

TABLE NUMERIQUE DU NOMBRE DE CLASSES ET DES UNITES  
=====

DES EXTENSIONS CYCLIQUES REELLES DE DEGRE 4 DE  $\mathbb{Q}$ .  
=====

Marie-Nicole GRAS

# TABLE DES MATIERES

=====

## INTRODUCTION

### I - GENERALITES SUR LES EXTENSIONS CYCLIQUES REELLES DE DEGRE 4 DE $\mathbb{Q}$ ; NOMBRE DE CLASSES ET UNITES

- 1) Description des éléments de  $K$
- 2) Structure du groupe des unités de  $K$ 
  - a) Détermination de l'indice  $Q_K$
  - b) Propriétés de  $Q_K$
- 3) Nombre de classes et unités de  $K$ 
  - a) Rappel des résultats de H. W. Leopoldt
  - b) Majoration de  $h_\chi = \left( |E_\chi| : |F_\chi| \right)$
  - c) Détermination de  $h_\chi$  et  $e_\chi$
  - d) Calcul de  $Q_K$
  - e) Calcul du nombre de classes  $h$  de  $K$
- 4) Présentation des tables
- 5) Corps cycliques réels de degré 4 admettant une unité  $\chi$ -relative telle que  $s = -1$  et  $r = -6$

### II - CLASSES DE $k$ QUI DEVIENNENT PRINCIPALES DANS $K$

### III - TABLE NUMERIQUE

## BIBLIOGRAPHIE

## INTRODUCTION

=====

Soient  $K$  une extension cyclique réelle de degré 4 de  $\mathbb{Q}$  et  $k$  son sous-corps quadratique. Dans [4], nous avons déterminé le nombre de classes et les unités de  $K$  et étudié le problème de la "capitulation" des classes de  $k$  dans  $K$ . Dans ce travail nous donnons les démonstrations de quelques propriétés, seulement énoncées dans [4], et nous publions dans la partie III la table numérique des résultats obtenus pour les 1536 corps  $K$  de conducteur inférieur à 4000 (nombre de classes, unités, capitulation) ; nous n'avons publié dans [4] qu'un court extrait de cette table.

I - GENERALITES SUR LES EXTENSIONS CYCLIQUES REELLES DE DEGRE 4 DE  $\mathbb{Q}$  ; NOMBRE DE CLASSES ET UNITES.

1) Description des éléments de K.

Soit K une extension cyclique de degré 4 de  $\mathbb{Q}$  de groupe de Galois  $G = \langle \sigma \rangle$  et de sous-corps quadratique k. Soient f le conducteur de K, m celui de k ; alors  $f = mg$  et le discriminant de K est égal à  $mf^2$ . Puisque K a pour conducteur f, on a  $K \subset \mathbb{Q}^{(f)}$  et il existe un caractère  $\chi^1$  de  $\text{Gal}(\mathbb{Q}^{(f)}/\mathbb{Q}) \simeq (\mathbb{Z}/f\mathbb{Z})^*$ , dont le noyau est  $\text{Gal}(\mathbb{Q}^{(f)}/K)$ , qu'on appellera caractère de K (il est unique à inversion près et est d'ordre 4). Le corps K sera réel si et seulement si  $\chi^1(-1) = +1$ .

Commençons par énoncer sans démonstration les résultats suivants démontrés dans [5] :

(i) Décomposition en facteurs premiers de f et m.

Pour tout  $i = 0, 1, \dots, n$ ,  $p_i$  désigne un nombre premier congru à 1 modulo 4, et g un entier sans facteur carré impair ; on désigne par  $v_2(g)$  l'exposant de la plus grande puissance de 2 qui divise g ; alors on a :

$\alpha)$  si m est impair,  $f = p_0 p_1 \dots p_n g$  et  $m = p_0 p_1 \dots p_n$ , avec  $v_2(g) = 0, 2$  ou 3 et  $(m, g) = 1$  ;

$\beta)$  si m est pair,  $f = 2^4 p_1 \dots p_n (g/2)$  et  $m = 2^3 p_1 \dots p_n$ , avec  $v_2(g) = 1$  et  $(m, g) = 2$ .

(ii) Dénombrement des corps réels de conducteur donné.

Supposons que f et m soient donnés ; on considère l'ensemble des corps cycliques réels de degré 4 de conducteur f et dont le sous-corps quadratique a pour conducteur m. Si  $f \equiv 0(8)$ , le nombre de ces corps est égal à  $2^n$  (et il y a autant de corps imaginaires). Si  $f \not\equiv 0(8)$ , le nombre de ces corps est égal à  $2^n$  ou 0 (le nombre de corps imaginaires est alors respectivement égal à 0 ou  $2^n$ ). En exprimant convenablement la condition  $\chi^1(-1) = +1$ , on montre que les corps sont réels si et seulement si  $\prod_{p|f} s_p = +1$ , où  $s_2 = -1$  et  $s_p = (-1)^{(p-1)/e_p}$  si p est impair, en désignant par  $e_p$  l'indice de ramification de p dans K. Dans tous les cas, ces différents corps sont caractérisés par les différentes décompositions de m sous la forme  $m = a^2 + b^2$ , a et b de signes fixés, b pair : on a  $K = k(\psi)$ ,

avec  $\psi = \pm \sqrt{g\sqrt{m} \frac{\sqrt{m} \pm a}{2}}$  (tout choix de signes donnant le même corps).

(iii) Base de  $K\mathbb{Q}(i)/\mathbb{Q}(i)$ .

Soient  $\zeta$  une racine primitive  $f^{\text{ième}}$  de l'unité,  $\theta = \text{Tr}_{\mathbb{Q}(f)/K}(\zeta)$  et

$$\tau = \tau(\chi'^{-1}) = \sum_{x \text{ mod } f} \chi'^{-1}(x) \zeta^x, \quad \chi' \text{ caractère de } K; \text{ alors}$$

$\tau = \theta - i\theta^\sigma - \theta^{\sigma^2} + i\theta^{\sigma^3}$ . Les éléments  $1, \sqrt{m}, \tau$  et  $\bar{\tau}$  forment une base de  $K\mathbb{Q}(i)/\mathbb{Q}(i)$ , avec le formulaire de multiplication suivant :

$$\tau \bar{\tau} = f,$$

$$\tau^2 = g(a+bi)\sqrt{m}, \quad \bar{\tau}^2 = g(a-bi)\sqrt{m},$$

$$\sqrt{m} \tau = (a+bi)\bar{\tau} \quad \text{et} \quad \sqrt{m} \bar{\tau} = (a-bi)\tau.$$

Ces formules permettent de déterminer les signes de  $a$  et  $b$  (ils dépendent du choix de la conjugaison  $\sigma$ ). Dans la table, nous ne donnerons que les valeurs absolues de  $a$  et  $b$ .

Tout élément  $\alpha$  de  $K$  s'écrit alors de manière unique :

$4\alpha = t + z\sqrt{m} + (x+yi)\tau + (x-yi)\bar{\tau}$ ,  $t, z, x, y \in \mathbb{Q}$ , et  $\alpha$  est un entier de  $K$  si et seulement si  $t, z, x, y \in \mathbb{Z}$  et vérifient les conditions supplémentaires :

$\alpha)$  si  $m$  est impair :  $t \equiv z(2)$ ,  $\frac{t+z}{2} \equiv gx(2)$  et  $\frac{t-z}{2} \equiv gy(2)$ ,

$\beta)$  si  $m$  est pair :  $t \equiv 0(4)$  et  $z \equiv 0(2)$ .

On pose  $\alpha = (t, z, x, y)$  ; on appelle  $t, z, x$  et  $y$  les coordonnées de  $\alpha$ .

Dans le cadre de cette représentation des éléments de  $K$ , on obtient les propriétés suivantes :

(iv) Base de  $K/\mathbb{Q}$ .

On a  $\tau = (\theta - \theta^{\sigma^2}) - i(\theta^\sigma - \theta^{\sigma^3})$  ; on déduit des égalités  $\tau \bar{\tau} = f$  et

$\tau^2 + \bar{\tau}^2 = 2ag\sqrt{m}$  que  $(\theta - \theta^{\sigma^2})^2 = \frac{f+ag\sqrt{m}}{2} = g\sqrt{m} \frac{\sqrt{m}+a}{2}$ . En fixant le signe

de  $a$ , on a donc  $\psi = \theta - \theta^{\sigma^2}$  ; on en déduit que :

$$4\alpha = t + z\sqrt{m} + 2x\psi + 2y\psi^\sigma, \text{ avec}$$

$$2\psi^2 = f + ag\sqrt{m}, \quad 2\psi^{2\sigma} = f - ag\sqrt{m},$$

$$2\psi\psi^\sigma = -bg\sqrt{m},$$

$$\psi\sqrt{m} = a\psi - b\psi^\sigma \quad \text{et} \quad \psi^\sigma\sqrt{m} = -b\psi - a\psi^\sigma.$$

(v) Polynome irréductible de  $\alpha$  sur  $\mathbb{Q}$ .

