Journal de Théorie des Nombres
de Bordeaux **8** *(1996), 75–92*

Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer

par Stéphane JEANNIN

Résumé. Le but de cet article est l'étude des corps cycliques quintiques définis par les polynômes d'E. Lehmer. On calcule premièrement le conducteur de ces corps dans le cas général (non nécessairement premier) puis on généralise un théorème (qui donne les unités de ces corps) démontré par R. Schoof et L.C. Washington. Par la méthode de dévissage des unités cyclotomiques, qui calcule le nombre de classes et les unités, on dresse une table de ces corps particuliers (de conducteur $f \leq 3000000$) et de leur nombre de classes. L'article se termine par une comparaison des différentes bornes majorant le nombre de classes de ces corps.

Abstract. The aim of this article is to study quintic cyclic fields defined by E. Lehmer's polynomials. We first compute the conductor of these fields in the general case (not necessarily prime) then we generalize a theorem proved by R. Schoof and L.C. Washington (which gives the units of these fields). By the method of "dévissage" of cyclotomic units, wich computes the class number and the units, we draw up a table for these particular fields (of conductor $f \leq 3000000$) and their class numbers. Finally we compare different upper bounds for the class number of these fields.

1. Introduction.

En 1986, E. Lehmer a exhibé dans [Le] une famille de corps de nombres cycliques et de degré 5, dont le groupe des unités est engendré par des unités de petite taille et conduisent donc à des grands nombres de classes. Cette famille de corps est définie par les polynômes irréductibles :

$$\begin{aligned}(1)\quad & F_t(x) = x^5 + t^2x^4 - (2t^3 + 6t^2 + 10t + 10)x^3 \\ & +(t^4 + 5t^3 + 11t^2 + 15t + 5)x^2 + (t^3 + 4t^2 + 10t + 10)x + 1,\ \ t \in \mathbb{Z},\end{aligned}$$

Manuscrit reçu le 25 mars 1995.

dont le discriminant est $(t^3+5t^2+10t+7)^2 P_t^4$, où :

$$P_t = t^4 + 5t^3 + 15t^2 + 25t + 25. \tag{2}$$

Dans le cas où P_t est un nombre premier p (qui est alors le conducteur du corps), les racines du polynôme $F_t(x)$ sont liées aux périodes de Gauss définies ainsi (cf. [La]) :
On note C_j, $j = 0, ..., 4$, les classes du quotient de $(\mathbb{Z}/p\mathbb{Z})^\times$ par $((\mathbb{Z}/p\mathbb{Z})^\times)^5$:

$$C_j = \{g^{5v+j} \bmod p \ ; \ v = 0, ..., (p-1)/5 - 1\}, \quad j = 0, ..., 4,$$

où g est une racine primitive modulo p. Les périodes de Gauss sont alors définies par :

$$\eta_j = \sum_{x \in C_j} e^{2i\pi x/p}, \quad j = 0, ..., 4.$$

Les racines de $F_t(x)$ sont désignées par θ_j, $j = 0, ..., 4$, et sont définies par :

$$\theta_j = \left(\frac{t}{5}\right)\eta_j + \left(\left(\frac{t}{5}\right) - t^2\right)/5, \quad j = 0, ..., 4,$$

où $\left(\frac{t}{5}\right)$ désigne le symbole de Legendre modulo 5.
En 1988, R. Schoof et L.C. Washington ont étudié dans [SW] la famille de corps de nombres d'E. Lehmer (au niveau de leurs unités et de leur nombre de classes) dans le cas où P_t est un nombre premier. On tire de [SW] quelques résultats élémentaires sur $F_t(x)$, valables pour tout $t \in \mathbb{Z}$:
i) $F_t(x)$ est irréductible sur $\mathbb{Q}$;
ii) les zéros de $F_t(x)$ engendrent une extension cyclique de degré 5 sur $\mathbb{Q}$. En effet la transformation :

$$x \longrightarrow \frac{t+2+tx-x^2}{1+(t+2)x} \tag{3}$$

permute les racines de $F_t(x)$ cycliquement.

On se propose dans le présent article d'étudier les corps K_t définis par les polynômes $F_t(x)$, pour tout $t \in \mathbb{Z}$ (ie : sans hypothèses restrictives sur le conducteur f_t de K_t). On démontre ici les résultats suivants :

THÉORÈME 1. *Le nombre* $P_t = t^4 + 5t^3 + 15t^2 + 25t + 25$ *s'écrit de façon unique :* $P_t = 5^c q^5 \prod_{i=1}^{n} p_i^{x_i}$, $c \in \{0, 2\}$, $q \in \mathbb{N}$, p_i *premiers distincts,* $x_i \in [1, 5[$. *Alors le conducteur de* K_t *est* $f_t = 5^c \prod_{i=1}^{n} p_i$.

THÉORÈME 2. *Si* $P_t 5^{-c}$ *est sans facteurs carrés, alors les zéros de* $F_t(x)$ *engendrent le groupe des unités du corps* K_t.

Ce théorème 2 généralise le théorème (3.5) démontré dans [SW] par R. Schoof et L.C. Washington (cas des conducteurs premiers).
Enfin on dresse une table des corps K_t (de conducteur $f_t \leq 3000000$) qui donne le nombre de classes de chacun de ces corps.

La méthode de calcul du nombre de classes h_t de K_t (qui donne aussi les unités de K_t, indépendamment du théorème 2) est différente de celle exposée dans [SW] ; c'est la méthode dite de dévissage des unités cyclotomiques qui repose sur la connaissance de f_t, du groupe d'Artin de K_t, et d'une borne effective majorant h_t. Elle replace donc l'étude des corps K_t dans le cadre du corps de classes et non plus au niveau des polynômes F_t ou de méthodes analytiques. Cette méthode de dévissage des unités cyclotomiques est exposée plus en détail dans [G] et également utilisée dans [J]. Ce dernier article dresse la table de tous les corps cycliques quintiques de conducteur $f \leq 10000$ en donnant les unités génératrices et le nombre de classes de chacun de ces corps. Cette table fut longue à obtenir, la plupart des corps traités étant principaux tandis que la borne majorant leur nombre de classes était très grande. Le contexte est tout autre pour les corps d'E. Lehmer ; en effet, comme il est dit plus haut, ces corps possèdent un nombre de classes très grand puisqu'une étude située au paragraphe 5 montre dans le cadre du théorème 2 (le conducteur de K_t étant alors P_t), que pour la borne B établie dans [G] on a :

$$\lim_{t\to\infty} \frac{B}{h_t} = \frac{71}{16} < 5. \tag{4}$$

Dans le cadre de cet article la méthode utilisée est donc très performante, le dévissage des unités cyclotomiques étant très rapide, et permet de dresser la table des corps cycliques quintiques d'E. Lehmer de conducteur $f_t \leq 3000000$ et des nombres de classes correspondants (cf. paragraphe 4).

