

**Minoration au point 1 des fonctions L et détermination
des corps sextiques abéliens
totalement imaginaires principaux**

par

STÉPHANE LOUBOUTIN (Caen)

THÉORÈME 1. *Avec un $O(\text{Log}^{-1}(f))$ effectif, il existe une constante explicite $\alpha > 0$ telle que pour toute fonction $L(s, \chi)$ associée à un caractère χ de Dirichlet complexe, primitif, non quadratique et défini modulo $f \geq 3$ nous ayons la minoration suivante :*

$$|L(1, \chi)|^2 \geq \frac{1}{\alpha \text{Log}^2(f/\pi)} (1 + O(\text{Log}^{-1}(f))).$$

Nous pouvons prendre $\alpha = 295$, et même $\alpha = 166$ lorsque 3 divise f , et $\alpha = 131$ lorsque f est pair. Si χ est d'ordre 4 ou 6, nous pouvons prendre $\alpha = 165$, et même $\alpha = 93$ lorsque 3 divise f , et $\alpha = 74$ lorsque f est pair.

Cette minoration est le pendant de la majoration $|L(1, \chi)| \leq \frac{1}{2} \text{Log}(f) + O(1)$ valable pour tout caractère de Dirichlet primitif et non principal modulo $f \geq 3$ (voir par exemple [6]).

Si cette minoration est légèrement moins bonne que celle donnée dans le cas particulier des caractères d'ordre 4 dans [3], notre démonstration en est incomparablement plus courte du fait que nous n'avons pas à connaître des majorants pour les modules des fonctions L dans des disques fermés du plan complexe. Après évaluation du $O(\text{Log}^{-1}(f))$ effectif, nous obtenons alors le premier résultat suivant à peine plus faible que celui de [3]: *Soit \mathbf{K} un corps quartique cyclique totalement imaginaire de conducteur f pair. Alors, en notant $h^*(\mathbf{K})$ son nombre de classes relatif, nous avons $h^*(\mathbf{K}) > 2$ pour $f \geq 450000$.*

Ce Théorème 1 est particulièrement bien adapté à la minoration des nombres de classes relatifs des corps abéliens totalement imaginaires pour lesquels ces nombres de classes relatifs peuvent être exprimés en fonction du module d'une seule fonction L . Par exemple, nous avons le second résultat nouveau suivant dont la minoration du nombre de classes relatif amende d'un

facteur $\text{Log}(f)$ celle donnée par K. Uchida dans [10], et dont la minoration du conducteur à partir de laquelle ce nombre de classes relatif est strictement plus grand que 1 est meilleure que celle donnée dans [10] :

THÉORÈME 2. *Soit \mathbf{K} un corps sextique cyclique totalement imaginaire de conducteur f et de nombre de classes relatif $h^*(\mathbf{K})$. Nous avons les minoration suivantes :*

$$h^*(\mathbf{K}) \geq \frac{1}{7300} \cdot \frac{f}{\text{Log}^2(f/\pi)} \quad \text{pour } f \geq 5 \cdot 10^5;$$

$$h^*(\mathbf{K}) \geq \frac{1}{4200} \cdot \frac{f}{\text{Log}^2(f/\pi)} \quad \text{pour } f \geq 5 \cdot 10^5 \text{ et } f \text{ divisible par } 3;$$

$$h^*(\mathbf{K}) \geq \frac{1}{3300} \cdot \frac{f}{\text{Log}^2(f/\pi)} \quad \text{pour } f \geq 5 \cdot 10^5 \text{ et } f \text{ pair.}$$

D'où $h^*(\mathbf{K}) > 1$ pour respectivement $f \geq 1,3 \cdot 10^6$;
 $f \geq 6,3 \cdot 10^5$ et f divisible par 3;
 $f \geq 5 \cdot 10^5$ et f pair.

De même, et avec les notations de [5], soit \mathbf{K} un corps quartique cyclique totalement réel de conducteur F , de nombre de classes $h_{\mathbf{K}}$ et de régulateur R . Soit \mathbf{k} le sous-corps quadratique réel de \mathbf{K} et soient $h_{\mathbf{k}}$ et $R_{\mathbf{k}}$ le nombre de classes et le régulateur de \mathbf{k} . Posons $R^- = R/R_{\mathbf{k}}$ et remarquons que $h_{\mathbf{k}}$ divise $h_{\mathbf{K}}$, de sorte que $h^*(\mathbf{K}) = h_{\mathbf{K}}/h_{\mathbf{k}}$ est entier. La formule analytique du nombre de classes donne

$$h^*(\mathbf{K}) = \frac{1}{4R^-} F |L(1, \chi)|^2,$$

où χ est un des deux caractères de Dirichlet d'ordre 4 et primitif modulo F qui engendre le groupe des caractères associé à \mathbf{K} . De la même manière que nous déduisons ce Théorème 2 du Théorème 1, on montre aisément que la preuve du Théorème 1 conduit au résultat explicite suivant :

$$h^*(\mathbf{K}) \geq \frac{1}{700R^-} \frac{F}{\text{Log}^2(F/\pi)} \quad \text{pour } F \geq 10^3.$$

Cette minoration amende fortement celles données aux Theorem L et Corollary 4.5 de [5], minoration obtenues dans [5] par des méthodes reposant sur les résultats de [9].

THÉORÈME 3. *Les seuls corps sextiques cycliques totalement imaginaires principaux sont ceux de conducteur une des 17 valeurs suivantes :*

- (i) $f = 7$ et alors $\mathbf{K} = \mathbb{Q}(\zeta_7)$, ou $f = 9$ et alors $\mathbf{K} = \mathbb{Q}(\zeta_9)$;
- (ii) $f = 19, 43$ et 67 (et \mathbf{K} est alors le seul sous-corps sextique du corps cyclotomique $\mathbb{Q}(\zeta_f)$) ;
- (iii) Les 12 corps $\mathbf{K} = \mathbf{K}_+ \mathbf{k}_{\text{im}}$ de conducteurs donnés au tableau suivant où \mathbf{K}_+ est l'unique corps cubique cyclique totalement réel de conducteur

$f_{\mathbf{K}_+}$ et \mathbf{k}_{im} l'unique corps quadratique imaginaire de conducteur m :

m	$f_{\mathbf{K}_+}$	3^2	7	13	19	31	43
3			21	39		93	129
4		36	28		76		
7		63		91			
8			56	104			
11			77				

Remarque. Notons que Ken Yamamura est récemment parvenu à déterminer tous les corps abéliens totalement imaginaires principaux : il y a 172 tels corps. Sa détermination s'appuie sur les minoration des nombres de classes relatifs des corps abéliens totalement imaginaires établies par K. Uchida. Avant ce résultat et le nôtre, seuls deux types de corps abéliens totalement imaginaires principaux nous semblent avoir été déterminés : les corps cyclotomiques principaux (voir [7]) et les corps quartiques cycliques principaux (voir [8]).

