\mathbb{Q}(\mu_{q-1})$

**3.1. The Vandiver and Furtwängler papers revisited.** — Consider a solution of the SFLT equation $(u{+}v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^{\delta}\,\mathfrak{w}_1^p$ in coprime integers $u$, $v$. Recall that necessarily $\delta \in \{0, 1\}$ and $\mathfrak{w}_1$ is prime to $p$ (see Conjecture 2.4).

We still consider a prime $q$ such that $q \nmid u\,v$ and such that $\frac{v}{u}$ is of order $n$ modulo $q$ (which is equivalent by Lemma 2.11 and Corollary 2.12 to $q \,|\, \Phi_n(u, v)$ & $q \equiv 1 \pmod{n}$ or to the fact that $(q, u\,\xi - v)$ is a prime ideal lying above $q \equiv 1 \pmod{n}$). We assume that $n$ is prime to $p$.

Consider now the following diagram, in which $L := \mathbb{Q}(\mu_n)$, $M := LK$, and $G = \mathrm{Gal}(M/L) \simeq g$ (we have $L \cap K = \mathbb{Q}$):

$$\begin{tikzcd}
L \arrow[r, dash, "G"] \arrow[d, dash] & M \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash, "g"] & K = \mathbb{Q}(\zeta)
\end{tikzcd}$$

***Definition 3.1.*** — The following definitions are valid for any coprime integers $u, v$ such that $q \nmid u\,v$; $n \,|\, q-1$ is still the order, assumed to be prime to $p$, of $\frac{v}{u}$ modulo $q$.
(i) *The prime ideals $\mathfrak{q}_{\rho,\xi}$ of $L = \mathbb{Q}(\mu_n)$ (see Lemma 2.11).* Let $q \equiv 1 \pmod{n}$ be a prime; so it splits completely in $L/\mathbb{Q}$. If $\mathfrak{q}$ is a prime ideal of $L$ lying above $q$, there exists a *unique* primitive $n$th root of unity $\xi$ such that $\xi \equiv \frac{v}{u} \pmod{\mathfrak{q}}$. Conversely, if $\xi$ is a primitive $n$th root of unity, there exists a *unique* prime ideal $\mathfrak{q}$ of $L$ lying above $q$ such that $\xi \equiv \frac{v}{u} \pmod{\mathfrak{q}}$. This ideal $\mathfrak{q}$, equal to $(q, u\,\xi - v) := q\,Z_L + (u\,\xi - v)\,Z_L$, will also be denoted by $\mathfrak{q}_{\frac{v}{u},\xi}$ or by $\mathfrak{q}_{\rho,\xi}$ (it indeed only depends on the class of $\rho := \frac{v}{u}$ in $(\mathbb{Z}/q\mathbb{Z})^\times$).

(ii) *The conjugacy class $\mathcal{C}_\rho(q)$ associated with $q$.* We associate with $q$ a pair $(\xi, \mathfrak{q})$ where the prime ideal $\mathfrak{q} = \mathfrak{q}_{\frac{v}{u}, \xi}$ lying above $q$ and the primitive $n$th root of unity $\xi$ are characterized by the congruence $\xi \equiv \frac{v}{u} \pmod{\mathfrak{q}}$ in $L$.

This pair is defined up to $\mathbb{Q}$-conjugation since $\xi \equiv \frac{v}{u} \pmod{\mathfrak{q}_{\frac{v}{u}, \xi}}$ is equivalent to $\xi^t \equiv \frac{v}{u}$ $(\mathrm{mod}\ \mathfrak{q}^t_{\frac{v}{u}, \xi} = \mathfrak{q}_{\frac{v}{u}, \xi^t})$ for all $t \in \mathrm{Gal}(L/\mathbb{Q})$. We obtain this way an equivalence relation. The class of $(\xi, \mathfrak{q})$ only depends on $q$ for given $u$, $v$. We denote by $\mathcal{C}_{\frac{v}{u}}(q)$ or $\mathcal{C}_\rho(q)$ this class.

For a solution $(u, v)$ of the SFLT equation, the class $\mathcal{C}_\rho(q)$ is ineffective among the $\phi(n)$ *a priori* possible classes ($\phi(n)$ being the Euler totient function); moreover, $n$ is also unknown.

This explains that, in some circumstances, we shall assume that $q$ is not congruent to 1 modulo $p$, since otherwise, we cannot assert that the order of $\rho$ modulo $q$ is prime to $p$.

***Definition 3.2* (The fundamental $\omega$-cyclotomic unit $\eta_1$).** — For a given $n$th root of unity $\xi$, $n \not\equiv 0 \pmod{p}$, we consider the cyclotomic number of $M$, associated to $\xi$,

$$\eta = \eta(\xi) := (1 + \xi\, \zeta)\, \zeta^{-\frac{1}{2}},$$

where, as we have explained, $\frac{1}{2}$ is regarded as an element of $(\mathbb{Z}/p\mathbb{Z})^\times$.

We know that $1 + \xi\, \zeta$ is a (cyclotomic) unit except if $-\xi\zeta$ is of prime power order, which is the case if and only if $\xi = -1$ (i.e., $n = 2$), in which case $1 + \xi\, \zeta = 1 - \zeta$ generates $\mathfrak{p}$.

Then we put (see Definition 2.8 (iii))

$$\eta_1 := \eta^{e_\omega} = (1 + \xi\, \zeta)^{e_\omega}\, \zeta^{-\frac{1}{2}} \in M\,.$$

We have $\eta_1 \in M^+$, where $M^+$ is the maximal real subfield of $M$: indeed, if $c$ is the complex conjugation, we have

$$\eta_1^c = (1 + \xi^{-1}\, \zeta^{-1})^{e_\omega}\, \zeta^{\frac{1}{2}} = \big((1 + \xi\, \zeta)\, \xi^{-1}\, \zeta^{-1}\, \zeta^{\frac{1}{2}}\big)^{e_\omega} = (1 + \xi\, \zeta)^{e_\omega}\, \zeta^{-\frac{1}{2}} = \eta_1,$$

since $\xi^{e_\omega} = 1$ and $\zeta'^{e_\omega} = \zeta'$ for any $\zeta' \in \mu_p$.

We note that $\eta_1$ is a cyclotomic unit and that $\eta_1 \equiv 1 \pmod{\pi\, Z_M}$, where $\pi = \zeta - 1$. We say that $\eta_1$ is a $\omega$-cyclotomic unit because of the writing $\eta_1 = \eta^{e_\omega}$ giving the $G$-module structure defined in $M^\times/M^{\times p}$ by $\eta_1^s \sim \eta_1^{\omega(s)}$ for all $s \in G \simeq g$ (see the general case in Subsection 4.6).

Let us return to a solution $(u, v)$ of the SFLT equation such that $\frac{v}{u}$ is of order $n$ modulo $q$, for some $n \,|\, q - 1$ prime to $p$. Starting from $\xi \equiv \frac{v}{u} \pmod{\mathfrak{q}}$, which defines $\mathfrak{q} := \mathfrak{q}_{\frac{v}{u}, \xi}$, and extending $\mathfrak{q}$ to $M$ we obtain

$$\eta_1 \equiv \big(1 + \tfrac{v}{u}\, \zeta\big)^{e_\omega}\, \zeta^{-\frac{1}{2}} \quad (\mathrm{mod}\ \prod_{\mathfrak{Q}\,|\,\mathfrak{q}} \mathfrak{Q})\,.$$

We note that these prime ideals $\mathfrak{Q}$ of $M$ may be written $\mathfrak{Q}_{\frac{v}{u}, \xi}$ since they lie above $\mathfrak{q}_{\frac{v}{u}, \xi}$; for fixed $\xi$, they are conjugate under $G$.

Lemma 2.14 shows that $\big(1 + \frac{v}{u}\, \zeta\big)^{e_\omega} = \zeta^{\frac{v}{u+v}} \cdot \mu_\omega^p$ (in the nonspecial cases, $p \geq 3$) or $\zeta^{\frac{1}{2}} \cdot \mu_\omega^p$ (in the special case, $p > 3$) or $\zeta^{\frac{1}{2} + \frac{1}{2}\, \frac{u+v}{3\, v}} \cdot \mu_\omega^3$ (in the special case, $p = 3$), with $\mu_\omega \in K^\times$. This yields the congruences

$$\eta_1 \equiv \zeta^{-\frac{1}{2}\, \frac{u-v}{u+v}} \cdot \mu_\omega^p \ \text{ or } \ \mu_\omega^p \ \text{ or } \ \zeta^{\frac{1}{2}\, \frac{u+v}{3\, v}} \cdot \mu_\omega^3 \quad (\mathrm{mod}\ \textstyle\prod_{\mathfrak{Q}\,|\,\mathfrak{q}} \mathfrak{Q})\ .$$

Using these congruences on $\eta_1$, the Definition 2.13, 3.1, and 3.2, we obtain in the context of SFLT the following essential result:

***Theorem 3.3***. — *Let $p$ be a prime $\geq 3$, let $K = \mathbb{Q}(\zeta)$ where $\zeta$ is a primitive $p$th root of unity, and let $\mathfrak{p} = (\zeta - 1)\,\mathbb{Z}[\zeta]$. Suppose that we have an equality $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^{\delta}\,\mathfrak{w}_1^{p}$ with coprime integers $u$, $v$, where $\delta \in \{0, 1\}$ and $\mathfrak{w}_1$ is an integral ideal of $K$ (see Conjecture 2.4). Let $q \neq p$, $q \nmid u\,v$, be a prime such that $\frac{v}{u}$ is of order $n$ modulo $q$, with $p \nmid n$.*
*Set $\eta := (1 + \xi\,\zeta)\,\zeta^{-\frac{1}{2}}$ and $\eta_1 := \eta^{e_\omega}$, where $\xi$ is a primitive $n$th root of unity. Finally let $\mathfrak{q} = (q, u\,\xi - v) \,|\, q$ in $L := \mathbb{Q}(\mu_n)$. Then we have in $M := LK$:*
$\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \zeta^{-\frac{1}{2}\,\frac{u-v}{u+v}\,\kappa}$, *for all $\mathfrak{Q} \,|\, \mathfrak{q}$, in the nonspecial cases ($p \nmid u + v$), $p \geq 3$,* [6]
$\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = 1$, *for all $\mathfrak{Q} \,|\, \mathfrak{q}$, in the special case ($p \,|\, u + v$), $p > 3$,*
$\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \zeta^{\frac{1}{2}\,\frac{u+v}{3\,v}\,\kappa}$, *for all $\mathfrak{Q} \,|\, \mathfrak{q}$, in the special case, $p = 3$.*

These relations show that $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M$ only depends on the Fermat quotient of $q$ once $u$ and $v$ are given. The class of the pairs $(\eta_1^t, \mathfrak{Q}^t)$, $t \in \mathrm{Gal}(M/K)$, for any choice of $\mathfrak{Q} \,|\, \mathfrak{q}$ in $M$, corresponds canonically to the class $\mathcal{C}_{\frac{v}{u}}(q)$ of the $(\xi^t, \mathfrak{q}^t)$, since we have the relation

$$\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M^t = \left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \left(\frac{\eta_1^t}{\mathfrak{Q}^t}\right)_M,$$

where $\mathfrak{Q}^t \,|\, \mathfrak{q}^t$, and $\eta_1^t = (1 + \xi^t\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}$. For $t \neq 1$, the symbol $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M$ may be different from $\left(\frac{\eta_1}{\mathfrak{Q}^t}\right)_M = \left(\frac{\eta_1^{t^{-1}}}{\mathfrak{Q}}\right)_M$ since there is no local information on $\dfrac{1 + \xi^{t^{-1}}\,\zeta}{1 + \xi\,\zeta}$. But as we have seen, $\left(\frac{\eta_1}{\mathfrak{Q}^s}\right)_M = \left(\frac{\eta_1}{\mathfrak{Q}}\right)_M$ holds for any $s \in G$.

***Remark 3.4***. — Since for g.c.d. $(u, v) = 1$ the relation $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^{\delta}\,\mathfrak{w}_1^{p}$ is equivalent to the relation $\mathrm{N}_{K/\mathbb{Q}}(u + v\,\zeta) = p^{\delta}\,w_1^{p}$, we deduce from $u + v\,\zeta \equiv u\,(1 + \xi\,\zeta) \pmod{\mathfrak{Q}}$ for all $\mathfrak{Q} \,|\, \mathfrak{q} = \mathfrak{q}_{\frac{v}{u},\xi}$ that for $n \neq 2$,

$$\mathrm{N}_{M/L}(u + v\,\zeta) \equiv \mathrm{N}_{M/L}(u\,(1 + \xi\,\zeta)) = u^{p-1}\,\frac{1 + \xi^p}{1 + \xi} = u^{p-1}\,(1 + \xi)^{t_p - 1} \pmod{\mathfrak{Q}}$$

for all $\mathfrak{Q} \,|\, \mathfrak{q}$, where $t_p$ is the Frobenius automorphism of $p$ in $L/\mathbb{Q}$. This implies

$$\left(\frac{(1 + \xi)^{t_p - 1}}{\mathfrak{Q}}\right)_M = \left(\frac{u}{\mathfrak{q}_K}\right)_K = \left(\frac{v}{\mathfrak{q}_K}\right)_K \ \left(\text{resp.} \ = \left(\frac{pu}{\mathfrak{q}_K}\right)_K = \left(\frac{pv}{\mathfrak{q}_K}\right)_K\right)$$

in the nonspecial cases (resp. the special case), for all $\mathfrak{Q} \,|\, \mathfrak{q}$ and all $\mathfrak{q}_K \,|\, q$ in $K$.
If $n = 2$ we have $\left(\frac{u}{\mathfrak{q}_K}\right)_K = \left(\frac{v}{\mathfrak{q}_K}\right)_K = \left(\frac{p}{\mathfrak{q}_K}\right)_K$ in the nonspecial cases, and $\left(\frac{u}{\mathfrak{q}_K}\right)_K = \left(\frac{v}{\mathfrak{q}_K}\right)_K = 1$ otherwise.

[6] In the first case of SFLT for $p > 3$ we may have $u - v \equiv 0 \pmod{p}$ (hence $u - v \equiv 0 \pmod{p^2}$) but not in the FLT context applied with $(u, v) = (x, y)$ or $(y, z)$. If $p = 3$, we have $u - v \equiv 0 \pmod{9}$ in the first case.

**3.2. Application to Fermat's equation.** — From a solution $(x, y, z)$ of Fermat's equation, we get the three relations (same notations as in Subsection 2.2)

$$(x + y\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{z}_1^p, \quad (y + z\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{x}_1^p, \quad (z + x\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\,\mathfrak{y}_1^p\,, \ \delta \in \{0, 1\}\,.$$

For $p > 3$, the conditions $p \nmid x^2 - y^2$, $p \nmid y^2 - z^2$ in the first and second cases, and the conditions $p \nmid z + x$ in the first case, are satisfied by the choice of the notation (Lemma 2.2). If the order of $\frac{y}{x}$ (resp. of $\frac{z}{y}$) is $\leq 2$, i.e., when $q \,|\, x^2 - y^2$ (resp. $q \,|\, y^2 - z^2$), then we have $M = K$, $\mathfrak{Q} = \mathfrak{q}_K \,|\, q$ in $K$, and $\xi = \pm 1$. Since $\eta_1 = (1 \pm \zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}} = 1$, we get from Theorem 3.3

$$\zeta^{-\frac{1}{2}\,\frac{x-y}{x+y}\,\kappa} = 1 \ \ (\text{resp. } \zeta^{-\frac{1}{2}\,\frac{y-z}{y+z}\,\kappa} = 1)\,.$$

Then these two values of $n$ again give the second theorem of Furtwängler [**Fur**] in the context of FLT for $p > 3$, i.e., when $q \,|\, x^2 - y^2$ (resp. $q \,|\, y^2 - z^2$), we then have $\zeta^\kappa = 1$, hence $\kappa \equiv 0 \pmod p$; see Corollaries 2.15 and 2.16 generalizing the FLT context to the SFLT one.

The same conclusion holds in the first case of FLT under the complementary condition $p \nmid z - x$ when $q \,|\, z^2 - x^2$ (in the second case of FLT this does not work for $(z, x)$ since for the special case $(u = z,\ v = x)$ the symbol is trivial).

***Remark 3.5*** **(Furtwängler's theorems and FLT)**. — (see e.g. [**Gr1**], Appendix or [**Ri**], IX, 3). Let $(x, y, z)$ be a solution of Fermat's equation for $p > 3$, under the conditions of Lemma 2.2.

(i) Recall that the first theorem of Furtwängler, which implies Wieferich's criteria, asserts that for any prime $q \neq p$, if $q \,|\, z$ (resp. $x$, resp. $y$ in the first case), then $\kappa \equiv 0 \pmod p$.

Of course, if $q \,|\, x + y$ (resp. $y + z$, resp. $z + x$ in the first case), then from Subsection 2.1 with obvious notations, $q \,|\, z_0$ (resp. $x_0$, resp. $y_0$ in the first case), and we then have $\kappa \equiv 0 \pmod p$ from the first theorem of Furtwängler. We can call it the *first part* of the second theorem of Furtwängler. We can call *second part* of the second theorem of Furtwängler the statement that if $q \,|\, x - y$ (resp. $y - z$), then $\kappa \equiv 0 \pmod p$.

(ii) If $q \,|\, z$ (resp. $x$, resp. $y$ in the first case) when $q \not\equiv 1 \pmod p$, then from Subsection 2.1, $q \,|\, z_0$ (resp. $x_0$, resp. $y_0$ in the first case). We deduce from this that $q^p \,|\, x + y = z_0^p$ (resp. $y + z = x_0^p$, resp. $z + x = y_0^p$ in the first case). This means, since $q \nmid x\,y$ (resp. $y\,z$, resp. $z\,x$ in the first case), that $\frac{y}{x}$ (resp. $\frac{z}{y}$, resp. $\frac{x}{z}$ in the first case) is of order 2 modulo $q$, which again proves the first part of the second theorem of Furtwängler and that $\kappa \equiv 0 \pmod p$.

Note that the two results above are not independent in the case $q \not\equiv 1 \pmod p$. For some more remarks on Furtwängler's theorems, see [**Que**].

(iii) As a consequence, if we choose $q \not\equiv 1 \pmod p$ such that $\kappa \not\equiv 0 \pmod p$, we then have $q \nmid xyz$ in the first case of FLT, and $q \nmid zx$ in the second case of FLT. Thus, under these assumptions on $q$, the hypothesis $q \nmid xyz$ (in the first case) or $q \nmid zx$ (in the second case) are useless for the development of our method and give effective criteria in practice for the first case (as we shall show in Remark 6.11).

It remains to consider the case when $q$ divides $y$ in the second case (i.e., $p \,|\, y$). When $q \not\equiv 1 \pmod p$ and $q \,|\, y_0$, then $q \,|\, z + x$; we obtain that $q \nmid z\,x$ and $q \,|\, z + x$ but we cannot conclude, except that the root $\xi''$ associated to $\frac{x}{z}$ is $-1$. To eliminate the case $q \,|\, y$ in the second case we must suppose $q$ large enough, a condition which is ineffective.

(iv) In any case of FLT we have the following result (see [**Ri**], IV.3 for the proof): if $q \neq p$ divides $y$ and does not divide $z+x$ then $q \equiv 1 \pmod{p^2}$.

This result is valid (by cyclic permutation of $x$, $y$, $z$) only in the first case of FLT since it may happen that $p$ (in $p^{\nu\, p-1} y_0^p$) is not a $p$th power modulo $q$.

Let $(x, y, z)$ be a solution of Fermat's equation. From Theorem 3.3 and the fact that in the second case for $p = 3$ we have $z + x \equiv 0 \pmod 9$ (special case of SFLT for the solution $(u, v) = (z, x)$ where we know that $u + v \equiv 0 \pmod 9$), we obtain:

***Corollary 3.6***. — *Let $q \neq p$ be a prime such that $q \nmid xyz$. Let $n, n', n''$ be the orders modulo $q$ of $\frac{y}{x}$, $\frac{z}{y}$, $\frac{x}{z}$, respectively, that we assume to be prime to $p$. Let $\xi$, $\xi'$, $\xi'' \in \mathbb{Q}(\mu_{q-1})$, of orders $n$, $n'$, $n''$, and let $\mathfrak{q}$, $\mathfrak{q}'$, $\mathfrak{q}''$ in $L = \mathbb{Q}(\mu_n)$, $L' = \mathbb{Q}(\mu_{n'})$, $L'' = \mathbb{Q}(\mu_{n''})$, constructed from $\frac{y}{x}$, $\frac{z}{y}$, $\frac{x}{z}$, respectively, according to Definition 3.1 (i).*
*Consider the corresponding $\omega$-cyclotomic units $\eta_1$, $\eta_1'$, $\eta_1''$ (Definition 3.2).*

*Then we have:*

*(i) First case of FLT, $p > 3$:* $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \zeta^{-\frac{1}{2}\frac{x-y}{x+y}\kappa}$, $\left(\frac{\eta_1'}{\mathfrak{Q}'}\right)_{M'} = \zeta^{-\frac{1}{2}\frac{y-z}{y+z}\kappa}$, $\left(\frac{\eta_1''}{\mathfrak{Q}''}\right)_{M''} = \zeta^{-\frac{1}{2}\frac{z-x}{z+x}\kappa}$, *with $x - y \not\equiv 0$ and $y - z \not\equiv 0 \pmod p$.*

*(ii) First case of FLT, $p = 3$:* $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \left(\frac{\eta_1'}{\mathfrak{Q}'}\right)_{M'} = \left(\frac{\eta_1''}{\mathfrak{Q}''}\right)_{M''} = 1$.

*(iii) Second case of FLT, $p \geq 3$:* $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \zeta^{-\frac{1}{2}\kappa}$, $\left(\frac{\eta_1'}{\mathfrak{Q}'}\right)_{M'} = \zeta^{\frac{1}{2}\kappa}$, $\left(\frac{\eta_1''}{\mathfrak{Q}''}\right)_{M''} = 1$.

***Remark 3.7***. — (i) Suppose that we are in the first case of FLT for $p > 3$; let $q \neq p$ be a prime such that $\kappa \not\equiv 0 \pmod p$, and let $n$ and $n'$ be the orders of $\frac{y}{x}$ and $\frac{z}{y}$ modulo $q$. Assume moreover that $p \nmid n\, n'$; we observe that we have $n, n' > 2$ by the second theorem of Furtwängler, and that $q \nmid xyz$ by Remark 3.5 (i) on the first theorem of Furtwängler.

If we find, for independent reasons, that at least one of the symbols $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M$ or $\left(\frac{\eta_1'}{\mathfrak{Q}'}\right)_{M'}$ is trivial, we get a contradiction (cf. Corollary 3.6 (i)). However reasoning on the third symbol does not work since $z - x$ can be divisible by $p$.

(ii) For $p = 3$ in the first case, all the right hand sides are trivial and a contradiction arises as soon as an independent fact implies that one of these symbols is nontrivial (cf. Corollary 3.6 (ii)).

(iii) In the second case for $p \geq 3$, when $\kappa \not\equiv 0 \pmod p$, we know that $q \nmid xz$. Since $p \nmid n\, n'$, we also have $p \nmid n''$. The symbol $\left(\frac{\eta_1''}{\mathfrak{Q}''}\right)_{M''}$ is trivial (cf. Corollary 3.6 (iii)), thus a contradiction arises otherwise.

To carry out, with the other two nontrivial symbols associated to $\xi$ and $\xi'$, arguments similar to those we used in the first case, we need the condition $q \nmid y$, and therefore we must suppose $q$ large enough. In practice, to get a contradiction, we need the existence of infinitely many $q$ (with $\kappa \not\equiv 0 \pmod p$) such that at least one of the symbols $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M$, $\left(\frac{\eta_1'}{\mathfrak{Q}'}\right)_{M'}$ is trivial.

(iv) If $\kappa \equiv 0 \pmod p$, in any case all the symbols are trivial in Corollary 3.6. Thus to obtain a contradiction, we need to find nontrivial symbols in an independent way for infinitely many such $q$.

(v) We can use the above remarks to give the following reciprocal statements; for the sake of simplicity we restrict ourselves to $p > 3$. Suppose that every solution $(x, y, z)$ of Fermat's equation satisfies the conventions of Lemma 2.2.

Let $\xi$ be a primitive $n$th root of unity with $p \nmid n$, $\eta_1 := (1+\xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}$, and let $q \equiv 1 \pmod n$ be a prime. Consider an *arbitrary* fixed ideal $\mathfrak{q} \,|\, q$ in $L := \mathbb{Q}(\mu_n)$, then any $\mathfrak{Q} \,|\, \mathfrak{q}$ in $M := LK$. We suppose that we are given coprime integers $u$, $v$, such that $q \nmid u\,v$ and $\frac{v}{u} \equiv \xi \pmod{\mathfrak{q}}$.

- If $\kappa \not\equiv 0 \pmod p$ and $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = 1$, then we have:

*If $u + v \not\equiv 0 \pmod p$, $(u, v)$ cannot be a part of a solution $(x, y, z) = (u, v, z)$, $(v, u, z)$, $(x, v, u)$, or $(x, u, v)$ of Fermat's equation.*

- If $\kappa \not\equiv 0 \pmod p$ and $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M \neq 1$, then we have:

*If $u + v \equiv 0 \pmod p$, $(u, v)$ cannot be a part of a solution $(x, y, z) = (u, y, v)$ or $(v, y, u)$ of the second case of Fermat's equation.*

- If $\kappa \equiv 0 \pmod p$ and $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M \neq 1$, then we have:

*The pair $(u, v)$ cannot be a part of a solution $(x, y, z)$ of any case of Fermat's equation.*

***Proposition 3.8.*** — *Let $(x, y, z)$ be a solution of Fermat's equation. Let $q \nmid xyz$ be a prime such that the orders $n$, $n'$, $n''$ modulo $q$ of $\frac{y}{x}$, $\frac{z}{y}$, $\frac{x}{z}$, respectively, are prime to $p$. Write $q =: 1 + d\,p^r$, with $r \geq 0$ and $p \nmid d$, and let $\widetilde{L} := \mathbb{Q}(\mu_d)$. Let moreover $\xi$, $\xi'$, $\xi''$, of orders $n$, $n'$, $n''$, defining the fields $L$, $L'$, $L''$, respectively.*
*Then there exist a prime ideal $\widetilde{\mathfrak{q}} \,|\, q$ in $\widetilde{L}$ and $t'$, $t'' \in \mathrm{Gal}(\widetilde{L}/\mathbb{Q})$ such that the two following congruences hold:*
*(i) $\xi'^{t'} \equiv -1 - \frac{1}{\xi} \pmod{\widetilde{\mathfrak{q}}}$;*
*(ii) $\xi''^{t''} \equiv \frac{-1}{\xi+1} \pmod{\widetilde{\mathfrak{q}}}$.*

*Proof.* — Since $L$, $L'$, $L''$ are subfields of $\widetilde{L}$, taking prime ideals $\widetilde{\mathfrak{q}}_0$, $\widetilde{\mathfrak{q}}'_0$, $\widetilde{\mathfrak{q}}''_0$ of $\widetilde{L}$ lying above the prime ideals $\mathfrak{q}_{\frac{y}{x},\xi}$, $\mathfrak{q}_{\frac{z}{y},\xi'}$, $\mathfrak{q}_{\frac{x}{z},\xi''}$, respectively, we have

$$\xi \equiv \tfrac{y}{x} \pmod{\widetilde{\mathfrak{q}}_0}, \quad \xi' \equiv \tfrac{z}{y} \pmod{\widetilde{\mathfrak{q}}'_0}, \quad \xi'' \equiv \tfrac{x}{z} \pmod{\widetilde{\mathfrak{q}}''_0}.$$

The ideals $\widetilde{\mathfrak{q}}'_0$ and $\widetilde{\mathfrak{q}}''_0$ are conjugate to $\widetilde{\mathfrak{q}}_0$, so that there exist $t'$, $t'' \in \mathrm{Gal}(\widetilde{L}/\mathbb{Q})$ such that

$$\xi \equiv \tfrac{y}{x},\ \xi'^{\,t'} \equiv \tfrac{z}{y},\ \xi''^{t''} \equiv \tfrac{x}{z} \pmod{\widetilde{\mathfrak{q}}_0}.$$

Writing $x^p + y^p + z^p = 0$ as $\left(\frac{x}{y}\right)^p + \left(\frac{z}{y}\right)^p = -1$, we obtain $\xi^{-p} + (\xi'^{t'})^p \equiv -1 \pmod{\widetilde{\mathfrak{q}}_0}$.

Since $p \nmid d$, we can use the inverse of the Frobenius automorphism $t_p$ of $p$ in $\widetilde{L}/\mathbb{Q}$ for which $\xi^{t_p} = \xi^p$, which easily leads to the relation (i) (for $\widetilde{\mathfrak{q}} := t_p^{-1}(\widetilde{\mathfrak{q}}_0)$).

From the obvious relation $\xi''^{\,t''}\xi'^{t'}\xi \equiv 1 \pmod{\widetilde{\mathfrak{q}}_0}$, which implies the equality $\xi''^{t''}\xi'^{t'}\xi = 1$, we proves (ii) since $\xi \neq -1$ (indeed, $\xi = -1$ means $x + y = z_0^p \equiv 0 \pmod q$, i.e., $q \,|\, z$, which is excluded; similarly, $\xi' \neq -1$ and $\xi'' \neq -1$). ☐

***Corollary 3.9.*** — *Let $m = \mathrm{l.c.m.}\,(n', n'')$. If $m > 3$ we have $\phi(m) > \frac{\log(q)}{\log(3)}$, where $\phi$ is the Euler totient function.*

*Proof.* — We have $\xi''^{\,t''} + \xi'^{-t'} + 1 \equiv 0 \pmod{\widetilde{\mathfrak{q}}}$; hence, since $\xi''^{\,t''} + \xi'^{-t'} + 1 \in \mathbb{Q}(\mu_m)$ by definition of $m$, we get $\mathrm{N}_{\mathbb{Q}(\mu_m)/\mathbb{Q}}(\xi''^{t''} + \xi'^{-t'} + 1) = q\,N$, $N \geq 1$ (the case when $N = 0$ is equivalent to $\xi = \xi'^{t'} = \xi''^{t''} \in \{j, j^2\}$ and implies $m = 3$).
Since $\mathrm{N}_{\mathbb{Q}(\mu_m)/\mathbb{Q}}(\xi''^{t''} + \xi'^{-t'} + 1) < 3^{\phi(m)}$, we get $N < \frac{1}{q}\,3^{\phi(m)}$, which proves the corollary.
The same results hold for $m' = \mathrm{l.c.m.}\,(n, n'')$ and $m'' = \mathrm{l.c.m.}\,(n, n')$. □

***Corollary 3.10.*** — *We can choose the representative pairs* $(\xi, \mathfrak{q}_{\frac{y}{x},\xi})$, $(\xi', \mathfrak{q}_{\frac{z}{y},\xi'})$, $(\xi'', \mathfrak{q}_{\frac{x}{z},\xi''})$ *of the classes* $\mathcal{C}_{\frac{y}{x}}(q)$, $\mathcal{C}_{\frac{z}{y}}(q)$, $\mathcal{C}_{\frac{x}{z}}(q)$ *in such a way that* $\xi' \equiv -1 - \frac{1}{\xi} \pmod{\widetilde{\mathfrak{q}}}$ *and* $\xi'' \equiv \frac{-1}{\xi+1} \pmod{\widetilde{\mathfrak{q}}}$ *for a suitable* $\widetilde{\mathfrak{q}}$ *of* $\widetilde{L}$ *lying above each of the ideals* $\mathfrak{q}_{\frac{y}{x},\xi}$, $\mathfrak{q}_{\frac{z}{y},\xi'}$, $\mathfrak{q}_{\frac{x}{z},\xi''}$.
*With such a choice, we have* $\xi\,\xi'\,\xi'' = 1$.

**3.3. Computation of the $\mathbb{F}_p$-dimension of a group of units.** — Since $\eta_1$ is considered as an element of $(E_M/E_M^p)^{e_\omega}$, it is necessary to make precise the $\mathbb{F}_p$-dimension of this group. The computation is the same for any odd character $\chi$.

***Proposition 3.11.*** — *Let* $M = LK$, *where* $L = \mathbb{Q}(\mu_n)$ $(n > 2,\ p \nmid n)$ *and* $K = \mathbb{Q}(\mu_p)$, $p > 2$. *Let* $E_M$ *be the group of units of* $M$ *and let* $\chi = \omega^k$ *be an odd character of* $\mathrm{Gal}(M/L) \simeq g$. *Then the* $\mathbb{F}_p$*-dimension of* $(E_M/E_M^p\,.\,\mu_p)^{e_\chi}$ *is equal to* $\frac{1}{2}\,[L : \mathbb{Q}] = \frac{1}{2}\,\phi(n)$.