2. Arithmétique des corps quintiques définis par $F_t(x)$, P_t premier ou non

On pose $K_t = \mathbb{Q}(\theta)$, pour tout $t \in \mathbb{Z}$, où θ désigne une racine de $F_t(x)$ (cf. (1)). Dans un premier temps on cherche le conducteur de K_t ; pour cela on regarde la décomposition dans $K_t/\mathbb{Q}$ d'un nombre premier p, diviseur du discriminant de $F_t(x)$, c'est à dire diviseur de $t^3 + 5t^2 + 10t + 7$ ou de P_t, que l'on précise à l'aide de la définition suivante :

Définition 2.0.1. *On définit p_i, $i = 1, ..., n$, p_i premiers distincts, en posant : $P_t = 5^c q^5 \prod_{i=1}^{n} p_i^{x_i}$, $c \in \{0, 2\}$, $q \in \mathbb{N}$, $x_i \in [1, 5[$.*

2.1. Cas $p \neq 5$.

LEMME 2.1.1. *i) Tout facteur premier $p \neq 5$ de P_t est totalement décomposé dans $\mathbb{Q}(\mu_5)/\mathbb{Q}$, c'est-à-dire congru à* 1 *modulo* 5.
ii) La plus grande puissance de 5 divisant P_t est 1, ou alors 25 si et seulement si $t \equiv 0(5)$.
Preuve.
i) On note ζ_5 une racine primitive cinquième de l'unité. On remarque que $\mathcal{N}_{\mathbb{Q}(\mu_5)/\mathbb{Q}}(t+2+2\zeta_5+\zeta_5^3) = P_t$ (cf. (2)). Si p n'est pas totalement décomposé dans $\mathbb{Q}(\mu_5)/\mathbb{Q}$ on aura, en appelant $\wp$ un idéal premier convenable de $\mathbb{Q}(\sqrt{5})$ au dessus de p :

$$t + 2 + 2\zeta_5 + \zeta_5^3 \equiv 0(\wp\mathbb{Z}[\mu_5]). \tag{5}$$

Soit τ l'automorphisme de $\mathbb{Q}(\mu_5)$ défini par $\tau : \zeta_5 \longrightarrow \zeta_5^2$ qui donne : $\tau_{/\mathbb{Q}(\sqrt{5})} : \sqrt{5} \longrightarrow -\sqrt{5}$; en conjuguant (5) par τ on trouve :

$$t + 2 + \zeta_5 + 2\zeta_5^2 \equiv 0(\wp^\tau\mathbb{Z}[\mu_5]),$$

que l'on peut multiplier membre à membre avec (5) pour obtenir :

$$t^2 + 4t + 5 + (3t+5)\zeta_5 + (2t+5)\zeta_5^2 + (t+5)\zeta_5^3 \equiv 0(p\mathbb{Z}[\mu_5]),$$

qui mène, en identifiant sur la $\mathbb{Z}$-base $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$, à une contradiction car $p \neq 5$. Donc p est totalement décomposé dans $\mathbb{Q}(\mu_5)$.
ii) est évident. □

En s'inspirant de la remarque de E. Lehmer sur le travail de Kummer (mentionnée à la page 536 de [Le]) d'une part, et en utilisant la transformation (3) d'autre part, on calcule le polynôme minimal de φ tel que :

$$\varphi = \theta - \frac{t + 2 + t\theta - \theta^2}{1 + (t+2)\theta}.$$

On remarque que $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ est une $\mathbb{Q}$-base de K_t ; soit M_θ la matrice de multiplication par θ dans K_t et soit I la matrice identité de dimention 5. A l'aide du logiciel PARI on calcule la matrice M_φ :

$$M_\varphi = M_\theta - [(t+2)I + tM_\theta - M_\theta^2].[I + (t+2)M_\theta]^{-1},$$

puis son polynôme minimal :

$$G_t(x) = x^5 - P_t x^3 + (t+1)P_t x^2 + (t^2+4t+5)P_t x - (t^3+5t^2+10t+7)P_t.$$

On a alors le lemme suivant :

LEMME 2.1.2. *i) Le pgcd de P_t et de $t+1$ divise* 11,
ii) Le pgcd de P_t et de t^2+4t+5 divise 25,

iii) Le pgcd de P_t et de $t^3+5t^2+10t+7$ est 1.

Preuve.

i) Le résultant de P_t et de $t+1$ est 11, donc le pgcd recherché divise 11. On procède de la même manière pour ii) et iii) avec le calcul des résultants :

ii) Le résultant de P_t et de t^2+4t+5 est 25.

iii) Le résultant de P_t et de $t^3+5t^2+10t+7$ est 1. □

On montre ensuite la proposition ci-dessous :

PROPOSITION 2.1.1. *i) Les diviseurs premiers p ($p \neq 5$) de $t^3+5t^2+10t+7$ ne sont pas ramifiés dans $K_t/\mathbb{Q}$.*

ii) Tout nombre premier p divisant q ($p \neq p_i, 5$) est non ramifié dans $K_t/\mathbb{Q}$.

iii) Tout p_i est ramifié dans $K_t/\mathbb{Q}$.