La preuve du Théorème 1 repose sur le fait bien connu (voir [1]) selon lequel la fonction

$$\xi(s) \stackrel{\text{def}}{=} \left(\frac{f}{\pi}\right)^s \Gamma^2\left(\frac{s + A_\chi}{2}\right) L(s, \chi) L(s, \bar{\chi})$$

avec $A_\chi = \begin{cases} 0 & \text{si } \chi(-1) = +1, \\ 1 & \text{si } \chi(-1) = -1, \end{cases}$

est une fonction entière d'ordre 1 vérifiant

$$\frac{\xi'}{\xi}(s) = \text{Log}\left(\frac{f}{\pi}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{s + A_\chi}{2}\right) + \frac{L'}{L}(s, \chi) + \frac{L'}{L}(s, \bar{\chi}) = \sum_{\varrho} \frac{1}{s - \varrho} + \frac{1}{s - \bar{\varrho}},$$

où $\varrho = \beta + i\gamma$ parcourt les zéros complexes de la fonction $L(s, \chi)$ tels que $0 < \beta < 1$.

LEMME (a).

$$\frac{\zeta'}{\zeta}(s) > -\frac{1}{s-1}, \quad s > 1; \quad \frac{\Gamma'}{\Gamma}(s) < 0, \quad 0 < s \leq \frac{5}{4}.$$

Preuve. Pour $s > 1$ nous avons

$$\zeta(s) = \frac{1}{2^{1-s} - 1} L(s)$$

où $L(s) = \sum_{n \geq 1} (-1)^n / n^s$. Par dérivation logarithmique nous en déduisons

que

$$\frac{\zeta'}{\zeta}(s) = -\frac{\text{Log}(2)}{2^{s-1}-1} + \frac{L'}{L}(s).$$

Maintenant, $2^{s-1}-1 \geq (s-1)\text{Log}(2)$ et pour $s > 1$ les deux séries suivantes étant alternées :

$$L(s) = \sum_{n \geq 1} \frac{(-1)^n}{n^s} \quad \text{et} \quad L'(s) = \sum_{n \geq 2} \frac{(-1)^{n+1} \text{Log}(n)}{n^s},$$

nous avons $L(s) < 0$ et $L'(s) < 0$. D'où le premier résultat, d'ailleurs connu (voir [2]).

Quant au second, il résulte de ce que

$$\frac{\Gamma'}{\Gamma}(s) = -\frac{1}{s} - \gamma + \sum_{n \geq 1} \frac{s}{n(n+s)}$$

est strictement croissante et de ce qu'un calcul numérique donne $(\Gamma'/\Gamma)(5/4) \leq 0$. ■

LEMME (b). Soit $s_0 > 1$. Alors,

$$\frac{1}{|L(s_0, \chi)|^2} \leq \left(\frac{\zeta(s_0)}{\zeta(2s_0)} \right)^2.$$

Preuve. Résulte de

$$\left| 1 - \frac{\chi(p)}{p^{s_0}} \right|^2 \leq \left(1 + \frac{1}{p^{s_0}} \right)^2 = \left(\frac{1 - 1/p^{2s_0}}{1 - 1/p^{s_0}} \right)^2. \quad \blacksquare$$

LEMME (c) (voir [3], Lemma 20). Soit ϱ un nombre complexe tel que $\text{Re}(\varrho) < 1$. Alors,

$$\text{Re} \left(\frac{1}{s - \varrho} \right) \leq \frac{1}{1 - (s_0 - s) \text{Re}(1/(s_0 - \varrho))} \text{Re} \left(\frac{1}{s_0 - \varrho} \right), \quad 1 \leq s \leq s_0.$$

Preuve. Il s'agit de voir que l'on a

$$\text{Re} \left(\frac{1}{s - \varrho} \right) \text{Re} \left(\frac{1}{(s_0 - \varrho)/(s - \varrho)} \right) \leq \text{Re} \left(\frac{1}{s_0 - \varrho} \right).$$

Puisque $\text{Re}(1/z) = \text{Re}(z)/|z|^2$, il s'agit de voir que l'on a

$$\text{Re} \left(\frac{s_0 - \varrho}{s - \varrho} \right) \leq \frac{\text{Re}(s_0 - \varrho)}{\text{Re}(s - \varrho)}.$$

En posant $z = s - \varrho$ et $t = s_0 - s$, il s'agit donc de voir que l'on a

$$\text{Re} \left(\frac{t + z}{z} \right) \leq \frac{\text{Re}(t + z)}{\text{Re}(z)},$$

i.e. que l'on a $\text{Re}(1/z) \leq 1/\text{Re}(z)$. Cela résulte de ce que l'on a $\text{Re}(z) > 0$. ■

LEMME (d). Soit χ un caractère de Dirichlet primitif modulo $f \geq 2$ non principal. Alors, pour $1 \leq s \leq 3/2$ nous avons

$$\frac{L'}{L}(s, \chi) + \frac{L'}{L}(s, \bar{\chi}) \geq -\text{Log}\left(\frac{f}{\pi}\right).$$

Preuve. Cela résulte de

$$\frac{1}{s - \varrho} + \frac{1}{s - \bar{\varrho}} \geq 0$$

pour $s \geq 1$ et $0 \leq \text{Re}(\varrho) < 1$. ■

LEMME (e). Soit χ un caractère de Dirichlet primitif modulo $f \geq 2$ non principal. Soit ψ le caractère primitif induisant χ^2 , et soient $a_0 \geq 0$, $a_1 \geq 0$ et $a_2 \geq 0$ tels que $a_0 + 2a_1 \cos(\theta) + 2a_2 \cos(2\theta) \geq 0$, $\theta \in \mathbb{R}$. Alors, pour $s > 1$ réel nous avons

$$a_0 \zeta'(s) + a_1 \left(\frac{L'}{L}(s, \chi) + \frac{L'}{L}(s, \bar{\chi}) \right) + a_2 \left(\frac{L'}{L}(s, \psi) + \frac{L'}{L}(s, \bar{\psi}) \right) \leq 0.$$

Puisque $2 + 2\sqrt{2} \cos(\theta) + \cos(2\theta) = (\sqrt{2} \cos(\theta) + 1)^2$, alors $(a_0, a_1, a_2) = (4, 2\sqrt{2}, 1)$ convient.

Preuve. Résulte de

$$\frac{L'}{L}(s, \chi) = - \sum_p \sum_{n \geq 1} \frac{\chi(p^n) \text{Log}(p)}{p^{ns}}$$

en posant $\chi(p^n) = e^{i\theta}$ et en remarquant que si $\chi(p^n) = 0$, alors $a_0 + a_1(\psi(p^n) + \bar{\psi}(p^n)) \geq a_0 - 2a_2 \geq 0$ (prendre $\theta = \pi/2$). ■

Preuve du Théorème 1. Supposons ce Lemme (e) satisfait et appliquons à ψ primitif modulo \tilde{f} induisant χ^2 le Lemme (d), en remarquant que $-\text{Log}(\tilde{f}/\pi) \geq -\text{Log}(f/\pi)$. Nous obtenons

$$2a_1 \sum_{L(\varrho, \chi)=0} \text{Re} \left(\frac{1}{s - \varrho} \right) - a_0 \frac{1}{s - 1} \leq (a_2 + a_1) \text{Log} \left(\frac{f}{\pi} \right).$$