Soit  $\alpha$  un élément générateur de  $K$ . On a

$$2(\alpha + \alpha^{\sigma^2}) = t + z\sqrt{m} \text{ et}$$

$$16\alpha^{1+\sigma^2} = t^2 + mz^2 - 2f(x^2 + y^2) + 2\sqrt{m} [zt - g(a(x^2 - y^2) - 2bxy)].$$

On en déduit que  $\text{Irr}(\alpha, \mathbb{Q}) = X^4 - S_1X^3 + S_2X^2 - S_3X + S_4$ , avec

$$S_1 = t,$$

$$8S_2 = t^2 + mz^2 - 2(x^2 + y^2)f + 2(t^2 - mz^2),$$

$$16S_3 = [t^2 + mz^2 - 2(x^2 + y^2)f]t - 2mz[tz - g(a(x^2 - y^2) - 2bxy)],$$

$$256S_4 = [t^2 + mz^2 - 2(x^2 + y^2)f]^2 - 4m[tz - g(a(x^2 - y^2) - 2bxy)]^2.$$

(vi) Unités  $\alpha$  de  $K$  telles que  $N_{K/k}(\alpha) = \pm 1$ .

Soit  $\alpha$  un entier de  $K$  ; on a  $\alpha^{1+\sigma^2} = s = \pm 1$  si et seulement si :

$$t^2 + mz^2 = 16s + 2f(x^2 + y^2)$$

$$\text{et } tz = g[a(x^2 - y^2) - 2bxy].$$

On a alors

$$\text{Irr}(\alpha, \mathbb{Q}) = X^4 - tX^3 + rX^2 - stX + 1,$$

$$\text{où } r = \frac{t^2 - mz^2}{4} + 2s.$$

2) Structure du groupe des unités de  $K$ .

a) Détermination de l'indice  $Q_K$ .

Soit  $\chi = \chi^1 + \chi^{1^{-1}}$  ; alors  $\chi$  est un caractère rationnel de  $\mathbb{Q}^{(f)}$  et  $K$  est fixe par le noyau commun de  $\chi^1$  et  $\chi^{1^{-1}}$  ; il est donc de la forme  $K = K_{\chi}$ , au sens de H. W. Leopoldt [7]. Soit  $E_K$  le groupe des unités de  $K$  ; alors  $|E_K|$  (groupe des valeurs absolues de  $E_K$ ) est un  $\mathbb{Z}$ -module libre de rang 3 que l'on munit canoniquement d'une structure de  $\mathbb{Z}[G]$ -module, en posant  $|u|^{\sigma} = |u^{\sigma}|$  pour tout  $u \in E_K$ .

Si on applique la définition de H. W. Leopoldt pour les unités  $\chi$ -relatives, on obtient qu'une unité  $w$  de  $K$  est  $\chi$ -relative si et seulement si  $w^{1+\sigma^2} = \pm 1$ . Soit  $E_{\chi}$  le groupe des unités  $\chi$ -relatives ; puisque

$\mathbb{Z}[G]/(1+\sigma^2)$  est isomorphe à  $\mathbb{Z}[i]$ , on considère  $|E_\chi|$  comme un  $\mathbb{Z}[i]$ -module ; il est libre de dimension 1, donc  $|E_\chi| \simeq \mathbb{Z}[i]$ , et il existe une unité  $\chi$ -relative  $\epsilon_\chi$  génératrice (dans l'isomorphisme  $\mathbb{Z}[G]/(1+\sigma^2) \simeq \mathbb{Z}[i]$ ,  $i$  correspond à  $\sigma$  ; ainsi tout élément  $u_\chi$  de  $E_\chi$  s'écrit de manière unique  $u_\chi = \pm \epsilon_\chi^{\mu+\nu\sigma}$ ,  $\mu, \nu \in \mathbb{Z}$ ). Soit  $E_K$  le groupe des unités de  $K$ . Soit  $E^K$  le sous- $G$ -module de  $E_K$  engendré par  $E_K$  et  $E_\chi$  ; alors  $|E^K| = |E_K| \oplus |E_\chi|$  et si  $\epsilon_0$  est un générateur de  $E_K$ , toute unité  $w$  de  $E^K$  s'écrit de façon unique  $w = \pm \epsilon_0^\lambda \epsilon_\chi^{\mu+\nu\sigma}$ ,  $\lambda, \mu, \nu \in \mathbb{Z}$ . On pose  $Q_K = (|E_K| : |E^K|)$ . Alors on a :

**Proposition 1** . - Soit  $Q_K = (|E_K| : |E_K| \oplus |E_\chi|)$  :

a) On a  $Q_K = 1$  ou  $2$  et  $Q_K = 2$  si et seulement s'il existe une "unité de Minkowski"  $\epsilon$  pour  $E_K$  (i. e. telle que toute unité de  $K$  s'écrive

$$\pm \epsilon^{\lambda+\mu\sigma+\nu\sigma^2}, \lambda, \mu, \nu \in \mathbb{Z}.$$

b) Soient  $\epsilon_0$  un générateur de  $E_K$  et  $\epsilon_\chi$  un générateur de  $E_\chi$ . Les conditions suivantes sont équivalentes :

(i)  $Q_K = 2$ ,

(ii) il existe  $u \in E_K$  telle que  $u^{1+\sigma^2} = \pm \epsilon_0$ ,

(iii) il existe  $v \in E_K$  telle que  $v^{1+\sigma} = \pm \epsilon_\chi$ ,

(iv) il existe  $w \in E_K$  telle que  $w^2 = \pm \epsilon_0 \epsilon_\chi^{1-\sigma}$  ;

lorsque ces conditions sont réalisées,  $w$  est une unité de Minkowski de  $E_K$  et on peut choisir  $u$  et  $v$  de telle sorte que  $u = v = w$ .

Cette propriété est démontrée par H. Hasse [5] et aussi par L. Bouvier et J. J. Payan [1]. Nous avons retrouvé directement ce résultat en déterminant toutes les structures possibles de  $G$ -modules  $\mathbb{Z}$ -libres de dimension 3 annihilés par la "norme"  $1 + \sigma + \sigma^2 + \sigma^3$  ; le résultat est le suivant :

**Proposition 2** . - Soit  $G = \langle \sigma \rangle$  un groupe cyclique d'ordre 4 ; soit  $M$  un  $\mathbb{Z}[G]$ -module  $\mathbb{Z}$ -libre de dimension 3 tel que pour tout  $u \in M$ ,

$$u^{1+\sigma+\sigma^2+\sigma^3} = 1. \text{ Soit } M^* = \{u \in M, u^{1+\sigma^2} = 1\} \text{ et soit } M^0 = \{u \in M, u^{\sigma^2} = u\}.$$

Alors en écartant le cas trivial où  $G$  opère sur  $M$  par  $u^\sigma = u^{-1}$  pour tout  $u$ , on a  $M^* \simeq \mathbb{Z}[G]/(1+\sigma^2) \simeq \mathbb{Z}[i]$  et  $M^2 \subset M^* \oplus M^0 \subset M$ ; soit  $Q_M = (M : M^* \oplus M^0)$ , alors nécessairement  $Q_M = 1$  ou  $2$  et :

- (i) si  $Q_M = 1$ , alors  $M \simeq (\sigma^2 - 1)\mathbb{Z}[G] \times \mathbb{Z}$ ,  $G$  opérant sur  $\mathbb{Z}$  par  $\sigma(1) = -1$  ;
- (ii) si  $Q_M = 2$ , alors  $M \simeq \mathbb{Z}[G]/(1 + \sigma + \sigma^2 + \sigma^3)$ .

Démonstration :

(i)  $M^* \simeq \mathbb{Z}[i]$  : On a  $M^* = \{u \in M, u^{1+\sigma^2} = 1\}$  ; donc  $M^*$  est un  $\mathbb{Z}[G]/(1 + \sigma^2)$ -module, donc un  $\mathbb{Z}[i]$ -module ; on vérifie que  $M^*$  est sans  $\mathbb{Z}[i]$ -torsion ; donc  $M^*$  est isomorphe à un idéal de  $\mathbb{Z}[i]$  ; comme  $M^*$  est de  $\mathbb{Z}$ -rang compris entre  $0$  et  $3$ , on a  $M^* = (1)$  ou  $M^* \simeq \mathbb{Z}[i]$ . Si  $M^* = (1)$ , comme  $M^{1+\sigma} \subset M^*$ , on a  $M^{1+\sigma} = (1)$  ; donc pour tout  $u \in M$ ,  $u^{1+\sigma} = 1$ , c'est-à-dire que  $u^\sigma = u^{-1}$  (alors  $M \simeq \mathbb{Z}^3$ ,  $G$  opérant sur  $\mathbb{Z}$  par  $\sigma(1) = -1$ ) ; cette situation n'est pas possible pour un groupe d'unités. On suppose donc  $M^* \simeq \mathbb{Z}[i]$  ; soit  $u_*$  un générateur de  $M^*$  ; une  $\mathbb{Z}$ -base de  $M^*$  est  $(u_*, u_*^\sigma)$ .

(ii) Etude de  $M^0$  et  $M^*M^0$  : Soit  $M^0 = \{u \in M, u^{\sigma^2} = u\}$  ; alors  $M^* \cap M^0 = (1)$  et  $M^*M^0 = M^* \oplus M^0$  ; comme  $2 = (1 - \sigma^2) + (1 + \sigma^2)$ , on a  $M^2 \subset M^* \oplus M^0 \subset M$ . Comme  $M$  et  $M^2$  sont deux  $\mathbb{Z}$ -modules libres de rang  $3$ , on a  $\dim_{\mathbb{Z}} M^* + \dim_{\mathbb{Z}} M^0 = 3$  ; donc  $\dim_{\mathbb{Z}} M^0 = 1$  ; soit  $u_o$  une  $\mathbb{Z}$ -base de  $M^0$  ; comme  $u_o^\sigma \in M^0$ , on a  $u_o^\sigma = u_o^\lambda$  qui conduit à  $u_o^{\sigma^2} = u_o^{\lambda^2} = u_o$ , et  $\lambda^2 = 1$ . L'opération  $u^\sigma = u$  est impossible sur  $u \neq 1$  car  $u^\sigma = u$  et  $u^{1+\sigma+\sigma^2+\sigma^3} = 1$  entraînent  $u^4 = 1$ , soit  $u = 1$ . On a donc  $\lambda = -1$ .

