

CLAUDE MOSER

**Sur le nombre de classes d'un corps  $K$  réel cyclique de conducteur premier,  $\deg K \leq 4$**

*Séminaire de théorie des nombres de Grenoble*, tome 8 (1979-1980), exp. n° 3, p. 1-17

[http://www.numdam.org/item?id=STNG\\_1979-1980\\_\\_8\\_\\_A3\\_0](http://www.numdam.org/item?id=STNG_1979-1980__8__A3_0)

© Institut Fourier – Université de Grenoble, 1979-1980, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

Grenoble

SUR LE NOMBRE DE CLASSES D'UN CORPS  $K$  REEL  
CYCLIQUE DE CONDUCTEUR PREMIER ,  $\deg K \leq 4$  .

par

Claude MOSER

0. - INTRODUCTION ET RESULTATS.

La conjecture de Vandiver dit que si  $p$  est un nombre premier, le nombre de classes du sous-corps réel maximal du  $p$ -ième corps cyclotomique est premier à  $p$  .

Le présent exposé se place modestement dans "l'environnement" de cette conjecture, motivé par le théorème suivant :

THEOREME 1. - Soit  $K/k$  une extension cyclique de degré premier  $\ell$  de corps de nombres. On suppose qu'un seul idéal premier est ramifié dans cette extension. Alors

- 1) La norme induit un homomorphisme surjectif du groupe  $U_K$  des unités de  $K$  sur le groupe  $U_k$  des unités de  $k$  .
- 2) Le nombre de classes  $h(k)$  de  $k$  divise le nombre  $h(K)$  de classes de  $K$  et  $\frac{h(K)}{h(k)} \equiv 1 \pmod{\ell}$ .

Ceci résulte d'une étude détaillée de la formule des classes ambiguës [6] . Une idée pour aborder la conjecture de Vandiver est donc de dévisser  $\mathbb{Q}_0^{(p)}/\mathbb{Q}$  en une tour d'extensions cycliques de degré premier et de démontrer que les rapports de nombres de classe successifs sont premiers à  $p$  et (si possible inférieur à  $p$ ).

III.2

On se propose de démontrer ici les deux résultats :

THEOREME A. - Soit  $p$  un nombre premier congru à 1 modulo 3 .  
Soit  $K$  le sous-corps cubique de  $\mathbb{Q}^{(p)}$  . Si  $p$  est de la forme  
 $\frac{1}{4}(a^2+27)$  le nombre de classe de  $K$  est inférieur à  $p/3$  . Sinon  
il est inférieur à  $p/4$  .

THEOREME B. - Soit  $p$  un nombre premier congru à 1 modulo 8 ,  
 $K$  le sous-corps réel de degré 4 de  $\mathbb{Q}^{(p)}$  et  $k$  le corps  $\mathbb{Q}(\sqrt{p})$  .

Alors

$$h(k) \leq \frac{\sqrt{p}}{2}$$

$$\frac{h(K)}{h(k)} \leq \frac{p}{4} .$$

Le second ingrédient est la formule analytique du nombre de classes qui s'écrit pour une extension réelle  $K/\mathbb{Q}$  :

$$2^{[K:\mathbb{Q}]-1} h(K) R(K) (\Delta(K))^{-\frac{1}{2}} = \lim_{s \rightarrow 1+} \frac{\zeta_K(s)}{\zeta_{\mathbb{Q}}(s)} .$$

Le terme de droite n'étant autre chose que le produit  $\prod_{\chi \neq \chi_0} L(1, \chi)$  avec les notations suivantes :

$h(K)$  le nombre de classes de  $K$  ,

$R(K)$  le régulateur de  $K$  ,

$\Delta(K)$  le discriminant de  $K$  ,

$\chi$  parcourt l'ensemble des caractères non principaux pairs de conducteur  $f(K)$  , dont l'ordre divise  $[K:\mathbb{Q}]$  . Voir [5] .

Pour ce qui concerne une extension cyclique  $K/k$  on aura en particulier pour un degré premier  $\ell$  .

$$\frac{h(K)}{h(k)} = 2^{-[K:\mathbb{Q}] + [k:\mathbb{Q}]} \frac{R(k)}{R(K)} \left\{ \frac{\Delta(K)}{\Delta(k)} \right\}^{\frac{1}{\ell}} \prod_{\substack{\chi \\ w(\chi) = [K:\mathbb{Q}]}} L(1, \chi)$$

le produit étant étendu aux caractères de Dirichlet d'ordre égal à  $[K:\mathbb{Q}]$  .

Il y en a  $\varphi([K:\mathbb{Q}])$  .

Dans le cas particulier qui nous intéresse, on a les deux formules suivantes :

$$[K:\mathbb{Q}] = 3, \quad h(K) = \frac{1}{4} \frac{P}{R(K)} |L(1, \chi)|^2 \quad (p \equiv 1 \pmod{6}),$$

$$\begin{aligned} [K:\mathbb{Q}] &= 4 \\ [K:k] &= 2, \quad \frac{h(K)}{h(k)} = \frac{P}{4} \frac{R(k)}{R(K)} |L(1, \chi)|^2 \quad (p \equiv 1 \pmod{8}). \end{aligned}$$

Le problème est donc de montrer que  $h(K)$  dans le cas cubique,  $h(k)$  et  $h(K)/h(k)$  dans le cas du degré 4 sont inférieurs à  $p$ . Il s'agit donc de majorer les  $|L(1, \chi)|$  et de minorer  $R(k)$  (resp.  $R(K)$  et  $R(K)/R(k)$ ).