Preuve.

i)Le discriminant de $G_t(x)$ est : $P_t^4(t^4+6t^3+14t^2+15t+5)^2(8t^4+48t^3+102t^2+70t-35)^2$. Le résultant de $t^3+5t^2+10t+7$ avec $t^4+6t^3+14t^2+15t+5$ est -5 et le résultant de $t^3+5t^2+10t+7$ avec $8t^4+48t^3+102t^2+70t-35$ est -7.25, il s'ensuit que le pgcd de ces résultants est -5, ce qui clos la démonstration de i).

ii) On a : $P_t = ep^{5m}$, $(e,p)=1$ (car $p \neq p_i, 5$), $m \in \mathbb{N}-\{0\}$. On pose $\psi = \varphi/p^m$ et dans $\mathbb{F}_p$ le polynôme $Irr(\psi,\mathbb{Q})$ devient $x^5-\bar{\delta}$ avec $(\delta,p)=1$ (cf. Lemme (2.1.2), iii)) donc :

a) Si δ n'est pas reste quintique modulo p alors $Irr(\psi,\mathbb{Q})$ est irréductible sur $\mathbb{F}_p$, donc p est inerte dans $K_t/\mathbb{Q}$.

b) Si δ est reste quintique modulo p alors $x^5-\delta \equiv x^5-v^5 \bmod p\mathbb{Z}[x]$, $v \in \mathbb{Z}$. Comme $p \equiv 1(5)$, $\mathbb{F}_p$ contient μ_5 et donc $x^5-\bar{v}^5$ admet cinq racines distinctes $\lambda\bar{v}$ ($\lambda^5=1$ dans $\mathbb{F}_p^\times$). Donc p est totalement décomposé dans $K_t/\mathbb{Q}$, ce qui achève ii).

iii) On a $P_t = e'p_i^{n_i}$, $(e',p_i)=1$, avec $n_i = 5y_i + x_i$, $x_i \in [1,5[$. Le polynôme $G_t(x)$ s'écrit alors : $x^5+\alpha p_i^{n_i}x^3+\beta p_i^{n_i}x^2+\gamma p_i^{n_i}x+\delta p_i^{n_i}$ (si $p_i \neq 11$) ou $x^5+\alpha p_i^{n_i}x^3+\beta p_i^{n_i+1}x^2+\gamma p_i^{n_i}x+\delta p_i^{n_i}$ (si $p_i=11$), avec $(\alpha,p_i)=(\beta,p_i)=(\gamma,p_i)=(\delta,p_i)=1$ (cf. Lemme(2.1.2)). Le polygone de Newton de ce polynôme a un seul côté de pente $\dfrac{n_i}{5} = y_i + \dfrac{x_i}{5}$; φ a donc pour valuation $y_i + \dfrac{x_i}{5}$ et donc p_i est ramifié. □

2.2. Cas $p = 5$.

Proposition 2.2.1. *Le nombre 5 est ramifié dans $K_t/\mathbb{Q}$ si et seulement si $t \equiv 0(5)$.*

Preuve.

On rappelle que F_t a pour discriminant $(t^3+5t^2+10t+7)^2P_t^4$. Il est aisé de voir que la congruence $t \equiv 0(5)$ est équivalente à la congruence $P_t \equiv 0(5)$ et que $t^3+5t^2+10t+7 \equiv 0(5)$ est équivalente à $t \equiv 2(5)$. On distingue donc les deux cas :

i) Cas $t \equiv 2(5)$.
On regarde $F_t(x)$ modulo 5 : on obtient $x^5-x^4-x+1 \equiv (x^5-x)+(1-x^4)$ mod 5, qui admet 1, 2, 3, 4 comme racines mod 5 (1 étant racine double). Il en résulte que 5 est totalement décomposé dans $K_t/\mathbb{Q}$.

ii) Cas $t \equiv 0(5)$.
On a, sachant que $t \equiv 0(5)$: $v_5(t+1) = 0$, $v_5(t^2+4t+5) = 1+u$, $u \in \mathbb{N}$, $v_5(t^3+5t^2+10t+7) = 0$ et $v_5(P_t) = 2$. D'où : $G_t(x) = x^5+5^2\alpha x^3+5^2\beta x^2+5^{3+u}\gamma x+5^2\delta$, avec $(\alpha,5) = (\beta,5) = (\gamma,5) = (\delta,5) = 1$, Donc $G_t(x)$ possède un polygone de Newton à un seul côté de pente $\frac{2}{5}$ et donc φ est de valuation $\frac{2}{5}$ ce qui signifie que 5 est ramifié dans K_t. □

Le théorème suivant (le théorème 1 cité dans l'introduction) découle des propositions (2.1.1) et (2.2.1):

Théorème 2.2.1. *Le nombre $P_t = t^4+5t^3+15t^2+25t+25$ s'écrit de façon unique : $P_t = 5^c q^5 \prod_{i=1}^{n} p_i^{x_i}$, $c \in \{0,2\}$, $q \in \mathbb{N}$, p_i premiers distincts, $x_i \in [1,5[$. Alors le conducteur de K_t est $f_t = 5^c \prod_{i=1}^{n} p_i$.*

Dans un deuxième temps on démontre le théorème 2 de l'introduction :

Théorème 2.2.2. *Si $P_t 5^{-c}$ est sans facteurs carrés, alors les zéros de $F_t(x)$ engendrent le groupe des unités du corps K_t.*

Preuve.

La démonstration se déroule en trois étapes, comme pour le théorème (3.5) démontré par R. Schoof et L.C. Washington dans [SW]. Soit σ un générateur de $G = Gal(K_t/\mathbb{Q})$. Soit E le groupe des unités de norme 1 de K_t et soit U le sous-groupe engendré par les opposés des zéros de $F_t(x)$.

On note $i_\theta = (E : U)$ et on a $i_\theta = R/R_t$, où R est le régulateur de U et R_t le régulateur du corps K_t. D'après [SW] on trouve :

$$i_\theta \leq \frac{25.R}{(\ln(P_t/2))^4}, \tag{6}$$

car $P_t 5^{-c}$ est sans facteurs carrés et donc P_t est le conducteur de K_t. De plus [SW] nous donne :

$$R \leq (71 + \frac{36}{\ln|t+1|})(\ln|t+1|)^4.$$

i) Il s'ensuit une majoration de i_θ en fonction de t et l'on sait d'après [SW] que pour $|t+1| \geq 20$ l'indice i_θ est < 11.

ii) L'indice i_θ n'est pas divisible par 5 : supposons le contraire ; alors il existe $\eta \in E$ telle que $\theta = -\eta/\sigma(\eta)$ (θ est de norme -1). Supposons dans un premier temps que $t \neq 0$. Soit alors p un diviseur premier de $P_t 5^{-c}$ (ramifié dans K_t) et soit $\mathcal{P}$ l'idéal premier au dessus de p dans K_t ; on a $p \equiv 1(10)$. Le groupe de Galois G agit trivialement modulo $\mathcal{P}$, on a donc, sachant que $\theta = -\eta/\sigma(\eta)$: $\theta \equiv -1(\mathcal{P})$ d'où $F_t(x) \equiv (x+1)^5(p)$ et l'on obtient par identification :

$$t^2 \equiv 5(p),$$

$$t^4 + 5t^3 + 11t^2 + 15t + 5 \equiv 10(p).$$

En outre p divise P_t, ce qui donne :

$$t^4 + 5t^3 + 15t^2 + 25t + 25 \equiv 0(p).$$

La différence de ces deux dernières équations conduit à : $2t^2+5t+15 \equiv 0(p)$, puis, en substituant à cette nouvelle égalité l'équation $t^2 \equiv 5(p)$, on obtient $t \equiv -5(p)$ et donc $t^2 \equiv 25(p)$. Enfin, en confrontant ce dernier résultat avec $t^2 \equiv 5(p)$, il vient aisément la congruence : $p \equiv 0(10)$ ce qui est exclu.