(iii) Etude de  $Q_M$  : Soit  $Q_M = (M : M^* \oplus M^0)$  ; comme  $M^2 \subset M^* \oplus M^0 \subset M$ , on a  $Q_M = 1, 2, 4$  ou  $8$ .

$\alpha$ ) Si  $Q_M = 1$ , on a  $M = M^* \oplus M^0$  ; alors  $M \simeq (\sigma^2 - 1)\mathbb{Z}[G] \times \mathbb{Z}$ ,  $G$  opérant sur  $\mathbb{Z}$  par  $\sigma(1) = -1$  ; on vérifie en effet que l'on définit un isomorphisme de  $G$ -modules grâce à l'application :

$$\begin{aligned} (\sigma^2 - 1)\mathbb{Z}[G] \times \mathbb{Z} &\longrightarrow M^* \oplus M^0 \\ ((\sigma^2 - 1)_w, n) &\longmapsto u_*^w u_o^n. \end{aligned}$$



β) Si  $Q_M = 2$ , soit  $u \in M$ ,  $u \notin M^* \oplus M^0$ . Il est impossible que  $u^{1+\sigma^2} = u_o^{2\lambda}$ ,  $\lambda \in \mathbb{Z}$ , sinon on aurait  $\frac{u}{u_o^\lambda} \in M^*$ , c'est-à-dire  $u \in M^* \oplus M^0$ , ce qui est absurde ; donc  $u^{1+\sigma^2} = u_o^{2\lambda+1}$ ,  $\lambda \in \mathbb{Z}$  et en modifiant  $u$  modulo  $M^0$ , on peut supposer que  $u^{1+\sigma^2} = u_o$ . Il est impossible que  $u^{1+\sigma} \in M_*^{1+\sigma}$ , sinon on pourrait écrire  $u^{1+\sigma} = v_*^{1+\sigma}$ ,  $v_* \in M^*$ , soit  $\left(\frac{u}{v_*}\right)^\sigma = \left(\frac{u}{v_*}\right)^{-1}$ , d'où en appliquant à nouveau  $\sigma$ ,  $\left(\frac{u}{v_*}\right)^{\sigma^2} = \left(\frac{u}{v_*}\right)$ , c'est-à-dire  $\frac{u}{v_*} \in M^0$ , ce qui est absurde. En modifiant  $u$  modulo  $M^*$  (ce qui ne change pas la relation  $u^{1+\sigma^2} = u_o$ ) on peut supposer que  $u^{1+\sigma} = u_*$ . Il existe donc  $u \in M$ ,  $u \notin M^* \oplus M^0$ , tel que  $u^{1+\sigma^2} = u_o$  et  $u^{1+\sigma} = u_*$ . Il existe donc  $u \in M$ ,  $u \notin M^* \oplus M^0$ , tel que  $u^{1+\sigma^2} = u_o$  et  $u^{1+\sigma} = u_*$ . Il en résulte que  $u$  est un générateur de  $M$  et que  $M \simeq \mathbb{Z}[G]/(1+\sigma+\sigma^2+\sigma^3)$ .

γ) Si  $Q_M = 4$ , on a  $(M^* \oplus M^0 : M^2) = 2$  ; on a donc deux classes dans  $M^* \oplus M^0 / M^2 : M^2$  et  $\alpha M^2$ ,  $\alpha \in M^* \oplus M^0$ . Soient  $u_*$  et  $u_o$  les générateurs de  $M_*$  et  $M_o$  ; alors  $u_* \in \alpha M^2$  et  $u_o \in \alpha M^2$  ; donc  $u_* u_o \in M^2$  et  $u_* u_o = v^2$ ,  $v \in M$  ; donc  $(u_* u_o)^{1-\sigma^2} = v^{2(1-\sigma^2)} = u_*^2$  ; donc  $u_* = v^{1-\sigma^2} = (v^{1+\sigma})^{1-\sigma}$  ; or  $w_* = v^{1+\sigma} \in M^*$  ; donc  $u_* = w_*^{1-\sigma}$ , ce qui est impossible.

δ) Si  $Q_M = 8$ , on a  $M^2 = M^* \oplus M^0$  ; soit  $u_*$  le générateur de  $M^*$  ; donc  $u_* = v^2$ ,  $v \in M$  ; mais  $v^{2(1+\sigma^2)} = 1$ , donc  $v^{1+\sigma^2} = 1$ , donc  $v \in M^*$ , ce qui est impossible.

Corollaire . - Les seules structures de  $\mathbb{Z}[G]$ -modules a priori possibles pour le groupe des unités d'un corps  $K$  cyclique réel de degré 4 sont les deux structures énoncées dans la proposition 1 et caractérisées par la valeur de  $Q_K$ .

b) Propriétés de  $Q_K$  .

Si  $Q_K = 1$ , toute unité  $w$  de  $E_K$  s'écrit  $w = \pm e_o^\lambda e_x^{\mu+\nu\sigma}$ ,  $\lambda, \mu, \nu \in \mathbb{Z}$  ; donc  $N_{K/\mathbb{Q}}(w) = +1$  .

Si  $Q_K = 2$ , il existe une unité  $\epsilon$  de  $E_K$  vérifiant  $\epsilon^2 = \pm \epsilon_o \epsilon_\chi^{1-\sigma}$ ; on a alors  $\epsilon^{1+\sigma} = \pm \epsilon_\chi$ ,  $\epsilon^{1+\sigma^2} = \pm \epsilon_o$  et  $\epsilon$  est un générateur de  $E_K$ . Toute unité  $w$  de  $E_K$  s'écrit  $w = \pm \epsilon^{\lambda+\mu\sigma+\nu\sigma^2}$ ,  $\lambda, \mu, \nu \in \mathbb{Z}$  et  $N_{K/Q}(w) = (N_{K/Q}(\epsilon))^{\lambda+\mu+\nu}$ ; on a aussi  $\epsilon^{1+\sigma+\sigma^2+\sigma^3} = \epsilon_\chi^{1+\sigma} = \epsilon_o^{1+\sigma}$ .

Soit  $\rho$  le rang de l'homomorphisme de  $E_K$  dans  $\{\pm 1\}^4$ :  
 $\epsilon \mapsto (\text{signe}(\epsilon), \text{signe}(\epsilon^\sigma), \text{signe}(\epsilon^{\sigma^2}), \text{signe}(\epsilon^{\sigma^3}))$ . On sait d'après [2] que  $\rho = 4$  si et seulement s'il existe une unité de  $E_K$  de norme absolue  $-1$ .  
 On a donc la proposition suivante (qui se trouve aussi dans [5]):

Proposition 3 . - Soit  $Q_K = (|E_K| : |E_K| \oplus |E_\chi|)$ .

- (i) S'il existe une unité  $u$  de  $E_K$  telle que  $N_{K/Q}(u) = -1$ , alors  $Q_K = 2$ ,  $N_{K/Q}(\epsilon_o) = N_{K/k}(\epsilon_\chi) = N_{K/Q}(\epsilon) = -1$  et  $\rho = 4$ .
- (ii) Si toute unité de  $E_K$  est de norme absolue  $+1$ , alors  $\rho \leq 3$  et :

ou bien  $Q_K = 1$ ,

ou bien  $Q_K = 2$  et  $N_{K/Q}(\epsilon_o) = N_{K/k}(\epsilon_\chi) = N_{K/Q}(\epsilon) = +1$ .

On établit simplement des conditions nécessaires pour que  $Q_K$  soit égal à 2 ; on a en effet la proposition suivante :

Proposition 4 . - Soit  $\epsilon_\chi = (t, z, x, y)$  l'unité  $\chi$ -relative génératrice de  $E_\chi$ ; soit  $\epsilon_o$  un générateur de  $E_K$  et soient  $s = N_{K/k}(\epsilon_\chi)$  et  $s_o = N_{K/Q}(\epsilon_o)$ . On a  $Q_K = 1$  lorsque l'une des conditions suivantes est vérifiée :

- (i)  $s \neq s_o$ ,
- (ii)  $t^2 \not\equiv 16s \pmod{f}$ ,
- (iii) il existe  $p \equiv 3 \pmod{4}$  qui divise  $f$  et,  $s$  ou  $s_o$  est égal à  $-1$ ,
- (iv)  $g = 4g'$ ,  $g'$  impair et,  $s$  ou  $s_o$  est égal à  $-1$ .

Démonstration :

- (i) Il résulte de la proposition 3.
- (ii) Supposons que  $Q_K = 2$ ; soient  $\epsilon = (T, Z, X, Y)$  et  $\epsilon_\chi = (t, z, x, y)$ ; de l'égalité  $\epsilon_\chi = \pm \epsilon^{1+\sigma}$ , on déduit que  $4z = \pm 2g[b(X^2 - Y^2) + 2aXY]$ ; or  $b$  est pair, donc  $b = 2b'$ ; alors

$z = \frac{t}{f} g[b'(X^2 - Y^2) + aXY]$  ; donc  $z \equiv 0 (g)$ . Or d'après le §1, (vi), on a  $t^2 + mz^2 = 16s + 2f(x^2 + y^2)$  ; donc si  $Q_K = 2$ , on a  $t^2 \equiv 16s \pmod{f}$  (on a alors  $r = \frac{t^2 - mz^2}{4} + 2s \equiv 6s \pmod{f}$ ).