#### 1. - MINORATION DE $L(1, \chi)$ .

A quelques modifications techniques près cette majoration est donnée en suivant une méthode de HUA [4] présentée dans le cas d'un caractère réel.

LEMME 2. - Soient  $f$  un entier naturel et  $\chi$  un caractère primitif pair de conducteur  $f$ . Pour tout entier naturel  $n$  on note respectivement  $n^*$  le plus petit reste de  $n$  modulo  $f$  et  $S(n)$  le nombre complexe

$$S(n) = \sum_{a=0}^n \sum_{j=0}^a \chi(j).$$

Alors, pour tout  $n > 0$ , on a  $|S(n)| \leq (n^*+1) \cdot \frac{1}{2} \left\{ \sqrt{f} - \frac{n^*+1}{\sqrt{f}} \right\}$ .

On utilise les propriétés relatives à la somme de Gauss associée au caractère  $\chi$ , à savoir

$$|\tau(\chi)| = f$$

$$\forall n \in \mathbb{N}, \quad \sum_{x \bmod f} \chi(x) \exp(2i\pi xn/f) = \bar{\chi}(n) \tau(\chi).$$

Si on pose  $\varphi(n, \chi) = \tau(\chi) \cdot \sum_{a=0}^n \sum_{j=-a}^a \bar{\chi}(j)$ , on a :

III.4

$$\begin{aligned} \varphi(n, \chi) &= \sum_{x \bmod f} \chi(x) \sum_{a=0}^n \sum_{j=-a}^a u^{2nj} \quad \text{avec } u = \exp(i\pi/f) \\ \varphi(n, \chi) &= \sum_{x \bmod f} \chi(x) (u^x - u^{-x})^{-1} \sum_{a=0}^n (u^{(2a+1)x} - u^{-(2a+1)x}) \\ &= \sum_{x \bmod f} \chi(x) \frac{\sin^2 \pi(n+1)x/f}{\sin^2 \pi x/f} . \end{aligned}$$

On a donc en premier lieu  $\varphi(n, \chi) = \varphi(n^*, \chi)$  pour tout  $n$  et en second lieu l'inégalité

$$|\varphi(n, \chi)| \leq \sum_{\substack{x \bmod f \\ x \neq 0}} \sum_{a=0}^{n^*} \sum_{j=-a}^a u^{2jx} .$$

C'est-à-dire  $|\varphi(n, \chi)| \leq \sum_{a=0}^{n^*} \left\{ \sum_{j=-a}^a -1 + \sum_{h=1}^f e^{2i\pi jh/f} \right\}^{-}$ . La quantité entre { } vaut  $f-1$  si  $j = 0$  et  $-1$  sinon. On obtient en fin de compte

$$\begin{aligned} |\varphi(n, \chi)| &\leq (n^*+1)[f-1] + \sum_{a=1}^{n^*} -2a \\ |\varphi(n, \chi)| &\leq (n^*+1)[f-1-n^*] . \end{aligned}$$

Du fait que  $\chi$  est pair on a  $S_\chi(n) = \frac{1}{2} \left\{ \frac{1}{\tau(\chi)} \varphi(n, \chi) \right\}$ . D'où le lemme.

Pour des raisons techniques qui interviendront à la fin de l'exposé, on est amené à considérer des caractères non primitifs.

LEMME 3. - Soient  $f$  un entier,  $\chi$  un caractère modulo  $f$ , non primitif, non principal et pair. Soit  $\chi_1$  le caractère primitif équivalent à  $\chi$ . Soient  $q$  le conducteur de  $\chi_1$  et  $d = (f/q)$ . Alors

$$S_\chi(n) = \sum_{r|d} \mu(r) \chi_1(r) S_{\chi_1}([n/r]) .$$

En particulier pour tout  $n \in [\sqrt{2q}, q]$ , si  $f = 2q$  on a

$$|S_\chi(n)| \leq \frac{3}{2} n\sqrt{q}$$

et pour tout entier  $n > q$ ,  $|S_\chi(n)| < \frac{3}{8} q\sqrt{q}$ .

On sait que  $\sum_{\delta|m} \mu(\delta)$  est égal à 1 si  $m = 1$ , sinon à 0.

Par suite avec les notations de l'énoncé, pour tout  $n \geq 1$  on a

$$\chi(n) = \chi_1(n) \sum_{\delta|(n,d)} \mu(\delta).$$

De là, il résulte les égalités suivantes

$$\begin{aligned} S_{\chi}(n) &= \sum_{\delta|d} \mu(\delta) \sum_{a=0}^n \sum_{\substack{j=0 \\ \delta|j}}^a \chi_1(j) \\ &= \sum_{\delta|d} \mu(\delta) \chi_1(\delta) \sum_{a=0}^n \sum_{j=0}^{[a/\delta]} \chi_1(j) \\ &= \sum_{\delta|d} \mu(\delta) \chi_1(\delta) \sum_{k=0}^{[n/\delta]} \delta \sum_{j=0}^k \chi_1(j) \\ S_{\chi}(n) &= \sum_{\delta|d} \delta \mu(\delta) \chi_1(\delta) S_{\chi_1}([n/\delta]). \end{aligned}$$