Dans le cas $t = 0$ on a alors $P_t = 25$ et le programme de dévissage des unités cyclotomiques montre que le corps K_0 est principal.
L'indice i_θ est donc non divisible par 5.

iii) L'indice i_θ est égal à 1. Pour $|t+1| \geq 20$ on a $i_\theta \leq 11$ et $i_\theta \neq 5$ donc $i_\theta = 1$ (i_θ est une norme d'entier dans $\mathbb{Q}(\mu_5)$). Si $|t+1| \leq 20$ on calcule une approximation de R et on remplace dans (6). Il s'ensuit que $i_\theta < 11$ (et donc $i_\theta = 1$) pour tout P_t tel que $P_t 5^{-c}$ est sans facteurs carrés, excepté peut-être pour $P_t = 25, 31, 101$ et 25.11. Pour ces quatre cas particuliers le programme de dévissage des unités cyclotomiques montre que les unités calculées par dévissage engendrent le même groupe que les zéros de $F_t(x)$, d'où le fait que $i_\theta = 1$. $\square$

3. Etude numérique des corps K_t.

3.1. Méthode de dévissage des unités cyclotomiques. La méthode dite de "dévissage des unités cyclotomiques" est une méthode qui permet de calculer le nombre de classes et les unités fondamentales des extensions abéliennes réelles de $\mathbb{Q}$ à partir de la connaîssance du groupe d'Artin de l'extension et du calcul de ses unités cyclotomiques connues par les formule de Hasse et rappelées dans [G].

Il est à noter que, dans le cas des corps d'E. Lehmer, cette méthode donne le nombre de classes et les unités fondamentales indépendamment du théorème 2.2.2. Cette méthode à donc l'avantage de procéder à une vérification par le calcul de ce dernier, mais aussi de calculer le nombre de classes et les unités de corps d'E. Lehmer ne vérifiant pas les hypothèses de ce théorème. Ainsi, pour tous les corps d'E. Lehmer figurant dans la table numérique du paragraphe 4 et ne vérifiant pas les hypothèses du théorème 2.2.2, nous avons pu constater que les unités calculées par dévissage engendrent le même groupe que les racines de $F_t(x)$.

Dans le cas des corps vérifiant le théorème 2.2.2, le polynôme $F_t(x)$ donne donc les unités fondamentales et grâce à la transformation (3) qui calcule les conjuguées successives d'une racine de $F_t(x)$, il s'ensuit aisément la valeur du régulateur R_t correspondant. La méthode de dévissage commence par calculer les unités cyclotomiques et le régulateur $\mathcal{R}_t$ correspondant. Le nombre de classes est alors connu par la formule :

$$h_t = \frac{\mathcal{R}_t}{R_t},$$

ce qui pourrait éviter le dévissage des unités cyclotomiques, mais afin de mettre en évidence l'intérêt de la méthode de dévissage et de manière à faire une double vérification des unités données par cette méthode et des unités données par le polynôme $F_t(x)$, il a été procédé au dévissage des unités cyclotomiques pour tous les corps d'E. Lehmer, de conducteur premier ou non, vérifiant - ou ne vérifiant pas - les hypothèses du théorème 2.2.2.

Soit F le sous-groupe de E des unités cyclotomiques de norme 1. On sait que E est un $\mathbb{Z}[\mu_5]$-module de dimension 1 et que $h_t = (E : F)$ avec $F =< \eta >$, où η est connue en termes de corps de classes (ie : via le groupe d'Artin de K_t dans $\mathbb{Q}(\mu_{f_t})$).

Supposons avoir trouvé une suite strictement croissante $F^{(i)} =< \eta^{(i)} >$, $0 \leq i \leq r$, de sous-$\mathbb{Z}[\mu_5]$-modules de E :

$$E \supseteq F^{(r)} \supset F^{(r-1)} \supset \cdots \supset F^{(1)} \supset F^{(0)} = F;$$

on a alors les équivalences entre les trois points suivants, pour un nombre premier p de degré résiduel n_p dans $\mathbb{Q}(\mu_5)$:

(7)
i) p divise $(E : F^{(r)})$,
ii) p^{n_p} divise $(E : F^{(r)})$,
iii) Il existe $\omega \in \mathbb{Z}[\mu_5]$, de norme p^{n_p}, et $\eta^{(r+1)} \in E$ tels que : $\eta^{(r)} = \eta^{(r+1)\omega}$.

L'algorithme de la méthode de dévissage des unités cyclotomiques réside dans le fait de reconnaître effectivement s'il existe $\omega \in \mathbb{Z}[\mu_5]$ de norme p^{n_p} et $\eta^{(r+1)} \in E$ tels que : $\eta^{(r)} = \eta^{(r+1)\omega}$. Pour ce faire on utilise l'idée suivante :

Soit $\omega' \in \mathbb{Z}[\mu_5]$ tel que $\omega\omega' = p^{n_p}$. Si $\eta^{(r)\omega'} \in K^{\times p^{n_p}}$, c'est à dire s'il existe $\varepsilon \in E$ tel que $(\eta^{(r)\omega'})^{\frac{1}{p^{n_p}}} = \varepsilon$, c'est donc que $\eta^{(r)} = \varepsilon^{\omega}$. On pose alors $\eta^{(r+1)} = \varepsilon$ puis $F^{(r+1)} =< \eta^{(r+1)} >$ et grâce aux équivalences (7) on en déduit que p^{n_p} divise $(E : F^{(r)})$.