(iii) et (iv) D'après [2], s'il existe  $p \equiv 3 (4)$  qui divise  $f$ , ou si 4 divise exactement  $f$ , alors  $N_{K/\mathbb{Q}}(u) = +1$  pour toute unité  $u$  de  $K$  ; en appliquant la proposition 3, on en déduit le résultat.

### 3) Nombre de classes et unités.

#### a) Rappel des résultats de H. W. Leopoldt [7].

Soit  $\eta_\chi$  l'unité cyclotomique  $\chi$ -relative génératrice ; on rappelle que  $\eta_\chi$  se détermine de la manière suivante : soit  $\mathfrak{u}$  un système de représentants modulo  $f$  correspondant à  $\text{Gal}(\mathbb{Q}_O^{(f)}/K)$  ; soit  $\xi = \exp\left(\frac{i\pi}{f}\right)$  et soit

$\Theta = \prod_{a \in \mathfrak{u}} (\xi^a - \xi^{-a})$ . D'après [7], l'extension  $K(\Theta)/\mathbb{Q}$  est abélienne et si  $\bar{\sigma}$  désigne un prolongement de  $\sigma$  à  $K(\Theta)$ , alors  $\eta = \Theta^{1-\bar{\sigma}}$  est une unité de  $K$  et  $\eta_\chi = \eta^{1+\sigma}$  est une unité  $\chi$ -relative de  $K$ . Soit  $F_\chi$  le sous-module de  $E_\chi$  engendré par  $\eta_\chi$  ; alors  $F_\chi$  est d'indice fini dans  $E_\chi$  et  $|F_\chi|$  est un sous- $\mathbb{Z}[i]$ -module libre de dimension 1 de  $|E_\chi|$  ; on a donc  $\eta_\chi = \frac{t}{f} \epsilon_\chi^{\mu+\nu\sigma}$  et  $(|E_\chi| : |F_\chi|) = \mu^2 + \nu^2$ .

D'après [7], le nombre de classes  $h$  de  $K$  est donné par la formule :  $h = \frac{Q_K}{2} h_\chi h_o$ , où  $h_\chi$  désigne l'indice de  $|F_\chi|$  dans  $|E_\chi|$ ,  $h_o$  le nombre de classes de  $k$  et  $Q_K$  l'indice de  $|E^K|$  dans  $|E_K|$ . Ces résultats sont aussi démontrés dans [5] sous une forme voisine.

#### b) Majoration de $h_\chi = (|E_\chi| : |F_\chi|)$ .

Proposition 5. - Soit  $E_\chi$  le groupe des unités  $\chi$ -relatives de  $K$  ; soit  $F_\chi$  le sous-module de  $E_\chi$  engendré par l'unité cyclotomique  $\eta_\chi$  ; soit  $h_\chi = (|E_\chi| : |F_\chi|)$  ; alors :

$$h_\chi \leq 4 \frac{(\text{Log } |\eta_\chi|)^2 + (\text{Log } |\eta_\chi^\sigma|)^2}{\left(\text{Log } \frac{f-6}{2}\right)^2}.$$

Lemme : Quelle que soit l'unité  $\chi$ -relative non triviale  $u_\chi$  de  $K$ , on a

$$\text{Max} \left( u_\chi^2, u_\chi^{2\sigma}, u_\chi^{2\sigma^2}, u_\chi^{2\sigma^3} \right) \geq \frac{f-6}{2}.$$

Démonstration : Soit  $\Phi$  le polynôme résolvante de Lagrange ; pour tout  $\alpha \in K^*$ , on a

$$\begin{aligned} \Phi(\alpha, \alpha^\sigma, \alpha^{\sigma^2}, \alpha^{\sigma^3}) &= (\alpha + i\alpha^\sigma - \alpha^{\sigma^2} - i\alpha^{\sigma^3}) (\alpha - i\alpha^\sigma - \alpha^{\sigma^2} + i\alpha^{\sigma^3}) \\ &= (\alpha - \alpha^{\sigma^2})^2 + (\alpha^\sigma - \alpha^{\sigma^3})^2. \end{aligned}$$

On sait que si  $\alpha$  est un entier de  $K$  n'appartenant pas à  $k$ , alors

$\Phi(\alpha, \alpha^\sigma, \alpha^{\sigma^2}, \alpha^{\sigma^3})$  est un entier rationnel non nul multiple de  $f$ .

Soit  $u_\chi$  une unité  $\chi$ -relative de  $K$  autre que  $\pm 1$  ; alors :

$$\begin{aligned} f \leq \left( u_\chi - u_\chi^{\sigma^2} \right)^2 + \left( u_\chi^\sigma - u_\chi^{\sigma^3} \right)^2 &= u_\chi^2 + u_\chi^{2\sigma} + u_\chi^{2\sigma^2} + u_\chi^{2\sigma^3} \pm 4 \\ &\leq 6 + 2 \text{Max} \left( u_\chi^2, u_\chi^{2\sigma}, u_\chi^{2\sigma^2}, u_\chi^{2\sigma^3} \right), \end{aligned}$$

puisque  $u_\chi^{1+\sigma^2} = \pm 1$  et que parmi les quatre éléments  $u_\chi^2, u_\chi^{2\sigma}, u_\chi^{2\sigma^2}$  et  $u_\chi^{2\sigma^3}$ , deux sont inférieurs à 1. Donc quelle que soit l'unité  $\chi$ -relative non triviale  $u_\chi$  de  $K$ , on a

$$\text{Max} \left( u_\chi^2, u_\chi^{2\sigma}, u_\chi^{2\sigma^2}, u_\chi^{2\sigma^3} \right) \geq \frac{f-6}{2}.$$

Le plus petit conducteur possible de  $K$  étant  $f = 15$ , on a toujours  $\frac{f-6}{2} > 1$ .

Nous allons donner deux démonstrations de la proposition 5, l'une étant l'application directe des résultats de [3], l'autre utilisant des arguments géométriques plus élémentaires.

Première démonstration : On applique le théorème II 1 de [3], p. 106.

On considère la fonction résolvante de Lagrange  $\Phi$  de degré  $d_\Phi = 2$  ; on obtient, d'après le lemme, que pour tout  $u_\chi \in E_\chi$ ,  $u_\chi \neq \pm 1$ ,

$$\text{Max} \left( u_\chi^2, u_\chi^{2\sigma}, u_\chi^{2\sigma^2}, u_\chi^{2\sigma^3} \right) \geq \frac{f-6}{2} > 1 ;$$

on a donc  $h_\chi \leq \frac{\pi_\chi(F_\chi)}{m_\chi} \left( \frac{1}{2d_\Phi} \text{Log} \frac{f-6}{2} \right)^{-2}$ , où  $\frac{\pi_\chi(F_\chi)}{m_\chi}$  est une constante

géométrique explicite :

D'après le corollaire II 1, p. 110, on a  $\eta_{\chi}(F_{\chi}) = R_{\chi}(F_{\chi})/2$ , où  $R_{\chi}(F_{\chi})$  désigne le  $\chi$ -régulateur de  $F_{\chi}$  :

$$\begin{aligned} R_{\chi}(F_{\chi}) &= \left( \text{Log}|\eta_{\chi}| - \text{Log}|\eta_{\chi}^{\sigma^2}| \right)^2 + \left( \text{Log}|\eta_{\chi}^{\sigma}| - \text{Log}|\eta_{\chi}^{\sigma^3}| \right)^2 \\ &= 4 \left( \left( \text{Log}|\eta_{\chi}| \right)^2 + \left( \text{Log}|\eta_{\chi}^{\sigma}| \right)^2 \right). \end{aligned}$$

D'après les définitions de la p. 103, on a

$$\mathfrak{D}_{\chi} = \{x = (x_1, x_2, x_3, x_4), |x_i| \leq 1, i = 2, 3, 4\},$$

$$\mathfrak{V}_{\chi} = \{x = (x_1, x_2, x_3, x_4), x_1 + x_3 = 0, x_2 + x_4 = 0\};$$

alors  $m_{\chi}$  est la mesure de  $\mathfrak{D}_{\chi} = \mathfrak{D}_{\chi} \cap \mathfrak{V}_{\chi}$ . On a donc

$$\begin{aligned} \mathfrak{D}_{\chi} &= \{x = (x_1, x_2, -x_1, -x_2), |x_1| \leq 1, |x_2| \leq 1\} \\ &= \{x_1(1, 0, -1, 0) + x_2(0, 1, 0, -1), |x_1| \leq 1, |x_2| \leq 1\}. \end{aligned}$$

Or les vecteurs  $(1, 0, -1, 0)$  et  $(0, 1, 0, -1)$  sont orthogonaux et de longueur  $\sqrt{2}$ ; donc  $m_{\chi} = (2\sqrt{2})^2 = 8$ .

$$\text{On a donc } h_{\chi} \leq \frac{4 \left( \left( \text{Log}|\eta_{\chi}| \right)^2 + \left( \text{Log}|\eta_{\chi}^{\sigma}| \right)^2 \right)}{2 \times 8} \left( \frac{1}{4} \text{Log} \frac{f-6}{2} \right)^{-2},$$

$$\text{c'est-à-dire } h_{\chi} \leq 4 \frac{\left( \text{Log}|\eta_{\chi}| \right)^2 + \left( \text{Log}|\eta_{\chi}^{\sigma}| \right)^2}{\left( \text{Log} \frac{f-6}{2} \right)^2}.$$