Puisque chacun des termes de la sommation précédente est positif ou nul, si ϱ est un zéro quelconque de cette fonction L , nous avons donc

$$2a_1(s_0 - s) \text{Re} \left(\frac{1}{s_0 - \varrho} \right) \leq \left(\frac{a_2 + a_1}{c} + a_0 \right) \frac{s_0 - s}{s_0 - 1},$$

et

$$2a_1 \sum_{L(\varrho, \chi)=0} \text{Re} \left(\frac{1}{s_0 - \varrho} \right) \leq \left(\frac{a_2 + a_1}{c} + a_0 \right) \frac{1}{s_0 - 1},$$

où $s_0 = 1 + 1/(c \text{Log}(f/\pi))$ avec c à choisir plus tard de sorte que nous obtenions une minoration optimale. Du Lemme (c), nous déduisons la majoration suivante:

$$\frac{\xi'}{\xi}(s) \leq 2 \frac{\frac{1}{2a_1} \left(\frac{a_2 + a_1}{c} + a_0 \right) \frac{1}{s_0 - 1}}{1 - \frac{1}{2a_1} \left(\frac{a_2 + a_1}{c} + a_0 \right) \frac{s_0 - s}{s_0 - 1}}.$$

Par intégration entre 1 et s_0 , nous obtenons

$$\frac{\xi(s_0)}{\xi(1)} \leq \left(1 - \frac{1}{2a_1} \left(\frac{a_2 + a_1}{c} + a_0 \right) \right)^{-2}.$$

D'où, d'après le Lemme (b), la minoration

$$(1) \quad |L(1, \chi)|^2 \geq \frac{f(s_0)}{g(c)} \text{Log}^{-2} \left(\frac{f}{\pi} \right)$$

avec

$$(2) \quad f(s_0) = \left(\frac{\zeta(2s_0)}{\pi^2/6} \frac{1}{(s_0 - 1)\zeta(s_0)} \frac{\Gamma((s_0 + A_\chi)/2)}{\Gamma((1 + A_\chi)/2)} \right)^2 = 1 + O(s_0 - 1),$$

et

$$g(c) = \frac{36}{\pi^4} \left(\frac{2a_1 c^2}{(2a_1 - a_0)c - (a_2 + a_1)} \right)^2 \exp \left(-\frac{1}{c} \right).$$

Le choix $(a_0, a_1, a_2) = (4, 2\sqrt{2}, 1)$, $c = 4,35$ nous donne $g(c) \leq 295$ et le résultat désiré.

Lorsque χ est de conducteur divisible par p premier, on a $\chi(p) = 0$ et le Lemme (b) ci-dessus pouvant être amendé en

$$\frac{1}{|L(s_0, \chi)|^2} \leq \left(\frac{p^{s_0}}{p^{s_0} + 1} \right)^2 \left(\frac{\zeta(s_0)}{\zeta(2s_0)} \right)^2,$$

la constante α de ce Théorème 1 peut être amendée en $\frac{9}{16}g(c)$ pour f divisible par 3, et en $\frac{4}{9}g(c)$ pour f pair. D'où le passage de $\alpha = 295$ à $\alpha = 166$ et $\alpha = 131$ dans son énoncé.

Si χ est d'ordre 4 ou 6, l'inégalité sur les fonctions L du Lemme (e) est satisfaite avec $(a_1, a_2, a_3) = (4, 3, 1)$. Nous obtenons alors

$$(3) \quad g(c) = \frac{1}{4} \left(\frac{6}{\pi} \right)^4 h^2(c) \quad \text{avec} \quad h(c) = \frac{c^2}{c-2} \exp \left(-\frac{1}{2c} \right).$$

Cette fonction $c \mapsto h(c)$ passe par son minimum pour $c = c_0 = (7 + \sqrt{65})/4$ et un calcul numérique donne alors $g(c_0) \leq 165$, $\frac{9}{16}g(c_0) \leq 93$ et $\frac{4}{9}g(c_0) \leq 74$. ■

Preuve du Théorème 2. Nous rendons effective la fin de cette preuve du Théorème 1 de la manière suivante : puisque χ est impair on a

$A_\chi = 1$. Nous remarquons alors que $\Gamma(1) = 1$, que $\zeta(s_0) < 1 + 1/(s_0 - 1)$, et que

$$\frac{s_0 + 1}{2} \Gamma\left(\frac{s_0 + 1}{2}\right) = \Gamma\left(1 + \frac{s_0 + 1}{2}\right) \geq \Gamma(2) = 1.$$

D'où la version effective suivante de la formule (2) de la preuve du Théorème 1 :

$$f(s_0) \geq \left(\frac{\zeta(2s_0)}{\pi^2/6} \frac{2}{s_0(s_0 + 1)}\right)^2.$$

Nous verrons au Lemme A(e) ci-dessous que l'on a

$$h^*(\mathbf{K}) \geq \frac{f|L(1, \chi)|^2}{4\pi^2}.$$

Les formules (1) et (3) de la preuve du Théorème 1 donnent donc

$$h^*(\mathbf{K}) \geq \left(\frac{\zeta(2s_0)}{3\pi s_0(s_0 + 1)h(c)}\right)^2 \frac{f}{\text{Log}^2(f/\pi)}.$$

Nous obtenons le résultat en nous rappelant que nous avons posé $s_0 = 1 + 1/(c \text{Log}(f/\pi))$, que nous avons choisi $c = (7 + \sqrt{65})/4$ et que $h(c)$ est donné à la formule (3) de la preuve du Théorème 1. De plus, cette minoration effective peut être amendée du facteur $((p^{s_0} + 1)/p^{s_0})^2$ lorsque p est premier et vérifie $\chi(p) = 0$. ■

Le nombre de classes relatif d'un corps sextique abélien totalement imaginaire. Soit \mathbf{K}/\mathbb{Q} une extension abélienne sextique, donc cyclique. Soient \mathbf{K}_+ le sous-corps cubique totalement réel de \mathbf{K} et \mathbf{k}_{im} le sous-corps quadratique imaginaire de \mathbf{K} , de sorte que $\mathbf{K} = \mathbf{K}_+ \mathbf{k}_{\text{im}}$. Soient f le conducteur de \mathbf{K} , m le conducteur de \mathbf{k}_{im} et $f_{\mathbf{K}_+}$ celui de \mathbf{K}_+ . Soient $H(\mathbf{K})$, $h(\mathbf{K})$, $U(\mathbf{K})$, $W(\mathbf{K})$ et $w(\mathbf{K})$ respectivement le groupe des classes d'idéaux de \mathbf{K} , son nombre de classes, son groupe des unités, son groupe des racines de l'unité et l'ordre de ce groupe de ses racines de l'unité. De même pour \mathbf{K}_+ et \mathbf{k}_{im} . Puisque \mathbf{K} est un corps à multiplication complexe, $h(\mathbf{K}_+)$ divise $h(\mathbf{K})$. Leur quotient noté $h^*(\mathbf{K})$ est appelé le *nombre de classes relatif* de \mathbf{K} , de sorte que $h(\mathbf{K}) = 1$ si et seulement si $h(\mathbf{K}_+) = h^*(\mathbf{K}) = 1$. Soit χ l'un des deux caractères de Dirichlet impairs et primitifs modulo f d'ordre 6 tels que $\{\chi^i; 0 \leq i \leq 5\}$ soit le groupe des caractères associé à \mathbf{K} . Soit χ_{im} le caractère impair et primitif modulo m induisant χ^3 et soit χ_+ le caractère pair et primitif modulo $f_{\mathbf{K}_+}$ induisant χ^2 . Notons que $f = m f_{\mathbf{K}_+}$ et $\chi = \chi_{\text{im}} \chi_+$ dès lors que m et $f_{\mathbf{K}_+}$ sont premiers entre eux. En notant Q l'indice de $W(\mathbf{K})U(\mathbf{K}_+)$ dans $U(\mathbf{K})$ (et on sait qu'il vaut 1 ou 2), nous disposons de la formule analytique suivante pour le nombre de classes relatif

d'un corps à multiplication complexe de degré n (voir [11]) :

$$h^*(\mathbf{K}) = \frac{Qw(\mathbf{K})(\prod_{\chi \text{ impair}} f_{\chi})^{1/2}}{(2\pi)^{n/2}} \prod_{\chi \text{ impair}} L(1, \chi).$$