Pour tester si cette égalité est vérifiée on utilise le lemme IV.1, démontré par M.-N. Gras et G. Gras dans [G], que nous rappelons ici tout en l'adaptant au cas des corps cycliques quintiques d'E. Lehmer :

LEMME 3.1.1. *Soit* μ *un entier primitif de* K_t *et soit* $q \in \mathbb{Z}$, $q > 1$. *On suppose que lorsque* q *est pair, tous les conjugués de* μ *sont positifs. Pour tout* $\sigma \in G = Gal(K_t/\mathbb{Q})$ *on pose* $x_\sigma = (\mu^\sigma)^{\frac{1}{q}}$ *(pour* q *pair,* $x_\sigma = \sqrt[q]{\mu^\sigma} > 0$ *; pour* q *impair,* x_σ *est la racine* q*-ième réelle de* μ^σ*) :*

i) Dans le cas q *impair, une condition nécessaire et suffisante pour que les nombres* x_σ *appartiennent à* K_t *est que le polynôme*

$$Q = \prod_{\sigma \in G} (X - x_\sigma)$$

soit à coefficients entiers rationnels. Lorsque cette condition est réalisée alors $x_\sigma = x_1^\sigma$ *pour tout* $\sigma \in G$.

ii) Dans le cas q *pair, une condition nécessaire et suffisante pour que les nombres* x_σ *appartiennent à* K_t *est qu'il existe des nombres* $\delta_\sigma \in \{-1, +1\}$ *tels que le polynôme :*

$$Q = \prod_{\sigma \in G} (X - \delta_\sigma x_\sigma)$$

soit à coefficients entiers rationnels. Lorsque cette condition est réalisée, on a $x_\sigma = \delta_1 \delta_\sigma x_1^\sigma$ *pour tout* $\sigma \in G$.

D'autre part si on a une majoration de la forme : $h_t = (E : F) \leq B$, alors on a, au r-ième stade de l'algorithme :

$$(E : F^{(r)}) \leq \frac{B}{(F^{(r)} : F)} = B^{(r)},$$

$B^{(r)}$ étant connue par hypothèse.

L'algorithme s'arrête si (7) est négatif pour tout p supérieur ou égal au dernier nombre premier testé et tel que $p^{n_p} \leq B^{(r)}$, auquel cas $F^{(r)} = E$ et $\eta^{(r)} = \varepsilon$ donne une $\mathbb{Z}[\mu_5]$-base de E. D'où l'algorithme comme dans [G] qui donne, en outre, la borne B majorant h_t :

$$B = \frac{16.\mathcal{R}_t}{(\ln(f_t/5))^4}. \tag{8}$$

D'autre part d'après [SW] on obtient une autre borne :

$$B' = \frac{25.\mathcal{R}_t}{(\ln(f_t/2))^4}, \tag{9}$$

qui est meilleure pour les petits conducteurs. Pratiquement, on utilisera la majoration (8), les conducteurs rencontrés étant assez grands pour les corps K_t d'E. Lehmer.

3.2. Recherche d'entiers de norme p^{n_p}. Toujours dans l'optique d'une programmation du dévissage, il est nécessaire de trouver, pour tout entier premier p, un entier ω de $\mathbb{Z}[\mu_5]$ de norme p^{n_p} en vue du test (7). Rappelons que le sous-corps réel maximal de $\mathbb{Q}(\mu_5)$ est $\mathbb{Q}(\sqrt{5})$. Nous traitons le cas $p \equiv 1(5)$ qui est le plus général; en effet, le cas $p = 5$ est connu, le cas d'inertie dans $\mathbb{Q}(\mu_5)/\mathbb{Q}$ est trivial, et celui d'inertie dans $\mathbb{Q}(\mu_5)/\mathbb{Q}(\sqrt{5})$ nous ramène au problème de norme dans $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ que nous rappelons ci-dessous :

i) Par la méthode de développement en fractions continues on sait trouver un entier de $\mathbb{Q}(\sqrt{5})$ de norme sur $\mathbb{Q}$ égale à $\pm p$, lorsque p est décomposé (le problème étant toujours soluble puisque $\mathbb{Q}(\sqrt{5})$ est principal).On rappel ici succintement cette méthode :

Soient $\Omega = \dfrac{\sqrt{5}+1}{2}$, $\Omega' = \dfrac{\sqrt{5}-1}{2}$ et $g(x) = x^2 - x - 1$ le polynôme irréductible de Ω. On balaye l'ensemble d'entiers $\{0, \ldots, p-1\}$ afin de trouver une racine d'un idéal $\wp$ au-dessus de p dans $\mathbb{Q}(\sqrt{5})$. Soit c une telle racine ; elle doit vérifier : $g(c) \equiv 0(p)$. On procède à la décomposition en fraction continue de $\dfrac{\Omega' + c}{p}$:

$$\begin{aligned}
&(\Omega' + a_{m+1})/b_{m+1} = e_{m+1} + \cdots \\
&\quad\vdots \\
&(\Omega' + a_{k+1})/b_{k+1} = e_{k+1} + \cdots \\
&(\Omega' + a_k)/b_k = e_k + \cdots \\
&\quad\vdots \\
&(\Omega' + a_0)/1 = e_0 + \cdots
\end{aligned}$$

avec $a_{m+1} = c$, $b_{m+1} = p$ et les formules :

$$\begin{cases} a_k = 1 - a_{k+1} + e_{k+1}b_{k+1}, \\ b_k = \dfrac{1 + a_k - a_k^2}{b_{k+1}}, \end{cases}$$

jusqu'à ce que $b_k = b_0 = 1$.
Ensuite on remonte jusqu'à la solution du problème, $p_m + q_m\Omega'$, qui est obtenue avec les formules de récurrences :
$(p_{k+1}, q_{k+1}) = (e_{k+1}p_k + p_{k-1}, e_{k+1}q_k + q_{k-1})$
où $(p_0, q_0) = (a_0, 1)$ et $(p_{-1}, q_{-1}) = (1, 0)$.

On a alors : $\mathcal{N}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(p_m + q_m\Omega') = (-1)^{m+1}p$.