Deuxième démonstration : Soit  $\eta_{\chi}$  l'unité cyclotomique  $\chi$ -relative génératrice ; on cherche s'il existe  $\mu$  et  $\nu \in \mathbb{Z}$  et une unité  $\epsilon_{\chi} \in E_{\chi}$  tels que  $|\eta_{\chi}| = |\epsilon_{\chi}|^{\mu+\nu\sigma}$  ; si ceci a lieu, on a

$$|\epsilon_{\chi}| = |\eta_{\chi}|^{\frac{\mu-\nu\sigma}{2+\nu}}, \quad |\epsilon_{\chi}^{\sigma}| = |\eta_{\chi}|^{\frac{\mu\sigma+\nu}{2+\nu}}, \quad |\epsilon_{\chi}^{\sigma^2}| = |\epsilon_{\chi}^{-1}| \quad \text{et} \quad |\epsilon_{\chi}^{\sigma^3}| = |\epsilon_{\chi}^{-\sigma}|.$$

On doit avoir, d'après le lemme :

$$\text{Max} \left( |\eta_{\chi}|^{\frac{2\mu-\nu\sigma}{2+\nu}}, |\eta_{\chi}|^{\frac{2\nu+\mu\sigma}{2+\nu}}, |\eta_{\chi}|^{\frac{2-\mu+\nu\sigma}{2+\nu}}, |\eta_{\chi}|^{\frac{2-\nu-\mu\sigma}{2+\nu}} \right) \geq \frac{f-6}{2}.$$

Or pour tout  $u, \nu > 0$  et tout  $x, y \in \mathbb{Z}$ , l'inégalité

$$\frac{2x}{u^2+y^2} \frac{2y}{\nu^2+y^2} \geq \frac{f-6}{2} \text{ est équivalente à l'inégalité}$$

$$\frac{2x}{x^2+y^2} \operatorname{Log} u + \frac{2y}{x^2+y^2} \operatorname{Log} v \geq \operatorname{Log} \frac{f-6}{2}, \text{ c'est-à-dire}$$

$$x^2+y^2 - 2x \frac{\operatorname{Log} u}{\operatorname{Log} \frac{f-6}{2}} - 2y \frac{\operatorname{Log} v}{\operatorname{Log} \frac{f-6}{2}} \leq 0 \text{ puisque } \frac{f-6}{2} > 1.$$

Ceci est équivalent à ce que le point  $(x, y)$  soit intérieur au cercle d'équation  $X^2+Y^2 - 2 \frac{\operatorname{Log} u}{\operatorname{Log} \frac{f-6}{2}} X - 2 \frac{\operatorname{Log} v}{\operatorname{Log} \frac{f-6}{2}} Y = 0$ .

Soient  $\ell_0 = \frac{\operatorname{Log} |\eta_\chi|}{\operatorname{Log} \frac{f-6}{2}}$  et  $\ell_1 = \frac{\operatorname{Log} |\eta_\chi^\sigma|}{\operatorname{Log} \frac{f-6}{2}}$ . Le point de coordonnées  $(\mu, \nu)$

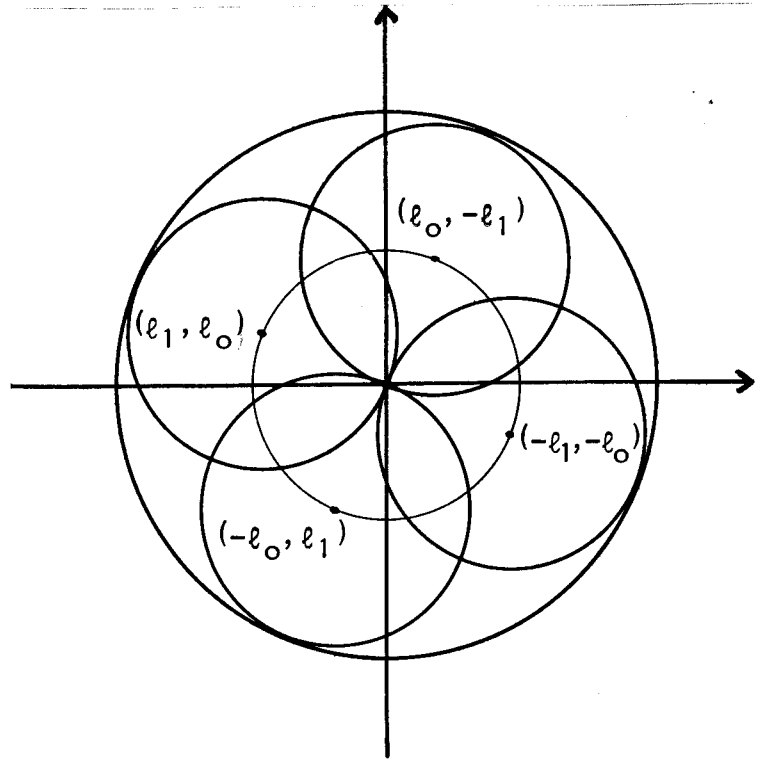
est donc intérieur à l'un au moins des quatre cercles :

$$X^2+Y^2 - 2\ell_0 X + 2\ell_1 Y = 0,$$

$$X^2+Y^2 - 2\ell_1 X - 2\ell_0 Y = 0,$$

$$X^2+Y^2 + 2\ell_0 X - 2\ell_1 Y = 0,$$

$$X^2+Y^2 + 2\ell_1 X + 2\ell_0 Y = 0,$$



On a donc  $\mu^2 + \nu^2 \leq 4(\ell_0^2 + \ell_1^2)$ ,

$$\text{soit } \mu^2 + \nu^2 \leq 4 \frac{(\operatorname{Log} |\eta_\chi|)^2 + (\operatorname{Log} |\eta_\chi^\sigma|)^2}{(\operatorname{Log} \frac{f-6}{2})^2}.$$

### c) Détermination de $h_\chi$ et $\epsilon_\chi$ .

On détermine  $\eta_\chi$  numériquement (voir paragraphe 4) ; on applique alors la méthode de dévissage des unités cyclotomiques décrite dans [3], IV, 1. Le principe a été décrit en détail dans [4]. Rappelons que :

(i) on effectue d'abord le dévissage en 2 (on sait d'après [5] que  $h_x$  est pair si et seulement si  $f$  est composé) ; soit  $2^d$  la plus grande puissance de 2 qui divise  $h_x$  et soit  $\varphi_x$  l'unité dévissée au maximum en 2, on a  $\eta_x = \varphi_x^\omega$ ,  $\omega \in \mathbb{Z}[i]$  de norme  $2^d$  ;

(ii) on teste ensuite la divisibilité de  $h_x$  pour les nombres impairs  $\ell$  ( $\ell = p$ ,  $p$  premier si  $p \equiv 1(4)$ ,  $\ell = q^2$ ,  $q$  premier si  $q \equiv 3(4)$ ) classés par ordre croissant et inférieurs à

$$\frac{4}{2^d} \frac{(\text{Log}|\eta_x|)^2 + (\text{Log}|\eta_x^\sigma|)^2}{\left(\text{Log}\frac{f-6}{2}\right)^2} .$$

On obtient ainsi la valeur de  $h_x$  et de l'unité

$x$ -relative génératrice  $\epsilon_x$ . On remarque que  $s = N_{K/k}(\epsilon_x) = N_{K/k}(\varphi_x)$ .

#### d) Calcul de $Q_K$ .

Le calcul de  $Q_K$  se fait de la manière suivante : soient  $\epsilon_0$  un générateur de  $E_k$  et  $\epsilon_x$  un générateur de  $E_x$  déterminé en c) (en réalité, l'unité  $\varphi_x$  suffit) ; soient  $s_0 = N_{k/Q}(\epsilon_0)$  et  $s = N_{K/k}(\epsilon_x)$ . D'après la proposition 4, (i),  $s \neq s_0$  entraîne  $Q_K = 1$  et lorsque  $s = s_0$ , on a  $Q_K = 2$  si et seulement s'il existe  $\epsilon \in E_K$  telle que  $\epsilon^2 = \pm \epsilon_0 \epsilon_x^{1-\sigma}$ . Deux méthodes sont alors possibles :

$$(i) \text{ Soient } w = \sqrt{|\epsilon_0 \epsilon_x^{1-\sigma}|}, \quad w_\sigma = \sqrt{|\epsilon_0^\sigma \epsilon_x^{\sigma-\sigma^2}|},$$

$$w_{\sigma^2} = \sqrt{|\epsilon_0 \epsilon_x^{\sigma^2-\sigma^3}|} \quad \text{et} \quad w_{\sigma^3} = \sqrt{|\epsilon_0^\sigma \epsilon_x^{\sigma^3-1}|} ;$$

il est facile de vérifier

(cf [3], lemme IV, 1) que  $w \in K$  si et seulement s'il existe des nombres  $\delta_\sigma, \delta_{\sigma^2}$  et  $\delta_{\sigma^3} \in \{-1, +1\}$  tels que le polynome

$$P = (X - w) (X - \delta_\sigma w_\sigma) (X - \delta_{\sigma^2} w_{\sigma^2}) (X - \delta_{\sigma^3} w_{\sigma^3})$$

soit à coefficients entiers

rationnels. On calcule en réel les quantités  $w, w_\sigma, w_{\sigma^2}$  et  $w_{\sigma^3}$  et on détermine les polynomes  $P$  pour les différentes valeurs de  $\delta_\sigma, \delta_{\sigma^2}$  et  $\delta_{\sigma^3}$  telles que  $\delta_\sigma \delta_{\sigma^2} \delta_{\sigma^3} = s$ . On a  $Q_K = 2$  si et seulement si l'un de ces polynomes est à coefficients entiers.