*Proof.* — Set $\Gamma := \mathrm{Gal}(M/\mathbb{Q}) = G \oplus H$ where $G := \mathrm{Gal}(M/L)$ and $H := \mathrm{Gal}(M/K)$. Let $\widehat{\Gamma} = \widehat{G} \oplus \widehat{H}$ be the group of irreducible characters of $\Gamma$; for any $\psi \in \widehat{\Gamma}$, let $\mathcal{E}_\psi$ be the idempotent

$$\mathcal{E}_\psi := \frac{1}{|\,\Gamma\,|} \sum_{\sigma \in \Gamma} \psi^{-1}(\sigma)\,\sigma \in \mathbb{C}_p[\Gamma]\,.$$

If $\psi = \omega^i \cdot \theta$, $\ \omega^i \in \widehat{G}$, $1 \leq i \leq p-1$, $\theta \in \widehat{H}$, then $\mathcal{E}_\psi = \mathcal{E}_{\omega^i} \cdot \mathcal{E}_\theta$.
From the Dirichlet–Herbrand theorem on units (see e.g. **[Gr2]**, I.3.7) we know that the $p$-adic representation $\mathbb{C}_p \oplus (\mathbb{C}_p \otimes_{\mathbb{Z}} E_M)$ is given by the representation of permutation

$$\mathbb{C}_p[\Gamma]\,\frac{1}{2}(1 + c) = \bigoplus_{\psi\ \text{even}} \mathbb{C}_p[\Gamma]\,\mathcal{E}_\psi\,.$$

Then, since the character $\chi$ is odd, $(\mathbb{C}_p \oplus (\mathbb{C}_p \otimes_{\mathbb{Z}} E_M))^{\mathcal{E}_\chi} = \big(\mathbb{C}_p \otimes_{\mathbb{Z}} E_M\big)^{\mathcal{E}_\chi}$ is the representation $\bigoplus_{\psi\ \text{even}} \mathbb{C}_p[\Gamma]\,\mathcal{E}_\psi\ \cdot\ \mathcal{E}_\chi$.
Put $\psi = \omega^i \cdot \theta$; then $\mathcal{E}_\psi = \mathcal{E}_{\omega^i} \cdot \mathcal{E}_\theta$ and $\mathcal{E}_\psi \cdot \mathcal{E}_\chi = 0$ except if $i = k$. In the direct sum above, $\psi$ runs through the products $\chi\,\theta$, with $\theta$ odd since $\psi$ must be even. Then we have

$$\big(\mathbb{C}_p \otimes_{\mathbb{Z}} E_M\big)^{\mathcal{E}_\chi} \simeq \bigoplus_{\theta \in \widehat{H},\,\text{odd}} \mathbb{C}_p[\Gamma]\,\mathcal{E}_{\chi.\,\theta}\,,$$

which shows that the $\mathbb{C}_p$-dimension of $\big(\mathbb{C}_p \otimes_{\mathbb{Z}} E_M\big)^{\mathcal{E}_\chi}$ is equal to $\frac{1}{2}[L : \mathbb{Q}]$.
This completes the proof of the proposition since $\mathcal{E}_\chi \equiv e_\chi \pmod{p\,\mathbb{Z}_p[g]}$. □

In particular, we observe that the $\mathbb{F}_p$-dimension of $(E_M/E_M^p\ \cdot\ \mu_p)^{e_\omega}$ is equal to $\frac{1}{2}[L : \mathbb{Q}]$, thus that the subgroup of $(E_M/E_M^p\ \cdot\ \mu_p)^{e_\omega}$ generated by the images of the units $\eta_1^t$, $t \in \mathrm{Gal}(M/K)/\langle\, t_{-1}\,\rangle$, is of $\mathbb{F}_p$-dimension less than or equal to $\frac{1}{2}[L : \mathbb{Q}] = \frac{1}{2}\,\phi(n)$.

## 4. The $\omega$-cyclotomic units $\eta_1$ – The extensions $F_\xi/L$, $H_L/L$, and $F_n/L$

In this section we use some classical elements of Kummer theory with base field $M$ and of the decomposition of a Kummer extension over a subfield of $M$; then, we interpret the previous results in terms of Abelian $p$-ramification over the fields $\mathbb{Q}(\mu_n)$.

**4.1. The $\omega$-cyclotomic unit $\eta_1$ and the extension $M(\sqrt[p]{\eta_1})/M$.** — We consider, independently of any solution of the SFLT equation, the cyclotomic number

$$\eta := (1 + \xi\,\zeta)\,\zeta^{-\frac{1}{2}}\,,$$

where $\xi$ is a primitive $n$th root of unity with $p \nmid n$, and the $\omega$-cyclotomic unit $\eta_1 := \eta^{e_\omega}$. We have $\eta_1 \in M := LK$, where $L = \mathbb{Q}(\mu_n)$, and $\eta_1$ is real (see Definition 3.2). We exclude the cases $n \leq 2$ for which $\eta_1 \in K^{\times p}$.

***Lemma 4.1.*** — *For any $n > 2$, the extension $M(\sqrt[p]{\eta_1})/M$ is $p$-ramified, cyclic of degree $p$.*

*Proof.* — Since $\eta_1$ is a unit, the extension $M(\sqrt[p]{\eta_1})/M$ is $p$-ramified (i.e., unramified outside $p$). Put $\pi = \zeta - 1$; since $\mathfrak{p}$ is not ramified in $M/K$, $\pi$ is still an uniformizing parameter at $p$ in $M$. We have $\eta \equiv 1 + \xi + \frac{1}{2}\,(\xi - 1)\,\pi\,(\mathrm{mod}\ \pi^2)$ giving, by the usual computation,

$$\eta_1 := \eta^{e_\omega} \equiv 1 + \frac{1}{2}\,\frac{\xi-1}{\xi+1}\,\pi \pmod{\pi^2}\,;$$

since $n > 2$, $\dfrac{\xi-1}{\xi+1}$ is a local unit at $p$, showing that $\eta_1$ is not $p$-primary. Thus in particular, the extension $M(\sqrt[p]{\eta_1})/M$ is cyclic of degree $p$. □

Kummer theory shows that the conductor of $M(\sqrt[p]{\eta_1})/M$ is the modulus $\mathfrak{p}^p$ extended to $M$ (see **[Gr2]**, II.1.6.3). In some sense, $M(\sqrt[p]{\eta_1})/M$ is maximally wildly $p$-ramified and has the same conductor as $M(\sqrt[p]{\zeta})/M$.

***Remark 4.2.*** — This extension does not depend on the choice of $\zeta$ since we have, for any $k$ prime to $p$,

$$\big((1 + \xi\,\zeta^k)\,(\zeta^k)^{-\frac{1}{2}}\big)^{e_\omega} = \big((1 + \xi\,\zeta)\,\zeta^{-\frac{1}{2}}\big)^{s_k\,e_\omega} \sim \big((1 + \xi\,\zeta)\,\zeta^{-\frac{1}{2}}\big)^{k\,e_\omega} = \eta_1^k$$

from the relation $s_k\,e_\omega \equiv k\,e_\omega \pmod{p\,\mathbb{Z}[g]}$, giving the same radical.

**4.2. The Abelian extension $F_\xi/L$.** — By definition of the character $\omega$, whose reflect is $\omega^* = \chi_0$ (the unit character), the extension $M(\sqrt[p]{\eta_1})/M$ is splitted over $L = \mathbb{Q}(\mu_n)$ by means of a cyclic $p$-ramified extension $F_\xi$, of degree $p$ over $L$ (i.e., $F_\xi M = M(\sqrt[p]{\eta_1})$).

This extension only depends on $\xi$ of order $n$. The family $(F_{\xi'})_{\xi' \text{ of order } n}$ is canonical.

Since $\eta_1$ is real, $\eta_1 = (1 + \xi^{-1}\,\zeta^{-1})^{e_\omega}\,\zeta^{\frac{1}{2}}$ which defines the same extension as $(1 + \xi^{-1}\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}$ as we have seen in Remark 4.2. Then we get $F_\xi = F_{\xi^{-1}}$.

In the cases $n \leq 2$, we have $L = \mathbb{Q}$, $\eta_1 \in K^{\times p}$, and $F_{\pm 1} = \mathbb{Q}$ (hence $F_1 = F_2 = \mathbb{Q}$).

For any $t \in \mathrm{Gal}(L/\mathbb{Q})$ we have the relation $F_{\xi^t} = t\,.\,F_\xi$, where by abuse of notation $t\,.\,F_\xi$ means $t'.\,F_\xi$ for any $\mathbb{Q}$-automorphism $t'$ of $F_\xi$ extending $t$; indeed, we have in the same way $t'(\sqrt[p]{\eta_1}) = \sqrt[p]{\eta_1^t}$ (up to a $p$th root of unity) where $\eta_1^t = (1+\xi^t\,\zeta)^{e_\omega}\,\zeta^{-\frac{t}{2}}$.[7]

Suppose now that we have chosen a prime $q$ such that $q \equiv 1 \pmod n$, $p \nmid n$, and let $\mathfrak{q}$ be a prime ideal lying above $q$ in $L$; later, we shall have $\mathfrak{q} = \mathfrak{q}_{\frac{v}{u},\xi}$ when $\xi$ is associated to the usual integers $u$, $v$, but in this subsection $\mathfrak{q}$ is arbitrary.

Consider the symbol $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M$ which is independent of the choice of $\mathfrak{Q}\,|\,\mathfrak{q}$ in $M$; this symbol is trivial if and only if the image of $\eta_1$ in the multiplicative group of the residue field $Z_M/\mathfrak{Q} \simeq \mathbb{F}_{q^f}$ is a $p$th power, thus if and only if $\mathfrak{Q}$ splits in $M(\sqrt[p]{\eta_1})/M$ (Hensel's Lemma) which is equivalent to the splitting of $\mathfrak{q}$ in $F_\xi/L$ (see Subsection 5.4 for an explicit computation).

**4.3. Class field theory and $p$-ramification.** — In this subsection we recall some class field theory results concerning the Abelian $p$-ramification over $L$.

Let $H_L$ be the maximal Abelian $p$-ramified $p$-extension of $L := \mathbb{Q}(\mu_n)$ in the case $n > 2$, $p \nmid n$ (so that $L$ is an imaginary cyclotomic field of even degree, unramified at $p$); $H_L$ contains all the extensions $F_{\xi'}$, $\xi'$ of order $n$, the cyclotomic $\mathbb{Z}_p$-extension $L_\infty = L\mathbb{Q}_\infty$ of $L$ which is Abelian over $\mathbb{Q}$, and $\frac{1}{2}[L:\mathbb{Q}]$ other independent $\mathbb{Z}_p$-extensions of $L$.

Since $q$ totally splits in $L/\mathbb{Q}$, the decomposition field of $q$ in $L_\infty/\mathbb{Q}$ is $L_e := L\,\mathbb{Q}_e$, where $\mathbb{Q}_e \subset \mathbb{Q}_\infty$ is the unique subfield of degree $p^e$ over $\mathbb{Q}$ such that $q^f =: 1 + p^{e+1}d$, $e \geq 0$, $p \nmid d$. For instance, $L_1 = L\mathbb{Q}_1$ where $\mathbb{Q}_1$ is the cyclic subextension of degree $p$ of $\mathbb{Q}(\mu_{p^2})$.

Note that $e = 0$ is equivalent to $\kappa \not\equiv 0 \pmod p$ (Definition 2.13 (i)).

Let $H_{L[p]} \subseteq H_L$ be the maximal $p$-elementary $p$-ramified extension of $L$. We consider its Galois group as a vector space over $\mathbb{F}_p$. Its dimension is given by the following Šafarevič formula (see e.g. **[Gr2]**, II.5.4.1 (ii)):

$$\dim_{\mathbb{F}_p}(\mathrm{Gal}(H_{L[p]}/L)) = \dim_{\mathbb{F}_p}(V_L/L^{\times p}) + \tfrac{1}{2}[L:\mathbb{Q}] + 1\,,$$

where $V_L$ is the group of pseudo-units of $L$ (i.e., elements $\alpha \in L$ such that $(\alpha)$ is the $p$th power of an ideal) which are local $p$th powers at each place dividing $p$ in $L$.

***Lemma 4.3.*** — *The conductor of $H_{L[p]}/L$ is equal to the modulus $(p^2)$ of $L$.*

*Proof.* — From Hensel's Lemma, since $p > 2$ is not ramified in $L/\mathbb{Q}$ ($p \nmid n$ by assumption), the modulus $(p^2)$ is sufficient for any $\alpha \in L^\times$, $\alpha \equiv 1 \pmod{p^2}$, to be locally a $p$th power, hence a local norm, at each place dividing $p$ in $L$ (use **[Gr2]**, II (c) for the computation of these local conductors). It is also necessary since the ramification is tame. □

Thus $H_{L[p]}$ is contained in the ray class field $L_{(p^2)}$ and this yields

$$\mathrm{Gal}(H_{L[p]}/L) \simeq I/I^p\,R\,,$$

where $I$ is the group of fractional ideals of $L$, prime to $p$, and $R$ is the ray group modulo $p^2$, i.e., $\{(\alpha) \in I,\ \alpha \equiv 1 \pmod{p^2}\}$.

(7) We use the same notations for the elements of the Galois groups $\mathrm{Gal}(M/K)$ and $\mathrm{Gal}(L/\mathbb{Q})$, then for $G = \mathrm{Gal}(M/L)$ and $g = \mathrm{Gal}(K/\mathbb{Q})$, and similarly for $\mathrm{Gal}(M(\sqrt[p]{\eta_1})/M)$ and $\mathrm{Gal}(F_\xi/L)$.

**4.4. The extension $F_n/L$.** — For $n > 2$, we can consider the biquadratic extension $M/L^+K^+$; then $M^+$ is the subfield of $M$ of relative degree 2, distinct from $LK^+$ and from $L^+K$. Let $t_{-1}$ be the element of order 2 of $\mathrm{Gal}(M/L^+K)$ and $s_{-1} \in G$ be the element of order 2 of $\mathrm{Gal}(M/LK^+)$. The complex conjugation in $M$ is $c = s_{-1}\, t_{-1}$ as generator of $\mathrm{Gal}(M/M^+)$. Since we have the relations $\eta_1^c = \eta_1$, $\eta_1^{s_{-1}} = \eta^{e_\omega \cdot s_{-1}} = \eta_1^{-1}$, giving the relation $\eta_1^{t_{-1}} = \eta_1^{-1}$, we deduce that

$$\mathrm{Gal}(M(\sqrt[p]{\eta_1})/L^+K) \simeq \mathrm{Gal}(F_\xi/L^+) \simeq D_{2p}\,,$$

the diedral group of order $2p$. [8]

In other words, $\mathrm{Gal}(L/L^+) = \langle\, t_{-1}\,\rangle = \{1, t_{-1}\}$ acts on $\mathrm{Gal}(F_\xi/L)$ by $\sigma^{t_{-1}} := t'_{-1} \cdot \sigma \cdot t'_{-1} = \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(F_\xi/L)$ and any extension $t'_{-1}$ of $t_{-1}$ in $\mathrm{Gal}(F_\xi/L^+)$.

It will be necessary to consider the compositum of the extensions $M(\sqrt[p]{\eta_1})$ when $\xi$ of order $n$ defining $\eta_1$ varies. Indeed, in the situation of a nontrivial solution $(u, v)$ of the SFLT equation, for $q \nmid uv$ such that $\frac{v}{u}$ is of order $n$ modulo $q$, the root $\xi$ such that $\xi \equiv \frac{v}{u} \pmod{\mathfrak{q}}$ for fixed $\mathfrak{q} \,|\, q$ (i.e., the class $\mathcal{C}_{\frac{v}{u}}(q)$), is ineffective and the properties of all the possible symbols $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M$ can be studied in this extension.

Let $F_n$ be the compositum of the corresponding extensions $F_{\xi'}$, $\xi'$ of order $n$, so that $F_n$ is also the compositum of the $F_{\xi^t}$, $t \in \mathrm{Gal}(M/K)$, for fixed $\xi$; since $\eta_1^{t_{-1}} = \eta_1^{-1}$ (or $F_\xi = F_{\xi^{-1}}$), we can consider the $\eta_1^t$ with $t$ modulo $\langle\, t_{-1}\,\rangle$. We have the equality $F_nM = M\big(\sqrt[p]{\langle\, \eta_1^t\,\rangle_{t \bmod <t_{-1}>}}\,\big)$.

Then as above $\mathrm{Gal}(L/L^+)$ acts on $\mathrm{Gal}(F_n/L)$ by $\sigma^{t_{-1}} = \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(F_n/L)$, hence by $\sigma^{\frac{1}{2}(1+t_{-1})} = 1$ for all $\sigma \in \mathrm{Gal}(F_n/L)$, using the group algebra $\mathbb{F}_p[\mathrm{Gal}(L/L^+)]$ (this will be useful in Subsection 4.5).

***Lemma 4.4.*** — *The Galois closure of $F_\xi$ over $\mathbb{Q}$ is $F_n$ which is linearly disjoint from $L_\infty/L$.*

*Proof.* — Over the field $K$, the Galois closure of $M(\sqrt[p]{\eta_1})$ is given by the Kummer radical $\langle\, \eta_1^t\,\rangle_{t \bmod <t_{-1}>}$ with $\eta_1^t = (1 + \xi^t\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}$, giving the first part of the lemma.

The relation $L_1 \subseteq F_n$ should be equivalent to $M(\sqrt[p]{\zeta}\,) \subseteq M\big(\sqrt[p]{\langle\, \eta_1^t\,\rangle_{t \bmod <t_{-1}>}}\,\big)$, then to the existence of a relation of the form $\displaystyle\prod_{t \bmod <t_{-1}>} (\eta_1^t)^{\lambda_t} = \zeta\,\mu^p$, $\lambda_t \in \mathbb{Z}$, $\mu \in M^\times$; but since the left member is real, the use of the complex conjugation implies $\zeta^2 \in M^{\times p}$, which is absurd. □

***Remark 4.5.*** — The $\mathbb{F}_p$-dimension of the above radical depends on the group of relations $\displaystyle\prod_{t \bmod <t_{-1}>} (\eta_1^t)^{\lambda_t} \in M^{\times p}$; this yields (see Subsection 4.1)

$$\prod_{t \bmod <t_{-1}>} \Big(1 + \frac{1}{2}\frac{\xi^t - 1}{\xi^t + 1}\,\pi\Big)^{\lambda_t e_\omega} \equiv 1 + \Big(\sum_{t \bmod <t_{-1}>} \lambda_t\,\frac{1}{2}\frac{\xi^t - 1}{\xi^t + 1}\Big)\,\pi \pmod{\pi^2}\,.$$

[8] Let $A := \mathrm{Gal}(M/L^+) = G \oplus \langle\, t_{-1}\,\rangle$. Let $\chi_1$ be the character of $A$ defined by $\chi_1(s) = 1$ for all $s \in G$ and $\chi_1(t_{-1}) = -1$. Put $\chi = \omega\,\chi_1$; is is easy to see that $\chi$ is the character of the radical $\langle\, \eta_1\,\rangle\, M^{\times p}/M^{\times p}$ as $A$-module, since $\eta_1 = \eta^{e_\omega}$ and $\eta_1^{t_{-1}} = \eta_1^{-1}$. From Kummer's duality, the character of $\mathrm{Gal}(M(\sqrt[p]{\eta_1})/M)$ is $\chi^* := \omega\,\chi^{-1} = \chi_1$ proving that $\mathrm{Gal}(M(\sqrt[p]{\eta_1})/L^+) \simeq G \times \mathrm{Gal}(F_\xi/L^+)$, with $\mathrm{Gal}(F_\xi/L^+) \simeq D_{2p}$.
We also have $\mathrm{Gal}(M(\sqrt[p]{\eta_1})/M^+) \simeq D_{2p}$.

Thus if the numbers $\dfrac{\xi^t - 1}{\xi^t + 1}$, $t \bmod \langle\, t_{-1}\, \rangle$, are linearly independent modulo $p$, we get the dimension $\frac{1}{2}[L:\mathbb{Q}]$ and $\dim_{\mathbb{F}_p}(\mathrm{Gal}(F_n/L)) = \frac{1}{2}[L:\mathbb{Q}] = \frac{1}{2}\phi(n)$.

Since $\eta_1$ is a cyclotomic unit of $M$, the classical study of the whole group of cyclotomic units of $M$ may give the exact $\mathbb{F}_p$-dimension of the radical (see [**Wa1**], Chap. 8); but this study depends, in a complicate manner, on the Galois group of $M/\mathbb{Q}$ and the law of decomposition of the prime divisors of $n$ in this extension (see Section 7 for an overview).

**4.5. Canonical decomposition of** $\mathrm{Gal}(H_L[p]/L)$**.** — For $L := \mathbb{Q}(\mu_n)$, $n > 2$, consider the finite Galois group $C_L := \mathrm{Gal}(H_L[p]/L)$ as a module over $\mathbb{F}_p[\mathrm{Gal}(L/L^+)]$. Write

$$C_L = C_L^+ \oplus C_L^-, \ \text{ with } \ C_L^+ := C_L^{\frac{1}{2}(1+t_{-1})}, \ \ C_L^- := C_L^{\frac{1}{2}(1-t_{-1})}.$$

We denote by $H_L^-[p]$ the subfield of $H_L[p]$ fixed by $C_L^+$ and by $H_L^+[p]$ the subfield of $H_L[p]$ fixed by $C_L^-$. We then have $F_n \subseteq H_L^-[p]$, $L_1 \subseteq H_L^+[p]$ (see Subsection 4.4), and the diagram:

$$\begin{tikzcd} H_L^+[p] \arrow[r, dash, "C_L^-"] & H_L[p] \arrow[d, dash, "C_L^+"] \\ L \arrow[u, dash] \arrow[r, dash] & H_L^-[p] \end{tikzcd}$$

***Lemma 4.6.*** — *Put* $\overline{V}_L := V_L/L^{\times p}$ *(see Subsection 4.3) and* $\overline{V}_L = \overline{V}_L^+ \oplus \overline{V}_L^-$ *as above. Then* $\overline{V}_L^+ \simeq V_{L^+}/(L^+)^{\times p}$ *giving*

$$\dim_{\mathbb{F}_p}(C_L^+) = \dim_{\mathbb{F}_p}(\overline{V}_L^+) + 1; \ \ \dim_{\mathbb{F}_p}(C_L^-) = \dim_{\mathbb{F}_p}(\overline{V}_L^-) + \tfrac{1}{2}[L:\mathbb{Q}]\,.$$

*Proof.* — Since $p \neq 2$, we have $C_L^+ \simeq \mathrm{Gal}(H_{L^+}[p]/L^+)$ for which the Šafarevič formula is $\dim_{\mathbb{F}_p}(C_L^+) = \dim_{\mathbb{F}_p}(\overline{V}_L^+) + 1$, proving the lemma. □

When the order of the group $C_L^-$ is minimal (which is equivalent to $\dim_{\mathbb{F}_p}(\overline{V}_L^-) = 0$) then $F_n = H_L^-[p]$ if and only if the $\eta_1^t$, $t \in \mathrm{Gal}(M/K)/\langle\, t_{-1}\, \rangle$, are independent in $M^\times/M^{\times p}$.

***Remark 4.7.*** — The group of pseudo-units $Y_L := \big\{\alpha \in L^\times,\ (\alpha) = \mathfrak{a}^p\big\}$, containing $V_L$, is elucidated by the following obvious exact sequence

$$1 \longrightarrow \overline{E}_L \longrightarrow \overline{Y}_L \longrightarrow {}_p\mathcal{C}\ell_L \longrightarrow 1\,,$$

where $\mathcal{C}\ell_L$ is the $p$-class group of $L$, ${}_p\mathcal{C}\ell_L$ the subgroup of $\mathcal{C}\ell_L$ of classes killed by $p$, $\overline{Y}_L := Y_L/L^{\times p}$, $E_L$ is the group of units of $L$, and $\overline{E}_L = E_L/E_L \cap L^{\times p} \simeq E_L/E_L^p$.

For $L^+$ we get the analogous exact sequence

$$1 \longrightarrow \overline{E}_{L^+} \longrightarrow \overline{Y}_{L^+} \longrightarrow {}_p\mathcal{C}\ell_{L^+} \longrightarrow 1\,.$$

We have, with the usual notations $\pm$, the relations $\overline{E}_L^+ \simeq \overline{E}_{L^+}$ and $\overline{E}_L^- = 1$, so that $\overline{Y}_L^- \simeq {}_p\mathcal{C}\ell_L^-$ and $\overline{V}_L^- \subseteq \overline{Y}_L^-$ only depends on the minus part of the $p$-class group of $L$ and is often trivial.

The group $\overline{V}_L^+ \simeq \overline{V}_{L^+} \subseteq \overline{Y}_{L^+}$ depends on the $p$-class group of $L^+$ (in general trivial) and more essentially on the subgroup of units of $L^+$ locally $p$th power at $p$; but $\varepsilon \in E_{L^+}$ is a local

$p$th power at each place dividing $p$ if and only if $\varepsilon^{p^{f_p}-1} \equiv 1 \pmod{p^2}$, where $f_p \mid \frac{1}{2}\phi(n)$ is the residue degree of $p$ in $L^+$, which is also very rare, giving often a trivial $\overline{V}_L^+$.

***Remark 4.8.*** — Suppose that the group $\overline{V}_L$ is trivial. Then we get $\dim_{\mathbb{F}_p}(C_L^+) = 1$ and $\dim_{\mathbb{F}_p}(C_L^-) = \frac{1}{2}[L:\mathbb{Q}]$. This situation is by definition equivalent to the $p$-rationality of the field $L$ (see e.g. **[Gr2]**, IV.3.5, for some equivalent conditions).

In this case $H_L$ is the compositum of the $\mathbb{Z}_p$-extensions of $L$ which is of the form $H_L^+ H_L^-$ where $H_L^+ = L_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $L$ and $H_L^-$ the compositum of $\frac{1}{2}[L:\mathbb{Q}]$ independent relative $\mathbb{Z}_p$-extensions of $L$ (i.e., which are pro-diedral over $L^+$).

Then $H_{L[p]}$ is the compositum of the first levels of these $\mathbb{Z}_p$-extensions, the extension $H_L^+[p]$ is $L_1$, and $H_L^-[p]\, M$ may be the Kummer extension defined by the radical generated by the $\eta_1^t$, $t$ modulo $\langle\, t_{-1}\,\rangle$, as soon as its $\mathbb{F}_p$-dimension is $\frac{1}{2}[L:\mathbb{Q}]$ (see Proposition 3.11).

***Remark 4.9.*** — It may be useful to introduce the extension $A_n^- \subseteq H_L^-[p]$ of $L$ such that $A_n^- M = M\big(\sqrt[p]{E_M^{+\,e_\omega}}\,\big)$, where $E_M^+ = E_{M^+}$ is the subgroup of real units of $M$; $A_n^-$ contains $F_n$ and is of degree $p^{\frac{1}{2}\,\phi(n)}$ over $L$. Then $A_n := A_n^- L_1$, with $A_n^- \cap L_1 = L$ where $L_1 M = M(\sqrt[p]{\zeta}\,)$, is such that $A_n M = M\big(\sqrt[p]{E_M^{e_\omega}}\big)$ since $E_M = E_M^+ \oplus \langle\, \zeta\,\rangle$. So, $A_n$ allows us to control the values of $\kappa$ as well as the laws of decomposition in $F_n/L$.

**4.6. Case of an odd character $\chi \neq \omega$.** — We now consider an odd character $\chi$ of $g$ distinct from $\omega$. Then $\chi = \omega^k$, $k$ odd, $k \not\equiv 1 \pmod{(p-1)}$, which excludes the case $p = 3$. As in the case where $k = 1$, we can represent modulo $p$ the corresponding idempotent $\mathcal{E}_\chi$ by an element in $\mathbb{Z}[g]$ of the form $e_\chi = (1 - s_{-1})\, e_\chi^\circ$, $e_\chi^\circ \in \mathbb{Z}[g]$ (see Subsection 2.3).

We suppose that the $\chi$-class group of $K$ is trivial (i.e., $\mathcal{C}\ell_L^{\mathcal{E}_\chi} = 1$ ). A necessary and sufficient condition for this assumption to hold is that the Bernoulli number $B_{p-k}$ be prime to $p$ (see e.g. **[Gr1]**, Section 2, for more details). Then for any relation of the form $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\, \mathfrak{w}_1^p$ in coprime integers $u$, $v$ (see Conjecture 2.4), we immediately have

$$(u + v\,\zeta)^{e_\chi} = \mu_\chi^p,\ \ \mu_\chi \in \mathbb{Z}[\zeta]\,,$$

since any $\chi$-unit of $K$ (i.e., of the form $\varepsilon^{e_\chi}$ for a unit $\varepsilon$) is trivial for $\chi$ odd distinct from $\omega$. Moreover $(\zeta - 1)^{e_\chi}$ is a $\chi$-unit, hence trivial.

Lemma 2.17 is valid for the character $\chi$, and the two equations in coprime integers $u, v$:

$$(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\, \mathfrak{w}_1^p \ \text{ and } \ (u + v\,\zeta)^{e_\chi} = \mu_\chi^p \text{ with } \mu_\chi \in K^\times,$$

are equivalent under the assumption that the $\chi$-class group of $K$ is trivial. So they are equivalent to the $\omega$-SFLT equation.

For $\chi \neq \omega$ odd, when the $\chi$-class group of $K$ is trivial, the relation $(u + v\,\zeta)^{e_\chi} = \mu_\chi^p$ may be called the $\chi$-SFLT equation associated to SFLT.

As in the previous subsections, let $q \neq p$ be a prime such that $q \nmid u\,v$ and $\frac{v}{u}$ is of order $n$ modulo $q$, i.e., $q \mid \Phi_n(u,v)$ & $q \equiv 1 \pmod{n}$ (see Lemma 2.11 and Corollary 2.12); we assume $n$ prime to $p$. Let $\xi$ be of order $n$ and let $\mathfrak{q} := \mathfrak{q}_{\frac{v}{u},\xi} \mid q$ in $L = \mathbb{Q}(\mu_n)$.

Let $\eta = (1 + \xi\,\zeta)\,\zeta^{-\frac{1}{2}}$ (see Definition 3.2). Set $\eta_k := \eta^{e_\chi} \in M$, where $M := LK$; then $\eta_k = (1 + \xi\,\zeta)^{e_\chi} \in M^+$, since $\zeta^{e_\chi} = 1$. Thus $\eta_k^{s_{-1}} = \eta_k^{t_{-1}} = \eta_k^{-1}$, and $\eta_k = 1$ when $n \leq 2$.

We deduce the fundamental congruence

$$\eta_k \equiv \big(1 + \tfrac{v}{u}\,\zeta\big)^{e_\chi} = \mu_\chi^p \pmod{\prod_{\mathfrak{Q}\,|\,\mathfrak{q}} \mathfrak{Q}} \ \text{ in } M\,.$$

We then have the relation $\Big(\frac{\eta_k}{\mathfrak{Q}}\Big)_M = 1$, for all $\mathfrak{Q}\,|\,\mathfrak{q}$, so that, in this situation, a contradiction to the existence of a nontrivial solution of the SFLT equation would be that this symbol is nontrivial for some $q$. Here the value of $\kappa$ does not matter.

This criterion may be used for any odd character $\chi \neq \omega$ such that the $\chi$-class group of $K$ is trivial. In some sense this is similar to the case $\kappa \equiv 0 \pmod p$ of the preceding case $\chi = \omega$, the symbols being trivial independently of $q$ (see Remark 3.7 (iv, v)).

By Kummer's duality, the extension $M(\sqrt[p]{\eta_k})/M$ is splitted by a $p$-cyclic extension over the extension $L_{\chi^*} := LK_{\chi^*}$, where $\chi^* = \omega^{1-k}$ and $K_{\chi^*}$ is the subfield of $K$ fixed by the kernel of $\chi^*$; this field $K_{\chi^*}$ is real. Of course, $L_{\chi^*} = L$ if and only if $K_{\chi^*} = \mathbb{Q}$, i.e., $\chi = \omega$.

But unfortunately, the corresponding extensions $M(\sqrt[p]{\eta_k})/L$ are metabelian (non-Abelian) extensions and are not associated with intrinsic arithmetic properties of the field $L$. Meanwhile it is possible, replacing $\mathbb{Q}$ by $K_{\chi^*}$, to work in the Abelian extension $M(\sqrt[p]{\eta_k})/L_{\chi^*}$ which is a compositum of the form $F_{\chi^*,\,\xi}\,.\,M$ where $F_{\chi^*,\,\xi}$ is $p$-ramified cyclic of degree $p$ over $L_{\chi^*}$. Subsection 4.2 was devoted to the case $\chi = \omega$, where $F_{\chi^*,\,\xi} = F_{\chi_0,\,\xi}$ was denoted by $F_\xi$.

This point of view has the following specificities:

(i) In contrast with the case $\chi = \omega$, the base field $K_{\chi^*}$ depends on $p$ and on the choice of $\chi$; moreover it is related to the arithmetic of $K$ and one of our goal was to avoid this aspect.

(ii) Any class field theory interpretation in terms of Frobenius automorphisms will have to do with the Abelian $p$-ramification over the fields $L_{\chi^*} := K_{\chi^*}(\mu_n)$ for which the $\mathbb{F}_p$-dimension of $\mathrm{Gal}(H_{L_{\chi^*}}[p]/L_{\chi^*})$ is not comparable to that of the radical generated by the conjugates of $\eta_k$. Indeed, we easily have (see Subsections 3.3, 4.5)

$$\begin{aligned}
&\dim_{\mathbb{F}_p}\big(\mathrm{Gal}(H^-_{L_{\chi^*}}[p]/L_{\chi^*})\big) \geq \frac{1}{2}\,\phi(n)\,[K_{\chi^*} : \mathbb{Q}],\\
&\dim_{\mathbb{F}_p}\big(\mathrm{Gal}\big(M\big(\sqrt[p]{\langle\, \eta_k^t\,\rangle_{t \bmod <t_{-1}>}}\,\big)/M\big)\big) \leq \frac{1}{2}\,\phi(n)\,.
\end{aligned}$$

So we are obliged to consider a suitable " $\chi^*$-subextension" of $H^-_{L_{\chi^*}}[p]/\mathbb{Q}$ to get compatible dimensions. But this context is still related to the arithmetic of $K$.

In other words, a " philosophical" approach indicates that, by its nature, the SFLT equation is essentially related to the universal base field $\mathbb{Q}$ corresponding to the reflect of the character $\omega$ (i.e., the unit character), hence to the properties of the corresponding extensions $F_\xi/L$.