Dans notre situation (corps sextique abélien totalement imaginaire), en tenant compte de $\sqrt{m}L(1, \chi_{\text{im}}) = (2\pi/w(\mathbf{k}_{\text{im}}))h(\mathbf{k}_{\text{im}})$, elle s'écrit sous les deux formes suivantes :

$$h^*(\mathbf{K}) = Q \frac{w(\mathbf{K})}{w(\mathbf{k}_{\text{im}})} h(\mathbf{k}_{\text{im}}) \frac{f|L(1, \chi)|^2}{4\pi^2},$$

$$h^*(\mathbf{K}) = Q \frac{w(\mathbf{K})}{w(\mathbf{k}_{\text{im}})} h(\mathbf{k}_{\text{im}}) |\tau_{\chi}|^2 \quad \text{avec} \quad \tau_{\chi} \stackrel{\text{def}}{=} -\frac{1}{2f} \sum_{a=1}^{f-1} a\chi(a).$$

Cette première expression pour $h^*(\mathbf{K})$ nous permet au point (e) du lemme ci-dessous de prouver la première assertion du Théorème 2. Cette seconde expression sera utilisée pour le calcul numérique des valeurs de $h^*(\mathbf{K})$ pour \mathbf{K} de conducteur majoré par $1,3 \cdot 10^6$.

LEMME A. (a) $w(\mathbf{K}) = w(\mathbf{k}_{\text{im}})$ excepté lorsque $\mathbf{K} = \mathbb{Q}(\zeta_7), \mathbb{Q}(\zeta_9)$, cas pour lesquels $h(\mathbf{K}) = 1$.

(b) $Q = 1$. Conséquemment, $h^*(\mathbf{K}) = h(\mathbf{k}_{\text{im}}) |\tau_{\chi}|^2$ pour $\mathbf{K} \neq \mathbb{Q}(\zeta_7), \mathbb{Q}(\zeta_9)$.

(c) $h(\mathbf{k}_{\text{im}})$ divise $h(\mathbf{K})$.

(d) Pour $\mathbf{K} \neq \mathbb{Q}(\zeta_7), \mathbb{Q}(\zeta_9)$ nous avons $h(\mathbf{K}) = 1$ si et seulement si les trois conditions suivantes sont satisfaites :

$$h(\mathbf{K}_+) = 1, \quad h(\mathbf{k}_{\text{im}}) = 1, \quad |\tau_{\chi}|^2 = 1.$$

(e) Nous avons $h^*(\mathbf{K}) \geq f|L(1, \chi)|^2/(4\pi^2)$.

Preuve du point (b). Il faut voir que toute unité ε de \mathbf{K} est de la forme $\varepsilon = \zeta\varepsilon_+$ avec ζ une racine de l'unité de \mathbf{K} et ε_+ une unité de \mathbf{K}_+ . Puisque $\bar{\varepsilon}/\varepsilon$ est une racine de l'unité (tous ses conjugués sont de module 1), c'est une racine de l'unité de \mathbf{K} , i.e. $\bar{\varepsilon} = \zeta\varepsilon$ où $\zeta \in W(\mathbf{K})$. En prenant les normes relatives sur \mathbf{k}_{im} et en posant $\eta = N_{\mathbf{K}/\mathbf{k}_{\text{im}}}(\varepsilon)$, nous avons donc $\bar{\eta} = \zeta^3\eta$. De plus, η étant une unité de \mathbf{k}_{im} en est une racine de l'unité. Puisque d'après le (a) nous avons $W(\mathbf{K}) = W(\mathbf{k}_{\text{im}})$ excepté dans les deux cas qu'il exclut, un examen systématique des trois occurrences possibles $W(\mathbf{K}) = \{\pm 1\}, \{\pm 1, \pm i\}$ ou $\{\pm 1, \pm j, \pm j^2\}$ montre que l'on peut dans tous les cas écrire ζ sous la forme $\zeta = \tau/\bar{\tau}$ avec $\tau \in W(\mathbf{K})$. D'où le résultat puisque d'après le Lemme 4.13 de [11], nous avons $Q = 1$ pour les deux corps précédemment exclus du raisonnement.

Preuve du point (c). Si l'extension cubique $\mathbf{K}/\mathbf{k}_{\text{im}}$ était non ramifiée, alors le discriminant absolu $D_{\mathbf{K}}$ du corps \mathbf{K} et celui $D_{\mathbf{k}_{\text{im}}} = -m$ du

corps \mathbf{k}_{im} vérifieraient $|D_{\mathbf{K}}| = |D_{\mathbf{k}_{\text{im}}}^3| = m^3$. D'un autre côté, la formule du conducteur discriminant conduisant à la relation $|D_{\mathbf{K}}| = f^2 f_{\mathbf{K}_+}^2 m$, nous aurions $f f_{\mathbf{K}_+} = m$. Puisque m divise f , nous aurions $f_{\mathbf{K}_+} = 1$, ce qui est évidemment absurde. Conséquemment, l'extension cubique $\mathbf{K}/\mathbf{k}_{\text{im}}$ est totalement ramifiée en au moins une place finie, et un résultat classique de la théorie du corps de classes (voir par exemple le Théorème 10.1 de [11]) nous donne le résultat. Remarquons que l'on pourrait même prouver que $h(\mathbf{k}_{\text{im}})$ divise $h^*(\mathbf{K})$. En effet, des points A) et C) du Lemme 4 de [7] nous déduisons que $|\tau_\chi|^2$ est un entier relatif, excepté lorsque $f = 7$ ou $f = 3^2$. Si $f = 7$, alors \mathbf{K} est de degré 6 et inclus dans $\mathbb{Q}(\zeta_7)$. D'où $\mathbf{K} = \mathbb{Q}(\zeta_7)$. Si $f = 3^2$, on a de même $\mathbf{K} = \mathbb{Q}(\zeta_9)$. Dans ces deux cas, $h(\mathbf{k}_{\text{im}}) = 1$ divise $h^*(\mathbf{K}) = 1$.

Preuve du point (d). Il résulte des trois précédents.