En particulier, si  $d = 2$  et  $n \in [\sqrt{2q}, q-1]$ ,  $n = n^*$  et d'après le lemme 2

$$\begin{aligned} |S_{\chi}(n)| &\leq \sum_{\delta=1}^2 \frac{1}{2} \delta \left\{ ([\frac{n}{\delta}]^* + 1) \left\{ \sqrt{q} - \frac{[n/\delta] + 1}{\sqrt{q}} \right\} \right. \\ |S_{\chi}(n)| &\leq \frac{1}{2} (n+1) \left\{ \sqrt{q} - \frac{n+1}{\sqrt{q}} \right\} + (\frac{n}{2} + 1) \left\{ \sqrt{q} - \frac{n}{2\sqrt{q}} \right\} \\ |S_{\chi}(n)| &\leq \frac{3}{2} n\sqrt{q} + \frac{\sqrt{q}}{2} - \frac{(n+1)^2}{2\sqrt{q}} + \sqrt{q} - \frac{n(n+2)}{4\sqrt{q}}. \end{aligned}$$

Or  $\frac{3\sqrt{q}}{2} - \frac{(n+1)^2}{2\sqrt{q}} - \frac{n(n+2)}{4\sqrt{q}} \leq -\frac{\sqrt{2}}{2}$  si  $n > \sqrt{2q}$ . Ceci achève la démonstration des deux premières parties. La dernière est immédiate, du fait d'après le lemme 2 que  $|S_{\chi_1}(n)| < \frac{q\sqrt{q}}{8}$  ■

LEMME 4. - Soient  $p$  un nombre premier et  $\chi_1$  un caractère primitif pair modulo  $p$ . On suppose  $p > 30$ . Alors

$$|L(1, \chi_1)| \leq \frac{1}{2} \text{Log } p + \gamma - \frac{1}{2}.$$

On pose  $S(0) = S(-1) = 0$  et pour  $n \geq 1$  on conserve les notations du lemme 2. On remarque que  $S(p) = S(p-1) = 0$ . Une majoration de  $|S(n)|$  est évidemment  $\frac{1}{2} n(n+1)$ , majoration meilleure que celle du

lemme 2 pour  $n < \sqrt{p}$ . Pour tout  $n \geq 1$ ,

$$\chi_1(n) = S(n) - 2S(n-1) + S(n-2)$$

ce qui permet d'écrire

$$L(1, \chi_1) = \sum_{n=1}^{\infty} \frac{2S(n)}{n(n+1)(n+2)} = \sum_{n=1}^{\infty} \rho(n).$$

Les remarques qui précèdent amènent à "couper" en trois morceaux :

$$\sum 1 = \sum_1^{\lfloor \sqrt{p} \rfloor} \rho(n); \quad \sum 2 = \sum_{n=1+\lfloor \sqrt{p} \rfloor}^{p-2} \rho(n); \quad \sum 3 = \sum_{p+1}^{\infty} \rho(n)$$

et il suffit de majorer  $|\sum 1|$ ,  $|\sum 2|$  et  $|\sum 3|$ .

- On a  $|\sum 1| \leq \sum_{n=1}^{\lfloor \sqrt{p} \rfloor} \frac{1}{n+2} = -\frac{3}{2} + \frac{1}{1+\lfloor \sqrt{p} \rfloor} + \frac{1}{2+\lfloor \sqrt{p} \rfloor} + \sum_1^{\lfloor \sqrt{p} \rfloor} \frac{1}{n}$ .

D'après la formule d'Euler-Mac-Laurin on obtient

$$\sum_1^A \frac{1}{j} \leq \text{Log } A + \gamma + \frac{1}{2A}$$

et donc

$$|\sum 1| \leq \frac{1}{2} \text{Log } p - \frac{3}{2} + \gamma + \frac{1}{2\lfloor \sqrt{p} \rfloor} + \frac{1}{1+\lfloor \sqrt{p} \rfloor} + \frac{1}{2+\lfloor \sqrt{p} \rfloor}.$$

- D'après la majoration fournie par le lemme 2, on a

$$|\sum 2| \leq \sum_{1+\lfloor \sqrt{p} \rfloor}^{p-2} \frac{\sqrt{p}}{n(n+2)} - (\sqrt{p})^{-1} \sum_{1+\lfloor \sqrt{p} \rfloor}^{p-2} \frac{n+1}{n(n+2)}$$

$$|\sum 2| \leq 1 - \frac{\sqrt{p}}{p-1} - \frac{1}{\sqrt{p}} \sum_{1+\lfloor \sqrt{p} \rfloor}^{p-2} \frac{1}{n+1} \leq 1 - \frac{\sqrt{p}}{p-1} + \frac{1}{p} - \frac{1}{2\sqrt{p}} \text{Log } p.$$

- On a immédiatement

$$|\sum 3| \leq \frac{1}{8} p^{3/2} \sum_{p+1}^{\infty} \frac{2}{n(n+1)(n+2)} \leq \frac{p^{3/2}}{8} \left( \frac{1}{p+1} - \frac{1}{p+2} \right) < \frac{1}{8\sqrt{p}}.$$

D'où

$$|L(1, \chi_1)| \leq \frac{1}{2} \text{Log } p + \gamma - \frac{1}{2} + \frac{1}{2\lfloor \sqrt{p} \rfloor} + \frac{1}{1+\lfloor \sqrt{p} \rfloor} + \frac{1}{2+\lfloor \sqrt{p} \rfloor} - \frac{\sqrt{p}}{p-1} + \frac{1}{p} + \frac{1}{8\sqrt{p}} - \frac{\text{Log } p}{2\sqrt{p}}$$

et on vérifie que  $|L(1, \chi_1)| \leq \frac{1}{2} \text{Log } p + \gamma - \frac{1}{2}$  pour  $p > 30$  ■

LEMME 5. - On utilise les notations du lemme 4. De plus, soit  $\chi$  le caractère modulo  $2p$  nul sur les entiers pairs qui coïncide avec  $\chi_1$  sur les entiers impairs. Alors :

- 1)  $L(1, \chi_1) = (1 - \chi_1(2)2^{-1})L(1, \chi)$  .
- 2)  $|L(1, \chi)| \leq \frac{1}{2} \text{Log } p + 1,546 + \frac{1}{\sqrt{p}} \cdot 0,1427$  .