But clearly, many generalizations of our method are available, with similar techniques.

**4.7. Conclusion.** — We have established, from Corollary 3.6 and Remark 3.7, that, under a solution $(x, y, z)$ of Fermat's equation for $p > 3$, for infinitely many particular primes $q$ in the case $\kappa \not\equiv 0 \pmod p$, using the classes $\mathcal{C}_r(q)$, $\mathcal{C}_{r'}(q)$, $\mathcal{C}_{r''}(q)$ (see Definition 3.1 (ii)), where $r := \frac{y}{x}$, $r' := \frac{z}{y}$, $r'' := \frac{x}{z}$, we get the following: there exist privileged pairs

$$(F_\xi, \mathfrak{q}_{r,\,\xi}),\ \ (F_{\xi'}, \mathfrak{q}_{r',v'}),\ \ (F_{\xi''}, \mathfrak{q}_{r'',\,\xi''})\,,$$

defined up to conjugation, with $p$-cyclic $p$-ramified extensions $F_\xi/L$, $F_{\xi'}/L'$, $F_{\xi''}/L''$ and prime ideals $\mathfrak{q}_{r,\,\xi}$, $\mathfrak{q}_{r',\,\xi'}$, $\mathfrak{q}_{r'',\,\xi''}$ of the subextensions $L = \mathbb{Q}(\xi)$, $L' = \mathbb{Q}(\xi')$, $L'' = \mathbb{Q}(\xi'')$ of $\mathbb{Q}(\mu_{q-1})$, respectively, for which:

(i) in the first case, $\mathfrak{q}_{r,\,\xi}$, $\mathfrak{q}_{r',\,\xi'}$ are inert in $F_\xi/L$, $F_{\xi'}/L'$, respectively,

(ii) in the second case, $\mathfrak{q}_{r,\,\xi}$, $\mathfrak{q}_{r',\,\xi'}$ are inert in $F_\xi/L$, $F_{\xi'}/L'$, $\mathfrak{q}_{r'',\,\xi''}$ splits in $F_{\xi''}/L''$, respectively.

In the case $\kappa \equiv 0 \pmod p$, for all the above pairs, the ideals split in the corresponding extensions.

This situation may be in contradiction, for most primes $q$, since the global arithmetical properties of the auxiliary fields $\mathbb{Q}(\mu_{q-1})$ are independent of the Fermat problem.

More precisely, a general philosophy is that the decomposition groups of prime ideals in Galois extensions do not fulfill any other laws than standard ones, and may be analyzed in a statistical point of view (see Section 6 for a direct study of these aspects).

About this, we shall explain in Subsection 5.3 and in Section 8 that the case $p = 3$ is precisely an exceptional counterexample to the above claim, since some constraints do exist; but we shall show that these constraints are not in contradiction with statistical considerations because of the structure of the *infinite* set of parametric solutions of the case $p = 3$.

One may object that $F_\xi$ comes from the radical $\big\langle\, (1+\xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}\,\big\rangle\, M^{\times p}$ over $M$, which is associated to a problem of SFLT type, and in a standard algebraic point of view the above circumstances on the laws of decomposition may be *equivalent* to a contradiction to SFLT.

Thus it will be necessary to obtain some analytic or geometric informations on the splitting of $q$ in the Abelian extensions $H_{L[p]}/L$, $L := \mathbb{Q}(\mu_n)$ (especially in the canonical family $(F_{\xi'}/L)_{\xi' \text{ of order } n}$) so as to prove that the above particularities do not exist.

Of course we strongly think to a suitable application of density theorems. For this we refer to **[Se1]**, **[Se2]**, which contain most general results and applications.

## 5. Sufficient conditions implying Fermat's Last Theorem

In this section, from Theorem 3.3 and from the results of Subsection 4.3, we study a sufficient condition implying FLT in the two cases; this condition only involves congruential properties of prime ideals lying above $q$ in $\mathbb{Q}(\mu_{q-1})$. Next, we shall examine some weaker forms of this condition.

**5.1. The most radical form of this condition.** — We suppose that $p > 3$ and that the primes $q$ considered are such that $f > 1$ & $\kappa := \frac{q^f-1}{p} \not\equiv 0 \pmod p$. Thus any divisor $n$ of $q-1$ is prime to $p$.

For a nontrivial solution $(u, v)$ of the SFLT equation in the nonspecial cases, we shall use Corollaries 2.15 (i) and 2.16 (i) on Furtwängler's theorems to obtain, respectively, that:

(i) $q \nmid uv$ in the first case, and similarly in the second case supposing $q$ large enough,

(ii) the order $n$ of $\frac{v}{u}$ modulo $q$ is $> 2$ under the assumption $u - v \not\equiv 0 \pmod p$ in the first case, and assuming $q$ large enough in the second case.

In the same way, from a solution $(x, y, z)$ of Fermat's equation (with the conventions of Lemma 2.2) we shall use Remark 3.5 on Furtwängler's theorems to obtain that $q \nmid xyz$ (supposing $q$ large enough in the second case).

Then the FLT case comes from the SFLT one (in the nonspecial cases) since the differences $u - v := \pm(x-y)$ or $\pm(y-z)$ are by definition nontrivial modulo $p$ under a solution of Fermat's equation; hence the condition $n > 2$ of the point (ii) is satisfied.

So we can consider a nontrivial solution $(u, v)$ of the SFLT equation (with $u^2 - v^2 \not\equiv 0 \pmod p$) and a prime $q$ of the above form. Then $q \nmid u\,v$ and $\rho := \frac{v}{u}$ is of order $n > 2$ modulo $q$ (which is equivalent to $q \nmid uv(u^2-v^2)$).

For a primitive $n$th root of unity $\xi$, we consider the pair $(\xi, \mathfrak{q}_{\rho,\xi})$ defined up to $\mathbb{Q}$-conjugation in $L := \mathbb{Q}(\mu_n)$, hence the class $\mathcal{C}_\rho(q)$ (see Definition 3.1). Let $\mathfrak{Q}_{\rho,\xi}$ be any prime ideal of $M := LK$ lying above $\mathfrak{q}_{\rho,\xi}$. Then the integer $n$, the class $\mathcal{C}_\rho(q)$ or the class of the pair $(\eta_1, \mathfrak{Q}_{\rho,\xi})$ where $\eta_1 = (1 + \xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}} \in M^+$, are unknown.

Let $\mathfrak{q}\,|\,q$ fixed *arbitrarily* in $L$ and let $\mathfrak{Q}\,|\,\mathfrak{q}$ in $M$. If we ensure that $\left(\frac{\eta_1}{\mathfrak{Q}^t}\right)_M = 1$ for all $t \in \mathrm{Gal}(M/K)/\langle\, t_{-1}\,\rangle$, then in particular for the "right" value of the pair $(\eta_1, \mathfrak{Q}^t)$ (i.e., such that $\mathfrak{q}^t = \mathfrak{q}_{\rho,\xi}$), we get

$$\left(\frac{\eta_1}{\mathfrak{Q}_{\rho,\xi}}\right)_M = \zeta^{-\frac{1}{2}\,\frac{u-v}{u+v}\,\kappa} = 1\,,$$

giving $u - v \equiv 0 \pmod p$ which is absurd.

Since $\left(\frac{\eta_1}{\mathfrak{Q}^t}\right)_M = \left(\frac{\eta_1^{t^{-1}}}{\mathfrak{Q}}\right)_M$, the triviality of all the symbols means that $\mathfrak{q}$ totally splits in $F_n/L$; then all the conjugates of $\mathfrak{q}$ have the same property since $F_n/\mathbb{Q}$ is Galois. In other words, $q$ totally splits in $F_n/\mathbb{Q}$.

The problem is to know if there exist infinitely many such primes $q$ with $F_n$ in the splitting field of $\mathfrak{q}$ in $H_{L[p]}/L$, for all $n\,|\,q-1$, $n > 2$. If so, this will prove FLT unconditionally and SFLT in the nonspecial cases, under the condition $u - v \not\equiv 0 \pmod p$.

Since $F_n \subseteq H^-_{L[p]}$, a sufficient condition to have the total splitting of $\mathfrak{q}$ in $F_n$ is that the Frobenius automorphism $\varphi$ of $\mathfrak{q}$ in $H_{L[p]}/L$ be an element of $C_L^+$, which is equivalent to $\varphi^{t_{-1}} = \varphi$, hence to $\varphi^{t_{-1}-1} = 1$. Note that $\varphi$ is of order $p$ since its restriction to $L_1$ is of order $p$ by assumption.

The image of $\varphi \in C_L$ by the isomorphism $\mathrm{Gal}(H_{L[p]}/L) \simeq I/I^p\,R$ of class field theory (see Subsection 4.3), is given by the class of $\mathfrak{q}$ in $I/I^pR$; thus the condition $\varphi^{t_{-1}-1} = 1$ is equivalent to $\mathfrak{q}^{t_{-1}-1} \in I^pR$, i.e.,

$$\mathfrak{q}^{t_{-1}-1} = \mathfrak{a}^p\,(\alpha), \quad \alpha \equiv 1 \pmod{p^2}\,,$$

for an ideal $\mathfrak{a}$ of $L$.

We must realize this for any divisor $n > 2$ of $q - 1$.

For $\widetilde{n} := q - 1$, $\widetilde{L} := \mathbb{Q}(\mu_{q-1})$, we assume that the above condition $\widetilde{\mathfrak{q}}^{\widetilde{t}_{-1}-1} = \widetilde{\mathfrak{a}}^p\,(\widetilde{\alpha})$, $\widetilde{\alpha} \equiv 1 \pmod{p^2}$, is satisfied (for $\widetilde{\mathfrak{q}}\,|\,q$ in $\widetilde{L}/\mathbb{Q}$).

Then let $n \mid q-1$, $n > 2$; since $L = \mathbb{Q}(\mu_n)$ is imaginary, $L^+$ is fixed by the restriction $t_{-1}$ of $\widetilde{t}_{-1}$ to $L$, and taking the norm $\mathrm{N}_{\widetilde{L}/L}$ we get

$$\mathrm{N}_{\widetilde{L}/L}(\widetilde{\mathfrak{q}}^{\,\widetilde{t}_{-1}-1}) = \mathrm{N}_{\widetilde{L}/L}(\widetilde{\mathfrak{a}})^p \, \mathrm{N}_{\widetilde{L}/L}(\widetilde{\alpha})\,.$$

Since $q$ is totally split in $\widetilde{L}$, we have by definition $\mathrm{N}_{\widetilde{L}/L}(\widetilde{\mathfrak{q}}) = \mathfrak{q}$ for some $\mathfrak{q} \mid q$ in $L$, and the above relation is of the form $\mathfrak{q}^{t_{-1}-1} = \mathfrak{a}^p\,(\alpha)$, with $\alpha \equiv 1 \pmod{p^2}$, as expected; this coherent choice of the ideals $\mathfrak{q}$ is possible since the required condition of splitting at each level is independent of the choice of the ideal.

So the whole condition for our purpose is given by the condition for $n = q-1$ and $L = \mathbb{Q}(\mu_{q-1})$.

We have obtained the following criterion, where $c$ is the complex conjugation:

***Theorem 5.1***. — *Let $p$ be a prime $> 3$. If there exists a prime $q \neq p$, $q \not\equiv 1 \pmod p$, $q^{p-1} \not\equiv 1 \pmod{p^2}$, such that for any prime ideal $\mathfrak{q} \mid q$ in $\mathbb{Q}(\mu_{q-1})$, we have the relation $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(\alpha)$ for an ideal $\mathfrak{a}$ and an element $\alpha$ of $\mathbb{Q}(\mu_{q-1})$ with $\alpha \equiv 1 \pmod{p^2}$, then the first case of FLT (and the first case of the SFLT equation $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{w}_1^p$ under the supplementary condition $u - v \not\equiv 0 \pmod p$) holds for $p$.*

*The second case of FLT (and unconditionally of SFLT) holds for $p$ as soon as there exist infinitely many such primes $q$.*

***Remark 5.2***. — (i) Since the multiplicative groups of the residue fields of $L$ at $p$ are of order prime to $p$, in any writing $\mathfrak{a}^p\,(\alpha)$ we can suppose $\alpha = 1 + p\,\beta$, $\beta$ $p$-integer of $L$.

(ii) The condition $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(\alpha)$, $\alpha \equiv 1 \pmod{p^2}$, is equivalent to $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(1 + p\,\beta)$, where $\beta \equiv \beta^+ \pmod p$ for a $p$-integer $\beta^+$ of $L^+$; indeed, this last condition implies $\mathfrak{q}^{2(1-c)} = \mathfrak{a}^{(1-c)p}\,(1 + p\,\beta)^{1-c}$ where $(1 + p\,\beta)^{1-c} \equiv 1 + p\,(1-c)\,\beta \equiv 1 \pmod{p^2}$, which leads to the result thanks to a Bézout relation between 2 and $p$.

(iii) The condition $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(\alpha)$, $\alpha \equiv 1 \pmod{p^2}$, is also equivalent to $\mathfrak{q} = \mathfrak{b}^{1+c}\mathfrak{a}'^p\,(\alpha')$, $\alpha' \equiv 1 \pmod{p^2}$; indeed, from $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(\alpha)$ we get $\mathfrak{q}^2 = \mathfrak{q}^{1+c}\mathfrak{a}^p\,(\alpha)$.

(iv) The condition $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(\alpha)$, $\alpha = 1 + p\,\beta$, is satisfied as soon as the class of $\mathfrak{q}^{1-c}$ is of order prime to $p$, a weaker condition which holds in general. Next, it remains to check the stronger condition $\beta \equiv \beta^+ \pmod p$ implying the theorem.

Proposition 3.11 shows that $F_{q-1}/\mathbb{Q}(\mu_{q-1})$ is of degree less or equal to $\frac{1}{2}\phi(q-1)$. So, if the torsion group $\overline{V}_{\mathbb{Q}(\mu_{q-1})}$ is trivial, the equality $F_{q-1} = H^-_{\mathbb{Q}(\mu_{q-1})}[p]$ is possible and the sufficient condition of Theorem 5.1 for the total splitting of $q$ in $F_{q-1}$ is also necessary.

From the Čebotarev density theorem, there exist infinitely many prime ideals $\mathfrak{l}$ of $\mathbb{Q}(\mu_{q-1})$ such that their Frobenius automorphisms $\varphi_{\mathfrak{l}}$ lie in $C^+_{\mathbb{Q}(\mu_{q-1})}$ (at least of dimension 1); the problem is to be sure that there is no obstruction to the fact that it is sometimes possible for $\mathfrak{l} = \mathfrak{q} \mid q$. An important fact is precisely that there exists an obvious obstruction for $p = 3$ to the existence of such primes $q$ totally split in $H^-_{\mathbb{Q}(\mu_{q-1})}[p]$. This is the subject of Subsections 5.3 and 8.1. Meanwhile, this obstruction seems to be specific of the case $p = 3$.

Such a set of primes $q$ would be of Dirichlet density 0, as for the set of primes $q$, such that the ring $\mathbb{Z}[\mu_{q-1}]$ contains a principal ideal of norm $q$, a result proved by Lenstra in [**Len**], Cor. 7.6.

Theorem 5.1 may be of empty use due to an excessive condition on the primes $q$. So we intend, in the forthcoming subsection, to try to give a weaker form of this result (see Conjecture 5.4).

**5.2. Some related viewpoints.** — We shall examine if some effective (or numerical) aspects allow us to justify the method of proof of FLT based on Theorem 5.1 for $p > 3$.

*5.2.1. A diophantine approach.* — In this first approach, we fix $q$ and $\widetilde{\mathfrak{q}} \,|\, q$ in $\widetilde{L} = \mathbb{Q}(\mu_{q-1})$, and we try to find some suitable values of $p$ for which $\widetilde{\varphi} := \Big(\frac{H^-_{\widetilde{L}}[p]/\widetilde{L}}{\widetilde{\mathfrak{q}}}\Big) \in C^+_{\widetilde{L}}$.

Let $k$ be the order of the class of $\widetilde{\mathfrak{q}}$ in $\widetilde{L}$; put $\widetilde{\mathfrak{q}}^k = (\widetilde{\alpha})$. Suppose that we find $d > 0$ such that $\widetilde{\alpha}^d \equiv \widetilde{\alpha}^+ \pmod{p^2}$, for some prime $p$ such that $p \nmid k\,d$, and some $\widetilde{\alpha}^+ \in \widetilde{L}^+$; then $\widetilde{\alpha}^{d(1-c)} \equiv 1 \pmod{p^2}$ giving a solution of the problem for the prime $p$. Then $d$ may be chosen a posteriori as a suitable divisor of the order of the multiplicative group of the residue field of $\widetilde{L}$ at $p$.

We have not necessarily $q \not\equiv 1 \pmod p$ & $q^{p-1} \not\equiv 1 \pmod{p^2}$.

Of course this relation looks like the general problem of the Fermat quotients of algebraic numbers as studied by Hatada in **[Hat]**. Considering the work of Hatada and others, a serious conjecture would be that there exist infinitely many solutions $p$ for any fixed $q$.

Since the numerical values of $p$ are out of range of any computer, this conjectural property is not of a practical use, but connect FLT to deep properties of algebraic numbers.

Meanwhile, we have found the following example which gives a very partial illustration but shows that there is, a priori, no systematic obstruction for this question.

***Example 5.3.*** — *Let $q = 5$ and $p = 463$. We then have $L = \mathbb{Q}(\mu_4) = \mathbb{Q}(i)$, where $i := \sqrt{-1}$, and $\mathfrak{q} = (2 + i)$. We see that $q$ is totally inert in $K$ (i.e., $f = 462$) and that $p$ is also inert in $L$. We obtain the following numerical informations:*

- $(5^{463-1} - 1)/463 \not\equiv 0 \pmod{463}$ *(i.e., $\kappa \not\equiv 0 \pmod p$),*
- $(2 + i)^{463+1} \equiv 43990 \pmod{463^2}$.

*This immediately implies $\mathfrak{q}^{1-c} = \big(\frac{2+i}{2-i}\big)$ and $\mathfrak{q}^{(p+1)(1-c)} = \big(\frac{2+i}{2-i}\big)^{p+1} \equiv 1 \pmod{p^2}$, giving the relation $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(\alpha)$ with $\mathfrak{a} = \mathfrak{q}^{c-1}$ and $\alpha \equiv 1 \pmod{p^2}$, proving the first case of FLT for $p = 463$.*

*5.2.2. A weaker form of Theorem 5.1.* — In a slightly different point of view, we must consider that in general, for a solution $(u, v)$ of the SFLT equation for fixed $p$, the order $n$ of $\frac{v}{u}$ modulo $q$ may be a strict divisor of $q - 1$, even if it is obvious directly that $n$ tends to infinity with $q$ (Corollary 3.9).

Let $m$ be an integer $> 2$ such that $p \nmid m$. Put $K_1 := K\mathbb{Q}_1 = \mathbb{Q}(\mu_{p^2})$, $L := \mathbb{Q}(\mu_m)$. Then $H^-_L[p]/\mathbb{Q}$ (see Section 4) and $K_1/\mathbb{Q}$ are linearly disjoint. Let $\varphi_1 \in \mathrm{Gal}\big(H^-_L[p]K_1/H^-_L[p]\big)$ of order $pf$, $f \,|\, p - 1$. From the Čebotarev density theorem, there exist infinitely many primes $q$ such that, for a suitable $\mathfrak{Q}_1 \,|\, q$ in $H^-_L[p]K_1$, the Frobenius automorphism of $\mathfrak{Q}_1$ satisfies the equality $\Big(\frac{H^-_L[p]K_1/\mathbb{Q}}{\mathfrak{Q}_1}\Big) = \varphi_1$. Since $H^-_L[p]K_1/L$ is Abelian we have $\varphi_1 = \Big(\frac{H^-_L[p]K_1/L}{\mathfrak{q}_1}\Big)$, where $\mathfrak{q}_1 = \mathfrak{Q}_1 \cap Z_L$, and by conjugation this yields $\Big(\frac{H^-_L[p]K_1/L}{\mathfrak{q}}\Big) \in \mathrm{Gal}\big(H^-_L[p]K_1/H^-_L[p]\big)$, for all $\mathfrak{q} \,|\, q$ in $L$, since $\mathrm{Gal}\big(H^-_L[p]K_1/H^-_L[p]\big)$ is normal in $\mathrm{Gal}\big(H^-_L[p]K_1/\mathbb{Q}\big)$.

This implies the following properties:

- $q \equiv 1 \pmod{m}$ (since $q$ splits in $L/\mathbb{Q}$),
- $q^f \not\equiv 1 \pmod{p^2}$ (since $q$ is inert in $K_1/K$),
- $q$ totally splits in $H_L^-[p]/L$.

Thus the condition $\mathfrak{q}^{1-c} = \mathfrak{a}^p(\alpha)$, $\alpha \equiv 1 \pmod{p^2}$, is satisfied for any prime ideal $\mathfrak{q} \,|\, q$ in $L = \mathbb{Q}(\mu_m)$ but not necessarily for $\widetilde{\mathfrak{q}} \,|\, \mathfrak{q}$ in $\widetilde{L} = \mathbb{Q}(\mu_{q-1})$; indeed, the Frobenius automorphism of $\mathfrak{q}$ in $H_L[p]/L$ fixes $H_L^-[p]$ but this is not necessarily true for the Frobenius automorphism of $\widetilde{\mathfrak{q}}$ in $H_{\widetilde{L}}[p]/L$, giving possible inertia of $\widetilde{\mathfrak{q}}$ in $H_{\widetilde{L}}^-[p]/\widetilde{L}\, H_L^-[p]$.

The order of $\frac{v}{u}$ modulo $q$ is $n \,|\, q-1$ and not necessarily $m$, and the obvious analogue of Theorem 5.1 only applies if $n \,|\, m$.

In other words, we try to replace the order $q-1$, probably too big under the condition that the Frobenius automorphism of $\widetilde{\mathfrak{q}}$ lies in $C_{\widetilde{L}}^+$, $\widetilde{L} := \mathbb{Q}(\mu_{q-1})$, by a strict divisor $m_q$ of $q-1$, for infinitely many $q$ for which we hope that the Frobenius automorphism of the corresponding ideal $\mathfrak{q}$ of $\mathbb{Q}(\mu_{m_q})$ lies in $C_{\mathbb{Q}(\mu_{m_q})}^+$.

Then, under the existence of a nontrivial solution $(u, v)$ of the SFLT equation in the nonspecial cases (with the condition $u - v \not\equiv 0 \pmod{p}$ in the first one), there is an obstruction to the existence of a pair $(q, m_q)$ ($m_q \,|\, q-1$, with the Frobenius automorphism of $\mathfrak{q}$ in $C_{\mathbb{Q}(\mu_{m_q})}^+$) such that the order of $\frac{v}{u}$ modulo $q$ is a divisor $n$ of $m_q$.

Of course, to get a contradiction to the existence of $(u, v)$, it is sufficient to find a prime $q \nmid u\, v\, (u^2 - v^2)$ with $\kappa \not\equiv 0 \pmod{p}$, totally split in $H_L^-[p]/L$ for $L = \mathbb{Q}(\mu_n)$, where the order $n$ of $\frac{v}{u}$ modulo $q$ is a small divisor of $q-1$.

The verification of the condition $q \nmid u\, v$ is ineffective (except when Furtwängler's theorems apply) and such a criterion must be replaced by the existence of infinely many primes $q$ such that the order of $\frac{v}{u}$ modulo $q$ is a small divisor of $q-1$.

These remarks may constitute a way of access to a proof of FLT by means of analytic investigations and we can propose the following general conjecture, independent of SFLT, which covers the above discussion.

For any prime $q \neq p$, set $\widetilde{L} = \mathbb{Q}(\mu_{q-1})$ and denote by $S_q$ the set of places of $\widetilde{L}$ dividing $q$; since $q$ totally splits in $\widetilde{L}/\mathbb{Q}$, we have $|\, S_q\,| = \phi(q-1)$. Then call $H_{\widetilde{L}}^{S_q}[p]/\widetilde{L}$ the maximal subextension of $H_{\widetilde{L}}[p]/\widetilde{L}$ in which $q$ totally splits.

***Conjecture 5.4.*** — *Let $p$ be a prime $> 2$. Let $\rho$ be a rational distinct from $0$ and $\pm 1$. Then there exist an infinite number of primes $q$, such that $q \not\equiv 1 \pmod{p}$ & $q^{p-1} \not\equiv 1 \pmod{p^2}$, for which $\widetilde{L}F_n \subseteq H_{\widetilde{L}}^{-S_q}[p]$, where $n \,|\, q-1$ is the order of $\rho$ modulo $q$ (see Subsection 4.4).*

Note that since $q$ totally splits in $\widetilde{L}/\mathbb{Q}$, the condition "$\widetilde{L}F_n \subseteq H_{\widetilde{L}}^{-S_q}[p]$" is equivalent to the condition "$q$ totally splits in $F_n/\mathbb{Q}$".

If Conjecture 5.4 is true, it applies to any rational $\rho$ associated to a nontrivial solution $(u, v)$ (with $u - v \not\equiv 0 \pmod{p}$) of the SFLT equation in the nonspecial cases and then gives a contradiction (the fact that we must only consider the nonspecial cases is sufficient for Fermat's equation).

The existence of infinitely many primes $q$ satisfying the conditions of Theorem 5.1 is equivalent to the conjecture with the supplementary very strong condition $H^-_{\widetilde L}[p] \subseteq H^{S_q}_{\widetilde L}[p]$.

See [**Gr2**], II.5.4.1 (ii), for the computation of $\dim_{\mathbb{F}_p}\big(\mathrm{Gal}(H^{-S_q}_{\widetilde L}[p]/\widetilde L)\big)$ which essentially depends on the group of $S_q$-units of $\widetilde L$ locally $p$th powers at each place dividing $p$.

The existence of such inclusions $\widetilde L F_n \subseteq H^{-S_q}_{\widetilde L}[p]$, $n \,|\, q-1$, depends on two phenomena:

(i) The order of magnitude of the primes $q \equiv 1 \pmod m$, totally split in $F_m/\mathbb{Q}$, obtained by Čebotarev density theorem in the extensions $F_m/\mathbb{Q}$, as shown above in 5.2.2.

(ii) The minimal possible value of the order $n$ modulo $q$ of a given rational $\rho$, by comparison with $q$, since $n$ tends to infinity with $q$.

***Example 5.5***. — *For $p = 5$, $m = 4$, we have $L = \mathbb{Q}(i)$, and an obvious family of ideals $\mathfrak{q}$ of $L$ such that $\mathfrak{q}^{1-c} = (\alpha)$, $\alpha \equiv 1 \pmod{25}$, is given by the expression*

$$\mathfrak{q} = (e + 5a + 25b\, i)\, \mathbb{Z}[i],\ 1 \le e < 5,\ \ a,\, b \in \mathbb{Z},$$

*$e, a, b$ being such that $(e + 5a)^2 + (25b)^2$ is a prime $q$.*

*The primes $q < 10000$, $q \not\equiv 1 \pmod 5$ and $q^4 \not\equiv 1 \pmod{25}$, of the above form, are the following ones:* 769, 1109, 1409, 2069, 2389, 2789, 3229, 3329, 3989, 5309, 5689, 6469, 6709, 7069, 7829, 8329, 8369, 8429.

*Taking $q = 769$, the pairs of coprime integers $u$, $v$, such that $u - v \not\equiv 0 \pmod 5$ and $62\,u - v \equiv 0 \pmod{769}$, cannot be a solution of the SFLT equation for $p = 5$; indeed, 62 is of order 4 modulo 769, and 769 is totally split in $F_4/\mathbb{Q}$ by construction.*

Such construction of a list of primes $q$ does exist for any prime $p$ and any $m > 2$, and the question is the following: $p$, $u$, and $v$ being given, is it possible to find in such infinite lists of primes (corresponding to arbitrary values of $m$), a prime $q$ for which the order of $\frac{v}{u}$ modulo $q$ is a divisor of $m$ (which is equivalent to $q \,|\, u^m - v^m$)? For each $m > 2$, only a finite number of $q$ in the list can be solution.

The existence of one solution $(m, q)$ gives the proof of the first case of FLT for $p$ and the existence of infinitely many solutions $(m, q)$ gives a complete proof of FLT for $p$.

**5.3. Simplest cubic fields – Obstruction for a total splitting of $q$ in $H^-_{\widetilde L}[3]/\widetilde L$.** — Independently of the existence of nontrivial solutions of the SFLT equation for $p = 3$, we intend to identify the obstruction giving, for $p = 3$, an empty Theorem 5.1.

More precisely, this obstruction shows that *for all prime $q$* such that $q \equiv -1 \pmod 3$ & $\kappa \not\equiv 0 \pmod 3$, the total splitting of $q$ in $H^-_{\mathbb{Q}(\mu_{q-1})}[3]/\mathbb{Q}$ is not possible (see Subsection 8.1 for a more precise viewpoint using explicitly the solutions).

Over $\mathbb{Q}$, the well-known polynomial

$$X^3 - \tau\, X^2 - (3 - \tau)\, X + 1,\ \ \tau \in \mathbb{Z}\,,$$

of discriminant $(\tau^2 - 3\tau + 9)^2$, defines the *simplest cyclic cubic field* introduced by D. Shanks in [**Sh**].[9] So we can consider the analogous polynomial over $L = \mathbb{Q}(\mu_n)$, $n > 2$, $n \not\equiv 0 \pmod 3$, taking $\tau := 3\,\xi^{-1}$ where $\xi$ is a primitive $n$th root of unity,

$$P_\xi^{sh} := X^3 - 3\,\xi^{-1}\,X^2 - 3\,(1 - \xi^{-1})\,X + 1\,,$$

for which we denote by $F_\xi^{sh}$ the corresponding cyclic cubic extension of $L$. The discriminant of $P_\xi^{sh}$ is $81\,(\xi^2 - \xi + 1)^2$ giving a 3-ramified extension since $\xi^2 - \xi + 1$ is a unit. Using the classical results on Kummer theory that we recall in Subsection 6.3, we obtain that $F_\xi^{sh}K = M\big(\sqrt[3]{(1+\xi\,j)^{e'_\omega}}\big)$ with the representative $e'_\omega = s + 2$ instead of $e_\omega = s - 1$, $s = s_{-1}$. By comparison, the polynomials defining $F_\xi$ from $\eta_1 = (1+\xi\,j)^{e_\omega}j^{-\frac{1}{2}}$ or $\eta'_1 = (1+\xi\,j)^{e'_\omega}j^{-\frac{1}{2}} \sim \eta_1$ are

$$P_\xi := X^3 - 3\,X + \frac{\xi^2 - 4\xi + 1}{\xi^2 - \xi + 1} \quad \text{or} \quad X^3 - 3\,(\xi^2 - \xi + 1)X + \xi^3 + 1\,.$$

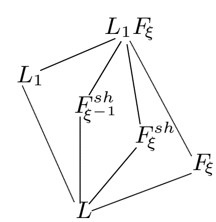
Let $c$ be the complex conjugation; then we have

$$\eta_1^{sh} := (1+\xi\,j)^{e'_\omega};\ (\eta_1^{sh})^c \sim \eta_1^{sh}\,j^{\frac{1}{2}};\ \eta_1^{sh+} := \eta_1^{sh\,\frac{1+c}{2}} \sim \eta_1^{sh}\,j^{-\frac{1}{2}} = \eta_1;\ \eta_1^{sh-} := \eta_1^{sh\,\frac{1-c}{2}} \sim j^{\frac{1}{2}}\,,$$

which are independent in $M^\times/M^{\times 3}$ (see Section 4).

So if we denote by $F_\xi^{sh}$, $cF_\xi^{sh}$, $F_\xi$, $L_1$ the four cyclic cubic extensions of $L$ contained in the fields $M\big(\sqrt[3]{\eta_1^{sh}}\big)$, $M\big(\sqrt[3]{(\eta_1^{sh})^c}\big)$, $M\big(\sqrt[3]{\eta_1^{sh+}}\big)$, $M\big(\sqrt[3]{\eta_1^{sh-}}\big)$, respectively, we know that $F_\xi \subseteq H_L^-[3]$ is diedral over $L^+$, that $L_1 \subseteq H_L^+[3]$, and we compute that $cF_\xi^{sh} = F_{\xi^{-1}}^{sh}$; so the polynomial $P_{\xi^{-1}}^{sh} := X^3 - 3\,\xi\,X^2 - 3\,(1-\xi)\,X + 1$ is the simplest cubic polynomial defining $c\,F_\xi^{sh}$.

Hence we have the following schema:




Let $\mathfrak{q} = (q, \xi - e)$ be a prime ideal lying above $q$ in $L$, where $e \in \mathbb{Z}$ is of order $n$ modulo $q$ (thus $e \not\equiv \pm 1 \pmod q$ since $n > 2$). Then $\mathfrak{q}$ splits in $F_\xi/L$ if and only if it is inert in $F_\xi^{sh}/L$ and in $F_{\xi^{-1}}^{sh}/L$ since it is inert in $L_1/L$ ($\kappa \not\equiv 0 \pmod 3$), thus if and only if $P_\xi^{sh}$ and $P_{\xi^{-1}}^{sh}$ are irreducible modulo $\mathfrak{q}$, hence if and only if (where $\overline{e}$ is the image of $e$ in $\mathbb{F}_q$)

$$P_{\overline{e}}^{sh} := X^3 - 3\,\overline{e}^{-1}\,X^2 - 3\,(1 - \overline{e}^{-1})\,X + 1 \text{ and } P_{\overline{e}^{-1}}^{sh} := X^3 - 3\,\overline{e}\,X^2 - 3\,(1 - \overline{e})\,X + 1$$

are irreducible in $\mathbb{F}_q[X]$.