(ii) Soit  $\delta_o$  le signe de  $\epsilon_o \epsilon_\chi^{1-\sigma}$  ; alors  $\epsilon^2 = \delta_o \epsilon_o \epsilon_\chi^{1-\sigma}$ ,  
 $\epsilon^{1+\sigma^2} = \delta_o \epsilon_o$  et  $\epsilon^{1+\sigma} = \delta \epsilon_\chi$ ,  $\delta \in \{+1, -1\}$ . Soient  $t = \text{Tr}_{K/Q}(\epsilon_\chi)$  et  
 $t_o = \text{Tr}_{k/Q}(\epsilon_o)$ . On a alors :

$$\epsilon^{1+\sigma} + \epsilon^{\sigma+\sigma^2} + \epsilon^{\sigma^2+\sigma^3} + \epsilon^{\sigma^3+1} + \epsilon^{1+\sigma^2} + \epsilon^{\sigma+\sigma^3} = \delta t + \delta_o t_o ;$$

on en déduit que :

$$T_1 = \left( \epsilon + \epsilon^\sigma + \epsilon^{\sigma^2} + \epsilon^{\sigma^3} \right)^2 \\ = \delta_o \epsilon_o \left( \epsilon_\chi^{1-\sigma} + \epsilon_\chi^{\sigma^2-\sigma^3} + 2 \right) + \delta_o \epsilon_o^\sigma \left( \epsilon_\chi^{\sigma-\sigma^2} + \epsilon_\chi^{\sigma^3-1} + 2 \right) + 2\delta t \quad \text{et}$$

$$T_2 = \left( \epsilon^{-1} + \epsilon^{-\sigma} + \epsilon^{-\sigma^2} + \epsilon^{-\sigma^3} \right)^2 \\ = s \delta_o \epsilon_o \left( \epsilon_\chi^{\sigma-\sigma^2} + \epsilon_\chi^{\sigma^3-1} + 2 \right) + s \delta_o \epsilon_o^\sigma \left( \epsilon_\chi^{1-\sigma} + \epsilon_\chi^{\sigma^2-\sigma^3} + 2 \right) + 2s\delta t.$$

Soit  $\epsilon_\chi = (t, z, x, y)$  ; alors

$$\epsilon_\chi^{1-\sigma} + \epsilon_\chi^{\sigma^2-\sigma^3} + 2 = \frac{2(sr+2) + sg\sqrt{m} [b(x^2-y^2) + 2axy]}{4}$$

$$\text{où } r = \frac{t^2 - mz^2}{4} + 2s. \text{ Soit } \epsilon_o = \frac{t_o + z_o \sqrt{m}}{2} ; \text{ alors}$$

$$T_1 = \delta_o \frac{2(sr+2)t_o + sgmz_o [b(x^2-y^2) + 2axy]}{4} + 2\delta t \quad \text{et}$$

$$T_2 = s \delta_o \frac{2(sr+2)t_o - sgmz_o [b(x^2-y^2) + 2axy]}{4} + 2s\delta t.$$

On a donc  $Q_K = 2$  si et seulement s'il existe  $\delta \in \{-1, +1\}$  tel que

$T_1$  et  $T_2 \in \mathbb{Z}^2$ . On vérifie que  $T_1 T_2 = (sr+2 + s\delta\delta_o t t_o)^2$ . Si  
 $sr+2 + s\delta\delta_o t t_o = 0$ , alors  $T_1 = 0$  et  $T_2 = \pm tmz_o^2$ , ou le contraire ; si  
 $m \neq 8$ , la congruence  $t^2 \equiv 16s \pmod{m}$  entraîne que  $tm \notin \mathbb{Z}^2$  ; si  $m = 8$ ,  
on vérifie que  $v_2(t) = 2$  ; donc  $tm \notin \mathbb{Z}^2$ . Il suffit donc de vérifier que  
 $T_1$  ou  $T_2 \in \mathbb{Z}^2 - \{0\}$ .

e) Calcul du nombre de classes h de K.

On a  $h = \frac{Q_K}{2} h_\chi h_o$  :

- (i) la quantité  $h_\chi$  a été déterminée en c)
- (ii) la quantité  $h_o$  est supposée connue,
- (iii) la quantité  $Q_K$  a été déterminée en d).



#### 4) Présentation de la table.

La table numérique a été établie sur l'ordinateur IRIS 50 du Centre de Calcul de l'Université de Besançon. Les quantités réelles ont été calculées avec la double précision (environ 15 chiffres). Pour certains corps, nous avons dû utiliser l'ordinateur du CIRCE muni de la quadruple précision. Les principales étapes sont les suivantes :

Pour chaque entier  $f$  sans facteur carré impair et tel que  $v_2(f) = 0, 2, 3$  ou  $4$ , on détermine le groupe de Galois de  $\mathbb{Q}^{(f)}/\mathbb{Q}$ , ainsi que ses caractères d'ordre 4. Après avoir éliminé les corps imaginaires pour lesquels  $\chi(-1) = -1$ , on trouve  $N$  corps réels  $K$  de conducteur  $f$ . Pour chacun de ces corps  $K$  :

- (i) on détermine le conducteur  $m$  du sous-corps quadratique  $k$ ,
- (ii) on détermine un générateur  $\epsilon_0$  de  $E_k$ ,
- (iii) on détermine le groupe de Galois de  $\mathbb{Q}^{(f)}/K$  grâce au caractère  $\chi'$ ,
- (iv) on détermine  $\theta$  et  $\eta_\chi$  (formules des §1, (iii) et §3, a),
- (v) on détermine  $a$  et  $b$  (formules du §1, (iv)),
- (vi) on calcule la constante qui majore  $h_\chi$  (§3, b),
- (vii) on détermine l'unité  $\varphi_\chi$  dévissée en 2 (§3, c),
- (viii) on calcule  $Q_K$  (§3, d),
- (ix) on effectue le dévissage de l'unité  $\varphi_\chi$  pour les nombres impairs (§3, c).

Nous avons ainsi établi la table du nombre de classes et des unités des corps  $K$  cycliques réels de degré 4 de conducteur  $f$  inférieur à 4000 (III). Pour quelques corps, les entiers  $t$  et  $r$  sont trop grands et la précision des ordinateurs employés ne nous a pas permis de les donner.

#### 5) Corps cycliques réels de degré 4 admettant une unité $\chi$ -relative telle que $s = -1$ et $r = -6$ .

Il existe une famille de corps cycliques réels de degré 4 qui possèdent une unité  $\chi$ -relative  $(t, z, x, y)$  dont les coordonnées sont "petites" ; ces corps sont intéressants car ils peuvent fournir des exemples de grands nombres de classes. Ils constituent, pour le cas cyclique de degré 4, l'analogue des "simplest cubic fields" étudiés notamment par D. Shanks dans [8]. On a les propriétés suivantes :

Proposition 6 . - Soit  $t \in \mathbb{Z}$ ,  $t \neq 0$ ,  $t \neq 3$  ; alors le polynome  $P = X^4 - tX^3 - 6X^2 + tX + 1$  est irréductible sur  $\mathbb{Q}$  et définit une extension  $K$  cyclique réelle de degré 4 de  $\mathbb{Q}$ .

Démonstration : elle résulte essentiellement du fait que si l'on désigne par  $w$  une racine de  $P$  dans  $\mathbb{C}$ , les autres racines sont  $-\frac{1}{w}$ ,  $\frac{w-1}{w+1}$  et  $-\frac{w+1}{w-1}$ , un élément d'ordre 4 de  $\text{Gal}(K/\mathbb{Q})$  étant défini par  $w \mapsto \frac{w-1}{w+1}$ . On peut remarquer que si l'on change  $w$  en  $-w$ ,  $t$  est changé de signe ; on supposera donc  $t > 0$  (et  $t \neq 3$ ).

On voit donc que  $w$  est une unité  $\chi$ -relative de norme  $-1$  sur  $k$ .

Lemme : Soit  $K$  une extension cyclique réelle de degré 4 de  $\mathbb{Q}$  de conducteur  $f$  et de sous-corps quadratique  $k$  de conducteur  $m$  ( $f = mg$ ). Soit  $(t, z, x, y)$  une unité  $\chi$ -relative de  $K$  que l'on suppose de norme  $-1$  sur  $k$ . On a  $r = -6$  si et seulement si, de plus, l'une des conditions équivalentes suivantes est vérifiée :

- (i)  $t^2 + 16 = mz^2$ ,
- (ii)  $z^2 = g(x^2 + y^2)$ .

Démonstration : Puisque  $(t, z, x, y)$  est une unité  $\chi$ -relative de norme  $-1$ , on a d'après le §1, (vi) :  $t^2 + mz^2 = -16 + 2f(x^2 + y^2)$ ,  $tz = g[a(x^2 - y^2) - 2bxy]$  et alors  $r = \frac{t^2 - mz^2}{4} - 2$ . Le lemme en résulte immédiatement.