La première assertion résulte du développement en produit eulérien de  $L(1, \chi)$  . En ce qui concerne la seconde, on procède à peu près comme dans la démonstration qui précède, en utilisant le lemme 3 au lieu du lemme 2 . On coupe de la façon suivante :

$$\sum 1 = \sum_{n=1}^{[\sqrt{2p}]}$$

$$\sum 2 = \sum_{n=1+[\sqrt{2p}]}^p \rho(n) \quad \text{avec} \quad \rho(n) = 2 S(n) \{n(n+1)(n+2)\}^{-1} .$$

$$\sum 3 = \sum_{n=p+1}^{\infty} \rho(n)$$

On obtient :

- $|\sum 1| \leq \frac{1}{2} \text{Log } p + \frac{1}{2} \text{Log } 2 + \gamma - \frac{3}{2} + \frac{1}{2[\sqrt{2p}]} + \frac{1}{1+[\sqrt{2p}]} + \frac{1}{2+[\sqrt{2p}]}$
- $|\sum 2| \leq 3\sqrt{p} \sum_{n=1+[\sqrt{2p}]}^p \frac{1}{(n+1)(n+2)} = 3\sqrt{p} \left\{ \frac{1}{2+[\sqrt{2p}]} - \frac{1}{p+2} \right\}$
- $|\sum 2| \leq \frac{3}{2} \sqrt{2} - \frac{3\sqrt{p}}{p+2}$  .
- $|\sum 3| < \frac{3}{8} \frac{1}{\sqrt{p}}$  .

$$\begin{aligned} \text{D'où} \quad |L(1, \chi)| &\leq \frac{1}{2} \text{Log } p + \frac{1}{2} \text{Log } 2 + \gamma + \frac{3}{2} (\sqrt{2} - 1) + \frac{1}{2[\sqrt{2p}]} + \frac{1}{1+[\sqrt{2p}]} \\ &\quad + \frac{1}{2+[\sqrt{2p}]} + \frac{3}{8\sqrt{p}} - \frac{2}{\sqrt{p}} . \end{aligned}$$

D'où le lemme ■



2. - MINORATIONS DE REGULATEURS.

On va distinguer ici le cas du degré 3 du cas du degré 4 .  
On utilisera les représentations d'entiers de telles extensions données par HASSE [3] . Celles-ci, au moins pour le degré 3, avaient été racontées par M.N.G. en 1971. On rappelle simplement ici les principales formules.

2.1. - Le cas cubique.

Tout nombre premier congru à 1 modulo 6 peut s'écrire de manière unique sous la forme

$$\left\{ \begin{array}{l} p = \frac{1}{4}(a^2 + 3b^2) \\ a \in \mathbb{Z} , a \equiv 2 \pmod{3} \\ b \in \mathbb{N} , b \equiv 0 \pmod{3} , b > 0 . \end{array} \right.$$

Si dans  $\mathbb{Q}(j)$  on pose  $\varphi = \frac{1}{2}(a + b\sqrt{-3})$  , alors il existe un caractère cubique modulo  $p$  , soit  $\chi$  tel que la somme de Gauss  $\tau(\chi)$  vérifie

$$\tau(\chi)^3 = -p\varphi . \quad (1)$$

Si on pose

$$T = -\tau(\chi)$$

on a les égalités

$$T^3 = p\varphi , \quad T^2 = \varphi \bar{T} . \quad (2)$$

Cela étant, tout élément  $A$  de  $K$  peut se mettre sous la forme

$$A = \frac{1}{3} \{x + yT + \bar{y}\bar{T}\} \stackrel{\text{df}}{=} [x, y] \left\{ \begin{array}{l} x \in \mathbb{Q} \\ y \in \mathbb{Q}(j) \end{array} \right. . \quad (3)$$

Un  $A \in K$  est un entier si et seulement si

$$\left. \begin{array}{l} x \in \mathbb{Z} \\ y \in \mathbb{Z}[j] \end{array} \right\} x \equiv y \pmod{(1-j)} \text{ dans } \mathbb{Z}[j] \quad (4)$$

Soit  $\sigma$  le générateur de  $\text{Gal}(K/\mathbb{Q})$  tel que  $\chi(\sigma) = j$  . Alors

$A^\sigma = [x, j^2 y]$  . Les formules qui nous seront utiles sont les suivantes :

$$\begin{aligned} N_{K/\mathbb{Q}} [x, y] &= \frac{1}{27} \{x^3 - 3pxNy + pS(\varphi y^3)\} \\ \text{Tr}_{K/\mathbb{Q}} ([x, y]^2) &= \frac{1}{3} (x^2 + 2pNy) \end{aligned} \quad (5)$$

où  $N$  (resp.  $S$ ) est la norme (resp. la trace) dans  $\mathbb{Q}(j)/\mathbb{Q}$ .