Preuve du point (e). On remarque que $Q(w(\mathbf{K})/w(\mathbf{k}_{\text{im}}))h(\mathbf{k}_{\text{im}})$ est un entier relatif. ■

Si $h(\mathbf{K}) = 1$ alors $h(\mathbf{K}_+) = 1$. Le groupe des classes d'idéaux de \mathbf{K}_+ est donc de 3-rang nul. En conséquence, $f_{\mathbf{K}_+} = 3^2$ ou $f_{\mathbf{K}_+} = p$ avec $p \equiv 1 \pmod{6}$ premier. De plus, puisqu'alors $h(\mathbf{k}_{\text{im}}) = 1$, nous avons $m \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$. Dans un premier temps, nous considérons les trois cas faciles : ceux pour lesquels m et p ne sont pas premiers entre eux. Dans un second temps, nous appellerons *générique* le cas où m et p sont premiers entre eux, de sorte qu'alors $f = mp$ et $\chi = \chi_{\text{im}}\chi_+$. Notons dès maintenant que les corps cubiques cycliques réels de conducteur $3^2, 7, 13, 19, 31$ et 43 sont principaux.

Les trois cas faciles. Dans toute la suite, pour $N \geq 1$ un entier et a un entier relatif, nous notons $\bar{a}^{(N)}$ l'unique entier vérifiant $0 \leq \bar{a}^{(N)} < N$ et $\bar{a}^{(N)} \equiv a \pmod{N}$.

(i) Si $f_{\mathbf{K}_+} = m = p \equiv 1 \pmod{6}$ avec p premier, alors $f = m = p$ et $(\mathbb{Z}/f\mathbb{Z})^*$ est cyclique. S'il est engendré par g , et si $j = e^{2i\pi/3}$, alors χ (ou son conjugué) est défini par $\chi(g) = -j$. D'où (à conjugaison près)

$$\tau_\chi = -\frac{1}{2p} \sum_{k=0}^{p-2} (-j)^k \overline{g^k}^{(p)}.$$

Nous avons donc les valeurs numériques suivantes :

p	7	19	43	67	163
g	3	2	3	2	2
$ \tau_\chi ^2$	$\frac{1}{7}$	1	1	1	4
$h^*(\mathbf{K})$	1	1	1	1	4

(ii) Si $f_{\mathbf{K}_+} = 3^2$ et $m = 3$, alors $\mathbf{K} = \mathbb{Q}(\zeta_9)$ et $h(\mathbf{K}) = 1$.

(iii) Si $f_{\mathbf{K}_+} = 3^2$ et $m \neq 3$, alors χ_+ (ou son conjugué) est défini par $\chi_+(2) = j$ puisque 2 engendre $(\mathbb{Z}/9\mathbb{Z})^*$. Posons $a = x + 9y$, $1 \leq x \leq 9$, $0 \leq y \leq m-1$ dans la somme définissant τ_χ . Puisque $\sum_{y=0}^{m-1} \chi_{\text{im}}(x+9y) = 0$, nous obtenons (à conjugaison près)

$$\begin{aligned} \tau_\chi &= -\frac{1}{2m} \sum_{x=1}^9 \left(\sum_{y=0}^{m-1} y \chi_{\text{im}}(x+9y) \right) \chi_+(x) \\ &= -\frac{1}{2m} \sum_{k=0}^5 \left(\sum_{y=1}^{m-1} y \chi_{\text{im}}(\overline{2^k}^{(9)} + 9y) \right) j^k, \end{aligned}$$

ainsi que le tableau de valeurs numériques suivant:

m	4	8	7	11	19	43	67	163
$h^*(\mathbf{K}) = \tau_\chi ^2$	1	3	1	3	4	13	43	64

Remarque. Le corps cubique cyclique de conducteur 3^2 étant principal, nous avons $h^*(\mathbf{K}) = h(\mathbf{K})$. Puisque l'on a $19 \equiv 1 \pmod{9}$ et $163 \equiv 1 \pmod{9}$, alors 19 et 163 sont totalement décomposés dans le corps cyclotomique de conducteur 3^2 . La Proposition B ci-dessous expliquera la divisibilité par 4 de $h^*(\mathbf{K})$ pour ces valeurs de m . Pour $m = 8$ ou 11, il est aisé de voir que 3 est totalement décomposé dans le corps quadratique imaginaire \mathbf{k}_{im} . La Proposition F expliquera la divisibilité par 3 de $h^*(\mathbf{K})$ pour ces deux valeurs de m .

Le cas générique

(iv) Reste à traiter le cas générique $m \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$ et $f_{\mathbf{K}_+} = p \equiv 1 \pmod{6}$ avec p premier et $p \neq m$, de sorte que $f = mp$, $\chi = \chi_{\text{im}}\chi_+$ et $h^*(\mathbf{K}) = |\tau_\chi|^2$.

PROPOSITION B. *Supposons \mathbf{K}_+ principal. Si un nombre premier est à la fois ramifié dans $\mathbf{k}_{\text{im}}/\mathbb{Q}$ et totalement décomposé dans \mathbf{K}_+/\mathbb{Q} , alors 4 divise $h^*(\mathbf{K})$. Conséquemment, si \mathbf{K} est principal et si p_{im} est le seul nombre premier ramifié dans $\mathbf{k}_{\text{im}}/\mathbb{Q}$, alors p_{im} n'est pas résidu cubique modulo p , i.e. $(p_{\text{im}})^{(p-1)/3} \not\equiv 1 \pmod{p}$.*

Preuve. Soit $H_{\text{reg}}(\mathbf{K})$ le sous-groupe du groupe des classes de \mathbf{K} formé des classes d'idéaux de \mathbf{K} contenant un idéal invariantsous l'action de la conjugaison complexe σ (notons que σ est le \mathbf{K}_+ -isomorphisme non trivial de l'extension quadratique \mathbf{K}/\mathbf{K}_+). Soit t le nombre d'idéaux premiers de \mathbf{K} ramifiés dans \mathbf{K}/\mathbf{K}_+ ; soient \mathbf{P}_i , $1 \leq i \leq t$, ces t idéaux premiers ramifiés de \mathbf{K} , et soit ϕ le morphisme surjectif de $(\mathbb{Z}/2\mathbb{Z})^t$ sur $H_{\text{reg}}(\mathbf{K})$ qui à $\vec{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_t)$ associe la classe de l'idéal $\mathbf{I}_{\vec{\varepsilon}} = \mathbf{P}_1^{\varepsilon_1} \cdots \mathbf{P}_t^{\varepsilon_t}$.