But $P_{\overline{e}}^{sh}$ is reducible in $\mathbb{F}_q[X]$ if and only if $\overline{e} = \overline{e}(\overline{a}) \in A := \big\{\frac{3\overline{a}(\overline{a} - \overline{1})}{\overline{a}^3 - 3\overline{a} + \overline{1}},\ \overline{a} \in \mathbb{F}_q \backslash \{\overline{0}, \overline{1}\}\big\}$ (we have $\overline{a}^3 - 3\overline{a} + \overline{1} \neq 0$ since $q \equiv -1 \pmod 3$). We compute that $\overline{e}(\overline{a}) = \overline{e}(\overline{b})$ if and only if

[9] There is an abundant literature on the cubic case and on the search of this kind of fields defined by similar polynomials of small degree depending linearly on a parameter; see for instance [**Gmn**], [**Le**], [**ScW**], [**Wa2**].

$\overline{b} = \overline{a}$, $\overline{b} = 1 - \overline{a}^{-1}$, or $\overline{b} = (\overline{1} - \overline{a})^{-1}$, which are distinct since $q \equiv -1 \pmod 3$, so that there are exactly $\frac{q-2}{3}$ distinct solutions $\overline{e}$ in $\mathbb{F}_q^\times$; they are of orders $> 2$ since $\pm\overline{1} \notin A$.

Since $P_{\overline{e}}^{sh}$ reducible implies $P_{\overline{e}^{-1}}^{sh}$ irreducible for $\overline{e} \neq \pm\overline{1}$, one obtains $q - 1 - 2 - 2\,\frac{q-2}{3} = \frac{q-5}{3}$ values of $\overline{e}$ (of orders $n > 2$) such that $P_{\overline{e}}^{sh}$ and $P_{\overline{e}^{-1}}^{sh}$ are irreducible.

So $\mathfrak{q} = (q, \xi - e)$ is inert in $F_\xi/L$ for $q - 1 - \frac{q-5}{3} = \frac{2}{3}\,(q+1)$ values of $\overline{e}$; which gives $\frac{2}{3}\,(q+1) - 2$ values of $\overline{e}$ of orders $n > 2$ and so $\frac{q-2}{3}$ pairs $(\overline{e}, \overline{e}^{-1})$ since we know that $F_\xi = F_{\xi^{-1}}$.

Of course, instead of the above method we could have count the number of irreducible polynomials $P_{\overline{e}} = X^3 - 3\,(\overline{e}^2 - \overline{e} + 1)\,X + \overline{e}^3 + 1$; but this does not seem directly accessible.

For instance, for $q = 23$, the 7 pairs $(\overline{e}, \overline{e}^{-1})$ solutions are

$$(\overline{2}, \overline{12}),\ (\overline{3}, \overline{8}),\ (\overline{4}, \overline{6}),\ (\overline{5}, \overline{14}),\ (\overline{7}, \overline{10}),\ (\overline{11}, \overline{21}),\ (\overline{15}, \overline{20})\,.$$

As a consequence, none of these primes $q \geq 5$ can totally split in $H_{\widetilde{L}}^-[3]/\widetilde{L}$ for $\widetilde{L} := \mathbb{Q}(\mu_{q-1})$ since there is a nontrivial inertia in $H_L^-[3]/L$, for various $L = \mathbb{Q}(\mu_n)$, $n \,|\, q-1$. So, for $p = 3$, Theorem 5.1 cannot apply (see Subsection 8.1 for more details).

For $p > 3$, the situation is of a different nature if we assume that the SFLT equation has a finite number of solutions, which is equivalent to consider Conjecture 5.4 for a fixed $\rho$, because, as we have seen in Subsection 5.2 (5.2.2), we can hope a weaker form of Theorem 5.1.

Moreover, for $p > 3$, the coefficients of the analogous polynomials $P_{\overline{e}}^{sh}$ or $P_{\overline{e}}$ have increasing degrees in $\overline{e}$ so that the number of irreducible $P_{\overline{e}}$ may be small regarding $q$.

The experimentation shows that a splitting in $\mathbb{F}_q[X]$ of the polynomial $P_{\overline{e}}$ (associated to the splitting of $(q, \xi - e)$ in $F_\xi$), is possible for small values of the order $n$ of $\overline{e}$. For instance, for $p = 5$, $\rho = \frac{5}{7}$, $q = 419$, we have $\rho \equiv 300 \pmod{419}$ and the order of $\overline{e} = \overline{300}$ is $n = 11$.

**5.4. Explicit formula for the $p$th power residue symbol $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M$.** — Let $q \neq p$ be a prime and let $n$ be such that $p \nmid n$. Let $\xi$ be a primitive $n$th root of unity and let $\mathfrak{q}$ be any prime ideal of $L = \mathbb{Q}(\mu_n)$ lying above $q$. We do not assume that $q \nmid n$.

We consider the real $\omega$-cyclotomic unit $\eta_1 := (1 + \xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}} \in M = LK$ (see Definition 3.2). Recall that for $n \leq 2$, $\eta_1 \in K^{\times p}$, so we assume $n > 2$.

Let $c$ be the complex conjugation. We suppose in this subsection that the ideal class of $\mathfrak{q}^{1-c}$ is the $p$th power of a class of $L$, which is equivalent to $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(\alpha)$ for an ideal $\mathfrak{a}$ of $L$ and an $\alpha \in L^\times$ such that $\alpha \equiv 1 \pmod p$ (see Remark 5.2). This assumption is stable by conjugation of $\mathfrak{q}$. So we get $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(1 + p\,\beta)$, $\ \beta$ $p$-integer of $L$.

Taking the absolute norm leads to $\mathrm{N}_{L/\mathbb{Q}}(1 + p\,\beta) = \mathrm{N}_{L/\mathbb{Q}}(\mathfrak{a})^{-p} \equiv 1 \pmod{p^2}$. Thus since $\mathrm{N}_{L/\mathbb{Q}}(1 + p\,\beta) \equiv 1 + p\,\mathrm{Tr}_{L/\mathbb{Q}}(\beta) \pmod{p^2}$, where $\mathrm{Tr}_{L/\mathbb{Q}}$ is the absolute trace, we obtain $\mathrm{Tr}_{L/\mathbb{Q}}(\beta) \equiv 0 \pmod p$. This remark will be used later.

We note that, as for the context of Theorem 5.1, if $q - 1 =: d\,p^r$, $r \geq 0$, $p \nmid d$, and if the analogous condition $\widetilde{\mathfrak{q}}^{1-c} = \widetilde{\mathfrak{a}}^p\,(1 + p\,\widetilde{\beta})$ is satisfied for $\widetilde{\mathfrak{q}} \,|\, q$ in $\widetilde{L} = \mathbb{Q}(\mu_d)$, then it is satisfied for any ideal $\mathfrak{q} = \mathrm{N}_{\widetilde{L}/L}(\widetilde{\mathfrak{q}})$ in $L = \mathbb{Q}(\mu_n)$, $n \,|\, d$; we then have $\beta \equiv \mathrm{Tr}_{\widetilde{L}/L}(\widetilde{\beta}) \pmod p$.

In $M$ we have

$$\left(\frac{\eta_1}{(\mathfrak{q})^{1-c}}\right)_M = \left(\frac{\eta_1}{\prod_{\mathfrak{Q}\,|\,\mathfrak{q}} \mathfrak{Q}^{1-c}}\right)_M = \prod_{\mathfrak{Q}\,|\,\mathfrak{q}} \left(\frac{\eta_1}{\mathfrak{Q}^{1-c}}\right)_M = \left(\frac{\eta_1}{\mathfrak{Q}}\right)_M^{2\,\frac{p-1}{f}}\,,$$

where $f$ is the residue degree of $q$ in $K/\mathbb{Q}$; indeed, $\eta_1$ being real, we have

$$\Big(\frac{\eta_1}{\mathfrak{Q}^{1-c}}\Big)_M = \Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M \cdot \Big(\frac{\eta_1}{\mathfrak{Q}^c}\Big)_M^{-1} = \Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M \cdot \Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M^{-c} = \Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M^2,$$

hence the result since the symbol of $\eta_1$ does not depend on the choice of $\mathfrak{Q}$ lying above $\mathfrak{q}$. But $\Big(\frac{\eta_1}{(\mathfrak{q})^{1-c}}\Big)_M = \Big(\frac{\eta_1}{(\mathfrak{a}^p)\,(\alpha)}\Big)_M = \Big(\frac{\eta_1}{(\alpha)}\Big)_M$. Then using the general $p$th reciprocity law (see e.g. [**Gr2**], II.7.4.4) we obtain, since $\eta_1$ is a unit,

$$\Big(\frac{\eta_1}{\alpha}\Big)_M = \Big(\frac{\eta_1}{\alpha}\Big)_M \Big(\frac{\alpha}{\eta_1}\Big)_M^{-1} = \prod_{\mathfrak{P}\,|\,p} (\eta_1, \alpha)_{\mathfrak{P}}^{-1},$$

product over the prime ideals $\mathfrak{P}$ of $M$ lying above $p$; since $M/L$ is totally ramified at $p$, we shall write by abuse $(\eta_1, \alpha)_{\mathfrak{p}}$ for these Hilbert symbols, where $\mathfrak{p}\,|\,p$ in $L$, knowing that they are defined on $M^\times \times M^\times$ with values in $\mu_p$ (in the literature, two definitions are possible, which give the Hilbert symbol or its inverse; this is the case with the reference [**Ko**] used below, by comparison with ours, see e.g. [**Gr2**], II.7.3.1).

Thus we have obtained

$$\Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M = \prod_{\mathfrak{p}\,|\,p} (\eta_1, \alpha)_{\mathfrak{p}}^{\frac{f}{2}}.$$

We now refer to the Brückner–Vostokov explicit formula proved in [**Ko**], 6.2, Th. 2.99, by giving some details for the convenience of the reader, and using similar notations.

Consider the uniformizing parameter $\pi := \zeta - 1$ of the completions $M_{\mathfrak{P}}$ of $M$ at $\mathfrak{P}\,|\,\mathfrak{p}\,|\,p$. The inertia field is $L_{\mathfrak{p}}$. We need the formal series $t(x) := 1 - (1 + x)^p$, such that $t(\pi) = 0$, for which $t(x)^{-1}$ is the Laurent series

$$-\frac{1}{x^p}\Big(1 - p\,\big(\frac{c_1}{x} + \cdots + \frac{c_{p-1}}{x^{p-1}}\big) + p^2\,\big(\frac{c_1}{x} + \cdots + \frac{c_{p-1}}{x^{p-1}}\big)^2 - \cdots\Big),$$

where the $c_i$ are integers.

We associate with $\eta_1 \equiv 1 + \theta\,\pi \pmod{\pi^2}$, where $\theta := \frac{1}{2}\frac{\xi-1}{\xi+1}$ (see Subsection 4.1), and with $\alpha = 1 + p\,\beta$, the series

$$F(x) \equiv 1 + \theta\,x \pmod{(x^2)},$$
$$G(x) := 1 + p\,\beta \text{ (a constant series)},$$

such that $F(\pi) \equiv \eta_1 \pmod{\pi^2}$ and $G(\pi) = \alpha$. Recall that log is the $p$-adic logarithm and dlog the logarithmic derivative; so $\mathrm{dlog}(G) = 0$ giving

$$(F, G) = -\frac{1}{p^2} \cdot \log\Big(\frac{G^p}{\sigma_p(G)}\Big) \cdot \mathrm{dlog}(\sigma_p(F)),$$

where $\sigma_p$ is the Frobenius automorphism in $L_{\mathfrak{p}}/\mathbb{Q}_p$ extended to series by putting $\sigma_p(x) := x^p$. Thus $\sigma_p(G) = 1 + p\,\sigma_p(\beta)$, $\sigma_p(F) \equiv 1 + \sigma_p(\theta)\,x^p \pmod{(x^{2p})}$, giving

$$\log\Big(\frac{G^p}{\sigma_p(G)}\Big) \equiv -p\,\sigma_p(\beta) \pmod{p^2}$$
$$\mathrm{dlog}(\sigma_p(F)) \equiv p\,\sigma_p(\theta)\,x^{p-1} \pmod{(x^{2p}, p\,x^{2p-1})},$$

and finally

$$(F, G) \equiv \sigma_p(\theta\,\beta)\,x^{p-1} \pmod{\big(p\,x^{p-1},\, x^{2p-1},\, \frac{x^{2p}}{p}\big)}.$$

Then the residue of $t(x)^{-1}\,(F,G)$ is that of

$$-\frac{1}{x^p}\,\sigma_p(\theta\,\beta)\,x^{p-1} = -\frac{1}{x}\,\sigma_p(\theta\,\beta) \pmod{\big(\tfrac{p}{x}, x^{p-1}, \tfrac{x^p}{p}\big)}\,,$$

hence it is $-\sigma_p(\theta\,\beta) \pmod{p}$ since the generator $\dfrac{x^p}{p}$ of the above ideal gives rise to a residue only with a term of the form $\frac{c_0}{x^{p+1}}$ of $t(x)^{-1}$ (to give $\dfrac{c_0}{p\,x}$) in which case $c_0$ is a multiple of $p^2$ (see the expression of $t(x)^{-1}$). To conclude we have to take the absolute local trace, which eliminates the action of the Frobenius automorphism and gives

$$\mathrm{Tr}_{M_{\mathfrak{P}}/\mathbb{Q}_p}(-\theta\,\beta) = (p-1)\,\mathrm{Tr}_{L_{\mathfrak{p}}/\mathbb{Q}_p}(-\theta\,\beta) \equiv \mathrm{Tr}_{L_{\mathfrak{p}}/\mathbb{Q}_p}(\theta\,\beta) \pmod{p}\,.$$

Then $\big(\eta_1,\alpha\big)_{\mathfrak{p}} = \zeta^{-\mathrm{Tr}_{L_{\mathfrak{p}}/\mathbb{Q}_p}\left(\frac{1}{2}\frac{\xi-1}{\xi+1}\,\beta\right)}$ because of our definition of the Hilbert symbol, and $\prod_{\mathfrak{p}}\big(\eta_1,\alpha\big)_{\mathfrak{p}} = \zeta^{-\sum_{\mathfrak{p}}\mathrm{Tr}_{L_{\mathfrak{p}}/\mathbb{Q}_p}\left(\frac{1}{2}\frac{\xi-1}{\xi+1}\,\beta\right)} = \zeta^{-\mathrm{Tr}_{L/\mathbb{Q}}\left(\frac{1}{2}\frac{\xi-1}{\xi+1}\,\beta\right)}$, the global trace being the sum of the local ones. We have $\dfrac{1}{2}\dfrac{\xi-1}{\xi+1}\,\beta = \big(\dfrac{1}{2} - \dfrac{1}{\xi+1}\big)\,\beta$, so the final expression of the trace is $-\,\mathrm{Tr}_{L/\mathbb{Q}}\big(\dfrac{\beta}{\xi+1}\big)$ since that of $\beta$ is zero modulo $p$. This yields

$$\Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M = \prod_{\mathfrak{p}}\big(\eta_1,\alpha\big)_{\mathfrak{p}}^{\frac{f}{2}} = \zeta^{\frac{1}{2}f\,\mathrm{Tr}_{L/\mathbb{Q}}\left(\frac{\beta}{\xi+1}\right)}\,.$$

We have obtained the following explicit formula.

***Theorem 5.6***. — *Let $q \neq p$ be a prime, let $n$ be such that $n > 2$ and $p \nmid n$. Let $\xi$ be a primitive* $n$th *root of unity and let $\mathfrak{q}$ be any prime ideal of $L = \mathbb{Q}(\mu_n)$ lying above $q$.*
*Let us assume that the class of $\mathfrak{q}^{1-c}$ (where $c$ is the complex conjugation) is the* $p$th *power of a class, which is equivalent to $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(1+p\,\beta)$ for an ideal $\mathfrak{a}$ of $L$ and $\beta$ $p$-integer of $L$.*[10]
*Put $\eta_1 := (1+\xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}$ (see Definition 3.2). Then for any $\mathfrak{Q}\,|\,\mathfrak{q}$ in $M := LK$ we have*

$$\Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M = \zeta^{\frac{1}{2}f\,\mathrm{Tr}_{L/\mathbb{Q}}\left(\frac{\beta}{\xi+1}\right)}\,,$$

*where $f$ is the residue degree of $q$ in $K/\mathbb{Q}$ and $\mathrm{Tr}_{L/\mathbb{Q}}$ the absolute trace in $L/\mathbb{Q}$.*

This gives again the situation of Theorem 5.1 when $\beta \equiv \beta^+ \pmod{p}$, $\beta^+ \in L^+$, since we then have $\mathrm{Tr}_{L/\mathbb{Q}}\big(\frac{\beta}{\xi+1}\big) \equiv \mathrm{Tr}_{L^+/\mathbb{Q}}\big(\frac{\beta^+}{\xi+1} + \frac{\beta^+}{\xi^{-1}+1}\big) = \mathrm{Tr}_{L^+/\mathbb{Q}}(\beta^+) \equiv 0 \pmod{p}$, since $\mathrm{Tr}_{L/\mathbb{Q}}(\beta) \equiv 0 \pmod{p}$.

This theorem confirms that the class field theory properties of the fields $\mathbb{Q}(\mu_n)$ are independent of the SFLT problem. Meanwhile, under a nontrivial solution $(u,v)$ of the SFLT equation, for suitable values of $q$ and for $\xi$ of order $n$ (the order of $\rho := \frac{v}{u}$ modulo $q$), the quantity $\mathrm{Tr}_{L/\mathbb{Q}}\big(\frac{\beta_{\rho,\xi}}{\xi+1}\big)$, where $\beta_{\rho,\xi}$ corresponds to $\mathfrak{q}_{\rho,\xi}$, is imposed, which yields infinitely many conditions.

But as usual we need to explain how the case $p = 3$ interferes appropriately with the arithmetic of the fields $\mathbb{Q}(\mu_n)$ (see Section 8).

[10] As we know, this condition is also equivalent to $\mathfrak{q} = \mathfrak{b}^{1+c}\mathfrak{a}'^{p}\,(1+p\,\beta')$ for ideals $\mathfrak{a}'$, $\mathfrak{b}$ of $L$ and $\beta'$ $p$-integer of $L$. It is satisfied as soon as the class of $\mathfrak{q}^{1-c}$ is of order prime to $p$.

***Remark 5.7***. — Suppose, as in Theorem 5.6, that $\mathfrak{q}^{1-c} = \mathfrak{a}^p\,(1+p\,\beta)$ for an ideal $\mathfrak{a}$ of $L$ and $\beta$ $p$-integer of $L = \mathbb{Q}(\mu_n)$, with $n \,|\, q-1$ such that $n > 2$ and $p \nmid n$.
(i) To obtain that $\mathfrak{q}$ totally splits in $F_n/L$, we study the equivalent condition $\left(\frac{\eta_1^t}{\mathfrak{Q}}\right)_M = 1$ for all $t \in \mathrm{Gal}(M/K)/\langle\, t_{-1}\,\rangle$; from the theorem this is equivalent, for all $t \in \mathrm{Gal}(L/\mathbb{Q})/\langle\, t_{-1}\,\rangle$, to

$$\mathrm{Tr}_{L/\mathbb{Q}}\big(\frac{\beta}{\xi^t+1}\big) = \mathrm{Tr}_{L/\mathbb{Q}}\big(\frac{\beta^{t^{-1}}}{\xi+1}\big) \equiv 0 \pmod{p}\,.$$

This can be written in the following two forms

$$\sum_{\tau\in\mathrm{Gal}(L/\mathbb{Q})} \frac{\beta^\tau}{\xi^{t\tau}+1} \equiv 0 \pmod{p}, \quad \text{for all } t \in \mathrm{Gal}(L/\mathbb{Q})/\langle\, t_{-1}\,\rangle\,.$$

$$\sum_{\tau\in\mathrm{Gal}(L/\mathbb{Q})} \frac{\beta^{t^{-1}\tau}}{\xi^{\tau}+1} \equiv 0 \pmod{p}, \quad \text{for all } t \in \mathrm{Gal}(L/\mathbb{Q})/\langle\, t_{-1}\,\rangle\,.$$

So we obtain two linear systems (with "variables" $\beta^\tau$ and $\frac{1}{\xi^\tau+1}$, respectively), whose matrices have $\phi(n)$ columns and $\frac{1}{2}\,\phi(n)$ lines; the rank over $\mathbb{F}_p$ of the first matrix (less than or equal to $\frac{1}{2}\,\phi(n)$) leads to a more precise approach of the required conditions on $\beta$; the condition $\beta \equiv \beta^+ \pmod{p}$ is sufficient (use the second system) but not necessary as soon as the rank of the matrix is less than $\frac{1}{2}\,\phi(n)$.
(ii) Let $Z'_L$ be the ring of $p$-integers of $L$. Then the knowledge of the image of $\beta$ in $Z'_L/p\,Z'_L$ summarizes all the needed local properties of $\eta_1$ at $p$. Since $Z'_L/p\,Z'_L$ is the product of the residue fields of $L$ at the primes $\mathfrak{p} \,|\, p$ in $L$, any analytic approach is available.
The trace map $Z'_L/p\,Z'_L \longrightarrow \mathbb{F}_p$ is surjective and its kernel of index $p$ in $Z'_L/p\,Z'_L$.

***Example 5.8***. — *Take $p = 5$, $q \neq 5$ a prime congruent to 1 modulo 4, and $n = 4$. Set as usual $q = a^2 + b^2$; then $\mathfrak{q} = (a + i\,b)$ and $\mathfrak{q}^4 = (A + i\,B)$, with $A = a^4 + b^4 - 6\,a^2b^2$, $B = 4\,ab(a^2 - b^2)$. We then have*

$$\mathfrak{q}^{1-c} = \mathfrak{q}^{5(1-c)}\Big(\frac{A - i\,B}{A + i\,B}\Big) =: \mathfrak{q}^{5(1-c)}\big(1 + 5\,\beta\big)\,.$$

*Since $A + i\,B \equiv 1 \pmod{5}$, we get $A \equiv 1$ and $B \equiv 0 \pmod{5}$, and a straightforward computation gives*

$$\beta \equiv -\frac{8\,i\,ab(a^2-b^2)}{5} \quad \text{and} \quad \frac{\beta}{i+1} \equiv -\frac{4\,(i+1)\,ab(a^2-b^2)}{5} \pmod{5}\,,$$

*which yields $\frac{1}{2}\mathrm{Tr}_{L/\mathbb{Q}}\big(\frac{\beta}{i+1}\big) \equiv -\frac{1}{2}\frac{8\,ab(a^2-b^2)}{5} \pmod{5}$, hence $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \zeta^{f\,\frac{ab(a^2-b^2)}{5}}$.*
*So the symbol is trivial if and only if $ab(a^2 - b^2) \equiv 0 \pmod{25}$. We find the values $q = 313$ $(a = 13,\ b = 12)$, $q = 317$ $(a = 14,\ b = 11)$, ...*
*For $q = 457$ $(a = 21,\ b = 4)$, we have $\kappa \equiv 0 \pmod{5}$. A case with $25 \,|\, ab$ is given by $q = 641$ $(a = 25,\ b = 4)$.*
*The symbol is nontrivial for the values $q = 13$ $(a = 3,\ b = 2)$ where $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \zeta^4$, $q = 17$ $(a = 4,\ b = 1)$ where $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \zeta^3, \ldots$*

## 6. Decomposition law of $q$ in $H_{\mathbb{Q}(\mu_{q-1})}[p]/\mathbb{Q}(\mu_{q-1})$ and conjectures

In this section we study in full generality the situations that we have encountered in the previous sections.

**6.1. Law of $\rho$-decomposition relative to the family $\mathcal{F}_n$ and Main Theorem.** — Let $p > 2$ be a prime and let $\rho = \frac{v}{u}$, with g.c.d. $(u, v) = 1$, be a rational distinct from 0 and $\pm 1$; this is *equivalent* to $u\,v\,(u^2 - v^2) \neq 0$. Since $u, v$ play a symmetrical role, it would be actually better to consider that $\rho \in \mathbb{Q} \cup \{\infty\}$ and that it is taken distinct from $\infty, 0, \pm 1$.

For now we do not suppose any relation of SFLT type between $u$ and $v$.

For any prime $q \neq p$ let $f$ be the residue degree of $q$ in $K := \mathbb{Q}(\mu_p)$ and let $\kappa := \frac{q^f - 1}{p}$.

Note that we have the relation (see Definition 2.13 (i))

$$\overline{\kappa} := \frac{q^{p-1} - 1}{p} \equiv \frac{p-1}{f}\,\kappa \equiv -\frac{1}{p}\log(q) \pmod{p}\,.$$

We consider the *infinite* set of primes

$$Q_\rho := \big\{q \text{ prime},\ q \nmid u\,v\,(u^2 - v^2)\ \&\ \text{the order of } \rho \text{ modulo } q \text{ is prime to } p\big\}\,.$$

For $q \in Q_\rho$, let $n$ be the order of $\rho$ modulo $q$. From Lemma 2.11 and Corollary 2.12, $q \in Q_\rho$ is equivalent to $q \equiv 1 \pmod{n}$ & $q \,|\, \Phi_n(u, v)$ & $n > 2$ prime to $p$. It is also equivalent to $q \equiv 1 \pmod{n}$ & $n > 2$ prime to $p$ & $\mathfrak{q} := (q, u\,\xi - v)$ ($\xi$ of order $n$) prime ideal of $\mathbb{Q}(\mu_n)$ lying above $q$.

The prime ideal $\mathfrak{q}$ is also denoted by $\mathfrak{q}_{\rho,\xi}$ as in the previous sections.

We associate with $q$ the class $\mathcal{C}_\rho(q)$ (see Definition 3.1) defined by the pair $(\xi, \mathfrak{q})$, up to $\mathbb{Q}$-conjugation.

We consider the fields $L := \mathbb{Q}(\mu_n)$ and $M := LK$ which only depend on $q$ (for fixed $\rho$).

Of course, the classes $\mathcal{C}_\rho(q_1)$ and $\mathcal{C}_\rho(q_2)$ corresponding to different primes $q_1$ and $q_2$, are relative to the fields $L_{(1)} = \mathbb{Q}(\mu_{n_1})$, $n_1 \,|\, q_1 - 1$, and $L_{(2)} = \mathbb{Q}(\mu_{n_2})$, $n_2 \,|\, q_2 - 1$, and one of the main problems would be to try to connect the two situations.

From the construction of the extensions $F_\xi$ and $F_n \subseteq H_L^-[p]$ given in Subsections 4.2 and 4.4 via the real $\omega$-cyclotomic unit

$$\eta_1 := (1 + \xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}\,,$$

the pair $(F_\xi, \mathfrak{q}_{\rho,\xi})$ is defined up to $\mathbb{Q}$-conjugation since $(tF_\xi, \mathfrak{q}_{\rho,\xi}^t) = (F_{\xi^t}, \mathfrak{q}_{\rho,\xi^t})$ corresponds to $(\xi^t, \mathfrak{q}_{\rho,\xi^t})$; thus the class of the pair $(F_\xi, \mathfrak{q}_{\rho,\xi})$ (or similarly of the pair $(\eta_1, \mathfrak{Q}_{\rho,\xi} \,|\, \mathfrak{q}_{\rho,\xi})$) characterizes the class $\mathcal{C}_\rho(q)$ and reciprocally. Recall that $F_\xi = F_{\xi^{-1}}$ is diedral over $L^+$.

The following lemma is elementary but gives details on the action of $\mathrm{Gal}(L/\mathbb{Q})$ on the Frobenius automorphism of $\mathfrak{q}_{\rho,\xi}$ in $F_\xi/L$.

***Lemma 6.1.*** — *Let $\rho$ be a rational distinct from 0 and $\pm 1$ and let $(\xi, \mathfrak{q}_{\rho,\xi})$ be a representative pair of the class $\mathcal{C}_\rho(q)$ associated to $q \in Q_\rho$.*
*Let $\varphi_{\rho,\xi} := \left(\frac{F_\xi/L}{\mathfrak{q}_{\rho,\xi}}\right)$ be the Frobenius automorphism of the ideal $\mathfrak{q}_{\rho,\xi} = (q, u\,\xi - v)$ in $F_\xi/L$.*
*(i) Then $\varphi_{\rho,\xi^t} := \left(\frac{F_{\xi^t}/L}{\mathfrak{q}_{\rho,\xi^t}}\right) = \varphi_{\rho,\xi}^t := t' \,.\, \varphi_{\rho,\xi} \,.\, t'^{-1}$ for all $t \in \mathrm{Gal}(L/\mathbb{Q})$.*
*(ii) If $t = t_{-1}$, then $\varphi_{\rho,\xi^{-1}} = \varphi_{\rho,\xi}^{t_{-1}} = t'_{-1} .\, \varphi_{\rho,\xi} \,.\, t'^{-1}_{-1} = \varphi_{\rho,\xi}^{-1}$ in $\mathrm{Gal}(F_\xi/L)$.*

*Proof.* — From the defining congruence $\varphi_{\rho,\xi}(\alpha) \equiv \alpha^q \pmod{\mathfrak{q}_{\rho,\xi}}$ for all integers $\alpha$ of $F_\xi$, we get $t' . \varphi_{\rho,\xi}(\alpha) \equiv t'(\alpha)^q \pmod{\mathfrak{q}_{\rho,\xi^t}}$, for any $\mathbb{Q}$-isomorphism $t'$ of $F_\xi$ such that $t'|_L = t$. Put $t'(\alpha) =: \beta \in F_{\xi^t}$; this yields $t' . \varphi_{\rho,\xi} . t'^{-1}(\beta) \equiv \beta^q \pmod{\mathfrak{q}_{\rho,\xi^t}}$ for all integers $\beta$ of $F_{\xi^t}$, proving the lemma by uniqueness of the Frobenius automorphism.

The case of $t_{-1}$ is obvious since $F_\xi/L^+$ is diedral. □

The Frobenius automorphism of $\mathfrak{q}_{\rho,\xi}$ in $F_\xi/L$ also defines the class $\mathcal{C}_\rho(q)$ since we have $(\xi^t, \varphi^t_{\rho,\xi}) = (\xi^t, \varphi_{\rho,\xi^t})$ by conjugation. This leads to give the following definitions.

***Definition 6.2.*** — Let $\rho := \frac{v}{u}$, with g.c.d. $(u, v) = 1$, be a rational, distinct from 0 and $\pm 1$. For any $n > 2$ prime to $p$, let $L = \mathbb{Q}(\mu_n)$, $M = LK$, and for $\xi$ of order $n$, let $F_\xi$ be such that $F_\xi M = M\big(\sqrt[p]{(1+\xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}}\,\big)$. Put

$$Q_\rho := \big\{q \text{ prime},\ q \nmid u\,v\,(u^2 - v^2)\ \&\ \text{the order of } \rho \text{ modulo } q \text{ is prime to } p\big\}\,.$$

(i) *The symbols* $\left[\frac{F_*/L}{\mathfrak{q}_*}\right]_\rho$. For any prime $q \in Q_\rho$, let $n \mid q-1$ be the order of $\rho$ modulo $q$; for $\mathfrak{q}_{\rho,\xi} = (q, u\,\xi - v) \mid q$, we consider the class of Frobenius automorphisms

$$\left(\frac{F_{\xi^t}/L}{\mathfrak{q}_{\rho,\xi^t}}\right) = \left(\frac{F_\xi/L}{\mathfrak{q}_{\rho,\xi}}\right)^t,\ \ t \in \mathrm{Gal}\,(L/\mathbb{Q})\,,$$

that we normalize in the following way depending on $\kappa := \frac{q^f-1}{p} \equiv f\,\frac{\log(q)}{p} \pmod{p}$:

– if $\kappa \not\equiv 0 \pmod{p}$, we put $\left[\frac{F_*/L}{\mathfrak{q}_*}\right]_\rho := \left(\left(\frac{F_{\xi^t}/L}{\mathfrak{q}_{\rho,\xi^t}}\right)^{\frac{p}{\log(q)}}\right)_{t\in\mathrm{Gal}\,(L/\mathbb{Q})}$;

– if $\kappa \equiv 0 \pmod{p}$, we put $\left[\frac{F_*/L}{\mathfrak{q}_*}\right]_\rho := \left(\left(\frac{F_{\xi^t}/L}{\mathfrak{q}_{\rho,\xi^t}}\right)\right)_{t\in\mathrm{Gal}\,(L/\mathbb{Q})}$.

(ii) *The canonical family* $\mathcal{F}_n$. For any $n > 2$ prime to $p$, call $\mathcal{F}_n$ the canonical family

$$(F_{\xi^t})_{t\in\mathrm{Gal}(L/\mathbb{Q})} = (F_{\xi'})_{\xi' \text{ of order } n}$$

defining $F_n \subseteq H^-_L[p]$ as the compositum of the $F_{\xi^t}$, $t \in \mathrm{Gal}(L/\mathbb{Q})$.

(iii) *Law of $\rho$-decomposition of $q$ for $\mathcal{F}_n$.* The symbol $\left[\frac{F_*/L}{\mathfrak{q}_*}\right]_\rho$ is called, by abuse of language, the *law of $\rho$-decomposition of $q$ for the family $\mathcal{F}_n$.* If $\left[\frac{F_*/L}{\mathfrak{q}_*}\right]_\rho = 1$ $\Big($resp. $\left[\frac{F_*/L}{\mathfrak{q}_*}\right]_\rho \neq 1$ $\Big)$, we speak of *$\rho$-splitting* (resp. *$\rho$-inertia) of $q$ for $\mathcal{F}_n$.*

***Remark 6.3.*** — The terminology "*$\rho$-decomposition of $q$ for $\mathcal{F}_n$*" is justified by what follows, where $n$ is the order of $\rho$ modulo $q \in Q_\rho$ and $L = \mathbb{Q}(\mu_n)$, $n$ assumed $> 2$.