LEMME 6. - Soit  $\epsilon = [x, y]$  une unité de  $K$  qui n'est pas rationnelle. Son régulateur vérifie

$$R(\epsilon) \geq \frac{1}{4} \text{Log}^2 \left\{ \frac{x^2 + 2pNy - 3}{6} \right\} .$$

On vérifie facilement que

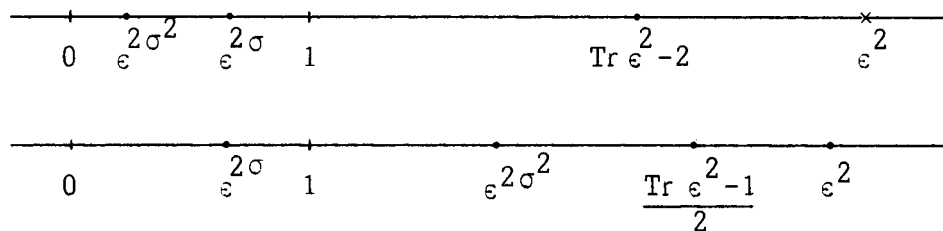
$$R(\epsilon) = \text{Log}^2 |\epsilon| + \text{Log} |\epsilon| \cdot \text{Log} |\epsilon^\sigma| + \text{Log}^2 |\epsilon^\sigma| .$$

C'est-à-dire

$$R(\epsilon) = \frac{1}{4} \left\{ (\text{Log} \epsilon^2 + \frac{1}{2} \text{Log} \epsilon^{2\sigma})^2 + \frac{3}{4} \text{Log}^2 \epsilon^{2\sigma} \right\}$$

ou l'une des deux autres égalités obtenues par permutation sur  $1, \sigma, \sigma^2$ .

Il n'est pas difficile de voir qu'on a, en supposant que  $\epsilon^2$  est la plus grande des trois unités  $\epsilon^2, \epsilon^{2\sigma}, \epsilon^{2\sigma^2}$  l'un des deux schémas suivants, à permutation près de  $\sigma$  et  $\sigma^2$



Dans le premier cas  $|\text{Log} \epsilon^{2\sigma} + \frac{1}{2} \text{Log} \epsilon^2| \geq \frac{1}{2} \text{Log} \epsilon^2$ . Donc

$$R(\epsilon) \geq \frac{1}{4} \text{Log}^2 (\epsilon^2) \geq \frac{1}{4} \text{Log}^2 (\text{Tr}(\epsilon^2) - 2) .$$

Dans le second cas  $|\text{Log} \epsilon^{2\sigma} - \frac{1}{2} \text{Log} \epsilon^2| \geq \frac{1}{2} \text{Log} \epsilon^2 + \text{Log} \epsilon^{2\sigma} \geq \frac{1}{2} \text{Log} \epsilon^2$ .

D'où cette fois

$$R(\epsilon) \geq \frac{1}{4} \text{Log}^2 \epsilon^2 \geq \frac{1}{4} \text{Log}^2 \left\{ \frac{1}{2} (\text{Tr}(\epsilon^2) - 1) \right\}$$

et le lemme ■

LEMME 7. - Soit  $p$  un nombre premier congru à 1 modulo 3. Le régulateur  $R(K)$  de  $K$  vérifie :

- Si  $p$  est de la forme  $\frac{1}{4}(a^2 + 27)$ , alors  $R(K) > \frac{1}{4} \text{Log}^2 \left( \frac{7}{15} p \right)$ .
- Sinon  $R(K) > \frac{1}{4} \text{Log}^2 \left( \frac{52}{30} p \right)$  dès que  $p > 130$ .

D'après les formules 4 et 5 ci-dessus l'unité fondamentale  $\varepsilon = [x, y]$  de  $K$  doit vérifier

$$\begin{cases} x \equiv y \pmod{1-j} \text{ dans } \mathbb{Q}(j) \\ (x-3)(x^2+3x+9) = p(3xNy - S(\varphi y^3)) \\ x^2 + 2pNy \text{ minimum.} \end{cases}$$

On essaie les diverses valeurs possibles pour  $Ny$ , telles que  $\text{Tr}(\varepsilon^2)$  soit minimum.

1) A conjugaison près pour  $\varepsilon$ , l'hypothèse  $Ny = 1$  implique  $y \in \{1, -1, (1+j), -(1+j)\}$ , ce qui conduit à

$$(x-3)(x^2+3x+9) = p(3x+a\theta(y))$$

$$\text{avec } \theta(y) = \begin{cases} -y & \text{si } y \in \{-1, 1\} \\ 1 & \text{si } y = 1+j, -1 & \text{si } y = 1-j \end{cases}.$$

On vérifie que  $p \mid (x-3)$  conduit à  $|a| > \sqrt{4p}$ , ce qui est contradictoire. Si on pose  $dp = x^2+3x+9$  on obtient

$$a^2 = \left\{ \frac{4}{d}(x^2+3x+9) - 3b^2 \right\} = ((d-3)x-3d)^2$$

c'est-à-dire

$$(d-1)^2(d-4)x^2 - 6[d^2(d-3)+2]x + 9d^3 + 3b^2d - 36 = 0$$

ou encore

$$(d-1)^2(d-4)x^2 - 6(d-1)(d^2-2d-2)x + 3(3d^3+b^2d-12) = 0.$$

La condition  $d = 1$  implique  $b = 3$ , donc  $p = \frac{1}{4}(a^2+27)$  avec

$x = \frac{a\theta(y)-3}{2}$ . Si  $d \neq 1$ , on a à résoudre l'équation

$$(d-1)^2(d-4)x^2 - 6(d^2-2d-2)(d-1)x + 3(3d^3+b^2d-12) = 0$$

On ne peut avoir  $d = 4$  car  $x^2+3x+9$  est impair. Le discriminant de cette équation est, en posant  $b = 3b_1$

$$9(d-1)^2 \{-3b_1^2d^2 + 4(b_1^2+2)d - 12\}$$

qui est négatif pour  $d > 4$ . On ne peut avoir  $d = 3$  car  $x$  est non multiple de 3.