Alors, $\bar{\varepsilon}$ est dans le noyau de ϕ si et seulement si $\mathbf{I}_{\bar{\varepsilon}} = (\alpha)$ avec $\bar{\alpha} = \eta\alpha$ où η est une unité de \mathbf{K} . Semblablement à la preuve du Lemme A(b), nous avons $\eta \in W(\mathbf{K})$. Conséquemment, le noyau de ϕ est isomorphe à $W(\mathbf{K})/W^{1-\sigma}(\mathbf{K}) = W(\mathbf{K})/W^2(\mathbf{K})$, donc est d'ordre 2. Donc 2^{t-1} divise $h(\mathbf{K})$. Sous les hypothèses de cette proposition, nous avons $t \geq 3$. (En effet, soient $\mathfrak{p}_1, \mathfrak{p}_2$ et \mathfrak{p}_3 les 3 idéaux premiers de \mathbf{K}_+ au dessus de q premier totalement décomposé dans \mathbf{K}_+/\mathbb{Q} . Puisque q est ramifié dans $\mathbf{k}_{\text{im}}/\mathbb{Q}$, alors chaque \mathfrak{p}_i est ramifié dans \mathbf{K}/\mathbf{K}_+ .) D'où le résultat. ■

COROLLAIRE C (Calcul numérique de τ_χ pour p et m donnés). *Supposons \mathbf{K}_+ principal. Nous avons*

$$\tau_\chi = -\frac{1}{6m} \sum_{x=1}^{p-1} \sum_{y=1}^{m-1} y \left(\chi_{\text{im}}(\bar{x}^3)^{(p)} + py) + \chi_{\text{im}}(\overline{p_{\text{im}}x^3})^{(p)} + py) + \chi_{\text{im}}(\overline{p_{\text{im}}^2x^3})^{(p)} + py) \right).$$

Preuve. Posons $a = x + py$ dans la formule $\tau_\chi = -(2f)^{-1} \sum_{a=1}^{f-1} a\chi(a)$. Nous obtenons

$$\tau_\chi = -\frac{1}{2m} \sum_{x=1}^{p-1} \left(\sum_{y=1}^{m-1} y\chi_{\text{im}}(x + py) \right) \chi_+(x).$$

Le résultat découle de ce que cette Proposition B donne qu'un système de représentants du groupe quotient \mathbf{H}/\mathbf{H}^3 (où $\mathbf{H} = (\mathbb{Z}/p\mathbb{Z})^*$) est donné par $\{1, p_{\text{im}}, p_{\text{im}}^2\}$. ■

THÉORÈME 4. *Soient m et p premiers entre eux. Soit $w(m)$ le nombre de racines de l'unité du corps quadratique imaginaire \mathbf{k}_{im} . Posons*

$$S_m(A, p) \stackrel{\text{def}}{=} \sum_{B=1}^{m-1} B\chi_{\text{im}}(A + pB)$$

(qui ne dépend que de A modulo m et de p modulo m). Alors,

$$\begin{aligned} \text{(a)} \quad \tau_\chi + \bar{\tau}_\chi &= \frac{\chi_{\text{im}}(p) - 1}{w(m)} - \frac{3}{m} \sum_{\substack{A=1 \\ \chi_+(A)=+1}}^{(p-1)/2} S_m(A, p), \\ \text{(b)} \quad \tau_\chi + \bar{\tau}_\chi &= \frac{\chi_{\text{im}}(p) - 1}{w(m)} - \frac{1}{m} \sum_{X=1}^{(p-1)/2} S_m(\bar{X}^3)^{(p)}, p). \end{aligned}$$

Preuve. De l'expression de τ_χ donnée au cours de la preuve du corollaire précédent et de $\chi_+(x) + \bar{\chi}_+(x) + 1 = 3$ ou 0 suivant que $\chi_+(x) = 1$ ou

$\chi_+(x) \neq 1$, nous déduisons

$$\begin{aligned} \tau_\chi + \bar{\tau}_\chi &= -\frac{3}{2m} \sum_{\substack{x=1 \\ \chi_+(x)=+1}}^{p-1} \left(\sum_{y=1}^{m-1} y\chi_{\text{im}}(x+py) \right) \\ &\quad + \frac{1}{2m} \sum_{x=1}^{p-1} \left(\sum_{y=1}^{m-1} y\chi_{\text{im}}(x+py) \right). \end{aligned}$$

Pour évaluer cette dernière somme double, nous remarquons que d'un côté:

$$\begin{aligned} \sum_{a=1}^{f-1} a\chi_{\text{im}}(a) &= \sum_{x=0}^{p-1} \sum_{y=0}^{m-1} (x+py)\chi_{\text{im}}(x+py) \\ &= p \sum_{x=0}^{p-1} \sum_{y=0}^{m-1} y\chi_{\text{im}}(x+py) \quad \text{car} \quad \sum_{y=0}^{m-1} \chi_{\text{im}}(x+py) = 0 \\ &= p \sum_{x=1}^{p-1} \sum_{y=1}^{m-1} y\chi_{\text{im}}(x+py) - p \frac{2m}{w(m)} \chi_{\text{im}}(p) \\ &\quad \text{car} \quad \sum_{y=1}^{m-1} y\chi_{\text{im}}(y) = -\frac{2m}{w(m)}; \end{aligned}$$

et que d'un autre côté, nous avons également

$$\begin{aligned} \sum_{a=1}^{f-1} a\chi_{\text{im}}(a) &= \sum_{x=0}^{p-1} \sum_{y=0}^{m-1} (y+mx)\chi_{\text{im}}(y+mx) \\ &= p \sum_{y=1}^{m-1} y\chi_{\text{im}}(y) = -p \frac{2m}{w(m)}. \end{aligned}$$

D'où

$$\tau_\chi + \bar{\tau}_\chi = \frac{\chi_{\text{im}}(p) - 1}{w(m)} - \frac{3}{m} \sum_{\substack{A=1 \\ \chi_+(A)=+1}}^{p-1} S_m(A, p).$$

Le point (a) résulte alors de ce que $S_m(A, p) = S_m(p - A, p)$ (poseri $B = m - 1 - B'$ dans $S_m(p - A, p)$ et utiliser l'imparité de χ_{im}). Le point (b) se déduit du point (a) en posant premièrement $A = \overline{X^3}^{(p)}$, $1 \leq X \leq p-1$, et en utilisant à nouveau la relation $S_m(A, p) = S_m(p - A, p)$. ■

COROLLAIRE D. *Soit $p \equiv 1 \pmod{6}$ premier avec $p \neq m$.*

(a) *Pour $m \in \{7, 8, 11, 19, 43, 67, 163\}$, la trace $\tau_\chi + \bar{\tau}_\chi$ de τ_χ est un*

entier relatif tel que

$$\tau_\chi + \bar{\tau}_\chi \equiv \frac{\chi_{\text{im}}(p) - 1}{2} \pmod{3},$$

de sorte que 3 divise $h^*(\mathbf{K})$ si et seulement si $\chi_{\text{im}}(p) = \left(\frac{-m}{p}\right) = +1$.

(b) Pour $m = 4$, la trace $\tau_\chi + \bar{\tau}_\chi$ de τ_χ est un entier relatif tel que

$$\tau_\chi + \bar{\tau}_\chi \equiv \frac{\chi_{\text{im}}(p) - p}{4} \pmod{3},$$

de sorte que 3 divise $h^*(\mathbf{K})$ si et seulement si $\chi_{\text{im}}(p) = \left(\frac{-4}{p}\right) = +1$.

(c) Pour $m = 3$, la trace $\tau_\chi + \bar{\tau}_\chi$ de τ_χ est un entier relatif tel que

$$\tau_\chi + \overline{\tau_\chi} \equiv \frac{p-1}{6} \pmod{3},$$

de sorte que 3 divise $h^*(\mathbf{K})$ si et seulement si $p \equiv 1 \pmod{18}$.