For fixed $\xi$ of order $n$ we look at the law of decomposition, in $F_\xi/L$, of the only prime ideal $\mathfrak{q}_{\rho,\xi} = (q, u\,\xi - v)$; this ideal, which then depends on the class of $\rho$ modulo $q$, is *one* of the $\phi(n)$ prime ideals of $L$ lying above $q$. These prime ideals are the ideals $\mathfrak{q}_i := (q, \xi - e_i)$, for the $\phi(n)$ integers $e_i$ of order $n$ modulo $q$; then the law of decomposition of $q$ in the whole extension $F_n/\mathbb{Q}$ is characterized by means of the values of the $\phi(n)$ Frobenius automorphisms $\left(\frac{F_\xi/L}{\mathfrak{q}_i}\right)$, $i = 1, ..., \phi(n)$. Indeed, these Frobenius automorphisms satisfy, for all $t \in \mathrm{Gal}(L/\mathbb{Q})$ and all $i = 1, ..., \phi(n)$, the relations $\left(\frac{F_{\xi^t}/L}{\mathfrak{q}_i}\right) = \left(\frac{F_\xi/L}{\mathfrak{q}_i^{t^{-1}}}\right)^t = \left(\frac{F_\xi/L}{\mathfrak{q}_j}\right)^t$, for some $j$ depending on $i$

and $t$, which proves the claim. In fact we need less than $\frac{1}{2}\,\phi(n)$ informations since we have the relations $\Big(\frac{F_\xi/L}{\mathfrak{q}_i^{t-1}}\Big) = \Big(\frac{F_\xi/L}{\mathfrak{q}_i}\Big)^{-1}$ (Lemma 6.1 (ii)) and possibly some others if $[F_n : L] < \frac{1}{2}\,\phi(n)$.
Here we only look at the Frobenius automorphism $\Big(\frac{F_\xi/L}{\mathfrak{q}_{i_0}}\Big)$ such that $e_{i_0} \equiv \rho \pmod q$. So $\mathfrak{q}_{i_0} = \mathfrak{q}_{\rho,\xi}$ and by Lemma 6.1 (i) the knowledge of the Frobenius automorphism of $\mathfrak{q}_{\rho,\xi}$ in $F_\xi/L$ does not depend, up to conjugation, on the choice of $\xi$ of order $n$; which defines the $\rho$-decomposition for $\mathcal{F}_n$.
Remark that $n$ is uniquely determined as soon as $q$ is selected in $Q_\rho$.

The above symbol, depending on $\rho$, is for each $q$ relative to a universal family $\mathcal{F}_n$, over $\mathbb{Q}(\mu_n)$, which is independent of any hypothetic nontrivial solution of the SFLT equation.

Let $\sigma$ be a generator of $\mathrm{Gal}(F_\xi/L)$; the automorphism $\Big(\frac{F_\xi/L}{\mathfrak{q}_{\rho,\xi}}\Big)^{\frac{p}{\log(q)}}$ $\Big($resp. $\Big(\frac{F_\xi/L}{\mathfrak{q}_{\rho,\xi}}\Big)\Big)$ is of the form $\sigma^r$, $r \in \mathbb{Z}/p\mathbb{Z}$, so that the symbol $\Big[\frac{F_*/L}{\mathfrak{q}_*}\Big]_\rho$ is the family

$$\big(\sigma^t\big)^r_{t\in \mathrm{Gal}(L/\mathbb{Q})} = \big(t\,.\,\sigma\,.\,t^{-1}\big)^r_{t\in \mathrm{Gal}(L/\mathbb{Q})}\,.$$

Thus the symbol $\Big[\frac{F_*/L}{\mathfrak{q}_*}\Big]_\rho$ can take $p-1$ nontrivial values (called the cases of *$\rho$-inertia of $q$ for $\mathcal{F}_n$*, when $r \not\equiv 0 \pmod p$) and a trivial one (the *$\rho$-splitting of $q$ for $\mathcal{F}_n$*).

In the previous sections, for infinitely many values of $q$ in the case $\kappa \not\equiv 0 \pmod p$, we have used, as a contradiction to the existence of a solution $(x, y, z)$ of Fermat's equation for $p > 3$, the splitting of $\mathfrak{q}_{\frac{v}{u},\xi}$ in $F_\xi$ (taking $(u, v) = (x, y)$ or $(y, z)$). This is equivalent to the $\rho$-splitting of $q \in Q_\rho$ for $\mathcal{F}_n$, with $\rho := \frac{v}{u}$, hence to $\Big[\frac{F_*/L}{\mathfrak{q}_*}\Big]_\rho = 1$.

Same remark for a solution $(u, v)$ of the SFLT equation in the nonspecial cases under the condition $u - v \not\equiv 0 \pmod p$.

***Remark 6.4***. — In a probabilistic point of view, the $\rho$-splitting for $\mathcal{F}_n$ of a fixed $q \in Q_\rho$ has a probability around $\frac{1}{p}$, and we can hope a strong incompatibility for analytic reasons since $Q_\rho$ is infinite.
If we ask that $q$ be totally split in $F_n$, this means that each $\mathfrak{q} \,|\, q$ splits in $F_\xi = F_{\xi^{-1}}$ (for any fixed $\xi$) and the probability is around $\big(\frac{1}{p}\big)^{\frac{1}{2}\,\phi(n)}$ which tends to 0 rapidly with $q \to \infty$.

With a nontrivial counterexample $(u, v)$ to SFLT, we have, from a representative pair $(\xi, \mathfrak{q}_{\rho,\xi})$ of $\mathcal{C}_\rho(q)$, $\rho := \frac{v}{u}$, the following results proved in Theorem 3.3:
For $p \geq 3$ in the nonspecial cases ($u + v \not\equiv 0 \pmod p$) we have, for all $\mathfrak{Q} \,|\, \mathfrak{q}_{\rho,\xi}$,

$$\Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M = \zeta^{-\frac{1}{2}\,\frac{u-v}{u+v}\,\kappa}\,.$$

In the special case ($u + v \equiv 0 \pmod p$) we have, for all $\mathfrak{Q} \,|\, \mathfrak{q}_{\rho,\xi}$,

$$\Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M = 1, \ \text{ if } p > 3, \quad \Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M = \zeta^{\frac{1}{2}\,\frac{u+v}{3\,v}\,\kappa}, \ \text{ if } p = 3\,.$$

Recall that for the first case of SFLT we cannot exclude the case $u-v \equiv 0 \pmod p$ in contrast with FLT for $(u,v) = (x,y)$, $(y,x)$, $(z,y)$, or $(y,z)$. This explain that for SFLT (first case and $\kappa \not\equiv 0 \pmod p$) we cannot use, as a general contradiction, the $\rho$-splitting of $q$ for $\mathcal{F}_n$.

More precisely, we have the following lemma giving the action of the Frobenius automorphism, which determines explicitly the law of $\rho$-decomposition in the SFLT context (we assume for simplicity $p > 3$):

***Lemma 6.5***. — *Let $p$ be a prime $> 3$. We suppose given a nontrivial solution in coprime integers $u, v$ of the SFLT equation $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\, \mathfrak{w}_1^p$ (see Conjecture 2.4).*

*Let $q$ be a prime such that $q \nmid u\,v$, and such that the order $n$ of $\rho := \frac{v}{u}$ modulo $q$ is prime to $p$.*

*Let $\mathfrak{Q} \,|\, \mathfrak{q}_{\rho,\xi}$ in $M$, where $(\xi, \mathfrak{q}_{\rho,\xi})$ represents the class $\mathcal{C}_\rho(q)$.*

*Let $\left(\frac{M(\sqrt[p]{\eta_1}\,)/M}{\mathfrak{Q}}\right)$ be the Frobenius automorphism of $\mathfrak{Q}$ in $M(\sqrt[p]{\eta_1}\,)/M$, where $\eta_1$ is the $\omega$-cyclotomic unit $(1+\xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}$.*

*(i) Nonspecial cases. If $u + v \not\equiv 0 \pmod p$, then $\left(\frac{M(\sqrt[p]{\eta_1}\,)/M}{\mathfrak{Q}}\right) \cdot \sqrt[p]{\eta_1} = \zeta^{-\frac{1}{2}\,\frac{u-v}{u+v}\,\kappa} \cdot \sqrt[p]{\eta_1}$.*

*(ii) Special case. If $u + v \equiv 0 \pmod p$, then $\left(\frac{M(\sqrt[p]{\eta_1}\,)/M}{\mathfrak{Q}}\right) \cdot \sqrt[p]{\eta_1} = \sqrt[p]{\eta_1}$.*

*Proof.* — From the defining congruence $\big(\sqrt[p]{\eta_1}\big)^\sigma \equiv \big(\sqrt[p]{\eta_1}\big)^{q^f} \pmod{\mathfrak{Q}}$, for the Frobenius automorphism $\sigma := \left(\frac{M(\sqrt[p]{\eta_1}\,)/M}{\mathfrak{Q}}\right)$, we get $\big(\sqrt[p]{\eta_1}\big)^{\sigma-1} \equiv \big(\sqrt[p]{\eta_1}\big)^{q^f-1} \equiv \eta_1^\kappa \equiv \left(\frac{\eta_1}{\mathfrak{Q}}\right)_M \pmod{\mathfrak{Q}}$. Hence the result since $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \zeta^{-\frac{1}{2}\,\frac{u-v}{u+v}\,\kappa}$ in the nonspecial cases and $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = 1$ in the special case, as recalled above. □

We now intend, in the following theorem, to translate this property into a property of the symbol $\left[\frac{F_*/L}{\mathfrak{q}_*}\right]_\rho$, which will give the main phenomenon about the existence of a nontrivial solution to the SFLT equation.

***Theorem 6.6***. — *Let $p$ be a prime $> 3$. We suppose given a nontrivial solution in coprime integers $u, v$ of the SFLT equation $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\, \mathfrak{w}_1^p$ (see Conjecture 2.4).*

*For $\rho := \frac{v}{u}$, let $Q_\rho := \big\{q$ prime, $q \nmid u\,v\,(u^2 - v^2)$ & the order of $\rho$ modulo $q$ is prime to $p\big\}$.*

*Then the symbol $\left[\frac{F_*/\mathbb{Q}(\mu_n)}{\mathfrak{q}_*}\right]_\rho$, where $n$ is the order of $\rho$ modulo $q$, only depends on $\rho$ when $q$ varies in $Q_\rho$; for all $q \in Q_\rho$ with $\kappa \equiv 0 \pmod p$, then $\left[\frac{F_*/\mathbb{Q}(\mu_n)}{\mathfrak{q}_*}\right]_\rho = 1$ (see Definition 6.2).*

*In other words, the law of $\rho$-decomposition of any $q \in Q_\rho$ for $\mathcal{F}_n$ only depends on $\rho$*[11].

*Proof.* — Let $\mathfrak{Q} \,|\, \mathfrak{q}_{\rho,\xi}$ in $M$, where $(\xi, \mathfrak{q}_{\rho,\xi})$ represents the class $\mathcal{C}_\rho(q)$. The Frobenius automorphism of $\mathfrak{q}_{\rho,\xi}$ in $F_\xi/L$ is given, by restriction, by the relation $\left(\frac{F_\xi/L}{\mathfrak{q}_{\rho,\xi}}\right)^f = \left(\frac{M(\sqrt[p]{\eta_1}\,)/M}{\mathfrak{Q}}\right)_{|F_\xi}$.

Indeed, in the projection $\mathrm{Gal}(M(\sqrt[p]{\eta_1}\,)/M) \longrightarrow \mathrm{Gal}(F_\xi/L)$, the Frobenius automorphism of $\mathfrak{Q}$ gives the Artin symbol of the norm in $M/L$ of $\mathfrak{Q}$, which is $\mathfrak{q}_{\rho,\xi}^f$; hence the result.

[11] See Remark 6.7 where we better justify the expression " only depends on $\rho$ when $q$ varies in $Q_\rho$ ", since $n$, depending on $\rho$ and $q$, is not constant and since the normalization of the symbol depends on $q$ via $\kappa$

If $\kappa \not\equiv 0 \pmod p$, using the relation $f\,\kappa^{-1} \equiv -\overline{\kappa}^{-1} \pmod p$ (see Definition 2.13 (i)) we get by Lemma 6.5 that $\left(\frac{F_\xi/L}{\mathfrak{q}_{\rho,\xi}}\right)^{-\overline{\kappa}^{-1}} = \left(\frac{M(\sqrt[p]{\eta_1}\,)/M}{\mathfrak{Q}}\right)^{\kappa^{-1}}_{|F_\xi}$ only depends on $\rho$ when $q$ varies. This proves the theorem in this case since $-\overline{\kappa} \equiv \frac{1}{p}\log(q) \not\equiv 0 \pmod p$.
If $\kappa \equiv 0 \pmod p$, we get $\left(\frac{F_\xi/L}{\mathfrak{q}_{\rho,\xi}}\right) = 1$ in any case. □

***Remark 6.7***. — Recall that $\mathbb{Q}_1$ is the cyclic extension of $\mathbb{Q}$ of degree $p$ contained in $\mathbb{Q}(\mu_{p^2})$ and that $L_1 = L\mathbb{Q}_1$. Let $\overline{F}_n := L_1 F_n$ and let $\overline{\varphi}_{\rho,\xi}$ be the Frobenius automorphism $\left(\frac{\overline{F}_n/L}{\mathfrak{q}_{\rho,\xi}}\right)$; we know that $\overline{\varphi}_{\rho,\xi}$ projects on $\varphi_{\rho,\xi} := \left(\frac{F_\xi/L}{\mathfrak{q}_{\rho,\xi}}\right)$ in $F_\xi/L$ and on $\varphi_1 := \left(\frac{L_1/L}{\mathfrak{q}_{\rho,\xi}}\right)$ in $L_1/L$. As in the proof of the theorem, in the projection $\mathrm{Gal}(M(\sqrt[p]{\zeta}\,)/M) \longrightarrow \mathrm{Gal}(L_1/L)$, we obtain (when $\kappa \not\equiv 0 \pmod p$) that $\left(\frac{L_1/L}{\mathfrak{q}_{\rho,\xi}}\right)^{\frac{p}{\log(q)}} = \left(\frac{M(\sqrt[p]{\zeta}\,)/M}{\mathfrak{Q}}\right)^{\kappa^{-1}}_{|L_1}$ is independent of $q$ because of the equality $\left(\frac{M(\sqrt[p]{\zeta}\,)/M}{\mathfrak{Q}}\right)^{\kappa^{-1}} . \sqrt[p]{\zeta} = \zeta \,.\, \sqrt[p]{\zeta}$.

Moreover, this is independent of the choice of $\xi$ (of order $n$) since for all $t \in \mathrm{Gal}(L/\mathbb{Q})$, $\overline{\varphi}_{\rho,\xi^t} = t' \,.\, \overline{\varphi}_{\rho,\xi} \,.\, t'^{-1}$ projects on $\overline{\varphi}_{\rho,\xi^t|_{L_1}} = t' \,.\, \overline{\varphi}_{\rho,\xi|_{L_1}} \,.\, t'^{-1} = t' \,.\, \varphi_1 \,.\, t'^{-1} = \varphi_1$, in $L_1/L$, since $\mathrm{Gal}(L_1/\mathbb{Q})$ is Abelian.

Which justifies the normalization and the fact that, in some sense, under the existence of a nontrivial solution of the SFLT equation, the symbol $\left[\frac{F_*/L}{\mathfrak{q}_*}\right]_\rho$ does not depend essentially on $q$ but on $\rho$. Of course, $n$ and $\kappa$ depend on $q$, but not in a deep arithmetical manner (especially for $\kappa$ taking a finite number of values modulo $p$) and another way to understand this independence is the following: if $q_1$ and $q_2$ are two distinct primes in $Q_\rho$, giving the same value of $n$ and of $\kappa \not\equiv 0 \pmod p$, then $\left[\frac{F_*/L}{\mathfrak{q}_{1*}}\right]_\rho = \left[\frac{F_*/L}{\mathfrak{q}_{2*}}\right]_\rho$ for $\mathcal{F}_n/L$; if $q_1, ..., q_r$ are such that $\kappa_i \equiv 0 \pmod p$, for$1 \le i \le r$, then we have $\left[\frac{F_*/L_i}{\mathfrak{q}_{i*}}\right]_\rho = 1$ for $\mathcal{F}_{n_i}/L_i$, for $1 \le i \le r$.
These facts may constitute an excessive link between these primes.

From Theorem 5.6, assuming that the class of $\mathfrak{q}_{\rho,\xi}^{1-c}$ is the $p$th power of a class, i.e.,

$$\mathfrak{q}_{\rho,\xi}^{1-c} = \mathfrak{a}^p\,(1 + p\,\beta_{\rho,\xi})\,,$$

for an ideal $\mathfrak{a}$ of $L$ and a $p$-integer $\beta_{\rho,\xi}$ of $L$, then $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = \zeta^{\frac{1}{2} f\,\mathrm{Tr}_{L/\mathbb{Q}}\left(\frac{\beta_{\rho,\xi}}{\xi+1}\right)}$, where $\mathrm{Tr}_{L/\mathbb{Q}}$ is the absolute trace in $L/\mathbb{Q}$. So with a counterexample to SFLT we must have

$$\begin{aligned}
\mathrm{Tr}_{L/\mathbb{Q}}\Big(\frac{\beta_{\rho,\xi}}{\xi+1}\Big) \;&\equiv\; -f^{-1}\,\frac{u-v}{u+v}\,\kappa \;\equiv\; -\frac{u-v}{u+v}\,\frac{\log(q)}{p} \pmod p \ \text{ in the nonspecial cases, } p \ge 3,\\
\mathrm{Tr}_{L/\mathbb{Q}}\Big(\frac{\beta_{\rho,\xi}}{\xi+1}\Big) \;&\equiv\; 0 \pmod p \ \text{ in the special case, } p > 3\,.
\end{aligned}$$

This means that, under a nontrivial counterexample $(u, v)$ to SFLT,

$$\Big(\frac{F_\xi/L}{\mathfrak{q}_{\rho,\xi}}\Big)^{\frac{p}{\log(q)}} \quad \& \quad \frac{p}{\log(q)}\,\mathrm{Tr}_{L/\mathbb{Q}}\Big(\frac{\beta_{\rho,\xi}}{\xi+1}\Big), \ \text{if} \ \ \kappa \not\equiv 0 \pmod p,$$
$$\Big(\text{resp.} \quad \Big(\frac{F_\xi/L}{\mathfrak{q}_{\rho,\xi}}\Big) \quad \& \ \ \mathrm{Tr}_{L/\mathbb{Q}}\Big(\frac{\beta_{\rho,\xi}}{\xi+1}\Big), \ \ \text{if} \ \kappa \equiv 0 \pmod p\Big),$$

both equivalent to the knowledge of $\Big[\frac{F_*/L}{\mathfrak{q}_*}\Big]_\rho$, only depend on $\rho = \frac{v}{u}$ for primes $q \in Q_\rho$ and are trivial when $\kappa \equiv 0 \pmod p$.

***Remark 6.8***. — In the context of Fermat's equation with $r = \frac{y}{x}$, $r' = \frac{z}{y}$, $r'' = \frac{x}{z}$ (supposed of orders $n$, $n'$, $n''$ modulo $q$, prime to $p$), we have similar writings to those of Lemma 6.5 by using the $\omega$-cyclotomic units $\eta_1$, $\eta'_1$, $\eta''_1$.

From the relation $x + y + z \equiv 0 \pmod p$, the values of $r'$, $r''$ modulo $p$ can be computed from $r$,[12] and we get the following relations valid for $p \geq 3$.

(i) If $\kappa \not\equiv 0 \pmod p$, then

$$\Big(\frac{M(\sqrt[p]{\eta_1})/M}{\mathfrak{Q}}\Big)^{\kappa^{-1}} \cdot \sqrt[p]{\eta_1} = \zeta^{\frac{1}{2}\frac{r-1}{r+1}} \cdot \sqrt[p]{\eta_1},$$
$$\Big(\frac{M(\sqrt[p]{\eta'_1})/M}{\mathfrak{Q}'}\Big)^{\kappa^{-1}} \cdot \sqrt[p]{\eta'_1} = \zeta^{\frac{1}{2}+r} \cdot \sqrt[p]{\eta'_1},$$
$$\Big(\frac{M(\sqrt[p]{\eta''_1})/M}{\mathfrak{Q}''}\Big)^{\kappa^{-1}} \cdot \sqrt[p]{\eta''_1} = \zeta^{-\frac{1}{2}-\frac{1}{r}} \cdot \sqrt[p]{\eta''_1}, \ \text{if} \ r \not\equiv 0 \pmod p,$$
$$\Big(\frac{M(\sqrt[p]{\eta''_1})/M}{\mathfrak{Q}''}\Big)^{\kappa^{-1}} \cdot \sqrt[p]{\eta''_1} = \sqrt[p]{\eta''_1}, \ \text{if} \ r \equiv 0 \pmod p .$$

(ii) If $\kappa \equiv 0 \pmod p$, the three Frobenius automorphisms $\Big(\frac{M(\sqrt[p]{\bullet})/M}{\bullet}\Big)$ are trivial.

**6.2. Law of $\rho$-decomposition relative to the family $\widehat{\mathcal{F}}_n$.** — We still suppose $p > 3$. We have, under a nontrivial solution $(u, v)$ of the SFLT equation and under the condition $q \nmid u\,v\,(u^2 - v^2)$, the following interpretation of the equality (Theorem 3.3):

$$\Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M = \zeta^{-\frac{1}{2}\frac{u-v}{u+v}\kappa} \ \Big(\text{resp.} \ \Big(\frac{\eta_1}{\mathfrak{Q}}\Big)_M = 1\Big) \ \text{for any} \ \mathfrak{Q} \,|\, \mathfrak{q}_{\rho,\xi}$$

in the nonspecial cases $u + v \not\equiv 0 \pmod p$ (resp. in the special case $u + v \equiv 0 \pmod p$).

Consider the $\omega$-cyclotomic unit $\widehat{\eta}_1 := \eta_1\,\zeta^{\frac{1}{2}\frac{u-v}{u+v}}$ (resp. $\widehat{\eta}_1 := \eta_1$) in the nonspecial cases (resp. in the special case) (see Definition 3.2).

(i) In the nonspecial cases we have $\widehat{\eta}_1 = (1 + \xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}+\frac{1}{2}\frac{u-v}{u+v}} = (1 + \xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{v}{u+v}}$, which is by construction such that $\Big(\frac{\widehat{\eta}_1}{\mathfrak{Q}}\Big)_M = 1$, but the unit $\widehat{\eta}_1$ is not anymore real and canonical; its definition from $\eta_1$ is independent of $q$ under a given solution of the SFLT equation.

[12] The notations $r$, $r'$, $r''$ correspond to $\rho = \frac{v}{u}$ in the equation $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\,\mathfrak{w}_1^p$, for $(u, v) = (x, y)$, $(y, z)$ in the nonspecial cases, then $(u, v) = (z, x)$ in the special case; this explains the changes of notations in the Fermat context. We obtain easily $r' \equiv -1 - \frac{1}{r}$, $r'' \equiv \frac{-1}{r+1} \pmod p$.

(ii) In the special case we have $\widehat\eta_1 := \eta_1 = (1+\xi\,\zeta)^{e_\omega}\,\zeta^{-\frac12}$, which is real and such that $\left(\frac{\widehat\eta_1}{\mathfrak{Q}}\right)_M = 1$.

The extension $M(\sqrt[p]{\widehat\eta_1}\,)/M$ is splitted over $L$ by a $p$-cyclic $p$-ramified extension $\widehat F_\xi$ similar to $F_\xi$ except that it is not diedral over $L^+$ in the nonspecial cases.

We note that the relation $\widehat\eta_1 = \eta_1\,\zeta^{\frac12\,\frac{u-v}{u+v}}$ in the nonspecial cases shows that $\widehat F_\xi$ is a subfield of the compositum $F_\xi L_1$ obtained in an obvious systematic way; $\widehat F_\xi/L$ is still of degree $p$ and $p$-ramified since $n>2$. We have $\widehat F_\xi = F_\xi$ if and only if $u^2-v^2 \equiv 0 \pmod p$.

We still have $t\,.\,\widehat F_\xi = \widehat F_{\xi^t}$. We call $\widehat F_n$ the compositum of the $\widehat F_{\xi^t}$, $t\in \mathrm{Gal}(L/\mathbb{Q})$. Hence $F_n\,L_1 = \widehat F_n\,L_1$. We denote, as in Definition 6.2 (ii), by $\widehat{\mathcal{F}}_n$ the family $(\widehat F_{\xi'})_{\xi' \text{ of order } n}$.

Then under a nontrivial solution $(u,v)$ of the SFLT equation, we must have for $\rho := \frac{v}{u}$ the splitting of $\mathfrak{q}_{\rho,\xi}$ in $\widehat F_\xi$ (i.e., a $\rho$-splitting of $q$ for $\widehat{\mathcal{F}}_n$).

In other words if we define in general, as in Definition 6.2 (i), the symbol

$$\left[\frac{\widehat F_*/L}{\mathfrak{q}_*}\right]_\rho := \left(\left(\frac{\widehat F_{\xi^t}/L}{\mathfrak{q}_{\rho,\xi^t}}\right)^{\frac{p}{\log(q)}}\right)_{t\in\mathrm{Gal}(L/\mathbb{Q})} \text{ if } \kappa\not\equiv 0 \pmod p,$$
$$\left[\frac{\widehat F_*/L}{\mathfrak{q}_*}\right]_\rho := \left(\left(\frac{\widehat F_{\xi^t}/L}{\mathfrak{q}_{\rho,\xi^t}}\right)\right)_{t\in\mathrm{Gal}(L/\mathbb{Q})} \text{ if } \kappa\equiv 0 \pmod p\ ,$$

the analog of Theorem 6.6 is that $\left[\frac{\widehat F_*/L}{\mathfrak{q}_*}\right]_\rho = 1$ for all $q\in Q_\rho$, where

$$Q_\rho := \big\{q \text{ prime},\ q\nmid u\,v\,(u^2-v^2)\ \&\ \text{the order of } \rho \text{ modulo } q \text{ is prime to } p\big\}\,.$$

A contradiction would be that there exist primes $q\in\mathbb{Q}_\rho$ such that $\left[\frac{\widehat F_*/L}{\mathfrak{q}_*}\right]_\rho \neq 1$, i.e., $\mathfrak{q}_{\rho,\xi}$ is inert in $\widehat F_\xi$, which is independent of the representative pair $(\widehat F_{\xi^t},\mathfrak{q}_{\rho,\xi^t})$ (we then speak of “ $\rho$-inertia of $q$ for $\widehat{\mathcal{F}}_n$ ”) and has a probability very near from $\frac{p-1}{p}$ since $p-1$ nontrivial values of the symbol are possible.

Since the rational $\rho$, corresponding to a nontrivial solution $(u,v)$ of the SFLT equation, is in general ineffective, in practice we must be able to find a contradiction with any rational $\rho$, distinct from 0 and $\pm1$, for infinitely many primes $q\in\mathbb{Q}_\rho$, i.e., to prove that $\left[\frac{\widehat F_*/L}{\mathfrak{q}_*}\right]_\rho \neq 1$ for infinitely many primes $q\in\mathbb{Q}_\rho$ (see Conjecture 6.10).

In the context of Fermat's equation, we deduce from the $\omega$-units $\eta_1$, $\eta'_1$, $\eta''_1$ (see Remark 6.8), the $\omega$-units, where $r := \frac{y}{x}\not\equiv \pm1 \pmod p$,

$$\begin{aligned}
&\widehat\eta_1 := (1+\xi\,\zeta)^{e_\omega}\,\zeta^{\frac{-r}{r+1}},\\
&\widehat{\eta'_1} := (1+\xi'\,\zeta)^{e_\omega}\,\zeta^{-r-1},\\
&\widehat{\eta''_1} := (1+\xi''\,\zeta)^{e_\omega}\,\zeta^{\frac1r},\ \text{if } r\not\equiv 0 \pmod p,\\
&\widehat{\eta''_1} := (1+\xi''\,\zeta)^{e_\omega}\,\zeta^{-\frac12},\ \text{if } r\equiv 0 \pmod p\,,
\end{aligned}$$

giving a trivial $p$th power residue symbol at $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, respectively.

We have the same conclusion as above for the extensions $\widehat F_\xi/L$, $\widehat F_{\xi'}/L'$, $\widehat F_{\xi''}/L''$ defined from $M\big(\sqrt[p]{\widehat\eta_1}\,\big)/M$, $M'\big(\sqrt[p]{\widehat{\eta'_1}}\,\big)/M'$, $M''\big(\sqrt[p]{\widehat{\eta''_1}}\,\big)/M''$.

Returning to SFLT with a nontrivial solution $(u, v)$, we put, for $\rho := \frac{v}{u}$,

$$\begin{aligned} Q_\rho^{\rm spl} &:= \big\{q \in Q_\rho,\ \kappa \not\equiv 0 \pmod p\ \&\ q \text{ has a } \rho\text{-splitting for } \mathcal{F}_n\big\},\\ \widehat{Q}_\rho^{\rm in} &:= \big\{q \in Q_\rho,\ \kappa \not\equiv 0 \pmod p\ \&\ q \text{ has a } \rho\text{-inertia for } \widehat{\mathcal{F}}_n\big\}. \end{aligned}$$

***Lemma 6.9.*** — *Let $p$ be a prime, $p > 3$. If $u^2 - v^2 \not\equiv 0 \pmod p$ then we have $Q_\rho^{\rm spl} \subseteq \widehat{Q}_\rho^{\rm in}$. If $u^2 - v^2 \equiv 0 \pmod p$ then we have $Q_\rho^{\rm spl} \cap \widehat{Q}_\rho^{\rm in} = \emptyset$.*

*Proof.* — We know that $\widehat{F}_\xi$ is contained in the compositum $L_1F_\xi$, is distinct from $L_1$ since $\xi \neq \pm 1$, and that $\widehat{F}_\xi = F_\xi$ if and only if $u^2 - v^2 \equiv 0 \pmod p$.

Suppose that $\widehat{F}_\xi$ is distinct from $F_\xi$; if $q \in Q_\rho^{\rm spl}$, $\mathfrak{q}_{\rho,\xi}$ splits in $F_\xi/L$ and the Frobenius automorphism of $\mathfrak{q}_{\rho,\xi}$ in $L_1F_\xi/L$ fixes $F_\xi$ and since this Frobenius automorphism must be nontrivial in $L_1/L$ ($\kappa \not\equiv 0 \pmod p$) then it projects to a nontrivial Frobenius automorphism in $\widehat{F}_\xi/L$. When $\widehat{F}_\xi = F_\xi$, the result is clear. □

It would be interesting to examine the problem of the law of $\rho$-decomposition of $q$ for $\mathcal{F}_n$ for arbitrary $\rho$ independently of any equation giving exceptional values of $\rho$.

The natural conjecture in this direction is the following; we consider two situations, both implying FLT: the first one, using the family $\mathcal{F}_n$, implies SFLT in the nonspecial cases under the supplementary assumption $u - v \not\equiv 0 \pmod p$, the second one, using the family $\widehat{\mathcal{F}}_n$, implies SFLT unconditionally.

To simplify the notations we still put $K = \mathbb{Q}(\mu_p)$, $L = \mathbb{Q}(\mu_n)$, $M = LK$.

***Conjecture 6.10.*** — *Let $p$ be a prime $> 3$, and let $\rho = \frac{v}{u}$, with g.c.d.$(u, v) = 1$, be a rational distinct from $0$ and $\pm 1$. Put:*

$$Q_\rho := \big\{q \text{ prime},\ q \nmid u\,v\,(u^2 - v^2)\ \ \&\ \text{ the order of } \rho \text{ modulo } q \text{ is prime to } p\big\}.$$

*(i) Nonspecial cases ($u + v \not\equiv 0 \pmod p$, $\kappa \not\equiv 0 \pmod p$). Let $q \in Q_\rho$ be such that $\kappa \not\equiv 0 \pmod p$, let $n$ be the order of $\rho$ modulo $q$, and let $\mathcal{F}_n$ be the family $\big(F_{\xi'}\big)_{\xi' \text{ of order } n}$ of the $p$-cyclic extensions of $L$ in $H_L^-[p]$, defined by the identity $F_{\xi'}K = M\big(\sqrt[p]{(1+\xi'\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}}\,\big)$.*

*Say that $q$ has a $\rho$-splitting for $\mathcal{F}_n$ if $\Big[\frac{F_*/L}{\mathfrak{q}_*}\Big]_\rho = 1$, i.e., $\mathfrak{q}_{\rho,\xi} := (q, u\,\xi - v)$ splits in $F_\xi/L$ (condition independent of the choice of $\xi$ of order $n$).*

*Then the set of primes $q \in Q_\rho$ having a $\rho$-splitting for $\mathcal{F}_n$, is infinite.*

*(ii) Nonspecial and special cases with arbitrary $\kappa$. Let $q \in Q_\rho$, let $n$ be the order of $\rho$ modulo $q$, and let $\widehat{\mathcal{F}}_n$ be the family $\big(\widehat{F}_{\xi'}\big)_{\xi' \text{ of order } n}$ of the $p$-cyclic extensions of $L$ in $H_L[p]$, defined by the identity $\widehat{F}_{\xi'}K = M\big(\sqrt[p]{(1+\xi'\,\zeta)^{e_\omega}\,\zeta^{-\frac{v}{u+v}}}\,\big)$ if $u + v \not\equiv 0 \pmod p$, and by $\widehat{F}_{\xi'}K = M\big(\sqrt[p]{(1+\xi'\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}}\,\big)$ otherwise.*

*Say that $q$ has a $\rho$-inertia for $\widehat{\mathcal{F}}_n$ if $\Big[\frac{\widehat{F}_*/L}{\mathfrak{q}_*}\Big]_\rho \neq 1$, i.e., $\mathfrak{q}_{\rho,\xi} := (q, u\,\xi - v)$ is inert in $\widehat{F}_\xi/L$ (condition independent of the choice of $\xi$ of order $n$).*

*Then the set of primes $q \in Q_\rho$ having a $\rho$-inertia for $\widehat{\mathcal{F}}_n$, is infinite.*

***Remark 6.11***. — Recall that to prove the first case of FLT for $p$, the existence of a unique $q \in Q_\rho$ with $\kappa \not\equiv 0 \pmod p$ ($\rho = \frac{y}{x}$ or $\frac{z}{y}$, for a solution $(x, y, z)$ of Fermat's equation) having a $\rho$-splitting for $\mathcal{F}_n$ is sufficient, in contrast with the second case which needs in practice infinitely many such primes since $\rho$ is ineffective.