Inversement si  $p$  est de la forme  $\frac{1}{4}(a^2+27)$ , le corps  $K$  admet

pour unité fondamentale  $[\frac{-a+3}{2}, -1]$ . La majoration du régulateur est alors facile. Maintenant si  $p$  n'est pas de la forme  $\frac{1}{4}(a^2+27)$ , l'hypothèse  $N(y) = 3$  implique que 3 divise  $x$ . Posant  $x = 3x_1$ , on obtient l'équation  $(x_1-1)(x_1^2+x+1) = p(x_1 - \frac{1}{27} S(\varphi y^3))$ . Or on vérifie que  $S(\varphi y^3) \in \{27b, -27b\}$ . D'où  $(x_1-1)(x_1^2+x+1) = p(x_1+eb)$ . On vérifie que le second membre est congru à  $x_1$  modulo 3 tandis que le premier est congru à  $x_1^3 - 1$ , c'est-à-dire à  $x_1 - 1$ . En conclusion si  $p$  n'est pas de la forme  $\frac{1}{4}(a^2+27)$  on a  $Ny \geq 4$ . En ce qui concerne  $x$ , ou bien  $x \geq p+3$ , ou bien  $p$  divise  $x_1^2+3x+9$  avec un quotient  $d$  qui vérifie

$$3 \mid d \Rightarrow N(y) \geq 6 \Rightarrow \text{Tr } \epsilon^2 > 4p$$

$$3 \nmid d \Rightarrow d \geq 5 \Rightarrow x > \frac{29\sqrt{p}}{10} \text{ dès que } p > 13.$$

On en déduit  $x^2 + 2pNy > 12,41 \cdot p$ . Donc

$$\frac{\text{Tr}(\epsilon^2) - 1}{2} > \frac{1}{6} \{12,41p - 3\} > 2p$$

et

$$R(K) \geq \frac{1}{4} \text{Log}^2(2p).$$

## 2.2. - Le cas du degré 4.

Soit  $k$  le corps quadratique intermédiaire entre  $K$  et  $\mathbb{Q}$ . On désigne par  $\epsilon_0$  l'unité fondamentale de  $k$  et par  $\epsilon$  une unité fondamentale relative de  $K$ , c'est-à-dire que  $\epsilon$  et  $\epsilon^\sigma$  engendrent le groupe des unités de  $K$  dont la norme dans  $K/k$  appartient à  $\{-1, 1\}$ . Il résulte facilement de la seconde assertion du théorème 1 qu'on a  $N_{K/k} \epsilon = -1$  et que dans le groupe  $U_K$  des unités de  $K$  le sous-groupe engendré par  $\epsilon_0, \epsilon, \epsilon^\sigma$  est d'indice 2. Par suite, on a

$$R(K) = \frac{1}{2} R(\epsilon_0, \epsilon, \epsilon^\sigma).$$

Or on a

$$R(\epsilon_0, \epsilon, \epsilon^\sigma) = \text{ABS} \begin{vmatrix} \text{Log } |\epsilon| & \text{Log } |\epsilon^\sigma| & -\text{Log } |\epsilon| \\ \text{Log } |\epsilon^\sigma| & -\text{Log } |\epsilon| & -\text{Log } |\epsilon^\sigma| \\ \text{Log } |\epsilon_0| & -\text{Log } |\epsilon_0| & \text{Log } |\epsilon_0| \end{vmatrix}.$$

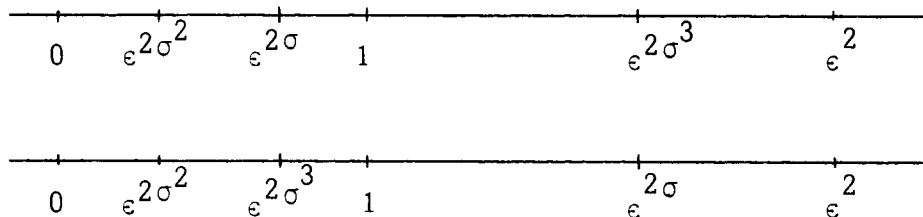
Ce qui donne

$$R(\epsilon_0, \epsilon, \epsilon^\sigma) = R(\epsilon_0) \cdot 2 \{ \text{Log}^2 |\epsilon| + \text{Log}^2 |\epsilon^\sigma| \} .$$

En conclusion provisoire

$$\frac{R(K)}{R(k)} = \frac{1}{4} \{ \text{Log}^2 \epsilon^2 + \text{Log}^2 \epsilon^{2\sigma} \} .$$

Par ailleurs, on a l'une des répartitions possibles des unités



Dans le premier cas on a :

$$\text{Tr}(\epsilon^2) \leq 2 + \epsilon^2 + \frac{1}{2\sigma} \leq 2 + 2\epsilon^2$$

Donc  $\text{Log}(\frac{1}{2}(\text{Tr} \epsilon^2 - 1)) \leq \text{Log}(\epsilon)^2$  et  $\text{Log}^2(\frac{1}{2} \text{Tr}(\epsilon^2) - 1) \leq \text{Max}_i |\text{Log}(\epsilon^{2\sigma^i})|$  .