(d) Dans le cas générique, τ_χ est un entier algébrique du corps $\mathbb{Q}(\sqrt{-3})$, de sorte que si $h^*(\mathbf{K}) = 1$ alors $|\tau_\chi + \bar{\tau}_\chi| = 1$ ou 2.

Preuve. Remarquons préalablement que $\chi_+(A) = +1$ si et seulement si $\chi_+(p-A) = +1$ (car χ_+ est pair), et qu'il y a donc exactement $(p-1)/6$ entiers A vérifiant $1 \leq A \leq (p-1)/2$ et $\chi_+(A) = +1$. Pour le premier point, on remarque que $S_m(A, p)$ est divisible par m . Pour le deuxième point, on remarque que $S_4(A, p) - 2$ est divisible par 4 (car il vaut $-4, 0$ ou $+4$) et que

$$\tau_\chi + \bar{\tau}_\chi = \frac{\chi_{\text{im}}(p) - p}{4} - \frac{3}{4} \sum_{\substack{A=1 \\ \chi_+(A)=+1}}^{(p-1)/2} (S_4(A, p) - 2).$$

Pour le troisième point, on remarque de même que $w(m) = 6$, que $\chi_{\text{im}}(p) = +1$ (car on a $p \equiv 1 \pmod{6}$), que $S_3(A, p) + 1$ est divisible par 3 (car il vaut 0 ou 3) et que

$$\tau_\chi + \bar{\tau}_\chi = \frac{p-1}{6} - \sum_{\substack{A=1 \\ \chi_+(A)=+1}}^{(p-1)/2} (S_3(A, p) + 1).$$

Pour le dernier point, on remarque que la norme $|\tau_\chi|^2 = h^*(\mathbf{K})$ et la trace $\tau_\chi + \bar{\tau}_\chi$ de τ_χ sont des entiers relatifs. ■

Notons que la preuve de ce corollaire précédent donne

COROLLAIRE E. (a) Pour $\mathbf{k}_{\text{im}} = \mathbb{Q}(\sqrt{-3})$ et $f_{\mathbf{K}_+} = p \equiv 1 \pmod{6}$, nous avons

$$\tau_\chi + \bar{\tau}_\chi = \frac{p-1}{6} - |\mathbf{F}_3|$$

où $\mathbf{F}_3 = \{X ; 1 \leq X \leq (p-1)/2 \text{ et } \overline{X^3}^{(p)} \equiv 2 \pmod{3}\}$.

(b) Pour $\mathbf{k}_{\text{im}} = \mathbb{Q}(\sqrt{-1})$ et $f_{\mathbf{K}_+} = p \equiv 7 \pmod{12}$, nous avons

$$\tau_\chi + \bar{\tau}_\chi = |\mathbf{F}_4| - \frac{p+1}{4}$$

où $\mathbf{F}_4 = \{X ; 1 \leq X \leq (p-1)/2 \text{ et } \overline{X^3}^{(p)} \equiv 1, 2 \pmod{4}\}$.

Les calculs numériques et la preuve du Théorème 3. Nous expliquons maintenant comment, dans le cas générique, ont été conduits les calculs numériques donnant les valeurs de p pour lesquelles $h^*(\mathbf{K}) = |\tau_\chi|^2 = 1$.

Pour $m = 3$, si $h^*(\mathbf{K}) = 1$ alors $f_{\mathbf{K}_+} = p$ est premier avec $p \equiv 1 \pmod{6}$, avec $p \leq 210000$ (Théorème 2), avec $3^{(p-1)/3} \not\equiv 1 \pmod{p}$ (Proposition B), avec $p \not\equiv 1 \pmod{18}$ et avec $|\tau_\chi + \bar{\tau}_\chi| = |(p-1)/6 - |\mathbf{F}_3|| = 1$ ou 2 (Corollaire D(c),(d) et Corollaire E(a)). Nous avons programmé sur micro-ordinateur le criblage des p premiers satisfaisant à successivement toutes ces contraintes. Nous avons obtenu les résultats suivants:

Il y a 9390 nombres premiers $p \equiv 1 \pmod{6}$ tels que $p \leq 210000$.

Seuls 6280 d'entre eux vérifient de plus $3^{(p-1)/3} \not\equiv 1 \pmod{p}$.

Seuls 4185 de ces derniers vérifient de plus $p \not\equiv 1 \pmod{18}$.

Seuls 84 de ces derniers vérifient de plus $|\tau_\chi + \bar{\tau}_\chi| = 1$ ou 2 (le plus grand d'entre eux étant $p = 209311$).

Le calcul de $h^*(\mathbf{K}) = |\tau_\chi|^2$ pour ces 84 valeurs de p à l'aide de l'expression pour τ_χ donnée au Corollaire C nous donne finalement la première ligne du tableau du Théorème 3, i.e. les 4 valeurs de p pour lesquelles $h^*(\mathbf{K}) = 1$, et donc pour lesquelles $h(\mathbf{K}) = 1$ puisque les corps cubiques cycliques de conducteurs 7, 13, 31 et 43 sont principaux.

Pour $m = 4$, on procède de même en remarquant que si $h^*(\mathbf{K}) = 1$, alors $f_{\mathbf{K}_+} = p$ est premier avec $p \equiv 7 \pmod{12}$ (Corollaire D(b)) et en utilisant le Corollaire E(b) pour calculer la trace de τ_χ . D'où la seconde ligne de ce même tableau.

Pour les 7 autres valeurs possibles de m , i.e. pour $m \in \{7, 8, 11, 19, 43, 67, 163\}$, les calculs numériques suivent le plan suivant :

(a) Pour m fixé, on précalcule premièrement le tableau des $S_m(\alpha, \beta)$, $0 \leq \alpha, \beta \leq m-1$.

(b) On fait secondement varier $p \equiv 1 \pmod{6}$ jusqu'à la borne donnée par le Théorème 2 (i.e. jusqu'à $f = mp \leq 1,3 \cdot 10^6$ pour $m \neq 8$) parmi les nombres premiers tels que $p_{\text{im}}^{(p-1)/3} \neq 1$, puis tels que $\chi_{\text{im}}(p) = \left(\frac{-m}{p}\right) = -1$ (ces deux dernières contraintes retiennent qu'approximativement le tiers des nombres premiers satisfaisant à la congruence $p \equiv 1 \pmod{6}$).

(c) On fixe alors p et on pose $\beta \stackrel{\text{def}}{=} \bar{p}^{(m)}$.

(d) Pour cette valeur fixée de p et d'après le Théorème 4(b), on calcule

$$\tau_\chi + \bar{\tau}_\chi = -1 - \frac{1}{m} \sum_{X=1}^{(p-1)/2} S_m(\overline{X^3}^{(p)}, p)$$

en calculant $Y \stackrel{\text{def}}{=} \overline{X^3}^{(p)}$ et $\alpha \stackrel{\text{def}}{=} \overline{Y}^{(m)}$, et en allant chercher $S_m(\overline{X^3}^{(p)}, p) = S_m(\alpha, \beta)$ dans le tableau précalculé à la première étape.