In the first case, $p \nmid xy\,(x^2 - y^2)$ (by Lemma 2.2) and so, if $\kappa \not\equiv 0 \pmod p$ then $q \nmid xy\,(x^2 - y^2)$ by the two theorems of Furtwängler (Corollaries 2.15, 2.16, and Remark 3.5).

Hence $q \in Q_\rho$ as soon as $\kappa \not\equiv 0 \pmod p$ & $q \not\equiv 1 \pmod p$ and it is possible to check the existence of a suitable $q$ as follows in the spirit of Example 5.3. Let $p$ be a large prime and let $q$ be a small prime ($q = 5, 7, 11, \ldots$), so that the above two conditions are in general trivially satisfied. Then as soon as, for all $n \,|\, q - 1$, $n > 2$, the $\omega$-cyclotomic unit $\eta_1 = (1 + \xi\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}$ (for fixed $\xi$ of order $n$) is locally a $p$th power at every prime ideal $\mathfrak{q} \,|\, q$, the first case of FLT is true for $p$.

The second case supposes to find $q$ large enough, hence this method does not work and needs at least analytic reasonings.

If we examine, for logical reasons, the case $p = 3$ for SFLT, we know that for any of the six families of solutions $(u, v)$ of the SFLT equation (see Remark 2.6), we have by Theorem 3.3 (supposing $\kappa \not\equiv 0 \pmod 3$ and defining $\widehat{\eta}_1$ in an analogous way to get a trivial symbol):

(i) $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = j^{-\frac{1}{2}\,\frac{u-v}{u+v}\,\kappa} = 1$, in the first case (i.e., $u\,v\,(u + v) \not\equiv 0 \pmod 3$ which implies $u - v \equiv 0 \pmod 3$), hence $\widehat{\eta}_1 = \eta_1$ and $\widehat{F}_\xi = F_\xi$;

(ii) $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = j^{\pm\frac{1}{2}\,\kappa}$ in the second case ($u\,v \equiv 0 \pmod 3$), thus $\widehat{\eta}_1 = \eta_1\,j^{\mp\frac{1}{2}}$ and $\widehat{F}_\xi \neq F_\xi$;

(iii) $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = j^{\frac{1}{2}\,\frac{u+v}{3\,v}\,\kappa}$ in the special case ($u + v \equiv 0 \pmod 3$) for which $\widehat{\eta}_1 = \eta_1\,j^{-\frac{1}{2}\,\frac{u+v}{3\,v}}$ and $\widehat{F}_\xi = F_\xi$ if and only if $u + v \equiv 0 \pmod 9$.

Note that $\widehat{F}_\xi$ associated to $\widehat{\eta}_1$ is in general distinct from the "simplest cyclic cubic field" $F_\xi^{sh}$, associated to $\eta_1^{sh} = (1 + \xi\,j)^{e'_\omega}$, defined in Subsection 5.3, with $e'_\omega = s + 2$.

If $u + v \equiv 0 \pmod 3$ and $u + v \not\equiv 0 \pmod 9$ then, for $\rho := \frac{v}{u}$, we get $Q_\rho^{\rm spl} \subseteq \widehat{Q}_\rho^{\rm in}$; if $u + v \equiv 0 \pmod 9$ or $u - v \equiv 0 \pmod 3$ then $Q_\rho^{\rm spl} \cap \widehat{Q}_\rho^{\rm in} = \emptyset$.

We see that $u - v \equiv 0 \pmod 3$ in case (i), $u\,v \equiv 0 \pmod 3$ in case (ii); for (iii), we verify from Remark 2.6 that $\rho \in \{-1, 2, 5\}$ modulo 9, which leads to $\frac{1}{2}\,\frac{u+v}{3\,v} \in \{0, 1, 2\}$ modulo 3.

See Section 8 to go thoroughly into the exceptional case $p = 3$.

**6.3. Construction of universal Abelian polynomials.** — In this subsection we intend to give equivalent conditions to those studied in the previous subsections, with a polynomial formalism over $\mathbb{Q}$.

The group $g = \mathrm{Gal}(K/\mathbb{Q})$ acts canonically on the field $K(Y)$ of rational fractions in the indeterminate $Y$. Consider

$$\eta_1(Y) := (1 + Y\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}} \in K(Y)\,.$$

Then if $s = s_r$ is a generator of $g$ we have

$$s\,.\,\eta_1(Y) := \big((1 + Y\,\zeta^s)\,\zeta^{-\frac{1}{2}s}\big)^{e_\omega} = \big((1 + Y\,\zeta)\,\zeta^{-\frac{1}{2}}\big)^{s\,e_\omega} = \big((1 + Y\,\zeta)\,\zeta^{-\frac{1}{2}}\big)^{r e_\omega + p\Lambda}\,,$$

since $s_r\, e_\omega = r\, e_\omega + p\,\Lambda$ for some $\Lambda \in \mathbb{Z}[g]$ (see Definition 2.8 (iii)). Then we obtain

$$s\,.\,\eta_1(Y) = \eta_1(Y)^r \,\cdot\, \big((1+Y\,\zeta)\,\zeta^{-\frac{1}{2}}\big)^{p\Lambda}\,.$$

Consider the Kummer extension $K(Y)(\sqrt[p]{\eta_1(Y)}\,)/K(Y)$; since this extension is Abelian over $\mathbb{Q}(Y)$, the $K(Y)$-automorphism of $K(Y)(\sqrt[p]{\eta_1(Y)}\,)$, still denoted by $s$, defined by

$$s \cdot \sqrt[p]{\eta_1(Y)} := (\sqrt[p]{\eta_1(Y)}\,)^r \,\cdot\, \big((1+Y\,\zeta)\,\zeta^{-\frac{1}{2}}\big)^{\Lambda},$$

is of order $p-1$ and it is a classical result that the trace $\Psi := \sum_{k=1}^{p-1} s^k \cdot \sqrt[p]{\eta_1(Y)}$, denoted by $\mathrm{Tr}_{M/L}\big(\sqrt[p]{\eta_1(Y)}\,\big)$ by abuse, defines a primitive element of the subextension cyclic of degree $p$ contained in $K(Y)(\sqrt[p]{\eta_1(Y)}\,)/\mathbb{Q}(Y)$, that we denote by $F_Y$, so that the specializations $Y \mapsto \xi$ define the extensions $F_\xi/\mathbb{Q}(\xi)$ (see Subsection 4.2).

For instance, for $p=3$, $e_\omega = s-1$, $s=s_2$, $s\,e_\omega = 1-s = -e_\omega$ (thus $r=2$, $\Lambda = -e_\omega$), $\eta_1(Y) = (1+Y\,j)^{e_\omega} j^{-\frac{1}{2}} = ((1+Y\,j)\,j^{-\frac{1}{2}})^{s-1}$. We have $\Psi = \Big(\dfrac{(1+Y\,j^2)\,j}{1+Y\,j}\Big)^{\frac{1}{3}} + \Big(\dfrac{(1+Y\,j)\,j^2}{1+Y\,j^2}\Big)^{\frac{1}{3}}$, for which $\Psi^3 = \dfrac{(1+Y\,j^2)\,j}{1+Y\,j} + \dfrac{(1+Y\,j)\,j^2}{1+Y\,j^2} + 3\,\Psi$, giving the irreducible polynomial defining $F_Y$

$$P_Y := \mathrm{Irr}(\Psi, \mathbb{Q}(Y)) = X^3 - 3\,X + \frac{Y^2-4Y+1}{Y^2-Y+1},\ \text{ of discriminant } \Big(\frac{9\,(Y^2-1)}{Y^2-Y+1}\Big)^2.$$

For $e'_\omega = s+2$ instead of $e_\omega = s-1$ and $\eta'_1(Y) := (1+Y\,j)^{e'_\omega} j^{-\frac{1}{2}}$, we obtain the monic polynomial

$$X^3 - 3\,(Y^2-Y+1)\,X + Y^3 + 1$$

of $\mathbb{Z}[Y][X]$ which defines the same field $F_Y$; so, to simplify, we still denote it by $P_Y$.

For $\eta_1^{sh}(Y) := (1+Y\,j)^{e'_\omega}$ we obtain $X^3 - 3\,(Y^2-Y+1)\,X + (Y-2)(Y^2-Y+1)$; then with the linear transformation $X \mapsto YX-1$) we get the polynomial

$$P_Y^{sh} := X^3 - 3\,Y^{-1}\,X^2 - 3\,(1-Y^{-1})\,X + 1$$

defining the field $F_Y^{sh}$, then defining, by specialization $Y \mapsto \xi$, the "simplest cyclic cubic fields" $F_\xi^{sh}$ over $\mathbb{Q}(\xi)$ used in Subsection 5.3.

***Definition 6.12.*** — (i) The general polynomial of degree $p$ obtained from the Kummer radical $\eta_1(Y) = (1+Y\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}}$, and denoted by

$$P_Y := X^p + A_{p-1}(Y)X^{p-1} + \cdots + A_0(Y),\, A_i(Y) \in \mathbb{Q}(Y)\,,$$

will be called the universal Abelian polynomial of degree $p$ for the SFLT problem; it defines $F_Y$. We denote by $P_\xi$ (resp. $P_\rho$) the Abelian polynomials obtained by the specializations $Y \mapsto \xi$ (resp. $Y \mapsto \rho$); $P_\xi$ define $F_\xi$ over $L = \mathbb{Q}(\xi)$.

(ii) The polynomial is canonical as soon as we take the unique representative $e'_\omega = \sum_k u_k\, s_k$ with $1 \le u_k \le p-1$, which gives $\eta'_1(Y) := (1+Y\,\zeta)^{e'_\omega}\,\zeta^{-\frac{1}{2}} \sim \eta_1(Y)$ and the monic polynomial, still defining $F_Y$ and still denoted $P_Y$,

$$P_Y := X^p + A_{p-1}(Y)X^{p-1} + \cdots + A_0(Y),\ \ A_i(Y) \in \mathbb{Z}[Y]\,.$$

The polynomial $P_\xi := X^p + A_{p-1}(\xi)X^{p-1} + \cdots + A_0(\xi)$ still defines the extension $F_\xi/\mathbb{Q}(\xi)$.

(iii) We consider the monic polynomial obtained from $\eta_1^{sh}(Y) := (1+Y\,\zeta)^{e'_\omega}$. Then a "simplest polynomial", denoted by

$$P_Y^{sh} := X^p + A_{p-1}^{sh}(Y) X^{p-1} + \cdots + A_0^{sh}(Y)\,,$$

may be deduced by linear $\mathbb{Q}(Y)$-translation of the variable $X$ minimizing the degrees in $Y$; an interesting problem would be to find a canonical expression as for $p = 3$ (if it exists). It defines the cyclic $p$-extension of $\mathbb{Q}(Y)$ denoted by $F_Y^{sh}$, hence the cyclic $p$-extensions $F_\xi^{sh}/\mathbb{Q}(\xi)$.

For $p = 5$, from $\eta'_1(Y) = (1 + Y\,\zeta_5)^{e'_\omega} \zeta_5^{-\frac{1}{2}}$, one obtains the following polynomial defining $F_Y$:

$$\begin{aligned}P_Y &= X^5 - 10\,(Y^4 - Y^3 + Y^2 - Y + 1)\,X^3 + 5\,(Y^4 - Y^3 + Y^2 - Y + 1)\,(Y^2 + 2\,Y + 1)\,X^2\\ &+5\,(Y^4 - Y^3 + Y^2 - Y + 1)\,(2\,Y^4 - 7\,Y^3 + 7\,Y^2 - 7\,Y + 2)\,X\\ &+(Y^4 - Y^3 + Y^2 - Y + 1)\,(Y^6 - 4\,Y^5 + 10\,Y^3 - 4\,Y + 1)\,.\end{aligned}$$

Then $\eta_1^{sh}(Y) = (1 + Y\,\zeta_5)^{e'_\omega}$, $e'_\omega = 4 + 2\,s + s^2 + 3\,s^3$ with $s = s_2$ yields to the polynomial

$$\begin{aligned}&X^5 - 10\,(Y^4 - Y^3 + Y^2 - Y + 1)\,X^3 + 5\,(Y^4 - Y^3 + Y^2 - Y + 1)\,(Y^2 + 2\,Y - 4)\,X^2\\ &+5\,(Y^4 - Y^3 + Y^2 - Y + 1)\,(2\,Y^4 - 2\,Y^3 + 2\,Y^2 + 3\,Y - 3)\,X\\ &+(Y^4 - Y^3 + Y^2 - Y + 1)\,(Y^6 - 9\,Y^5 + 10\,Y^4 - 10\,Y^3 + 5\,Y^2 + 6\,Y - 4)\,.\end{aligned}$$

The linear transformation $X \mapsto Y^2 X - 1 - Y$ gives the polynomial

$$\begin{aligned}P_Y^{sh} &= X^5 - 5\,Y^{-2}\,X^4 + 10\,(-1 + Y^{-1} - Y^{-2} + Y^{-3})\,X^3 + 5\,(1 + Y^{-1} + Y^{-2} - Y^{-3} + Y^{-4})X^2\\ &+5\,(2 - 4Y^{-1} + 4Y^{-2} - 5Y^{-3} + 4Y^{-4} - 2Y^{-5})X + 1 - 10Y^{-1} + 10Y^{-2} - 10Y^{-3} + 10Y^{-4} - 8Y^{-5}\end{aligned}$$

which may be regarded as a "simplest quintic cyclic polynomial" defining $F_Y^{sh}$.

***Proposition 6.13.*** — *Let $p$ be a prime $> 3$, and let $\rho = \frac{v}{u}$, with g.c.d.$\,(u,v) = 1$, be a rational distinct from $0$ and $\pm 1$; suppose $u - v \not\equiv 0 \pmod p$.* [13] *Put*

$$Q_\rho := \big\{q \text{ prime},\ q \nmid u\,v\,(u^2 - v^2)\ \&\ \text{the order of } \rho \text{ modulo } q \text{ is prime to } p\big\}\,.$$

*Let $q \in Q_\rho$. We have the following results from Definition 6.12 (i, ii) on the universal Abelian polynomials $P_\rho = X^p + A_{p-1}(\rho) X^{p-1} + \cdots + A_0(\rho)$:*

*(i) Case $u + v \not\equiv 0 \pmod p$. If $\kappa \not\equiv 0 \pmod p$ and if $P_\rho$ is reducible modulo $q$, then $(u,v)$ cannot be a solution in the nonspecial cases of the SFLT equation $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{w}_1^p$.*

*(ii) Case $u + v \equiv 0 \pmod p$. If $\kappa \not\equiv 0 \pmod p$ and if $P_\rho$ is irreducible modulo $q$, then $(u,v)$ cannot be a solution in the special case of the SFLT equation $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}\,\mathfrak{w}_1^p$.*

*(iii) If $\kappa \equiv 0 \pmod p$ and if $P_\rho$ is irreducible modulo $q$, then $(u,v)$ cannot be a solution in any case of the SFLT equation $(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^\delta\,\mathfrak{w}_1^p$, $\delta \in \{0,1\}$.*

*Proof.* — Let $n$ be the order of $\rho$ modulo $q$; since $q \in Q_\rho$, we have $n > 2$, $n \mid q - 1$, $p \nmid n$, and for any choice of a $n$th root of unity $\xi$, $\mathfrak{q}_{\rho,\xi} := (q, u\,\xi - v)$ is a prime ideal of $L$ lying above $q$ (Lemma 2.11 and Corollary 2.12).

[13] When $(u,v) = (x,y)$ or $(y,z)$ for a solution $(x,y,z)$ of Fermat's equation, this assumption is satisfied (Lemma 2.2).

Then $\rho \equiv \xi \pmod{\mathfrak{q}_{\rho,\xi}}$ and in case (i) there exists $\lambda \in \mathbb{Z}$, a root modulo $q$ of the polynomial $P_\rho$, such that

$$P_\rho(\lambda) = \lambda^p + A_{p-1}(\rho)\lambda^{p-1} + \cdots + A_0(\rho) \equiv \lambda^p + A_{p-1}(\xi)\lambda^{p-1} + \cdots + A_0(\xi) \equiv 0 \pmod{\mathfrak{q}_{\rho,\xi}},$$

since $q$ divides the left member. This means that $P_\xi$ has the root $\lambda$ modulo $\mathfrak{q}_{\rho,\xi}$ and that $\mathfrak{q}_{\rho,\xi}$ splits in $F_\xi/L$. If $(u, v)$ is a counterexample to SFLT, Theorem 3.3 in the nonspecial cases gives $\left(\frac{\eta_1}{\mathfrak{Q}_{\rho,\xi}}\right)_M = \zeta^{-\frac{1}{2}\frac{u-v}{u+v}\kappa} \neq 1$ by assumption, which is equivalent to the inertia of $\mathfrak{q}_{\rho,\xi}$ in $F_\xi/L$ (contradiction). The proofs of cases (ii) and (iii) are similar but inverted; we have

$$P_\rho = X^p + A_{p-1}(\rho)X^{p-1} + \cdots + A_0(\rho) \equiv X^p + A_{p-1}(\xi)X^{p-1} + \cdots + A_0(\xi) \pmod{\mathfrak{q}_{\rho,\xi} Z_L[X]}$$

giving, by assumption on the left polynomial $P_\rho$, that the image in $Z_L/\mathfrak{q}_{\rho,\xi}[X] \simeq \mathbb{F}_q[X]$ of $P_\xi = X^p + A_{p-1}(\xi)X^{p-1} + \cdots + A_0(\xi)$ is irreducible. Thus $\mathfrak{q}_{\rho,\xi}$ is inert in $F_\xi/L$ while $\left(\frac{\eta_1}{\mathfrak{Q}_{\rho,\xi}}\right)_M = 1$ for a solution in these cases (contradiction). □

In other words, the two corresponding properties giving a proof of SFLT (under the assumption $u - v \not\equiv 0 \pmod p$) are the following; they can also be obtained from Lemma 2.14 considering the expression of $\gamma_\omega \zeta^{-\frac{1}{2}}$:

(a) For any rational $\rho = \frac{v}{u}$ (with g.c.d. $(u, v) = 1$), distinct from 0 and $\pm 1$, we have:

(a$_1$) Case $u + v \not\equiv 0 \pmod p$. There exists at least one prime $q \in Q_\rho$ with $\kappa \not\equiv 0 \pmod p$ such that $P_\rho$ is reducible modulo $q$.

(a$_2$) Case $u + v \equiv 0 \pmod p$. There exists at least one prime $q \in Q_\rho$ with $\kappa \not\equiv 0 \pmod p$ such that $P_\rho$ is irreducible modulo $q$.

(b) For any rational $\rho = \frac{v}{u}$ (with g.c.d. $(u, v) = 1$), distinct from 0 and $\pm 1$, there exists at least one prime $q \in Q_\rho$ with $\kappa \equiv 0 \pmod p$ such that $P_\rho$ is irreducible modulo $q$.

Of course, without an independent approach (analytic or geometric), the problem has no solution since $P_\rho$ can be, in case (a$_1$), a polynomial defining $\mathbb{Q}_1$ (the subfield of degree $p$ of $\mathbb{Q}(\mu_{p^2})$), in which case all the primes which split in $\mathbb{Q}_1/\mathbb{Q}$ are such that $\kappa \equiv 0 \pmod p$, in cases (a$_2$), $P_\rho$ can be splitted over $\mathbb{Q}$, and in case (b), it can define $\mathbb{Q}$ or $\mathbb{Q}_1$.

The proof of (a) implies the two cases of FLT, taking $(u, v) = (x, y)$ or $(z, y)$ (case (a$_1$)). It implies the second case of FLT, taking $(u, v) = (x, z)$ (case (a$_2$)).

The proof of (b) implies the two cases of FLT, taking any pair for $(u, v)$.

This reasoning leads to the following polynomial obstructions (concerning the universal Abelian polynomial $P_Y$) for a proof of FLT: Let $\mathcal{K}_\rho$ be the number field defined by the universal Abelian polynomial

$$P_\rho = X^p + A_{p-1}(\rho)X^{p-1} + \cdots + A_0(\rho).$$

We know that $\mathcal{K}_\rho/\mathbb{Q}$ is a cyclic extension of degree 1 or $p$.

If $\mathcal{K}_\rho$ is distinct from $\mathbb{Q}$ and $\mathbb{Q}_1$, the Čebotarev density theorem leads to a proof of the existence of infinitely many primes $q \in Q_\rho$ verifying each of the conditions (a$_1$), (a$_2$), (b). The condition $q \in Q_\rho$ can be easily realized taking primes $q$ not totally split in $K/\mathbb{Q}$. In case (a$_1$), it is sufficient to consider $\mathcal{K}_\rho\mathbb{Q}(\mu_{p^2})$ taking a Frobenius automorphism of $q$ in $\mathcal{K}_\rho\mathbb{Q}(\mu_{p^2})/\mathbb{Q}$ which fixes $\mathcal{K}_\rho$ and does not fix the fields $\mathcal{K}_\rho\mathbb{Q}_1$ and $\mathcal{K}_\rho K$. In case (a$_2$), the Frobenius automorphism must not fix $\mathcal{K}_\rho$ nor $\mathbb{Q}_1$. In case (b), it must fix $\mathbb{Q}_1$ but not $\mathcal{K}_\rho$.

If $\mathcal{K}_\rho = \mathbb{Q}$, then (a$_2$) and (b) are of empty use since $P_\rho$ cannot be irreducible in any $\mathbb{F}_q[X]$; but (a$_1$) applies, if $\rho \not\equiv -1 \pmod p$, to the two cases of FLT.

If $\mathcal{K}_\rho = \mathbb{Q}_1$, then (a$_1$) and (b) are of empty use since the assumptions on the decomposition of $q$ are incompatible; then (a$_2$) applies, if $\rho \equiv -1 \pmod p$, to the second case of FLT.

Using the nonspecial cases of SFLT to obtain the first and second cases of FLT (see (i)), then the special case of SFLT to obtain again the second cases of FLT (see (ii)), we can state:

***Corollary 6.14***. — *Let $p$ be a prime $> 3$ and let $P_Y = X^p + A_{p-1}(Y)X^{p-1} + \cdots + A_0(Y)$ be the universal Abelian polynomial (see Definition 6.12 (i, ii)), and let $P_\rho$ be the universal Abelian polynomial of $\mathbb{Q}[X]$ obtained by specialization $Y \mapsto \rho$, for any rational $\rho$.*

*(i) Fermat's Last Theorem holds for $p$ as soon as the following property is satisfied:*

*For all rationals $\rho$, distinct from $0$ and $\pm 1$ and such that $\rho \not\equiv -1 \pmod p$, the universal Abelian polynomial $P_\rho$ does not define the subfield $\mathbb{Q}_1$ of degree $p$ of $\mathbb{Q}(\mu_{p^2})$.*

*(ii) The second case of Fermat's Last Theorem holds for $p$ as soon as the following property is satisfied:*

*For all rationals $\rho$, distinct from $0$ and $\pm 1$ and such that $\rho \equiv -1 \pmod p$, the universal Abelian polynomial $P_\rho$ is irreducible over $\mathbb{Q}$ (i.e., has no rational roots).* □

The universal Abelian polynomial

$$P_Y = X^p + A_{p-1}(Y)X^{p-1} + \cdots + A_0(Y)$$

has the nontrivial property that $P_\xi = X^p + A_{p-1}(\xi)X^{p-1} + \cdots + A_0(\xi)$ is irreducible in $\mathbb{Q}(\mu_n)[X]$ for all primitive $n$th root of unity $\xi$, $n > 2$, $n \not\equiv 0 \pmod p$, and defines a $p$-ramified cyclic extension $F_\xi$ of $\mathbb{Q}(\mu_n)$, distinct from $\mathbb{Q}(\mu_n)\mathbb{Q}_1$, satisfying to the fundamental Theorem 6.6.

## 7. Normic relations for cyclotomic units

In this section we give a relation between two $\omega$-units $\eta_1^0$ and $\eta_1$, for instance associated with the classes $\mathcal{C}_\rho(q_0)$ and $\mathcal{C}_\rho(q)$ of two primes $q_0$ and $q$, for which the pairs $(\xi_0, \mathfrak{q}^0_{\rho,\xi_0})$, $(\xi, \mathfrak{q}_{\rho,\xi})$, are such that the order $n_0$ of $\xi_0$ divides the order $n$ of $\xi$, with the condition $p \nmid n$.

Put $n = n_0 d$. We introduce the following notations:

$$L_0 = \mathbb{Q}(\mu_{n_0}),\ L = \mathbb{Q}(\mu_n),\ M_0 = L_0\, K,\ M = L\, K,$$
$$\mathrm{N} := \mathrm{N}_{M/M_0},\ \eta_1^0 = (1 + \xi_0\, \zeta)^{e_\omega}\, \zeta^{-\frac{1}{2}},\ \eta_1 = (1 + \xi\, \zeta)^{e_\omega}\, \zeta^{-\frac{1}{2}}\ ;$$

to fix the notations, we suppose that $\xi_0 = \xi^d$.

Since $\eta_1$ is a cyclotomic unit, the action of the relative norm N on this unit is well-known and we now recall the result in our particular context.

***Proposition 7.1***. — *Let $S$ be the set of distinct primes dividing $d$ and not dividing $n_0$. Then we have $\mathrm{N}(\eta_1) = (\eta_1^0)^{\Lambda_0}$, where $\Lambda_0 \equiv d \,.\, \prod_{\ell \in S} (1 - \ell^{-1}\, (t_\ell^0)^{-1}) \pmod p$, $t_\ell^0 \in \mathrm{Gal}(M_0/K)$ being the Artin automorphism defined by $\xi_0^{t_\ell^0} := \xi_0^\ell$.*

*Proof.* — By induction we can suppose that $d$ is a prime $\ell$. Let $\psi := \xi^{n_0}$ which is a primitive $\ell$th root of unity.

(i) Case $\ell \,|\, n_0$. In this case $S = \emptyset$, $[M : M_0] = \ell$, and

$$\begin{aligned} \mathrm{N}(1+\xi\,\zeta) &= \prod_{\lambda=0}^{\ell-1}(1+\xi^{1+\lambda n_0}\zeta) = \prod_{\lambda=0}^{\ell-1}(1+\xi\,\psi^{\lambda}\zeta) \\ &= 1+\xi^{\ell}\,\zeta^{\ell} = 1+\xi_0\,\zeta^{\ell} = (1+\xi_0\,\zeta)^{s_\ell}\,. \end{aligned}$$

Then $\mathrm{N}(\eta_1) = (1+\xi_0\,\zeta)^{s_\ell e_\omega}\,\mathrm{N}(\zeta)^{-\frac{1}{2}} \sim (1+\xi_0\,\zeta)^{\ell\,e_\omega}\,\zeta^{-\frac{1}{2}\ell} = (\eta_1^0)^{\ell}$ since $s_\ell e_\omega \equiv \ell e_\omega \pmod p$.

(ii) Case $\ell \nmid n_0$. In this case $S = \{\ell\}$ and $\mathrm{N}(1+\xi\,\zeta) = \prod\limits_{\lambda=0,\,\lambda\neq\lambda_0}^{\ell-1}(1+\xi^{1+\lambda n_0}\zeta)$, where $\lambda_0$ is the unique value modulo $\ell$ such that $1+\lambda_0 n_0 \equiv 0 \pmod \ell$, giving from the computation in (i)

$$\mathrm{N}(1+\xi\,\zeta) = \frac{1+\xi^{\ell}\,\zeta^{\ell}}{1+\xi^{1+\lambda_0 n_0}\,\zeta} = \frac{(1+\xi_0\,\zeta)^{s_\ell}}{1+\xi_0^{\mu}\,\zeta}\,,$$

where $1+\lambda_0 n_0 = \mu\,\ell$, so that $\mu \equiv \ell^{-1} \pmod{n_0}$. Thus

$$\begin{aligned} \mathrm{N}(1+\xi\,\zeta) &= \frac{(1+\xi_0\,\zeta)^{s_\ell}}{1+\xi_0^{\ell^{-1}}\zeta} = \frac{(1+\xi_0\,\zeta)^{s_\ell}}{1+\xi_0^{(t_\ell^0)^{-1}}\zeta} \\ &= \Big(\frac{1+\xi_0\,\zeta}{1+\xi_0^{(t_\ell^0)^{-1}}\,\zeta^{s_\ell^{-1}}}\Big)^{s_\ell} = \Big(\frac{1+\xi_0\,\zeta}{1+(\xi_0\,\zeta)^{(\sigma_\ell^0)^{-1}}}\Big)^{s_\ell}, \end{aligned}$$

where $\sigma_\ell^0 \in \mathrm{Gal}(M_0/\mathbb{Q})$ is the Artin automorphism defined by $\sigma_\ell^0(\theta) = \theta^{\ell}$ for any $pn_0$th root of unity $\theta$; thus, since $\sigma_\ell^0 = s_\ell\,t_\ell^0$, this yields

$$\mathrm{N}(1+\xi\,\zeta)^{e_\omega} \sim \Big(\frac{1+\xi_0\,\zeta}{1+(\xi_0\,\zeta)^{(\sigma_\ell^0)^{-1}}}\Big)^{\ell\,e_\omega} = \big(1+\xi_0\,\zeta\big)^{\ell\,(1-(\sigma_\ell^0)^{-1})\,e_\omega}\,;$$

from $(\sigma_\ell^0)^{-1}\,e_\omega = s_\ell^{-1}\,(t_\ell^0)^{-1}\,e_\omega \equiv \ell^{-1}\,(t_\ell^0)^{-1}\,e_\omega \pmod p$, we get the relation $\mathrm{N}(1+\xi\,\zeta)^{e_\omega} \sim \big(1+\xi_0\,\zeta\big)^{\ell\,(1-\ell^{-1}(t_\ell^0)^{-1})\,e_\omega}$. Finally, since in this case $[M : M_0] = \ell-1$ and $\mathrm{N}(\zeta) = \zeta^{\ell-1} = \zeta^{\ell\,(1-\ell^{-1}\,(t_\ell^0)^{-1})}$, we obtain $\mathrm{N}(\eta_1) \sim (\eta_1^0)^{\ell\,(1-\ell^{-1}\,(t_\ell^0)^{-1})}$ and the proposition follows. $\square$

If for instance $\Lambda_0$ is invertible modulo $p$, with inverse $\Omega_0$, then $\eta_1^0 \sim \mathrm{N}(\eta_1)^{\Omega_0}$ and, over $L$, we can see the extension $F_{n_0}$ (compositum of the conjugates of the $F_{\xi_0}$) as a subfield of $F_n$ with the precise laws of $\rho$-decomposition of $q_0$ and $q$ studied in this paper, in which case the properties of the corresponding Frobenius automorphisms can be compared to give strengthened conditions.

***Remark 7.2.*** — For $\ell \in S$, let $d_\ell^0$ be the order of $t_\ell^0$; then $1-\ell^{-1}\,(t_\ell^0)^{-1}$ is invertible modulo $p$ if and only if $\ell^{d_\ell^0} \not\equiv 1 \pmod p$.

## 8. Analysis of the case $p = 3$ versus $p \neq 3$

In this section we consider the solutions of the SFLT equation for $p = 3$. They are a logical obstruction to the relevance of general statements similar to Theorem 5.1, and we have explicited this obstruction in Subsection 5.3. Moreover these solutions are also related to the law of $\rho$-decomposition of Theorem 6.6 and we intend to explain why this theorem is compatible, for $p = 3$, with the classical density theorems.

The main differences between the cases $p = 3$ and $p > 3$ are the following:

(i) There is an infinite number of solutions for the case $p = 3$, in contrast with the case $p > 3$, even though we have not proved this probable result: the finiteness of the set of solutions of Fermat's equation for $p$ was known before Wiles' proof (Faltings' Theorem); but the SFLT equation has, a priori, more solutions; at least we can hope that there does not exist any parametric family of solutions.

(ii) We shall exhibit a group of automorphisms of order 12, isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, acting on the set of solutions for $p = 3$, which creates some exceptional relations of compatibility with density theorems, then we shall prove (Theorem 8.5) that for $p > 3$ the corresponding group of automorphisms is of order 2, reduced to the identity and the inversion.

**8.1. Another analysis of the case $p = 3$ for the obstruction to Theorem 5.1.** — We have proven in Subsection 5.3 the existence of this obstruction without considering the solutions of the SFLT equation. We need a more precise analysis to understand this phenomenon and to replace Theorem 6.6 in this context; this we shall explain in Subsection 8.2.