Remarque 1 . - Par construction, le corps  $K$  est entièrement déterminé par la donnée de  $t > 0$ ,  $t \neq 3$ . Pour déterminer  $m$ ,  $f$  et les coordonnées d'une racine  $w$  de  $P$ , on procède de la manière suivante :

(i) On a  $t^2 + 16 = mz^2$ , ce qui détermine  $m$  (avec la condition  $v_2(m) = 0$  ou  $3$ ) et  $z$ . Il existe un nombre fini de décompositions de  $m$  sous la forme  $m = a^2 + b^2$ .

(ii) Les entiers  $g$ ,  $x$  et  $y$  sont alors solutions du système d'équations :

$$\begin{aligned} z^2 &= g(x^2 + y^2), \\ tz &= g[a(x^2 - y^2) - 2bxy] ; \end{aligned}$$

on vérifie que ce système est équivalent à :

$$\begin{aligned} z(mz + at + 4b) &= 2mgx^2, \\ z(mz - at - 4b) &= 2mgy^2. \end{aligned}$$

Il existe donc des entiers a et b tels que  $m = a^2 + b^2$  et tels que ce système admette une solution g, x et y (on rappelle que l'on doit avoir  $(g, m) = 1$  si m est impair et  $(g, m) = 2$  sinon).

La solution trouvée est unique aux signes de t, z, x et y près.

Proposition 7 . - Soit  $t \geq 5$  et soit  $K = \mathbb{Q}(w)$ , où  $\text{Irr}(w, \mathbb{Q}) = X^4 - tX^3 - 6X^2 + tX + 1$ . Soit f le conducteur de K. Soit  $E_w$  le sous-module de  $E_x$  engendré par w ;

$$\text{alors } (E_x : E_w) \leq 4 \frac{(\text{Log}(t+1))^2 + \left(\text{Log} \frac{t-1}{t+1}\right)^2}{\left(\text{Log} \frac{f-6}{2}\right)^2}.$$

Démonstration : D'après le §3, b), on sait que

$$(E_x : E_w) \leq 4 \frac{(\text{Log} |w|)^2 + (\text{Log} |w^\sigma|)^2}{\left(\text{Log} \frac{f-6}{2}\right)^2}. \text{ Soit } P = X^4 - tX^3 - 6X^2 + tX + 1 ;$$

alors  $P(t) = -5t^2 + 1$  et  $P(t+1) = t^3 - 2t^2 - 8t - 4$  ; si  $t \geq 5$ , on a  $P(t) < 0$  et  $P(t+1) > 0$ . Il existe donc une racine w de P telle que  $t < w < t+1$  ;

comme  $w^\sigma = \frac{w-1}{w+1}$  est une fonction croissante de w, on en déduit que

$$\frac{t-1}{t+1} < w^\sigma < \frac{t}{t+2} ; \text{ donc } (\text{Log} |w|)^2 \leq (\text{Log}(t+1))^2 \text{ et } (\text{Log} |w^\sigma|)^2 \leq \left(\text{Log} \frac{t-1}{t+1}\right)^2, \text{ et la proposition en résulte.}$$

Corollaire 1 . - Avec les notations de la proposition 7, si  $t \leq \frac{f}{2} - 4$ , alors l'unité w est génératrice dans  $E_x$ .

En effet puisque  $s = -1$ , l'indice  $(E_x : E_w)$  est impair ; la plus petite valeur possible de  $(E_x : E_w)$  est donc égale à 5. Si  $t \leq 4$ , on vérifie directement que les unités sont génératrices. Si  $t \geq 5$ , montrons que  $(E_x : E_w) < 5$ .

$$\text{On a } \left(\text{Log} \frac{t-1}{t+1}\right)^2 \leq \left(\text{Log} \frac{2}{3}\right)^2 < \frac{1}{4} ; \text{ donc } 4 \frac{\left(\text{Log} \frac{t-1}{t+1}\right)^2}{\left(\text{Log} \frac{f-6}{2}\right)^2} < \frac{1}{\left(\text{Log} \frac{f-6}{2}\right)^2} < 1$$

puisque  $f > 15$  ; donc si  $t \leq \frac{f}{2} - 4$ , alors  $t+1 \leq \frac{f-6}{2}$  et

$$(E_x : E_w) < 4 \frac{(\text{Log}(t+1))^2}{\left(\text{Log} \frac{f-6}{2}\right)^2} + 1 < 5, \text{ c. q. f. d.}$$

Exemple où  $w$  n'est pas génératrice : Soit  $K = \mathbb{Q}(w)$ , où  $\text{Irr}(w, \mathbb{Q}) = X^4 - 22X^3 - 6X^2 + 22X + 1$  ; alors  $t^2 + 16 = 500 = 5 \cdot (10)^2$  ; on a  $m = 5$  ( $a = -1$ ,  $b = 2$ ) et  $z = 10$ . Les équations  $10gx^2 = 360$  et  $10gy^2 = 640$  admettent la solution  $g = 4$ ,  $x = 3$  et  $y = 4$  ; on a  $w = (22, 10, 3, 4)$ ,  $m = 5$  et  $f = 20$ . Mais  $\epsilon_{\chi} = (2, 2, 1, 0)$  ; donc  $w$  n'est pas génératrice (on a  $w = \epsilon_{\chi}^{2+\sigma}$ ), mais on remarque qu'alors  $\epsilon_{\chi}$  est de la forme précédente (elle correspond à  $t = 2$ ). Nous conjecturons que cette propriété est toujours vraie.

Corollaire 2 . - Avec les notations de la proposition 7, soit  $w = (t, z, x, y)$  et  $\lambda = x^2 + y^2$  ; l'unité  $w$  est génératrice si  $t \geq \lambda + \sqrt{\lambda^2 + 8\lambda - 16}$ .

En effet, puisque  $f = \frac{t^2 + 16}{\lambda}$ , l'inégalité  $t \leq \frac{f}{2} - 4$  est équivalente à  $t^2 - 2\lambda t + 16 - 8\lambda \geq 0$ , d'où le résultat.

On obtient quatre familles infinies de tels corps de la manière suivante :

Proposition 8 . - Les corps cycliques réels de degré 4, de conducteur  $f$  et de sous-corps quadratique  $k$  de conducteur  $m$  admettent pour générateur  $\epsilon_{\chi}$  de  $E_{\chi}$  une unité telle que  $s = -1$  et  $r = -6$  dans chacun des 4 cas suivants :

- (i)  $m = a^2 + 16$ ,  $a$  impair et  $f = m$ ,
- (ii)  $m = a^2 + 4$ ,  $a$  impair et  $f = 4m$ ,
- (iii)  $m = 4 + b^2$ ,  $b$  pair,  $b/2$  impair et  $f = 2m$ ,
- (iv)  $m = 1 + b^2$ ,  $b$  pair et  $f = 8m$ .

Démonstration : on vérifie que les éléments ci-dessous sont des unités  $\chi$ -relatives qui vérifient  $s = -1$  et  $r = -6$  :

dans le cas (i) :  $\epsilon_{\chi} = (a, 1, 1, 0)$ ,

dans le cas (ii) :  $\epsilon_{\chi} = (2a, 2, 1, 0)$ ,

dans le cas (iii) :  $\epsilon_{\chi} = (2b, 2, 1, 1)$ ,

dans le cas (iv) :  $\epsilon_{\chi} = (4b, 4, 1, 1)$ .

Ces unités sont génératrices ; en effet, dans les cas (i) et (ii), on a  $\lambda = x^2 + y^2 = 1$  ; dans les cas (iii) et (iv), on a  $\lambda = x^2 + y^2 = 2$  ; en appliquant le corollaire 2 de la proposition 7, on voit que ces unités sont génératrices.

Remarque 2 . - On vérifie que les nombres premiers impairs qui divisent  $m$  sont congrus à 1 modulo 4 et que les conditions de parité sur  $a$  et  $b$  entraî-

nent que  $v_2(m) = 0$  ou  $3$ . Il en résulte que pour tout  $a$  ou  $b$  tel que  $m$  soit sans facteur carré impair, il existe un tel corps. Il existe une infinité de corps de chacune des formes (i) à (iv) ; en effet, pour tout nombre  $p$ ,  $p \equiv 1 \pmod{4}$  et tout  $\mu \not\equiv 0 \pmod{p}$ , l'équation  $c^2 + \mu^2 \equiv 0 \pmod{p^2}$  admet deux solutions  $\pm c_0 \pmod{p^2}$ . Soit  $N$  un entier donné ; parmi les  $N$  premiers entiers d'une des formes (i) à (iv), il y en a un nombre inférieur ou égal à  $\frac{2N}{p} + 2$  qui sont divisibles par  $p^2$  ; le nombre de ces entiers, sans facteurs carrés, est

$$\begin{aligned}
 &> N \left( 1 - \frac{2}{N} \sum_{\substack{p \text{ premier} \\ p \leq 4N}} \frac{1}{p} - 2 \sum_{\substack{p \text{ premier} \\ p \equiv 1 \pmod{4}}} \frac{1}{p^2} \right); \text{ or } 2 \sum_{\substack{p \text{ premier} \\ p \equiv 1 \pmod{4}}} \frac{1}{p^2} \leq 2 \sum_{n=1}^{\infty} \frac{1}{(4n+1)^2} \\
 &\leq \sum_{n=1}^{\infty} \left( \frac{1}{(4n+1)^2} + \frac{1}{(4n-1)^2} \right) = \frac{\pi^2}{6} - \frac{\pi^2}{24} - 1 < 0,25, \text{ et } \frac{1}{N} \sum_{\substack{p \text{ premier} \\ p \leq 4N}} \frac{1}{p} \rightarrow 0
 \end{aligned}$$

lorsque  $N \rightarrow +\infty$ . Il en résulte que chacune des familles (i) à (iv) est infinie.