(e) Finalement, si $|\tau_\chi + \bar{\tau}_\chi|^2 = 1$ ou 2 , on calcule τ_χ à l'aide du Corollaire C. Semblablement au cas $m = 3$ détaillé précédemment, cette évaluation numérique de τ_χ n'étant à faire que pour peu de valeurs de p , nous n'avons pas à en programmer une version sophistiquée.

Considéré comme une fonction de m , le temps de calcul de cet algorithme est *grosso modo* une fonction quadratiquement décroissante de m , donc de plus en plus bref. Pour $m = 3$, le cas le plus gourmand, il nous a suffi d'une quinzaine d'heures de calcul sur micro-ordinateur avec un programme écrit en Turbo Pascal. ■

Nous concluons cet article en donnant une preuve algébrique du Corollaire D(a), (b).

PROPOSITION F. *Soit \mathbf{K} un corps sextique abélien totalement imaginaire de sous-corps cubique réel cyclique \mathbf{K}_+ et de sous-corps quadratique imaginaire \mathbf{k}_{im} . Supposons \mathbf{k}_{im} principal et $\mathbf{k}_{\text{im}} \neq \mathbb{Q}(\sqrt{-3})$. Si un nombre premier est à la fois ramifié dans \mathbf{K}_+/\mathbb{Q} et totalement décomposé dans $\mathbf{k}_{\text{im}}/\mathbb{Q}$, alors 3 divise $h(\mathbf{K})$. Conséquemment, si \mathbf{K} est principal et si p est le seul nombre premier ramifié dans \mathbf{K}_+/\mathbb{Q} , alors $(\frac{-m}{p}) \neq -1$.*

Preuve. Nous procédons semblablement à la Proposition B. Soit $\tilde{H}_{\text{reg}}(\mathbf{K})$ le sous-groupe du groupe des classes de \mathbf{K} formé des classes d'idéaux de \mathbf{K} contenant un idéal invariant sous l'action de σ , où σ est un générateur du groupe de Galois de $\mathbf{K}/\mathbf{k}_{\text{im}}$ qui est cyclique d'ordre 3. Soit \tilde{t} le nombre d'idéaux premiers de \mathbf{K} ramifiés dans $\mathbf{K}/\mathbf{k}_{\text{im}}$; soient \mathbf{P}_i , $1 \leq i \leq \tilde{t}$, ces \tilde{t} idéaux premiers ramifiés de \mathbf{K} , et soit $\tilde{\phi}$ le morphisme surjectif de $(\mathbb{Z}/3\mathbb{Z})^{\tilde{t}}$ sur $\tilde{H}_{\text{reg}}(\mathbf{K})$ qui à $\vec{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_{\tilde{t}})$ associe la classe de l'idéal $\mathbf{I}_{\vec{\varepsilon}} = \mathbf{P}_1^{\varepsilon_1} \dots \mathbf{P}_{\tilde{t}}^{\varepsilon_{\tilde{t}}}$. Alors, $\vec{\varepsilon}$ est dans le noyau de $\tilde{\phi}$ si et seulement si $\mathbf{I}_{\vec{\varepsilon}} = (\alpha)$ avec $\sigma(\alpha) = \eta\alpha$ où η est une unité de \mathbf{K} telle que $N_{\mathbf{K}/\mathbf{k}_{\text{im}}}(\eta) = +1$. Soit donc $U_1(\mathbf{K})$ le groupe des unités de \mathbf{K} satisfaisant à $N_{\mathbf{K}/\mathbf{k}_{\text{im}}}(\eta) = +1$. Il est immédiat que le noyau de $\tilde{\phi}$ est isomorphe à $U_1(\mathbf{K})/U_1^{1-\sigma}(\mathbf{K})$. Puisque $U(\mathbf{K}) = W(\mathbf{K})U(\mathbf{K}_+)$ et que pour x dans \mathbf{K}_+ nous avons $N_{\mathbf{K}/\mathbf{k}_{\text{im}}}(x) = N_{\mathbf{K}_+/\mathbb{Q}}(x)$, nous en déduisons que $U(\mathbf{K}) = W(\mathbf{K})U_1(\mathbf{K})$ et que le noyau de $\tilde{\phi}$ est isomorphe à $U_1(\mathbf{K})/U_1^{1-\sigma}(\mathbf{K})$. De plus, $U_1(\mathbf{K})$ est un \mathbb{Z} -module de rang fini, et sans torsion lorsque $W(\mathbf{K})$ ne contient pas de racine cubique de l'unité. Puisque $U_1(\mathbf{K})$ est un $\mathbb{Z}[\sigma]/(1 + \sigma + \sigma^2)$ -module de rang fini

également sans torsion lorsque $W(\mathbf{K})$ ne contient pas les racines cubiques de l'unité, il est libre et de rang 1, donc isomorphe à $\mathbb{Z}[\sigma]/(1 + \sigma + \sigma^2)$, donc isomorphe à $\mathbb{Z}[j]$. Le noyau de $\tilde{\phi}$ est donc de cardinal égal à celui de $\mathbb{Z}[j]/(1 - j)$, i.e. de cardinal 3. D'où le résultat semblablement à la Proposition B. ■

Remarque finale. Notons que pour établir notre Théorème 2, il ne nous est pas nécessaire de supposer connue la détermination des corps quadratiques imaginaires principaux (Théorème de Baker–Stark). Il nous suffit de savoir qu'il en existe précisément 9 de conducteurs m tels que $m \leq f/p \leq f/7 \leq 2 \cdot 10^5$ (Lemme A(e)), résultat lui sans profondeur puisque ressortant tout simplement à un calcul numérique.

Références

- [1] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Math.74, 2nd ed., Springer, 1980.
- [2] H. Delange, *Une remarque sur la dérivée logarithmique de la fonction zêta de Riemann*, Colloq. Math. 53 (1987), 333–335.
- [3] K. Hardy, R. H. Hudson, D. Richman and K. S. Williams, *Determination of all imaginary cyclic quartic fields with class number 2*, Trans. Amer. Math. Soc. 311 (1989), 1–55.
- [4] E. Landau, *Über Dirichletsche Reihen mit komplexen Charakteren*, J. Reine Angew. Math. 157 (1926), 26–32.
- [5] A. J. Lazarus, *On the class number and unit index of simplest quartic fields*, Nagoya Math. J. 121 (1991), 1–13.
- [6] S. Louboutin, *Majoration au point 1 des fonctions L associées aux caractères de Dirichlet primitifs, ou au caractère d'une extension quadratique d'un corps quadratique imaginaire principal*, J. Reine Angew. Math. 419 (1991), 213–219.
- [7] J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization*, ibid. 286/287 (1976), 248–256.
- [8] B. Setzer, *The determination of all imaginary, quartic, abelian number fields with class number 1*, Math. Comp. 35 (1980), 1383–1386.
- [9] H. M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. 23 (1974), 135–152.
- [10] K. Uchida, *Imaginary abelian number fields with class number one*, Tôkoku Math. J. 24 (1972), 487–499.
- [11] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer, 1982.

UNIVERSITÉ DE CAEN, U.F.R. SCIENCES DÉPARTEMENT DE MATHÉMATIQUES ESPLANADE DE LA PAIX F-14032 CAEN CEDEX, FRANCE

Reçu le 28.6.1991
et révisé le 26.2.1992

(2153)