Or $p_m + q_m\Omega' = \dfrac{2p_m - q_m}{2} + \dfrac{q_m}{2}\sqrt{5}$; on pose alors : $a = \varepsilon_a\dfrac{2p_m - q_m}{2}$ et $b = \varepsilon_b\dfrac{q_m}{2}$, $\varepsilon_a = \pm 1$ et $\varepsilon_b = \pm 1$, pris de telle sorte que $a - b > 0$, $a - b$ minimum.

ii) On veut maintenant trouver un entier de $\mathbb{Q}(\mu_5)$ de norme sur $\mathbb{Q}(\sqrt{5})$ égale à $a+b\sqrt{5}$. On sait que $\sqrt{5} = 1+2(\zeta_5+\zeta_5^{-1})$; on a alors : $a+b\sqrt{5} = a-b-2b(\zeta_5^2+\zeta_5^3)$, $a-b \in \mathbb{N}-\{0\}$. Soit un entier de $\mathbb{Q}(\mu_5)$: $\lambda = \alpha+\beta\zeta_5+\gamma\zeta_5^2+\delta\zeta_5^3$, $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Donc $\mathcal{N}_{\mathbb{Q}(\mu_5)/\mathbb{Q}(\sqrt{5})}(\lambda) = \lambda(\alpha + \beta\zeta_5^{-1} + \gamma\zeta_5^{-2} + \delta\zeta_5^{-3}) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 - \alpha\beta - \beta\gamma - \gamma\delta + (\alpha\delta + \alpha\gamma + \beta\delta - \alpha\beta - \beta\gamma - \gamma\delta)(\zeta_5^2 + \zeta_5^3)$. En identifiant avec $a - b - 2b(\zeta_5^2 + \zeta_5^3)$ on obtient :

$$(10) \qquad \begin{cases} \alpha^2 + \beta^2 + \gamma^2 + \delta^2 - \alpha\beta - \beta\gamma - \gamma\delta = a - b. \\ \alpha\delta + \alpha\gamma + \beta\delta - \alpha\beta - \beta\gamma - \gamma\delta = -2b. \end{cases}$$

La première forme quadratique s'écrit en fait :

$$\left(\alpha - \frac{\beta}{2}\right)^2 + \left(\delta - \frac{\gamma}{2}\right)^2 + 3\left(\frac{\beta}{2} - \frac{\gamma}{3}\right)^2 + \frac{5}{12}\gamma^2 = a - b > 0,$$

donc chacun des termes de la somme est $\leq a-b$. Il reste alors à balayer les intervalles ainsi définis et à détecter une solution au système (10). On peut choisir une solution telle que $\alpha \neq 0$ et $\gamma \geq 0$, ce qui entraîne, en posant $\mu = \sqrt{a-b}$:

$$\begin{gathered}
0 \leq \gamma \leq 2\mu\sqrt{\frac{3}{5}}, \\
\frac{\gamma}{2} - \mu \leq \delta \leq \frac{\gamma}{2} + \mu, \\
2\left(\frac{\gamma}{3} - \frac{\mu}{\sqrt{3}}\right) \leq \beta \leq 2\left(\frac{\gamma}{3} + \frac{\mu}{\sqrt{3}}\right), \\
\frac{\beta}{2} - \mu \leq \alpha \leq \frac{\beta}{2} + \mu.
\end{gathered}$$

3.3. Identification du corps K_t. Dans le cas où f_t n'est pas premier, $\mathbb{Q}(\mu_{f_t})$ possède plusieurs sous-corps cycliques de degré 5 sur $\mathbb{Q}$ de conducteur f_t dont un seul correspond à $F_t(x)$. Afin de redéfinir ce corps K_t particulier, en termes de corps de classes, on procède de la manière suivante :
Soit une série d'entiers premiers l_i, $i = 1, \ldots, s$, l_i ne divisant pas f_t, tels que $F_t(x)$ admette une racine modulo l_i. On en déduit que l_i est décomposé dans K_t donc appartient au groupe d'Artin de K_t. D'autre part on choisit les l_i tels que leurs Frobenius soient indépendants dans G/G^5 (ce qui implique que $l_i \notin G^5$, c'est-à-dire l_i non totalement décomposé dans le composé des sous-corps de degré 5). Le Frobenius de l_i fixe donc un corps L_i, composé de corps de degré 5, dont K_t. On pose $s = dim_{\mathbb{F}_5}(G/G^5) - 1$; il suffit alors de s Frobenius indépendants définis à partir de l_i, $i = 1, \ldots, s$, choisis convenablement tels que $K_t = \bigcap_{i=1}^{s} L_i$.

4. Table numérique.

Dans le cas où f_t n'est pas premier, la dernière colonne de la table suivante donne les l_i, $i = 1, \ldots, s$, définissant le corps K_t. Les unités des corps figurant dans la table sont engendrées par les racines des polynômes $F_t(x)$.

Table pour $f_t \leq 3000000$:

t	P_t	f_t	h_t	$l_i,\ i = 1, \ldots, s$
$-1, -2$	11	11	1	
0	5^2	5^2	1	
-3	31	31	1	
1	71	71	1	

t	P_t	f_t	h_t	$l_i,\ i=1,\ldots,s$
-4	101	101	1	
2	191	191	11	
-5	$5^2.11$	275	5	31
3	11.41	451	5	118
-6	631	631	11	
4	941	941	2^4	
14	11.71^2	781	5	7
-7	31.41	1271	$55=5.11$	7
5	$5^2.71$	1771	$80=2^4.5$	31
-8	11.211	2321	$305=5.61$	5
44	$41^3.61$	2501	5	181
6	11.281	3091	$80=2^4.5$	61
-9	3931	3931	$256=2^8$	
-16	$11^2.401$	4411	$55=5.11$	59
7	5051	5051	1451	
-10	$5^2.251$	6275	$275=5^2.11$	31
8	7841	7841	421	
-11	9551	9551	541	
9	11.1061	11671	$655=5.131$	29
-12	11.31.41	13981	$1375=5^3.11$	$19,29$
10	$5^2.11.61$	16775	$1775=5^2.71$	$23,3511$
-13	11.1801	19811	$4705=5.941$	5
-23	$11^2.1871$	20581	$1775=5^2.71$	1889
11	41.571	23411	$2000=2^4.5^3$	19
83	11.2141^2	23551	$505=5.101$	19
-14	31.881	27311	$7255=5.1451$	19
12	151.211	31861	$9680=2^4.5.11^2$	5
-15	$5^2.1471$	36775	$3505=5.701$	6661
13	151.281	42431	$9455=5.31.61$	139
-17	61.1031	62891	$9455=5.31.61$	227
15	$5^2.2851$	71275	$14275=5^2.571$	67
-18	80251	80251	$37631=11^2.311$	
16	90281	90281	19301	
-19	11.9181	100991	$20305=5.31.131$	139
17	11.31.331	112871	$83275=5^2.3331$	$5,29$
-35	$5^2.11^2.431$	118525	$41525=5^2.11.151$	$7,37$
-20	$5^2.5021$	125525	$62480=2^4.5.11.71$	29
18	211.661	139471	$32605=5.6521$	61
-21	154291	154291	$108691=11.41.241$	
19	31.5501	170531	$44605=5.11.811$	1721