Dans le second cas on a :

$$\text{Tr}(\epsilon^2) \leq 2 + \epsilon^{2\sigma} + \epsilon^2$$

et aussi  $(\frac{1}{2} \text{Tr} \epsilon^2 - 1) \leq \text{Max} \epsilon^{2\sigma^i}$  . Donc, dans tous les cas :

$$\text{Max}(\text{Log}^2(\epsilon^{2\sigma^i})) \geq \text{Log}^2(\frac{1}{2} \text{Tr}(\epsilon^2) - 1) .$$

Il en résulte en définitive :

$$\boxed{\frac{R(K)}{R(k)} \geq \frac{1}{4} \text{Log}^2(\frac{1}{2} \text{Tr}(\epsilon^2) - 1)} .$$

Donnons maintenant la représentation de Hasse des entiers de  $K$  . Le nombre premier  $p$  congru à 1 modulo 8 peut s'écrire de manière unique sous la forme

$$\begin{cases} a^2 + b^2 \\ a \in \mathbb{Z} , a \equiv 1 \pmod{4} \\ b \in \mathbb{N} , b \equiv 0 \pmod{4} . \end{cases}$$

Si on pose  $\pi = a + bi$  , il existe un caractère  $\chi$  pair d'ordre 4 , de conducteur  $p$  tel que la somme de Gauss  $\tau(\chi)$  vérifie

$$\begin{cases} T^2 = -\sqrt{p}\pi \\ T\bar{T} = p \end{cases} .$$

Le caractère  $\chi$  étant ainsi choisi, on note  $\sigma$  un générateur de  $K/\mathbb{Q}$  tel que  $\chi(\sigma) = i$ . Alors les entiers de  $K$  peuvent être représentés sous la forme

$$A = \frac{1}{2} \left\{ x + \frac{1}{2} (yT + \bar{y}\bar{T}) \right\} , \begin{cases} x \text{ entier de } k , & x = \frac{1}{2}(x_1 - x_2)\sqrt{p} \\ y \in \mathbb{Z}[i] , & y = y_1 + iy_2 \\ x_1 \equiv x_2 \equiv y_1 + y_2 \pmod{2} . \end{cases}$$

Alors si  $A = [x, y]$  on a  $A^\sigma = [\tilde{x}, iy]$ . Les formules qui nous seront utiles sont les suivantes : si on pose

$$\phi(y) = a(y_1^2 - y_2^2) - 2by_1y_2$$

on a

$$\begin{aligned} N_{K/k}(A) &= \frac{1}{4} \left\{ x^2 - \frac{1}{2}(p(y_1^2 + y_2^2)) - \sqrt{p}\phi(y) \right\} \\ \text{Tr}_{K/\mathbb{Q}} A^2 &= \frac{1}{2} \left\{ \frac{1}{2}(x_1^2 + px_2^2) + p(y_1^2 + y_2^2) \right\} . \end{aligned}$$

En particulier, si  $\varepsilon$  est une unité relative fondamentale, on aura si  $\varepsilon = [x, y]$ ,

$$-1 = \frac{1}{4} \left\{ x^2 - \frac{1}{2}(p(y_1^2 + y_2^2)) - \sqrt{p}\phi(y) \right\} .$$

PROPOSITION 8. - Soit  $m(K)$  le minimum de la forme quadratique  $u \rightarrow \text{Tr } u^2$  sur le groupe  $E$  des unités relatives. Alors

- 1) Si  $b = 4$ ,  $m(K) = p - 4$
- 2) Si  $b > 4$ ,  $m(K) \geq 5p - 4$ .

Si  $\varepsilon$  est une unité relative fondamentale sa norme relative est  $-1$ . Si on pose  $\varepsilon = [x, y]$  on devra avoir

$$\frac{x_1^2 + px_2^2}{4} - \frac{1}{2} p(y_1^2 + y_2^2) = -4$$

$$x_1x_2 = a(y_1^2 - y_2^2) - 2by_1y_2$$

$$x_1 \equiv x_2 \equiv y_1 + y_2 \pmod{2} .$$

Dans ces conditions la trace absolue de  $\varepsilon^2$  est égale à

$$p(y_1^2 + y_2^2) - 4 .$$

Il est donc suffisant de regarder quelles sont les valeurs minimum possibles pour  $y_1^2 + y_2^2$ .

• On essaie  $y_1^2 + y_2^2 = 1$ . Modulo la conjugaison, on peut alors supposer  $y_1 \in \{-1, 1\}$  et  $y_2 = 0$ . On obtient

$$\begin{aligned} x_1^2 &\equiv -16 \text{ modulo } p \\ x_1 x_2 &= a \\ x_1 &\equiv x_2 \equiv 1 \text{ modulo } 2 . \end{aligned}$$

De la majoration  $|x_1| \leq |a| < \sqrt{p}$  on déduit  $x_1^2 = p^2 - 16$ . Donc  $x_1^2 = a^2 + (b^2 - 16)$ , d'où  $b = 4$  et  $p = a^2 + 16$ . Une unité relative fondamentale est  $\varepsilon = \left[ \frac{a - \sqrt{p}}{2}, 1 \right]$ .

Réciproquement, il est évident que si  $p = a^2 + 16$ ,  $y_1^2 + y_2^2 = 1$ . Supposons dorénavant  $p$  non de la forme  $a^2 + 16$ .

• L'hypothèse  $y_1^2 + y_2^2 = 2$  implique à conjugaison ou changement de signe près  $y_1 = y_2 = 1$ . D'où le système

$$\begin{aligned} x_1 \text{ et } x_2 &\text{ pairs} \\ x_1 x_2 &= -2b . \end{aligned}$$

Donc  $|x_1| \leq b < \sqrt{p}$  si par suite  $x_1^2 = 4p - 16 = 4a^2 + 4b^2 - 16 > 2b^2$  contradiction. On ne peut avoir  $y_1^2 + y_2^2 = 3$ . L'hypothèse  $y_1^2 + y_2^2 = 4$  permet de supposer  $y_1 = 2$ ,  $y_2 = 0$ . D'où le système

$$\begin{cases} x_1 \text{ et } x_2 \text{ pairs} \\ x_1 x_2 = 4a \\ x_1^2 \equiv -16 \text{ mod } p . \end{cases}$$

On aurait

$$\begin{aligned} &|x_1| < 2|a| \\ \text{et} \quad &x_1^2 = 4p - 16 = 4a^2 + 4b^2 - 16 > 4a^2 , \end{aligned}$$

nouvelle contradiction ; d'où le lemme ■

3. - DEMONSTRATION DES RESULTATS.