Let $(u, v)$, g.c.d. $(u, v) = 1$, be a solution of the SFLT equation, let $q$ be a prime such that $q \nmid uv$ and such that $\rho := \frac{v}{u}$ is of order $n$ modulo $q$, $n \not\equiv 0 \pmod 3$. Consider the prime ideal $\mathfrak{q}_{\rho,\xi} = (q, u\,\xi - v)$, where $\xi$ is of order $n$. Denoting $j$ the 3th root $\zeta$, let $\eta_1 = (1 + \xi\, j)^{e_\omega}\, j^{-\frac{1}{2}}$, with $e_\omega = s - 1$.

Put $L = \mathbb{Q}(\mu_n)$ and $M = LK$; then recall Theorem 3.3 for $p = 3$:

(i) First case. We have $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = j^{-\frac{1}{2}\,\frac{u-v}{u+v}\,\kappa} = 1$ for any $\mathfrak{Q} \,|\, \mathfrak{q}_{\rho,\xi}$ in $M$, since $u \equiv v \equiv \pm 1 \pmod 3$.

(ii) Second case. We have $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = j^{\pm\frac{1}{2}\,\kappa}$ for any $\mathfrak{Q} \,|\, \mathfrak{q}_{\rho,\xi}$ since $3 \,|\, u\,v$.

(iii) Special case. We have $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = j^{\frac{1}{2}\,\frac{u+v}{3\,v}\,\kappa}$ for any $\mathfrak{Q} \,|\, \mathfrak{q}_{\rho,\xi}$, with $3 \,|\, u + v$; we have seen, at the end of Subsection 6.2, that $\frac{u+v}{3\,v}$ can take any value modulo 3.

From this, we see that the existence of $q$ totally split in $H^-_{\widetilde{L}}[3]/\mathbb{Q}$ for $\widetilde{L} = \mathbb{Q}(\mu_{q-1})$, or at least $\widetilde{L} = \mathbb{Q}(\mu_m)$ for a large $m \,|\, q - 1$, may be in contradiction with the existence of the solutions of the second and special cases when $\kappa \not\equiv 0 \pmod 3$. Indeed, such a solution implies the existence of a nontrivial Frobenius automorphism of $\mathfrak{q} \,|\, q$ in a suitable cubic cyclic extension $F_\xi/L$, $F_\xi \subseteq H^-_L[3]$.

***Definition 8.1.*** — The following definitions and notations are valid for any $p \geq 3$. Consider the field $k(Y)$, where $k$ is any field of characteristic distinct from 2 and 3. Then let $T$ be the automorphism of $k(Y)$ such that $T(Y) := \frac{2\,Y-1}{Y+1}$.

Let $\eta_1(Y) := (1 + Y\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}} \in K(Y)$ be the formal $\omega$-cyclotomic unit (see Subsection 6.3).

Recall that for any $p$, the automorphism of inversion $T_0$ defined by $T_0(Y) := Y^{-1}$ is such that $T_0(\eta_1(Y)) = (1 + Y^{-1}\,\zeta)^{e_\omega}\,\zeta^{-\frac{1}{2}} \sim \eta_1(Y)^{-1}$. So we shall not consider it.

We intend to prove below various properties of compatibility, for $p = 3$, of the automorphism $T$, with the method of $\omega$-cyclotomic units developed here.

***Proposition 8.2.*** — *(i) The automorphism $T$ is of order 6 and the orbit of $Y$ is*

$$\Big\{Y;\ \frac{2\,Y-1}{Y+1};\ \frac{Y-1}{Y};\ \frac{Y-2}{2\,Y-1};\ \frac{-1}{Y-1};\ \frac{-Y-1}{Y-2}\Big\}.$$

*(ii) We have for $\zeta = j$ of order 3 and for $\eta_1(Y) = (1 + Y j)^{e_\omega} j^{-\frac{1}{2}}$, the formula*

$$T^i(\eta_1(Y)) \sim \eta_1(Y)\, j^{\frac{1}{2}\, i},\quad 0 \le i < 3\ \textit{(equality up to a 3th power in } K(Y)\textit{)}.$$

*Proof.* — The point (i) is obvious. For (ii) we have

$$T(\eta_1(Y)) = \big(1 + \frac{2\,Y-1}{Y+1} j\big)^{e_\omega} j^{-\frac{1}{2}} = (Y + 1 + (2\,Y - 1)j)^{e_\omega} j^{-\frac{1}{2}} = (1 - j + (2j + 1)Y)^{e_\omega} j^{-\frac{1}{2}}\,;$$

since $2j+1 = j\,(1-j)$, we get finally $T(\eta_1(Y)) = (1-j)^{e_\omega}(1+Yj)^{e_\omega} j^{-\frac{1}{2}}$; but $(1-j)^{e_\omega} = -j^{\frac{1}{2}}$, hence the result in this case.

The general formula is obtained by induction noting that $T^3(\eta_1(Y)) = \eta_1(Y)$. □

Now, we show that $T$ acts on the set of solutions of the SFLT equation for $p = 3$ in the following way.

***Proposition 8.3.*** — *For any coprime integers $u, v$, put $T(\frac{v}{u}) =: \frac{V}{U}$ in $\mathbb{Q} \cup \{\infty\}$, where $(U, V)$ is defined up to the sign. By abuse of notation we also write $T(u, v) =: (U, V)$.*

*Then the orbit of the solution $(u, v) = (-s^3 - t^3 + 3s^2t, -s^3 - t^3 + 3st^2)$ (see Remark 2.6) gives rise to the following identities:*

$$\begin{aligned}
T^0\big(\frac{v}{u}\big) &= \frac{v}{u} &&= \frac{-s^3 - t^3 + 3st^2}{-s^3 - t^3 + 3s^2t}\,,\\
T^1\big(\frac{v}{u}\big) &= \frac{2v-u}{u+v} &&= \frac{-s^3 - t^3 - 3s^2t + 6st^2}{-2s^3 - 2t^3 + 3s^2t + 3st^2}\,,\\
T^2\big(\frac{v}{u}\big) &= \frac{v-u}{v} &&= \frac{3s^2t - 3st^2}{s^3 + t^3 - 3st^2}\,,\\
T^3\big(\frac{v}{u}\big) &= \frac{v-2u}{2v-u} &&= \frac{-s^3 - t^3 + 6s^2t - 3st^2}{s^3 + t^3 + 3s^2t - 6st^2}\,,\\
T^4\big(\frac{v}{u}\big) &= \frac{-u}{v-u} &&= \frac{s^3 + t^3 - 3s^2t}{3st^2 - 3s^2t}\,,\\
T^5\big(\frac{v}{u}\big) &= \frac{-v-u}{v-2u} &&= \frac{2s^3 + 2t^3 - 3s^2t - 3st^2}{s^3 + t^3 - 6s^2t + 3st^2}\,,
\end{aligned}$$

*which leads to the six fundamental families of solutions of the SFLT equation for $p = 3$.*

***Remark 8.4.*** — The orbit of 0 in $\mathbb{Q} \cup \{\infty\}$ (i.e., the $T^i(\frac{0}{1})$, $0 \le i < 6$) is $\{0;\ -1;\ \infty;\ 2;\ 1;\ \frac{1}{2}\}$ and corresponds to the set of the six trivial solutions of the case $p = 3$.

For $q \not\equiv 1 \pmod 3$, $q \ne 2$, all the orbits in $\mathbb{F}_q \cup \{\infty\}$ have six elements; indeed, all the equations of the form $\dfrac{ay+b}{cy+d} = y$, deduced from the rational fractions of Proposition 8.2 (i), reduce to $y^2 - y + 1 = 0$ which is irreducible over $\mathbb{F}_q$. The orbit of $\overline{0}$ in $\mathbb{F}_q \cup \{\infty\}$ is $\{\overline{0};\ -\overline{1};\ \infty;\ \overline{2};\ \overline{1};\ \overline{2}^{-1}\}$. Later on we shall assume, for technical reasons, that the image of $\frac{v}{u}$ in $\mathbb{F}_q \cup \{\infty\}$ is not in this orbit; this is equivalent to $q \nmid u\,v\,(u^2 - v^2)\,(2u - v)\,(u - 2v)$; we compute that this is also equivalent to the analogous condition $q \nmid s\,t\,(s^2 - t^2)\,(2s - t)\,(s - 2t)$ for the parameters $(s, t)$ defining the solutions. Under this assumption, the orders modulo $q$ of the $T^i\big(\frac{v}{u}\big)$, $0 \le i < 6$, are defined and $> 2$.

Let $q \neq 3$ be a prime; we suppose $q \not\equiv 1 \pmod 3$. Call $n_i \,|\, q-1$ the orders modulo $q$ of $T^i\big(\frac{v}{u}\big) =: \frac{v_i}{u_i}$, $0 \le i < 6$, for any solution $(u, v)$. As usual we put, with $\rho_i := \frac{v_i}{u_i}$,

$$T^i\Big(\frac{v}{u}\Big) = \frac{v_i}{u_i} \equiv \xi_i \pmod{\mathfrak{q}_{\rho_i,\xi_i} = (q, u_i\,\xi_i - v_i)},\ \ 0 \le i < 6,\ \ \xi_i \text{ of order } n_i\,.$$

where we recall that the pair $(\xi_i, \mathfrak{q}_{\rho_i,\xi_i})$ is defined up to conjugation, so that we can replace $(\xi_i, \mathfrak{q}_{\rho_i,\xi_i})$ by any conjugate $(\xi'_i, \mathfrak{q}_{\rho_i,\xi'_i})$ to define the class $\mathcal{C}_{\rho_i}(q)$. To simplify the formulas we keep the notations $(u, v) = (u_0, v_0)$, $\rho = \rho_0$, $\xi = \xi_0$, $n = n_0$.

Consider for instance $T\big(\frac{v}{u}\big) = \frac{v_1}{u_1} \equiv \xi_1 \pmod{\mathfrak{q}_{\rho_1,\xi_1}}$ noting that $\frac{v}{u} \equiv \xi \pmod{\mathfrak{q}_{\rho,\xi}}$ of order $n$. To compare the two congruences we can take a prime ideal $\widetilde{\mathfrak{q}} \,|\, \mathfrak{q}_{\rho,\xi}$ in $\widetilde{L} := \mathbb{Q}(\mu_{q-1})$ and make sure that $\widetilde{\mathfrak{q}} \,|\, \mathfrak{q}_{\rho_1,\xi_1}$ by suitable conjugation of $(\xi_1, \mathfrak{q}_{\rho_1,\xi_1})$, which leads to the congruences $\frac{v}{u} \equiv \xi \pmod{\widetilde{\mathfrak{q}}}$ and $\frac{v_1}{u_1} \equiv \xi_1 \pmod{\widetilde{\mathfrak{q}}}$, hence $\xi_1 \equiv \frac{v_1}{u_1} = T\big(\frac{v}{u}\big) \equiv T(\xi) \pmod{\widetilde{\mathfrak{q}}}$.

More generally we can write, for suitable choices of the $\xi_i$,

$$\xi_i \equiv T^i(\xi) \pmod{\widetilde{\mathfrak{q}}},\ \ 0 \le i < 6\,,$$

which yields, for the units $\eta_1^i$ associated to the $\xi_i$ (with $\eta_1^0 = \eta_1$),

$$\begin{aligned} \eta_1^i &:= (1 + \xi_i\, j)^{e_\omega} j^{-\frac{1}{2}} \\ &\equiv (1 + T^i(\xi)\, j)^{e_\omega} j^{-\frac{1}{2}} \equiv \eta_1\, j^{\frac{1}{2}\,i} \pmod{\widetilde{\mathfrak{Q}}},\ \ 0 \le i < 3 \end{aligned}$$

(by Proposition 8.2 (ii)), for all $\widetilde{\mathfrak{Q}}$ lying above $\widetilde{\mathfrak{q}}$ in $\widetilde{M} := \widetilde{L}K$.

Thus we have

$$\Big(\frac{\eta_1^i}{\widetilde{\mathfrak{Q}}}\Big)_{\widetilde{M}} = \Big(\frac{\eta_1}{\widetilde{\mathfrak{Q}}}\Big)_{\widetilde{M}} \Big(\frac{j^{\frac{1}{2}\,i}}{\widetilde{\mathfrak{Q}}}\Big)_{\widetilde{M}} = \Big(\frac{\eta_1}{\widetilde{\mathfrak{Q}}}\Big)_{\widetilde{M}} j^{\frac{1}{2}\,i\,\kappa} \ \text{ for all } \widetilde{\mathfrak{Q}} \,|\, \widetilde{\mathfrak{q}},\ \ 0 \le i < 3\,,$$

proving that the three symbols never coincide when $\kappa \not\equiv 0 \pmod 3$.

These symbols are identical to the symbols $\Big(\frac{\eta_1^i}{\mathfrak{Q}_i}\Big)_{M_i}$, for any $\mathfrak{Q}_i \,|\, \mathfrak{q}_{\rho_i,\xi_i}$, $0 \le i < 3$, where $M_i = L_i K$, with $L_i = \mathbb{Q}(\mu_{n_i})$.

This proves that if for instance $\mathfrak{q}_{\rho_0,\xi_0}$ splits in $F_{\xi_0}/L_0$ then $\mathfrak{q}_{\rho_1,\xi_1}$ and $\mathfrak{q}_{\rho_2,\xi_2}$ are inert in $F_{\xi_1}/L_1$ and $F_{\xi_2}/L_2$, respectively (this happens when $(u_0, v_0)$ is the solution of the first case or that of the special case with $u_0 + v_0 \equiv 0 \pmod 9$); in other words, the three laws of $\rho_i$-decomposition, i.e., the three symbols $\Big[\frac{F_*/L_i}{\mathfrak{q}_*}\Big]_{\rho_i}$ of Definition 6.2, yield the three possibilities when $\kappa \not\equiv 0 \pmod 3$. See Example 8.9.

So, since this phenomenon happens in $\widetilde{L} = \mathbb{Q}(\mu_{q-1})$, statements like that of Theorem 5.1 are empty for $p = 3$ since $q$ cannot be totally split in $H^-_{\widetilde{L}}[3]/\widetilde{L}$ (compare with Subsection 5.3).

This distribution of the three possible Frobenius automorphisms, in the context of laws of $\rho_i$-decomposition, must be compatible with the Čebotarev density theorem. See Subsection 8.2 for this aspect and Subsection 8.3 for some numerical evidence, especially Example 8.9 and 8.13.

Returning to the general case, it is necessary to see whether such a nontrivial automorphism $T$ can exist for $p > 3$ or not. If not, this will be a favorable argument for our purpose.

***Theorem 8.5***. — *Let $p$ be a prime and let $K := \mathbb{Q}(\zeta)$ where $\zeta$ is a primitive $p$th root of unity. Put $g := \mathrm{Gal}(K/\mathbb{Q})$.*

*Consider $\mathcal{M} := \mathbb{Z}_p \otimes_{\mathbb{Z}} K(Y)^\times$, as a multiplicative $\mathbb{Z}_p[g]$-module, and consider the idempotent $\mathcal{E}_\omega := \frac{1}{p-1} \sum_{s\in g} \omega^{-1}(s)\, s \in \mathbb{Z}_p[g]$ (see Definition 2.8 (i, ii)).*

*Then for $p > 3$ there does not exist any automorphism $T$ of $\mathbb{Q}(Y)$, distinct from the identity and the inversion $Y \mapsto Y^{-1}$, such that*

$$T\big((1 + Y\,\zeta)^{\mathcal{E}_\omega}\big) := \big(1 + T(Y)\,\zeta\big)^{\mathcal{E}_\omega} \sim \big(1 + Y\,\zeta^\lambda\big)^{\mathcal{E}_\omega}\,\zeta^\mu \ \ \textit{(equality up to a $p$th power in $\mathcal{M}$)},$$

*for some $\lambda, \mu \in \mathbb{Z}$, $\lambda \not\equiv 0 \pmod p$.*

*Proof.* — Suppose that such a nontrivial automorphism does exist and put $T(Y) = \dfrac{aY+b}{cY+d}$ with $a, b, c, d \in \mathbb{Q}$, $ad - bc \neq 0$. Note that the associated matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is considered in $\mathrm{G}\ell_2(\mathbb{Q})/D$, where $D$ is the subgroup of scalar matrices $e\,I_2$, $e \in \mathbb{Q}^\times$, where $I_2$ is the unit matrix. In particular, $T$ is of finite order if and only if there exists $n > 0$ such that $M^n = e\,I_2$. For instance, $M = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$ is such that $M^6 = -27\,I_2$.

For simplicity we work in $K(Y)^\times/K(Y)^{\times p} \simeq \mathcal{M}/\mathcal{M}^p$ and we use the representative $e'_\omega$ of $\mathcal{E}_\omega$ defined by $e'_\omega = \sum\limits_{k=1}^{p-1} u_k\, s_k \in \mathbb{Z}[g]$, with $1 \le u_k \le p-1$ (see Definition 2.8 (iii)).

Then from the above identity we get the relation

$$(cY + d + (aY+b)\,\zeta)^{e'_\omega} = (1 + Y\,\zeta^\lambda)^{e'_\omega}\,\zeta^\mu .\, G(Y)^p, \ \ G(Y) = \frac{A(Y)}{B(Y)} \in K(Y)^\times ,$$

with $A, B \in K[Y]$, g.c.d. $(A, B) = 1$, hence the polynomial identity in $K[Y]$

$$B(Y)^p\,(cY + d + (aY+b)\,\zeta)^{e'_\omega} = A(Y)^p\,(1 + Y\,\zeta^\lambda)^{e'_\omega}\,\zeta^\mu .$$

The polynomials $(cY+d+(aY+b)\,\zeta)^{e'_\omega}$ and $(1+Y\,\zeta^\lambda)^{e'_\omega}$ each have $p-1$ distinct roots of orders of multiplicity $u_k$, with $1 \le u_k \le p-1$: indeed, for the roots $y_k := -\frac{d+b\,\zeta^k}{c+a\,\zeta^k}$, $1 \le k \le p-1$, $y_k = y_{k'}$ is equivalent to $(ad-bc)\,(\zeta^k - \zeta^{k'}) = 0$, hence the result; the other case is trivial.

We deduce that $(cY + d + (aY+b)\,\zeta)^{e'_\omega}$ and $(1 + Y\,\zeta^\lambda)^{e'_\omega}$ each are prime to $A$ and $B$, then have the same roots with the same multiplicity; since the $u_k$ are distinct, we get $\dfrac{d+b\,\zeta}{c+a\,\zeta} = \zeta^{-\lambda}$.

Then we have to solve

$$\zeta^{1-\lambda}\,a + \zeta^{-\lambda}\,c - \zeta\,b - d = 0 .$$

If $\lambda \not\equiv \pm 1 \pmod p$, then $1-\lambda$, $-\lambda$, $1$, and $0$ are distinct modulo $p$, since $p > 3$. So, in general, $a \equiv b \equiv c \equiv d \equiv 0 \pmod p$ except if we have to consider the unique relation

$$\zeta^{p-1} = -1 - \zeta - \cdots - \zeta^{p-2} ;$$

we verify that this cannot occur since $p - 2 \ge 3$.

Hence $\lambda \equiv 1$ or $-1 \pmod p$, giving the solutions $(a, b, c, d) = (1, 0, 0, 1)$ (identity), $(a, b, c, d) = (0, 1, 1, 0)$ (inversion). □

**8.2. Analysis of the case $p=3$ for the principle of Theorem 6.6.** — We now have to explain why the existence of a law of $\rho$-decomposition (i.e., $\left[\frac{F_*/L}{\mathfrak{q}_*}\right]_\rho$ independent of $q$ in the sense of Remark 6.7) is indeed compatible for $p=3$ but conjecturally not for $p>3$.

The following analysis suggests a suitable property of repartition (in the meaning of the Čebotarev density theorem) of the values of the Frobenius automorphisms, due to the infiniteness of the set of solutions of the SFLT equation for $p=3$ and to the fact that this set is the union of six parametric families giving complementary values of these Frobenius automorphisms.

Let $q$ be given such that $\kappa \not\equiv 0 \pmod 3$. As usual, for the solutions $(u,v)=(u(s,t),v(s,t))$ of the SFLT equation, put $\rho := \frac{v}{u}$ and call $\xi$ any primitive $n$th root of unity, where $n \,|\, q-1$ is the order of $\rho$ modulo $q$, $n$ assumed prime to 3.

Set $\eta_1 := (1+\xi\, j)^{e_\omega} j^{-\frac{1}{2}}$, then $\mathfrak{q}_{\rho,\xi} := (q, u\,\xi - v)$, and denote by $\mathfrak{Q}$ any prime ideal of $M=LK$ lying above $\mathfrak{q}_{\rho,\xi}$.

Of course, in this study $n$ is not constant when the parameters $s$, $t$ defining the solution $(u,v)$ vary, so that the statistical analysis cannot be done over a fixed field $L=\mathbb{Q}(\mu_n)\subseteq\mathbb{Q}(\mu_{q-1})$. This problem is probably not too tricky since the number of divisors $n$ of $q-1$ is finite, $q$ being fixed.

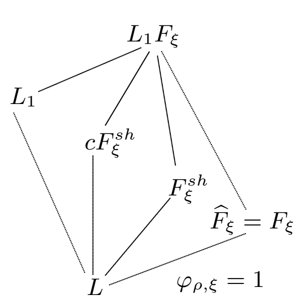
We give below the distribution of the possible cases, which is in a remarkable accordance with the definition of the solutions of the SFLT equation; we summarize this fact by means of the diagram of the compositum $L_1F_\xi$, $L_1 = L\mathbb{Q}_1$; note that $L_1M = M(\sqrt[p]{\zeta})$.

For $p=3$ the compositum $L_1F_\xi$ contains $L_1$, $F_\xi$, and two other cubic fields, $F_\xi^{sh}$ and its conjugate $c\,F_\xi^{sh}$ by the complex conjugation $c$; recall that $F_\xi^{sh}$ and $c\,F_\xi^{sh} = F_{\xi^{-1}}^{sh}$ are the "simplest cubic fields" described in Subsection 5.3, and that $F_\xi/L^+$ is diedral, $L_1/L^+$ Abelian, so that $L_1F_\xi/L^+$ is Galois.

Moreover we get $\widehat{F}_\xi$ among the three extensions distinct from $L_1$ (see Subsection 6.2). We denote by $\sigma$ a generator of $\mathrm{Gal}(F_\xi/L)$ and call $\varphi_{\rho,\xi}$ the Frobenius automorphism of $\mathfrak{q}_{\rho,\xi}$ in $F_\xi/L$. We refer to Theorem 3.3 giving $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M$ for $p=3$, hence the value of the Frobenius automorphism $\varphi_{\rho,\xi}$ in an easy way (Lemma 6.5) by projection of $\left(\frac{M(\sqrt[3]{\eta_1})/M}{\mathfrak{Q}}\right)$ in $\mathrm{Gal}(F_\xi/L)$.

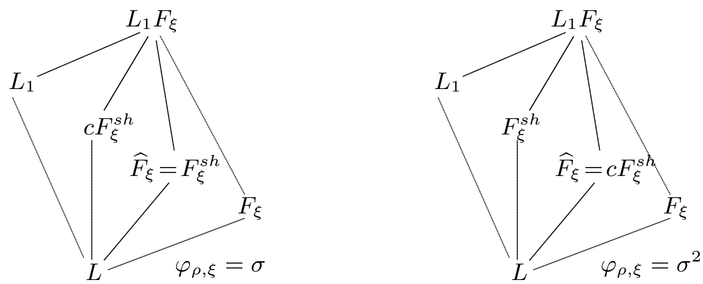
(i) First case ($u\,v\,(u+v)\not\equiv 0 \pmod 3$) corresponding to the relation $u+v\,j = j^2\,(s+t\,j)^3$.

We have $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = j^{-\frac{1}{2}\,\frac{u-v}{u+v}\,\kappa} = 1$ since $u-v\equiv 0 \pmod 3$, $\widehat{F}_\xi = F_\xi$, and the diagram:



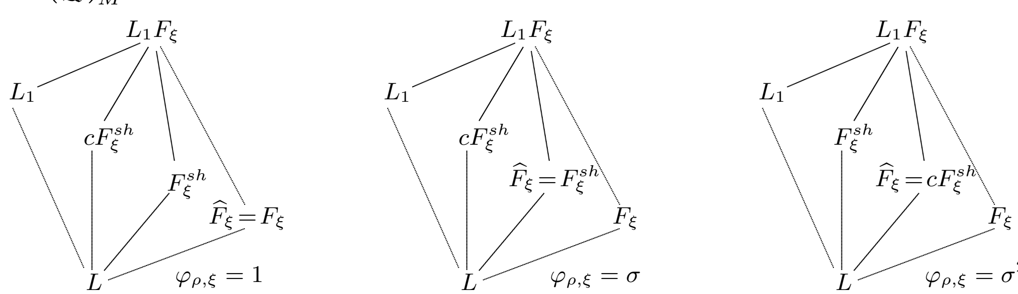

in which $\mathfrak{q}_{\rho,\xi}$ is inert in $F_\xi^{sh}/L$, $cF_\xi^{sh}/L$, and $L_1/L$.

(ii) Second case ($u\,v \equiv 0 \pmod 3$) corresponding to the relations $u + v\,j = (s + t\,j)^3$ and $u + v\,j = j\,(s + t\,j)^3$.
We have $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = j^{-\frac{1}{2}\,\frac{u-v}{u+v}\,\kappa} = j^{\pm\frac{1}{2}\,\kappa} = j$ or $j^2$; we get $\widehat{F}_\xi \neq F_\xi$, and the two equidistributed diagrams




in which $\mathfrak{q}_{\rho,\xi}$ is inert in $F_\xi/L$, $cF_\xi^{sh}/L$, and $L_1/L$.

(iii) Special case ($u+v \equiv 0 \pmod 3$) corresponding to the relations $u+v\,j = j^h\,(j-1)\,(s+t\,j)^3$, $0 \leq h < 3$.
We have $\left(\frac{\eta_1}{\mathfrak{Q}}\right)_M = j^{\frac{1}{2}\,\frac{u+v}{3\,v}\,\kappa} = 1$, $j$, or $j^2$, and the three equidistributed diagrams




in which the decomposition of $\mathfrak{q}_{\rho,\xi}$ assembles all the above cases.

This suggests that the infiniteness of the set of solutions of the SFLT equation and their particular repartition into six families, is a necessary fact for the compatibility with the Čebotarev density theorem.

**8.3. Numerical data for the case $p = 3$.** — We give some numerical experimentations, using [**PARI**], in the case $p = 3$, to highlight the above properties of this case.

We refer to Remark 2.6 for the six expressions of the solutions of the SFLT equation; when we speak of " a solution $(u, v)$", we consider *one* of the six families $(u, v) = (u(s, t), v(s, t))$ with parameters $s$ and $t$.

***Proposition 8.6.*** — *Let $n \geq 1$ be a fixed integer not divisible by 3; for any coprime integers $u$, $v$, let* $\Phi_n(u, v) := \prod_{\xi' \text{ of order } n} (u\,\xi' - v)$.

*(i) For any odd prime $q \equiv 1 \pmod n$, with $q \equiv -1 \pmod 3$ & $\kappa \not\equiv 0 \pmod 3$, there exist an infinite number of pairs $(s, t)$, $s, t \in \mathbb{Z}$ with* g.c.d. $(s, t) = 1$, $s + t \not\equiv 0 \pmod 3$, *such that $q \mid \Phi_n(u, v)$ where $(u, v) := (u(s, t), v(s, t))$ is any fixed family of solutions.*

*More precisely we have the following results:*

*($i_1$) Let $(u',v') := T(u,v) = (u+v, 2v-u)$ be the solution deduced from the action of $T$ (Proposition 8.3). When the images of $\rho = \frac{v}{u}$ and $\rho' = \frac{v'}{u'}$ in $\mathbb{F}_q \cup \{\infty\}$ are in $\mathbb{F}_q^\times$, the conditions $q \,|\, \Phi_n(u,v)$ and $q \,|\, \Phi_{n'}(u',v')$ are equivalent, where $n'$ is the order of $\rho'$ modulo $q$.*

*($i_2$) The prime $q \equiv 1 \pmod n$, with $q \equiv -1 \pmod 3$ & $\kappa \not\equiv 0 \pmod 3$, divides at least one of the integers $\Phi_n(u,v)$, where $(u,v) = (s^3+t^3-3st^2, 3st(s-t))$ (second case), if and only if there exists $\overline{e} \in \mathbb{F}_q^\times$, of order $n$, such that the "simplest cubic polynomial" (see Subsection 5.3) $P^{sh}_{\overline{e}} = X^3 - 3\,\overline{e}^{-1}\,X^2 - 3\,(1-\overline{e}^{-1})\,X + 1$ splits in $\mathbb{F}_q[X]$.*

*($i_3$) For each $\overline{e}$ giving a splitted polynomial $P^{sh}_{\overline{e}}$, the pairs $(s,t)$ giving the solutions $(u,v)$ such that $\rho := \frac{v}{u} \equiv e \pmod q$ and $q \,|\, \Phi_n(u,v)$, are given via the three roots $\overline{\theta}_k \in \mathbb{F}_q^\times$ of $P^{sh}_{\overline{e}}$, by means of the relation $s - t\,\theta_k \equiv 0 \pmod q$, $s,t \in \mathbb{Z}$, $\mathrm{g.c.d.}\,(s,t) = 1$, $s+t \not\equiv 0 \pmod 3$. The image of $\rho$ in $\mathbb{F}_q^\times$ is in the exceptional orbit if and only if $\overline{e} = \overline{2}$.*

*(ii) For any given $q > 2$ ($q \equiv -1 \pmod 3$ & $\kappa \not\equiv 0 \pmod 3$), there exist $\frac{q-2}{3}$ values of $\overline{e}$, of orders $> 2$, such that the polynomial $P^{sh}_{\overline{e}} = X^3 - 3\,\overline{e}^{-1}\,X^2 - 3\,(1-\overline{e}^{-1})\,X + 1$ splits in $\mathbb{F}_q[X]$, then $\frac{q-5}{3}$ values of $\overline{e}$ such that $P^{sh}_{\overline{e}}$ splits and such that $\overline{e}$ is not in the exceptional orbit.*

*(iii) Under the assumptions $n > 2$, $q \equiv 1 \pmod n$, $q \equiv -1 \pmod 3$ & $\kappa \not\equiv 0 \pmod 3$, for any of the six families of solutions $(u,v)$, the relation $q \,|\, \Phi_n(u,v)$ is equivalent to the $\rho := \frac{v}{u}$-splitting of $q$ for the family of "simplest cubic fields" $\mathcal{F}^{sh}_n := \big(F^{sh}_{\xi'}\big)_{\xi' \text{ of order } n}$ $\Big($i.e., equivalent to $\Big[\frac{F^{sh}_*/L}{\mathfrak{q}_*}\Big]_\rho = 1\Big)$ where $F^{sh}_{\xi'}\,K = M\big(\sqrt[3]{(1+\xi' j)^{e'_\omega}}\big)$ (see Subsection 6.2).*

*Proof.* — Let $\xi$ of order $n$ and let $L = \mathbb{Q}(\mu_n)$. Since $\mathrm{g.c.d.}\,(s,t) = 1$ and $s+t \not\equiv 0 \pmod 3$, this yields immediately $\mathrm{g.c.d.}\,(u,v) = 1$ for any solution $(u,v) = (u(s,t), v(s,t))$ among the six families; thus $u$ and $v$ are not divisible by any prime $q$ dividing $\Phi_n(u,v)$ which is homogeneous of the form $u^{\phi(n)} \pm \cdots \pm v^{\phi(n)}$ in coprime integers $u, v$. So the image of $\rho = \frac{v}{u}$ in $\mathbb{F}_q \cup \{\infty\}$ lies in $\mathbb{F}_q^\times$. From Lemma 2.11 and Corollary 2.12, since $q \equiv 1 \pmod n$, $q \,|\, \Phi_n(u,v)$ is thus equivalent to the fact that $\rho = \frac{v}{u}$ is of order $n$ modulo $q$, hence it is equivalent to the fact that $(q, u\,\xi - v) =: \mathfrak{q}_{\rho,\xi}$ is a prime ideal lying above $q$ in $L$.

We first prove that the condition $q \equiv 1 \pmod n$ & $q \,|\, \Phi_n(u,v)$ is independent of the choice of the six solutions given by the action of the powers of $T$ on $(u,v)$. The writings $\rho$, $\rho'$, $n$, $n'$ are always defined except possibly if the image of $\rho = \frac{v}{u}$ in $\mathbb{F}_q \cup \{\infty\}$ is in the exceptional orbit $\{\overline{0};\, -\overline{1};\, \infty;\, \overline{2};\, \overline{1};\, \overline{2}^{-1}\}$, which is equivalent to $q \,|\, s\,t\,(s^2-t^2)\,(2s-t)\,(s-2t)$, see Remark 8.4. Meanwhile, only the cases where the image of $\rho' := \frac{v'}{u'}$ takes the two values $\overline{0}$ ($u - 2v \equiv 0 \pmod q$, $\overline{\rho} = \overline{2}^{-1}$) and $\infty$ ($u + v \equiv 0 \pmod q$, $\overline{\rho} = -\overline{1}$) are not defined.

We suppose implicitly that $\overline{\rho} \notin \{-\overline{1};\, \overline{2};\, \overline{1};\, \overline{2}^{-1}\}$, otherwise we verify directly that if (for instance) $\frac{v}{u} \equiv -1 \pmod q$, we have $\Phi_2(u,v) \equiv \Phi_{n_0}(T^2(u,v)) \equiv \Phi_1(T^3(u,v)) \equiv \Phi_{n_0}(T^4(u,v)) \pmod q$, where $n_0 \,|\, q-1$ is the order of 2 modulo $q$.