t	P_t	f_t	h_t	$l_i,\ i=1,...,s$
-22	187751	187751	$76901 = 11.6991$	
20	$5^2.11.751$	206525	$101525 = 5^2.31.131$	$179, 257$
21	11.22541	247951	$308605 = 5.11.31.181$	7
-24	11.24611	270721	$153005 = 5.71.431$	73
22	281.1051	295331	$478775 = 5^2.11.1741$	5
-25	$5^2.71.181$	321275	$231275 = 5^2.11.29^2$	$73, 179$
23	349211	349211	$186091 = 71.2621$	
-26	241.1571	378611	$189305 = 5.37861$	31
24	31.101.131	410161	$591775 = 5^2.23671$	$11, 19$
-27	11.91.211	443311	$289025 = 5^2.11.1051$	$19, 73$
71	$61^2.7331$	447191	$75275 = 5^2.3011$	53
25	$5^2.11.1741$	478775	$349525 = 5^2.11.31.41$	$61, 89$
-28	241.2141	515981	$2372005 = 5.181.2621$	7
26	555671	555671	$721151 = 661.1091$	
-29	61.9791	597251	$540905 = 5.251.431$	31
27	641491	641491	1566401	
-30	$5^2.11.41.61$	687775	$1206875 = 5^4.1931$	$19, 23, 67$
28	11.31.2161	736901	$1764400 = 2^4.5^2.11.401$	$7, 47$
-31	788231	788231	$1217821 = 11.110711$	
29	41.20551	842591	$760055 = 5.71.2141$	43
-32	899321	899321	$798256 = 2^4.49891$	
30	$5^2.38371$	959275	$1615280 = 2^4.5.61.331$	17
-33	491.2081	1021771	$4680055 = 5.281.3331$	19
31	11.61.1621	1087691	$1386275 = 5^2.11.71^2$	$71, 79$
-34	11.31.3391	1156331	$1402000 = 2^4.5^3.701$	$71, 79$
32	11.61.1831	1228601	$4822625 = 5^3.41.941$	$5, 89$
33	101.13691	1382791	$2148080 = 2^4.5.11.2441$	23
-36	1464901	1464901	$4628591 = 11.420781$	
34	41.37831	1551071	$2160455 = 5.11^2.3571$	139
-37	1640531	1640531	1636721	
35	$5^2.69371$	1734275	$12190055 = 5.421.5791$	11
-38	11.31.41.131	1831511	$11812625 = 5^3.11^3.71$	$17, 59, 107$
36	11.181.971	1933261	$3869525 = 5^2.11.14071$	$31, 433$
-39	1171.1741	2038711	$4521505 = 5.31^2.941$	53
37	661.3251	2148911	$27105755 = 5.5421151$	23
-40	$5^2.131.691$	2263025	$6813125 = 5^4.11.991$	$41, 83$
38	1301.1831	2382131	$6728105 = 5.1345621$	37
-41	11.421.541	2505371	$6340275 = 3^4.5^2.31.101$	$29, 31$
39	11.239441	2633851	$7503505 = 5.1500701$	37
-42	2766691	2766691	$20599841 = 31.664511$	
40	$5^2.116201$	2905025	$6564400 = 2^4.5^2.16411$	61

Notons que cette table concorde avec celle fournie, pour les conducteurs premiers, dans [SW]. Le théorème (3.5) qu'ont démontré R. Schoof et L.C. Washington (cas des conducteurs premiers) concerne environ 1/3 des corps satisfaisant aux hypothèses du théorème (2.2.2) et figurant dans cette table. R. Schoof et L.C. Washington ont mis en évidence le premier corps de nombres de degré 5 (corps figurant dans cette table pour $t = 27$) dont le nombre de classes est divisible par un nombre premier supérieur au conducteur de ce corps. On remarque que la table présente fournit un exemple dans le cas où le conducteur du corps n'est pas premier : Pour $t = 37$ et $f = 661.3251 = 2148911$ le nombre de classes du corps correspondant à $l_1 = 23$ est divisible par 5421151.

Etudions deux cas particuliers :

i) Cas $t = 83$: On a $P_{83} = 11.2141^2$; le corps K_{83},de conducteur $f_{83} = 11.2141 = 23551$, ne vérifie donc pas les hypothèses du théorème 2.2.2. L'unité cyclotomique génératrice de F est :

$$\eta^{(0)} = 572037.916726935257639182676001710038077457762489620895529747968677741063109164452952430170226489490324159135083912502344917677369479969645605264910 5,$$

avec, en posant $\mathrm{Tr} = \mathrm{Tr}_{K_t/\mathbb{Q}}$:

$\mathrm{Tr}(\eta^{(0)}) = -221251282084835019,$

et $B = 47258$.

Le dévissage en 5, avec $\omega = -1 + \zeta_5^3$, donne :

$$\eta^{(1)} = 4.740806759303056364380660045597358146263223472303923386721922833746737569419750495077899920957412591021645690843331487501635790712635079184449914091 8.10^{-18},$$

avec :

$\mathrm{Tr}(\eta^{(1)}) = 30254219679181,$

et $B^{(1)} = 9451$.

Le dévissage en 101 est positif avec $\omega = -1 + 3\zeta_5 + \zeta_5^2 + \zeta_5^4$ et donne :

$$\eta^{(2)} = 84.000143329516802934068480987842494358283642723940199515081874644109810700066629256682164789126580611887102163570618987733511340869063204659560369 3,$$

avec $B^{(2)} = 93 < 101$ et l'algorithme s'arrête. Finalement on obtient $h_{83} = 5.101 = 505$ et l'unité fondamentale est η_2 dont le polynôme irréductible est :

$$x^5 - 600183x^4 + 50394285x^3 + 1185748x^2 + 6889x - 1,$$

ce qui montre que le groupe des unités engendré par ce polynôme est le même que celui engendré par

$$F_{83}(x) = x^5 + 6889x^4 - 1185748x^3 + 50394285x^2 + 600183x + 1.$$

ii) Cas $t = -21$: On a $P_{-21} = f_{-21} = 154291$ qui est premier et :

$$\begin{aligned}\eta^{(0)} = -8.&47690024026937887788280851768089280992736068745829\,5\\ &37572284651742100844135475982187978626583147000270373486643\,0\\ &11699136368612018549783215514167109768961455157548704202176\,8\\ &9427297483693983234872042463739030620481881429.10^{-67},\end{aligned}$$

avec :

$$\mathrm{Tr}(\eta^{(0)}) = 87508223268576089810477233266858875496232770833503295704,$$

et $B = 926273$.