3.1. Le cas cubique.

• Si  $p$  n'est pas de la forme  $\frac{1}{4}(a^2+27)$ , s'il est congru à 1 modulo 3 et supérieur à 30, le nombre de classes  $h(K)$  du sous-corps cubique de  $\mathbb{Q}^{(p)}$  est majoré par

$$\frac{p}{4} \cdot \frac{(1/4) \{ \text{Log } p + 2\gamma - 1 \}^2}{1/4 \{ \text{Log}^2(2p) \}} < \frac{p}{4} .$$

Les nombres premiers inférieurs à 30 congrus à 1 modulo 3 sont tous de la forme  $\frac{1}{4}(a^2+27)$ .

• Si  $p$  est de la forme  $\frac{1}{4}(a^2+27)$ , alors 2 n'est pas reste cubique modulo  $p$  et on a

$$\left| 1 - \frac{\chi_1(2)}{2} \right|^{-1} = \left| 1 - \frac{1}{2} \right|^{-1} = \frac{2}{\sqrt{7}} .$$

On utilise alors le lemme 5 qui fournit la majoration

$$R(K) \leq \frac{p}{4} \frac{(1/4) \{ \text{Log } p + 16/5 \}^2}{(1/4) \{ \text{Log } p - \text{Log } \frac{15}{7} \}^2} \cdot \frac{4}{7} .$$

On vérifie alors que pour  $p > 4000$  le terme de droite est inférieur à  $p/3$ . Pour  $p < 4000$  la table 1 de [1] fournit le résultat suivant :

p	7	13	19	37	79	97	139	163	313
h(K)	1	1	1	1	1	1	1	4	7
p	349	607	709	877	937	1063	1129	1489	1567
h(K)	4	4	4	7	4	13	7	19	7
p	1987	2557	2659	3313	3547				
h(K)	7	7	19	19	19				

3.2. Le cas du degré 4.

• En premier lieu on considère le corps quadratique  $\mathbb{Q}(\sqrt{p}) = k$ . Du fait que  $p$  est congru à 1 modulo 8, l'unité fondamentale  $\varepsilon_0$



de  $k$  est de la forme  $a+b\sqrt{p}$ , avec  $a$  et  $b$  entiers naturels. En particulier on a (grossoièrement)  $\epsilon > \sqrt{2p}$  et le régulateur de  $k$  est supérieur à  $\frac{1}{2} \text{Log } 2p$ . Il résulte de ce qui précède que

$$h(k) \leq \frac{\sqrt{p}}{2} \frac{\frac{1}{2} \text{Log } p + \gamma - \frac{1}{2}}{\frac{1}{2} \text{Log } p + \frac{1}{2} \text{Log } 2} < \frac{\sqrt{p}}{2}$$

dès que  $p > 30$ . De plus,  $\mathbb{Q}(\sqrt{17})$  est principal. La majoration ci-dessus est donc valable pour tout nombre premier  $p$  congru à 1 modulo 8.

• En second lieu, si  $p$  n'est pas de la forme  $a^2+16$  on a la majoration

$$\frac{h(K)}{h(k)} \leq \frac{p}{4} \left\{ \frac{\text{Log } p + 2\gamma - 1}{\text{Log } \frac{5p-6}{2}} \right\}^2 < \frac{p}{4} \quad (p > 30).$$

• Enfin, si  $p$  est de la forme  $a^2+16$ , 2 est reste quadratique modulo  $p$  mais n'est pas reste de puissance quatrième. On a donc  $|1 - \frac{\chi(2)}{2}|^2 = |1 + \frac{1}{2}|^2 = \frac{9}{4}$ . On utilise le lemme 5 pour obtenir la majoration

$$\frac{h(K)}{h(k)} \leq \frac{p}{4} \cdot \frac{4}{9} \left\{ \frac{\text{Log } p + 3,092 + 0,1427 \cdot p^{\frac{1}{2}} \times 2}{\text{Log}(\frac{p-6}{2})} \right\}^2$$

et on vérifie que le terme de droite est inférieur à  $p/4$  dès que  $p > 4000$ . Pour les nombres premiers inférieurs à 4000 la table [2] donne le résultat :

p	17	41	97	137	241	457	641	857	977
h(K)	1	1	1	1	1	5	5	5	5
p	1697	2417	2617	3041					
h(K)	17	17	13	13					

Ce qui achève les démonstrations ■

- [1] GRAS Marie-Nicole - Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités d'une extension cyclique cubique de  $\mathbb{Q}$ . Jour. F. die reine und ange. Math. 277 (1975).
- [2] GRAS Marie-Nicole - Tables numériques du nombre de classes et des unités des extensions cycliques de degré 4 de  $\mathbb{Q}$ . Sémin. Th. des nbres, Besançon (77/78).
- [3] HASSE Helmut - Arithmetische Bestimmung von Grundeinheit... Mathematische Abhandlungen 3 de Gzuyter (1975).
- [4] HUA Loo-Keng - On the least solution of Pell's equation. American Jour. of Math. (1942).
- [5] LANG Serge - Cyclotomic Fields, GTM 59, Springer.
- [6] YOKOI Hideo - On the class number of a relatively cyclic Number Field. Nagoya Math. Jour. 29 (1967).