Then the set of solutions $(u_i, v_i) := T^i(u,v)$, $0 \leq i < 6$, is such that the orders modulo $q$ of the $\frac{v_i}{u_i}$ are defined and distinct from 1 and 2.

Starting from such a parametric solution $(u,v)$, we fix some prime ideal $\widetilde{\mathfrak{q}} \,|\, \mathfrak{q}_{\rho,\xi}$ in $\widetilde{L} = \mathbb{Q}(\mu_{q-1})$. We then have $u\,\xi - v \equiv 0 \pmod{\widetilde{\mathfrak{q}}}$.

Consider the solution $(u', v')$ defined by $\frac{v'}{u'} := T\big(\frac{v}{u}\big) = \frac{2v-u}{u+v}$. Let $\xi'$ be the unique $(q-1)$th root of unity congruent to $T(\xi) = \frac{2\xi-1}{\xi+1}$ modulo $\widetilde{\mathfrak{q}}$ (the order $n'$ of $\xi'$ divides $q-1$ and is distinct from 1 and 2). Then we have

$$\begin{aligned} u'\,\xi' - v' &\equiv (u+v)\,\frac{2\,\xi-1}{\xi+1} - (2v-u) \\ &\equiv \frac{1}{\xi+1}\big((u+v)\,(2\xi-1) - (2v-u)\,(\xi+1)\big) \equiv \frac{3}{\xi+1}\,(u\,\xi - v) \pmod{\widetilde{\mathfrak{q}}}, \end{aligned}$$

proving the equivalence of the two congruences. The result follows by induction on the powers of $T$ and gives the congruences $u_i\,\xi_i - v_i \equiv 0 \pmod{\widetilde{\mathfrak{q}}}$ for which $\frac{v_i}{u_i} := T^i\big(\frac{v}{u}\big)$, $\xi_i \equiv T^i(\xi) \pmod{\widetilde{\mathfrak{q}}}$, $0 \le i < 6$; each congruence reduces to a congruence modulo $\mathfrak{q}_{\rho_i,\xi_i}$ in $L_i := \mathbb{Q}(\mu_{n_i})$, where $\mathfrak{q}_{\rho_i,\xi_i} = \widetilde{\mathfrak{q}} \cap Z_{L_i}$ and $n_i$ is the order of $\xi_i$.

The orders $n_i > 2$ are divisors of $q-1$, not necessarily equal to $n$ (see Example 8.9). But the conditions $q \,|\, \Phi_{n_i}(u_i, v_i)$ & $n_i > 2$, $0 \le i < 6$, are equivalent to each other. This proves (i$_1$).

So we can chose any family of solutions to prove the assertions (i$_2$) and (i$_3$) for the non exceptional orbit.

For instance, take the general solution of the second case $(3\,|\,v)$, let $\xi$ of order $n\,|\,q-1$, and let $\mathfrak{q} = \mathfrak{q}_{\rho,\xi} \,|\, q$ in $L$; then we have to study the congruence

$$u\,\xi - v = (s^3 + t^3 - 3\,st^2)\,\xi - 3\,st(s-t) \equiv 0 \pmod{\mathfrak{q}}.$$

Put $\theta := \frac{s}{t}$, which yields the congruence $\theta^3 - 3\xi^{-1}\,\theta^2 - 3(1-\xi^{-1})\,\theta + 1 \equiv 0 \pmod{\mathfrak{q}}$.

For fixed $n > 2$, the $\phi(n)$ ideals of $L$ lying above $q \equiv 1 \pmod n$ are the $(q, \xi - e)$, where $e \in \mathbb{Z}$, defined modulo $q$, is of order $n$ in $\mathbb{F}_q^\times$; so the congruence

$$\theta^3 - 3\xi^{-1}\,\theta^2 - 3(1-\xi^{-1})\,\theta + 1 \equiv 0 \pmod{\mathfrak{q} = (q, \xi - e)}$$

is equivalent to

$$\theta^3 - 3e^{-1}\,\theta^2 - 3(1-e^{-1})\,\theta + 1 \equiv 0 \pmod{q}$$

for the choice of $e \equiv \xi \equiv \frac{v}{u} \pmod{\mathfrak{q}}$.

When $q$, $e$ are such that this congruence has a solution, there exist infinitely many $(u,v)$ such that $q \,|\, \Phi_n(u,v)$: for a root $\overline{\theta} \in \mathbb{F}_q^\times$, $\theta \in \mathbb{Z}$, of the above congruence, the parameters $(s,t)$ are obtained from the congruence $s \equiv \theta\, t \pmod q$ (see Example 8.12).

At this step we have proved (i$_2$), (i$_3$) for the non exceptional orbit, under the existence of $e$, of order $n$ modulo $q$, such that $P^{sh}_{\overline{e}} = X^3 - 3\overline{e}^{-1}\,X^2 - 3(1-\overline{e}^{-1})\,X + 1$ splits in $\mathbb{F}_q[X]$.

As we have seen in Subsection 5.3, this splitting happens in $\mathbb{F}_q[X]$ if and only if $\overline{e}$ is of the form $\overline{e}(\overline{a}) := \dfrac{3\,\overline{a}\,(\overline{a}-\overline{1})}{\overline{a}^3 - 3\overline{a} + \overline{1}}$, $\overline{a} \in \mathbb{F}_q \backslash \{\overline{0}, \overline{1}\}$ giving exactly $\frac{q-2}{3}$ distinct solutions $\overline{e}$ in $\mathbb{F}_q^\times$; they are of orders $> 2$ since $\overline{e} = \pm\overline{1}$ are not solutions.

We compute that the exceptional orbit is obtained for the unique value $\overline{e} = \overline{2}$ (obtained for $\overline{a} = -\overline{1}$, $\overline{2}$, $\overline{2}^{-1}$), hence the result in that case.

This proves (ii) and completes the proof of (i).

The polynomial

$$P^{sh}_{\xi} = X^3 - 3\xi^{-1}\,X^2 - 3(1-\xi^{-1})\,X + 1$$

defines the cyclic extension $F_\xi^{sh}$ used in Subsection 5.3; it is the universal Abelian polynomial obtained from the cubic root of $(1+\xi\, j)^{s+2} = \eta_1^{sh}$ up to a 3th power (Subsection 6.3).

Thus, for $q \equiv 1 \pmod n$, the condition $q \,|\, \Phi_n(u,v)$ is equivalent to the $\rho$-splitting of $q$ for $\mathcal{F}_n^{sh}$, where $\rho := \frac{v}{u}$ or to the $\rho_i$-splitting of $q$ for $\mathcal{F}_{n_i}^{sh}$ where $\rho_i := \frac{v_i}{u_i} = T^i(\frac{v}{u})$, and $n_i$ is the order modulo $q$ of $\rho_i$, $0 \le i < 6$. This proves (iii). □

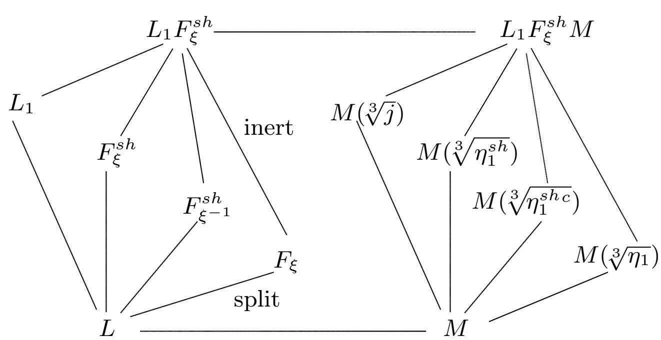
***Remark 8.7***. — For the solution $(u,v)$ of the second case $(3\,|\,v)$ of SFLT, the orders 1 and 2 of $\frac{v}{u} \pmod q$ correspond to the congruences $s^3+t^3-3\,st^2 \pm 3\,st(s-t) \equiv 0 \pmod q$, equivalent to the splitting of the image of $X^3+1-3\,X \pm 3\,X(X-1)$ in $\mathbb{F}_q[X]$. These polynomials define the field $\mathbb{Q}_1$; so, as by assumption $\kappa \not\equiv 0 \pmod 3$, we obtain that the orders 1 and 2 are never possible.

But this property is not necessary satisfied for the solutions $(u_i,v_i) = T^i(u,v)$ of the orbit. For instance, set $q = 11$, $s = 5$, $t = -1$ for which $2\,s - t = 11$. Then for the solution $(u,v) = (-s^3-t^3+3s^2t, -s^3-t^3+3st^2)$ (first case), we get the orbit

$$\left\{ \frac{109}{199}, \frac{19}{308}, \frac{-90}{109}, \frac{-289}{19}, \frac{199}{90}, \frac{308}{289} \right\}$$

giving in $\mathbb{F}_q \cup \{\infty\}$ the exceptional orbit $\{-\overline{1},\ \infty,\ \overline{2},\ \overline{1},\ \overline{2}^{-1},\ \overline{0}\,\}$; so we get $\Phi_2(199,109) = 11.28$; $\Phi_{10}(109,-90) = 11.45365261$; $\Phi_1(19,-289) = 11.28$; $\Phi_{10}(90,199) = 11.100026581$.

***Remark 8.8***. — Consider the following diagram with $\eta'_1 = (1+\xi\, j)^{s+2}\, j^{-\frac{1}{2}}$, $\eta_1^{sh} := \eta'_1\, j^{\frac{1}{2}}$, $(\eta_1^{sh})^c := \eta'_1 j^{-\frac{1}{2}}$, where we know that $M(\sqrt[3]{\eta'_1}) = M(\sqrt[3]{\eta_1})$:




From the Dirichlet–Čebotarev density theorem, we get a precise result taking a Frobenius automorphism of order 6 in $L_1 F_\xi M / F_\xi$, where $L_1 = L\mathbb{Q}_1$, which leads to a prime $q$ such that $q \equiv -1 \pmod 3$ & $\kappa \not\equiv 0 \pmod 3$; then we obtain the ideals $\mathfrak{q}_{\rho,\xi} = (q, u\,\xi - v)\,|\,q$ where the solutions $(u,v)$ are obtained from the roots $\overline{\theta}_1$, $\overline{\theta}_2$, $\overline{\theta}_3$ of the polynomial as explained in $(\mathrm{i}_3)$.

We obtain infinitely many values of $q$ with clearly a nonzero computable density. These primes $q$ give again the splitting of $\mathfrak{q}_{\rho,\xi}$ in $F_\xi/L$, hence its inertia in $L_1/L$, $F_\xi^{sh}/L$, and $F_{\xi^{-1}}^{sh}/L$.

This makes clear the point (i) of the proposition.

***Example 8.9***. — *We illustrate an aspect of Proposition 8.6 with the prime* $q = 41$ *and the solution* $(u,v) = (139193, 76626)$ *of the second case obtained with the parameters* $(s,t) = (-11, 43)$. *We note that* $\frac{v}{u} \equiv 22 \pmod{41}$.

*For* $\overline{e} = \overline{22} \in \mathbb{F}_{41}$ *the polynomial* $X^3 - 3\overline{e}^{-1} X^2 - 3(1 - \overline{e}^{-1}) X + 1$ *splits in* $\mathbb{F}_{41}[X]$ *into* $(X - \overline{38})(X - \overline{31})(X - \overline{15})$ *and we have chosen* $\overline{\theta} = \overline{15}$ *for which* $s - 15\,t \equiv 0 \pmod{41}$.
*Using the automorphism* $T$, *we obtain the six steps*

$$\begin{aligned}
T^0(\overline{e}) &= \overline{e} &= &\ \overline{22} \text{ of order } 40 \\
T^0(\tfrac{v}{u}) &= \tfrac{v}{u} &= &\ \frac{76626}{139193}, \text{ solution of the second case}, \\
T\ (\overline{e}) &= \overline{e}_1 &= &\ \overline{9} \text{ of order } 4 \\
T\ (\tfrac{v}{u}) &= \tfrac{v_1}{u_1} &= &\ \frac{14059}{215819}, \text{ solution of the special case}, \\
T^2(\overline{e}) &= \overline{e}_2 &= &\ \overline{14} \text{ of order } 8 \\
T^2(\tfrac{v}{u}) &= \tfrac{v_2}{u_2} &= &\ \frac{-62567}{76626}, \text{ solution of the second case}, \\
T^3(\overline{e}) &= \overline{e}_3 &= &\ \overline{10} \text{ of order } 5 \\
T^3(\tfrac{v}{u}) &= \tfrac{v_3}{u_3} &= &\ \frac{-201760}{14059}, \text{ solution of the special case},
\end{aligned}$$

$$\begin{aligned}
T^4(\overline{e}) &= \overline{e}_4 &= &\ \overline{39} \text{ of order } 20 \\
T^4(\tfrac{v}{u}) &= \tfrac{v_4}{u_4} &= &\ \frac{139193}{62567}, \text{ solution of the first case}, \\
T^5(\overline{e}) &= \overline{e}_5 &= &\ \overline{5} \text{ of order } 20 \\
T^5(\tfrac{v}{u}) &= \tfrac{v_5}{u_5} &= &\ \frac{215819}{201760}, \text{ solution of the special case}.
\end{aligned}$$

*As a consequence, we have*

$$\begin{aligned}
&\Phi_{40}(139193, 76626) \equiv \Phi_4(215819, 14059) \equiv \Phi_8(76626, -62567) \equiv \\
&\Phi_5(14059, -201760) \equiv \Phi_{20}(62567, 139193) \equiv \Phi_{20}(201760, 215819) \equiv 0 \pmod{41}.
\end{aligned}$$

*We have obtained the set of orders* $\{40, 4, 8, 5, 20\}$.
*This implies the inertia of* $\mathfrak{q}_{\rho,\xi_{40}}$ *in* $F_{\xi_{40}}/\mathbb{Q}(\mu_{40})$ *for* $\rho = \frac{76626}{139193}$ *(second case), that of* $\mathfrak{q}_{\rho',\xi_5}$ *in* $F_{\xi_5}/\mathbb{Q}(\mu_5)$ *for* $\rho' = \frac{-201760}{14059}$, *resp.* $\frac{215819}{201760}$ *(special cases since* $u_3 + v_3 \equiv 3 \pmod 9$, *resp.* $u_5 + v_5 \equiv 6 \pmod 9$*) but the splitting of* $\mathfrak{q}_{\rho'',\xi_4}$ *in* $F_{\xi_4}/\mathbb{Q}(\mu_4)$ *for* $\rho'' = \frac{14059}{215819}$ *(another special case since* $u_1 + v_1 \equiv 0 \pmod 9$*), and the splitting of* $\mathfrak{q}_{\rho''',\xi_{20}}$ *in* $F_{\xi_{20}}/\mathbb{Q}(\mu_{20})$ *for* $\rho''' = \frac{139193}{62567}$ *(solution of the first case), which illustrates the incompatibility with statements like Theorem 5.1 for* $p = 3$.

***Example 8.10***. — *Let* $q$ *be a prime such that* $\kappa \not\equiv 0 \pmod 3$. *Then for a divisor* $m > 2$ *of* $q - 1$, *there is not necessarily a solution* $(u, v) = (s^3 + t^3 - 3\,st^2, 3\,st(s - t))$, $s, t \in \mathbb{Z}$, $\mathrm{g.c.d.}\,(s, t) = 1$, $s + t \not\equiv 0 \pmod 3$, *such that the order* $n$ *of* $\frac{v}{u}$ *modulo* $q$ *is equal to* $m$.
*We have found the following numerical example with* $m = 5$ *for which* $L = \mathbb{Q}(\mu_5)$ *is principal. Consider the prime* $q = 48738631$ *for which* $q - 1 = 2 \cdot 3 \cdot 5 \cdot 163 \cdot 9967$ *and* $\kappa \not\equiv 0 \pmod 3$.
*Let* $\xi$ *be a primitive* 5th *root of unity.*
*Then* $\mathfrak{q} = (\xi^2 + \xi^{-2} - 3 - 90\,(3\,\xi^2 + 5\,\xi + 3))\,\mathbb{Z}[\xi]$ *is a prime ideal lying above* $q$.
*Since* $\xi^2 + \xi^{-2} - 3 \in L^+$, *this ideal satisfies the relation* $\mathfrak{q}^{1-c} = (\alpha)\,\mathbb{Z}[\xi]$, $\alpha \equiv 1 \pmod 9$, *which means that* $q$ *totally splits in* $H_L^-[3]/\mathbb{Q}$.
*Concerning the solutions* $(u, v) = (s^3 + t^3 - 3\,st^2, 3\,st(s - t))$, $s, t \in \mathbb{Z}$, $\mathrm{g.c.d.}\,(s, t) = 1$, $s + t \not\equiv 0 \pmod 3$, *such that* $\Phi_5(u, v) \equiv 0 \pmod q$, *we try to find the smallest values of the order* $n$

*of* $\frac{v}{u}$ *modulo* $q$. *The value* $n = 5$ *is by construction impossible. There is also no solution for* $n = 10$ *since* $\mathbb{Q}(\mu_{10}) = \mathbb{Q}(\mu_5) = L$ *with* $q$ *totally split in* $H_L^-[3]/\mathbb{Q}$.
*We find the values*

$$\begin{aligned} &n = 6 \quad \text{for } (s,t) = (357, 42643),\\ &n = 15 \ \ \text{for } (s,t) = (1531, 3232),\\ &n = 163 \text{ for } (s,t) = (143, 947),\\ &n = 326 \text{ for } (s,t) = (132, 883),\\ &n = 489 \text{ for } (s,t) = (79, 526),\\ &n = 815 \text{ for } (s,t) = (9, 971)\ldots \end{aligned}$$

*As we have seen, the orders* $n = 1$ *and 2 are impossible here.*

***Example 8.11***. — *In another point of view, in the following example we fix the solution* $(u, v) = (19, 18)$ *corresponding to* $(s, t) = (3, 1)$ *of the above second case and we give the order* $n$ *of* $\frac{v}{u}$ *modulo* $q$ *for primes* $q < 3.10^6$ *with* $\kappa \not\equiv 0 \pmod 3$, *such that* $n < q^{\frac{1}{3}}$ *to limit the data.*

| $q$ | $n$ | $q$ | $n$ | $q$ | $n$ | $q$ | $n$ |
|---|---|---|---|---|---|---|---|
| 79 | 3 | 137 | 4 | 751 | 5 | 17341 | 17 |
| 46663 | 11 | 49999 | 13 | 97373 | 44 | 225751 | 43 |
| 352771 | 55 | 419693 | 13 | 464549 | 47 | 536609 | 41 |
| 809359 | 22 | 816401 | 52 | 1037471 | 35 | 1115447 | 41 |
| 1167937 | 84 | 1252057 | 104 | 1403627 | 14 | 1529249 | 32 |
| 1995781 | 29 | 2040601 | 25 | 2743501 | 59 | 2912521 | 39 |

□

***Example 8.12***. — *Let* $q = 113 = 1 + 2^4 . 7$. *In the following example we fix* $n$ *and use a polynomial* $P_{\overline{e}}^{sh} = X^3 - 3\overline{e}^{-1} X^2 - 3(1 - \overline{e}^{-1}) X + 1$ *which splits in* $\mathbb{F}_{113}$; *for* $\overline{e} = 83$, *of order* $n = 14$, *its roots are* $\overline{5}$, $\overline{28}$, *and* $\overline{46}$.

*Recall that for* $\xi$ *of order* $n$ *and* $e \in \mathbb{Z}$ *defining the prime ideal* $\mathfrak{q} = (q, \xi - e) \,|\, q$, *the solutions* $(s, t)$ *giving* $q \,|\, \Phi_n(u, v)$ *for the corresponding solutions* $(u, v) = (s^3 + t^3 - 3st^2, 3st(s-t))$ *of the second case, are defined via the congruences* $s - 5t \equiv 0$, $s - 28t \equiv 0$, $s - 46t \equiv 0 \pmod{113}$, *g.c.d.* $(s, t) = 1$ *and* $s + t \not\equiv 0 \pmod 3$.
*For* $s - 5t \equiv 0 \pmod{113}$ *we obtain*

| $s$ | $t$ | $\Phi_n(u,v)$ |
|---|---|---|
| 118 | 1 | $113 \cdot 3557 \cdot 3942401 \cdot 744072113 \cdot 16254128953756891$ |
| 231 | 1 | $113 \cdot 211 \cdot 239 \cdot 116929 \cdot 550757191489 \cdot 9432961248517529143$ |
| 457 | 1 | $113 \cdot 8821 \cdot 18484859 \cdot 4489993033 \cdot 90773827635383643832209 67$ |
| 123 | 2 | $29 \cdot 43 \cdot 113 \cdot 3011 \cdot 11047 \cdot 1005000683 \cdot 8371388009051383$ |
| 128 | 3 | $113 \cdot 385897 \cdot 8800908691961 \cdot 205376563933889209$ |
| 241 | 3 | $29 \cdot 113 \cdot 3557 \cdot 26209 \cdot 136067 \cdot 2120693 \cdot 2348198329 \cdot 34945284137$ |
| 467 | 3 | $113 \cdot 1451130199 \cdot 66735784434197381694580233562944729 59$ |
| 133 | 4 | $113 \cdot 421 \cdot 43270571265013 \cdot 745141557964566593 33$ |
| 138 | 5 | $113 \cdot 2577267166287809480749101354040384043$ |
| 251 | 5 | $113 \cdot 547 \cdot 2381 \cdot 75688397 \cdot 318274119451 \cdot 4136563302302243$ |
| 477 | 5 | $29 \cdot 113 \cdot 5503 \cdot 26385694924317373 \cdot 33244364936549219215405 03$ |
| 143 | 6 | $113 \cdot 1847609 \cdot 2588587173822250293234785701459$ |
| 148 | 7 | $29 \cdot 113^2 \cdot 265142063021024752248004432557875 3$ |
| 261 | 7 | $113 \cdot 7351 \cdot 67651949 \cdot 2608374259 \cdot 9265394797 \cdot 21291362107$ |
| 487 | 7 | $43 \cdot 113 \cdot 127 \cdot 379 \cdot 2087 \cdot 64303 \cdot 1464961 \cdot 23929487 \cdot 2062162788609847841$ |

*We observe a unique case where* $113^2$ *divides* $\Phi_n(u,v)$.

***Example 8.13.*** — *We consider the prime* $q = 401 = 1+2^4 \,.\, 5^2$*; we give all the possible values taken by the order of* $\rho := \frac{v}{u}$ *modulo* $q$*, for the solutions* $(u,v) = (s^3+t^3-3st^2, 3st(s-t))$ *of the second case.*
*The resolution of* $\dfrac{3st(s-t)}{s^3+t^3-3st^2} \equiv \rho \pmod q$ *is of course equivalent to get the values* $\rho$ *such that the polynomial* $P_\rho^{sh} = X^3 - 3\rho^{-1} X^2 - 3(1-\rho^{-1})\, X + 1$ *splits modulo* $q$.

*We find that there are as expected* $\frac{401-2}{3} = 133$ *distinct values of such* $\rho$ *(Proposition 8.6 (ii)) with the following repartition of the orders* $n$:

*53 for order 400; 28 for 200; 13 for 80; 12 for 100; 7 for 50 and 25; 4 for 40; 3 for 20; 2 for 10; 1 for 16, 8, 5, 4. As we know, orders 1, 2 cannot exist for the second case. The value* $\overline{\rho} = \overline{2}$ *of order* 200*, is associated to the exceptional orbit. These numbers are near from* $\frac{1}{3}\phi(n)$.

## 9. Conclusion

In Subsections 5.3 and 8.1, we have proved that Theorem 5.1 (or any weak form) is of empty use for $p = 3$. We have justified, in Subsection 8.2, why the case $p = 3$ is specific for the arithmetic of the fields $\mathbb{Q}(\mu_n)$ in relation with the Abelian 3-ramification over these cyclotomic fields and the existence of a law of $\rho$-decomposition in the extensions $F_n/\mathbb{Q}(\mu_n)$ (Theorem 6.6); then we have shown how the Čebotarev density theorem applies in this context.

In the two cases the infiniteness of the set of solutions was used, and probably the parametric form of these solutions is an important fact. If we suppose that for $p > 3$ the set of solutions is finite, this suggests that a result like Theorem 6.6, on the constraints fulfilled by infinitely many primes $q$ (due to the laws of $\rho$-decomposition), is a nontrivial obstruction and is likely to lead to a proof of SFLT.

In the same way, Conjectures 5.4 and 6.10 have a particular interest.

In other words, we can hope that for $p > 3$ any statistical analysis of the decomposition laws is legitimate and that it is not excluded that the two main principles of approach of the SFLT problem that we have developed in this paper may be successful for $p > 3$.

However, it should be noted that Theorem 5.1 and Conjecture 5.4 are sufficient diophantine conditions, probably too strong, and that it would be better to consider the constraints given by the laws of $\rho$-decomposition of infinitely many primes $q$ for the canonical families $\mathcal{F}_n$ (see Subsection 6.1, Theorem 6.6, and Conjecture 6.10); this last aspect can be approached from an analytic point of view with the aim to show that such constraints are impossible for $p > 3$. Meanwhile, Conjecture 5.4 is more credible in an analytic point of view and depends on supplementary informations on the order modulo $q$ of a given rational.

About these considerations, an interesting fact would be that the case $p = 3$ would have, in some sense, a reciprocal statement, namely that the infiniteness of the set of solutions of the SFLT equation and their particular repartition into six parametric families, is in fact necessary for the Čebotarev density theorem.

Thus for $p > 3$, in the same spirit as for $p = 3$, the set of nontrivial solutions (if nonempty) would be necessarily infinite with some structural properties in order to be compatible with the above principle, which seems impossible for geometric reasons (Theorem 8.5 for a part).

See an application of this paper in: A product formula related to the diophantine equation $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(u+v\,\zeta)=w_1^p$, $p\nmid uv\,(u^2-v^2)$, *Journal of Algebra, Number Theory: Advances and Applications*, **7**, 2 (2012), 1–38, for which we provide here a summary:

Let $u$, $v$ be coprime integers such that $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(u+v\,\zeta)$ is the $p$th power of an integer, where $\zeta := e^{2i\pi/p}$. Using the Brückner–Vostokov explicit formula, we establish a product formula for the $p$th power residue symbols $\big(\frac{\eta_1}{\Omega}\big)_M$ computed in the present article.
This product formula is equivalent to the relations $\mathrm{Tr}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}\big(\frac{\xi_n-\rho}{1+\xi_n}\,\frac{1}{p}\log(\xi_n-\rho)\big)\equiv 0 \pmod p$, for all integer $n$ ($p\nmid n$, $n\nmid p-1$), where $\xi_n$ is a primitive $n$th root of unity, $\rho := \frac{v}{u}$, log is the $p$-adic logarithm. This allows us to verify, for given values of $p$, the insolubility of the above equation under the assumption $p\nmid uv\,(u^2-v^2)$.
We then show that this insolubility is equivalent to the existence of an integer $n$ ($p\nmid n$, $n\nmid p-1$) such that $\sum_{k=1}^{p-1}\frac{1}{k}\,\rho^k\,\mathrm{Tr}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}\Big(\frac{\xi_n^k}{1+\xi_n^p}\Big)\not\equiv 0 \pmod p$, constituting an alternative to Kummer–Mirimanoff congruences without any reference to Bernoulli numbers.
For instance for $p=5$ and the only possible classes $\rho_0\equiv 2,3 \pmod 5$, the above condition is fulfilled for $n=3$. For $p=37$ and $n=8$, the condition is fulfilled for all $\rho_0$.

**References**

[A–H] L.M. Adleman and D.R. Heath-Brown, The first case of Fermat's last theorem, *Invent. math.* **79** (1985), 409–416.

[Co] L. Corry, On the history of Fermat's last theorem: fresh views on an old tale, *Math. Semesterber.* **57**, 1 (2010), 123–138.

[D] P. Dénes, An extension of Legendre's criterion in connection with the first case of Fermat's last theorem, *Publ. Math. Debrecen* **2** (1951), 115–120.

[Fo] E. Fouvry, Théorème de Brun–Titchmarsh; application au Théorème de Fermat, *Invent. Math.* **79** (1985), 383–407.

[Fur] P. Furtwängler, Letzter Fermatschen Satz und Eisensteins'sches Reciprozitätsgesetz, *Sitzungsber, Akad. Wiss. Wien., Abt. IIa,* **121** (1912), 589–592. Die Reciprozitätsgesetz für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern, II, *Math. Annalen* **72** (1912), 346–386.

[Gr1] G. Gras, Analysis of the classical cyclotomic approach to Fermat's Last Theorem, *Publ. Math. de Besançon, Algèbre et Théorie des Nombres*, Actes de la conférence " Fonctions $L$ et arithmétique ", Besançon 2009. Presses Universitaires de Franche-Comté 2010, 85–119.

[Gr2] G. Gras, Class Field Theory: from theory to practice, SMM, Springer-Verlag, 2003; second corrected printing 2005.

[Gmn] M-N. Gras, Arithmétique des extensions cycliques de $\mathbb{Q}$ de degré 3 et 4, *Publications Mathématiques de l'Université de Laval, Québec* (1984), 27–53.

[Hat] K. Hatada, Chi-square tests for mod 1 distribution of Fermat and Fibonacci quotients, *Sci. Rep. Fac. Educ., Gifu Univ., Nat. Sci.* **12** (1988), 1–2. Mod 1 distribution of Fermat and Fibonacci quotients and values of zeta functions at $2-p$, *Comment. Math. Univ. St. Pauli* **36** (1987), 41–51.

[He1] C. Helou, Norm residue symbol and cyclotomic units, *Acta Arith.* **73** (1995), 147–188. Corrigendum, *Acta Arith.* **98**, 3 (2001), p. 311.

[He2] C. Helou, Proof of a conjecture of Terjanian for regular primes, *C. R. Math. Rep. Acad. Sci. Canada* **18** (1996), 5, 193–198.

[Ko] H. Koch (Parshin, A.N., Šafarevič, I.R., and Gamkrelidze, R.V., Eds.), Number theory II, Algebraic number theory, Encycl. of Math. Sci., vol. 62, Springer-Verlag 1992; second printing: Algebraic Number Theory, Springer-Verlag 1997.

[Kr] M. Krasner, A propos du critère de Sophie Germain–Furtwängler pour le premier cas du théorème de Fermat, *Mathematica, Cluj* **16** (1940), 109–114.

[Le] O. Lecacheux, Surfaces elliptiques modulaires et corps cubiques cycliques, *Ann. Sci. Math. Québec* **28**, 1 (2007), 51-66.

[Len] H.W. Lenstra, Jr., Rational functions invariant under a finite abelian group, *Invent. math.* **25** (1974), 299–325.

[Mih1] P. Mihăilescu, Class number conditions for the diagonal case of the equation of Nagell–Ljunggren, In: Diophantine Approximation, H.P. Schlickewei et al. (Editors), Springer-Verlag 2008, 245–273.

[Mih2] P. Mihăilescu, On Vandiver's best result on FLT1, In: Nonlinear Analysis: Stability, Approximation and Inequalities - A volume dedicated to the 60th anniversary of Themistocles M. Rassias, G. Georgiev, P. Pardalos and H.M. Srivastava (Editors), Springer-Verlag, New York 2012.

[PARI] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, *PARI GP 2.0.12 alpha PowerPC version*, Université Bordeaux I, 1989–1998.

[Que] R. Quême, Complements on Furtwängler's second theorem and Vandiver's cyclotomic integers, preprint 2011.

[Ri] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer-Verlag, 1979.

[ScW] R. Schoof and L.C. Washington, Quintic Polynomials and Real Cyclotomic Fields with Large Class Number, *Mathematics of Computation* **50**, 182 (1988), 543–556.

[Se1] J-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math., Inst. Hautes Étud. Sci.* **54** (1981), 123–202.

[Se2] J-P. Serre, Lectures on $N_X(p)$, AK Peters, Taylor and Francis Research Notes in Mathematics Vol. **11**, New York 2012, 163 pp.

[Sh] D. Shanks, The Simplest Cubic Fields, *Mathematics of Computation* **28** (1974), 1137–1152 .

[Si] S. Sitaraman, Vandiver revisited, *J. Number Theory*, **57, 1** (1996), 122–129.

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

[Van1] H.S. Vandiver, A property of cyclotomic integers and its relation to Fermat's Last Theorem, *Ann. of Math.* **21** (1919/1920), 73–80.

[Van2] H.S. Vandiver, Summary of results and proofs concerning Fermat's Last Theorem, *proceedings of National Academy of Sciences* **12** (1926), 106–109. Summary of results and proofs concerning Fermat's Last Theorem (second note), *proceedings of National Academy of Sciences* **12** (1926), 767–772. Summary of results and proofs concerning Fermat's Last Theorem (third note), *proceedings of National Academy of Sciences* **15** (1928), 43–48.

[Van3] H.S. Vandiver, Application of the Theory of Relative Cyclic Fields to both Cases of Fermat's Last Theorem, *Transaction of the AMS* **28** (1926), 554–560. Application of the Theory of Relative Cyclic Fields to both Cases of Fermat's Last Theorem (second paper), *Transactions of the AMS* **29** (1927), 154–162.

[Wa1] L.C. Washington, Introduction to cyclotomic fields, Springer second edition 1997.

[Wa2] L.C. Washington, Class Numbers of the Simplest Cubic Fields, *Mathematics of Computation* **48**, 177 (1987), 371–384.

*September 25, 2011*

Georges Gras, Villa la Gardette, chemin Château Gagnière, F-38520 Le Bourg d'Oisans
*E-mail :* `g.mn.gras@wanadoo.fr` • *Url :* `http://monsite.orange.fr/maths.g.mn.gras/`

Roland Quême, 13 Avenue du château d'eau, F-31490 Brax • *E-mail :* `roland.queme@wanadoo.fr`
*Url :* `http://roland.queme.free.fr/`