Le dévissage en 11 est positif avec $\omega = -1 - 2\zeta_5^3$ et donne :

$$\begin{aligned}\eta^{(1)} = -82868719084056871.&824694218933271501545303225644364930\\ &393309767435024762983891214115520978603901792047418505298141\\ &831456587209240566199584220807470335548427402480375316784161\\ &944530821361660250868145228049425975243565 7438,\end{aligned}$$

avec :

$$\mathrm{Tr}(\eta^{(1)}) = 377299423297460425 7520914,$$

et $B^{(1)} = 84206$.

Le dévissage en 41 est positif avec $\omega = -1 + \zeta_5 - 2\zeta_5^2 + \zeta_5^4$ et donne :

$$\begin{aligned}\eta^{(2)} = 9023762528378.&29931303744130317403272522003229824318598\\ &574984258540478870211845564691312718380739617942561988698563\\ &061532353953190897905036275713193573655021602211005145579275\\ &174408204738973191021014305377219908618277826 0,\end{aligned}$$

avec :

$$\mathrm{Tr}(\eta^{(2)}) = 9023762674764,$$

et $B^{(2)} = 2053$.

Le dévissage en 241 est positif avec $\omega = -1 - \zeta_5 + 4\zeta_5^2$ et donne :

$$\begin{aligned}\eta^{(3)} = -1.&0026119695145140118631749125593481619880486829595 9\\&1359763366661259815065268587484580315048460313357933223556 8\\&7867085841684336658057157715949924270904794520386702443279 7\\&7633460947868933324258036545364024098520050 9,\end{aligned}$$

avec $B^{(3)} = 8$ et l'algorithme s'arrête.
Finalement on obtient $h_{-21} = 11.41.241 = 108691$ et l'unité fondamentale est $\eta^{(3)}$ dont le polynôme irréductible est :

$$x^5 - 8038x^4 + 2916135x^3 + 3084938x^2 + 153504x - 1.$$

Et l'on peut vérifier que le groupe des unités engendré par les racines de ce polynôme est le même que celui engendré par celles de

$$F_{-21}(x) = x^5 + 441x^4 + 16076x^3 + 152717x^2 - 7697x + 1.$$

5. Etude des bornes majorant h_t

On regarde les quotients des bornes B (cf. (8)) et B' (cf. (9)) par le nombre de classes h_t. On note encore $\theta_i, i = 0, \ldots, 4$, les zéros de $F_t(x)$, que P_t soit premier ou non. Sachant que les $\dfrac{1}{\theta_i}, i = 0, \ldots, 4$, sont les zéros de $x^5 F_t\left(\dfrac{1}{x}\right)$, on trouve :

$$\begin{aligned}
\theta_0 &= -t^2 - 2t - 3 - \frac{1}{t} + \frac{1}{t^2} + O\left(\frac{1}{t^3}\right),\\
\theta_1 &= t + 1 + \frac{1}{t} - \frac{1}{t^2} + O\left(\frac{1}{t^3}\right),\\
\frac{1}{\theta_2} &= -t^3 - 4t^2 - 9t - 9 - \frac{2}{t} + \frac{5}{t^2} + O\left(\frac{1}{t^3}\right),\\
\theta_3 &= t + 2 + \frac{1}{t} - \frac{1}{t^2} + O\left(\frac{1}{t^3}\right),\\
\frac{1}{\theta_4} &= -t - 1 - \frac{1}{t^2} + O\left(\frac{1}{t^3}\right).
\end{aligned}$$

Ce qui conduit à :

$$R_t = 71 \ln^4 t + \frac{340 \ln^3 t}{t} + \frac{110 \ln^3 t + 615 \ln^2 t}{t^2} + O\left(\frac{1}{t^3}\right).$$

Pour $P_t 5^{-c}$ sans facteurs carrés le conducteur de K_t est alors P_t et on a les limites suivantes :

$$\lim_{t\to\infty} \frac{B}{h_t} = \lim_{t\to\infty} \frac{16.R_t}{\ln^4(P_t/5)} = \frac{71}{16} = 4,4375,$$

et

$$\lim_{t\to\infty} \frac{B'}{h_t} = \lim_{t\to\infty} \frac{25.R_t}{\ln^4(P_t/2)} = \frac{25.71}{16^2} \simeq 6,93,$$

sous l'hypothèse de l'existence d'une infinité d'entiers P_t distincts tels que $P_t 5^{-c}$ soit sans facteurs carrés.

BIBLIOGRAPHIE

[G] G. Gras et M.-N. Gras, *Calcul du nombre de classes et des unités des extentions abéliennes réelles de* $\mathbb{Q}$, Bull. Sci. Math. , V. 101 (1977), pp. 97-129.

[J] S. Jeannin, *Tables des nombres de classes et unités des corps quintiques cycliques de conducteur* $f \leq 10000$, Publ. Math. Fac. sci. Besançon (Théorie des nombres) (A paraître).

[La] A.J. Lazarus, *Cyclotomy and Delta Units*, Math. Comp. , V. 61 (1993), pp. 295-305.

[Le] E. Lehmer, *Connection Between Gaussian Period and Cyclic Units*, Math. Comp. , V. 50 (1988), pp. 535-541.

[SW] R. Schoof and L.C. Washington, *Quintic Polynomials and Real Cyclotomic Fields with Large Class Numbers*, Math. Comp. , V. 50 (1988), pp. 543-556.

Stéphane JEANNIN
Laboratoire de Mathématiques
URA 741 CNRS
25030 Besançon Cedex
e-mail : jeannin@vega.univ-fcomte.fr

Stéphane Jeannin
Laboratoire de Mathématiques
URA 741 CNRS
25030 Besançon Cedex, France
e-mail: jeannin vega.univ-fcomte.fr