Remarque 3 .- Si on applique la majoration de la proposition 7, en posant  $w = (t, z, x, y)$  et  $\lambda = x^2 + y^2$ , on obtient

$$\left( E_x : E_w \right) \leq 4 \frac{(\text{Log}(t+1))^2 + 1/4}{(\text{Log}(t^2+16-6\lambda) - \text{Log}(2\lambda))^2}. \text{ Or } \lambda = 1 \text{ ou } 2; \text{ il en résulte}$$

que pour ces quatre familles infinies,  $(E_x : E_w) \rightarrow 1^+$  lorsque  $t \rightarrow +\infty$ . La majoration obtenue au §3, b est donc, en un sens, la "meilleure possible" (les constantes géométriques de la proposition 5 du §3, b ne peuvent pas être améliorées pour l'ensemble des corps cycliques réels de degré 4).

L'unité  $\chi$ -relative des corps  $K$  dont les conducteurs  $f$  et  $m$  sont de l'une des formes énoncées dans la proposition 8 est connue ; le nombre de classes de ces corps se calcule simplement. Nous en donnons la table lorsque  $4000 \leq f \leq 10000$ . Les résultats correspondants à  $f \leq 4000$  se trouvent dans la table (III).

cas (i) :	f	m	t	$Q_K$	$h_x$	$h_o$	h
	4241	4241	65	2	9	1	9
	4505	4505	67	1	20	4	40
	4777	4777	69	1	16	4	32
	5057	5057	71	1	20	2	20
	5345	5345	73	1	20	2	20
	5641	5641	75	2	9	1	9
	5945	5945	77	1	40	4	80
	6257	6257	79	2	29	1	29
	6577	6577	81	2	17	1	17
	6905	6905	83	1	36	2	36
	7241	7241	85	1	26	2	26
	7585	7585	87	1	16	8	64
	7937	7937	89	2	41	1	41
	8297	8297	91	2	45	1	45
	8665	8665	93	1	26	2	26
	9041	9041	95	2	17	1	17
	9817	9817	99	2	17	1	17

cas (ii) :	f	m	t	$Q_K$	$h_x$	$h_o$	h
	4372	1093	66	1	26	5	65
	4916	1229	70	1	50	3	75
	5492	1373	74	1	58	3	87
	6740	1685	82	1	68	2	68
	7412	1853	86	1	68	2	68
	8116	2029	90	1	50	7	175
	8852	2213	94	1	50	3	75
	9620	2405	98	1	200	4	400

cas (iii) :	f	m	t	$Q_K$	$h_\chi$	$h_o$	h
	4240	2120	92	1	68	4	136
	5008	2504	100	1	40	4	80
	5840	2920	108	1	20	12	120
	6736	3368	116	1	50	6	150
	7696	3848	124	1	100	4	200
	8720	4360	132	1	52	12	312
	9808	4904	140	1	106	10	530

cas (iv) :	f	m	t	$Q_K$	$h_\chi$	$h_o$	h
	4616	577	96	1	32	7	112
	5416	677	104	1	50	1	25
	6280	785	112	1	80	6	240
	7208	901	120	1	32	4	64
	9256	1157	136	1	68	2	68

## II - CLASSES DE K QUI DEVIENNENT PRINCIPALES DANS K.

Soient  $k$  un corps de nombres,  $K$  une extension cyclique totalement réelle de degré premier de  $k$ . Soit  $j$  l'homomorphisme "extension des classes" du groupe des classes de  $k$  dans le groupe des classes de  $K$ . On sait, d'après le théorème 94 de Hilbert, que si l'extension  $K/k$  est non ramifiée pour toute valuation, alors  $\ker j$  est non trivial ([6]), mais sans l'hypothèse de non ramification, la nature de  $\ker j$  est mal connue. Dans notre cas, nous avons montré dans [4] que  $\ker j$  est d'ordre 1 ou 2 et que la connaissance de l'unité  $\chi$ -relative génératrice  $\epsilon_\chi$  de  $E_\chi$  (ou plus simplement de l'unité  $\phi_\chi$  dévissée au maximum en 2) permet de le déterminer. Nous avons démontré dans [4] le théorème et la proposition dont les énoncés sont les suivants :

Théorème . - Soit  $K$  une extension cyclique réelle de degré 4 de  $\mathbb{Q}$ , de sous-corps quadratique  $k$ . Soit  $\epsilon_\chi$  l'unité  $\chi$ -relative génératrice de  $E_\chi$  et soit  $Q_K = (|E_K| : |E_k| \oplus |E_\chi|)$ . Soit  $s = N_{K/k}(\epsilon_\chi)$  et soit  $\text{Irr}(\epsilon_\chi, \mathbb{Q}) = X^4 - tX^3 + rX^2 - sX + 1$  ; pour tout nombre premier  $p$ , on pose

$c = v_p(t)$  et  $e = v_p(sr + 2)$ . On a les propriétés suivantes :

a) Il existe au plus une classe non triviale de  $k$  devenant principale dans  $K$  et lorsqu'une telle classe existe, on a  $(1 + \epsilon_x^{1-\sigma})A_K = \mathfrak{a} A_K$ , où  $\mathfrak{a}$ , idéal non principal de  $A_K$ , représente la classe en question.

b) Si  $Q_K = 2$ , alors aucune classe non triviale de  $k$  ne devient principale dans  $K$ .

c) Si  $Q_K = 1$ , une condition nécessaire et suffisante pour qu'une classe non triviale de  $k$  devienne principale dans  $K$  est que tout nombre premier  $p$  ramifié dans  $K/k$  vérifie l'une des trois conditions suivantes :

- (i)  $p$  est ramifié dans  $k/\mathbb{Q}$ ,
- (ii)  $p$  est inerte dans  $k/\mathbb{Q}$  et  $c$  est pair,
- (iii)  $p$  est décomposé dans  $k/\mathbb{Q}$  et  $\min(c, e)$  est pair.

Proposition 9 . - Soit  $p$  (ramifié dans  $K/k$ ) et inerte dans  $k/\mathbb{Q}$  ; la condition  $c \equiv 0 \pmod{2}$  est vérifiée si :

- (i)  $p \equiv 1 \pmod{4}$  (on a même plus précisément  $c = 0$ ),
- ou (ii)  $s = +1$  (si  $p$  est impair, alors  $c = 0$ ).

Nous démontrons, en complément de ce que nous avons dit dans [4], les propriétés suivantes :

Proposition 10 . - Soit  $p$  ramifié dans  $K/k$  :

- (i) si  $s = -1$  et si  $p \equiv 3 \pmod{4}$ , alors  $p$  est inerte dans  $k/\mathbb{Q}$  et  $c$  est impair.
- (ii) si  $s = -1$  et si  $g = 4g'$ ,  $g'$  impair, alors 2 est inerte et  $c = 1$ .

Démonstration : D'après les relations I, §1, (vi), si  $\epsilon_x = (t, z, x, y)$

et  $\epsilon_x^{1+\sigma} = s$ , on a

$$t^2 + mz^2 = 16s + 2f(x^2 + y^2) \quad \text{et} \quad tz = g[a(x^2 - y^2) - 2bxy] ;$$

$$\text{alors } r + 2s = \frac{t^2 - mz^2}{4} + 4s = \frac{t^2 - f(x^2 + y^2)}{2} .$$

(i) On suppose que  $s = -1$  et que  $g = pg'$ ,  $p \equiv 3 \pmod{4}$  ; alors :

- 1)  $p$  est inerte dans  $k$  : si  $p$  était décomposé, il existerait  $\rho$



rationnel tel que  $\epsilon_{\chi} \equiv \rho \pmod{\mathfrak{P}}$ ,  $\mathfrak{P} | p$  dans  $K$ ; alors  $\epsilon_{\chi}^{1+\sigma^2} \equiv \rho^2 \equiv -1 \pmod{p}$ , ce qui est impossible, puisque  $p \equiv 3 \pmod{4}$ .

2) On a  $t \equiv 0 \pmod{p}$ : puisque  $p$  est inerte, il existe  $\gamma$  entier de  $k$  tel que  $\epsilon_{\chi} \equiv \gamma \pmod{\mathfrak{P}}$  et  $\gamma^{\sigma} \equiv \gamma^p \pmod{p}$ ; mais  $\gamma^2 \equiv -1 \pmod{p}$  et  $p \equiv 3 \pmod{4}$ , donc  $\gamma^p \equiv -\gamma \pmod{p}$  et  $t = 2(\gamma + \gamma^p) \equiv 0 \pmod{p}$ .

3) On pose  $t = p^c t'$ ,  $c > 0$ , alors  $c$  est impair: soit  $p^{\ell}$  la plus grande puissance de  $p$  qui divise  $x$  et  $y$ ; on pose  $x = p^{\ell} x'$  et  $y = p^{\ell} y'$ ; alors  $x'^2 + y'^2 \not\equiv 0 \pmod{p}$  puisque  $p \equiv 3 \pmod{4}$ . En reportant dans  $tz = g[a(x^2 - y^2) - 2bxy]$ , on obtient  $p^c t' z = p g' p^{2\ell} [a(x'^2 - y'^2) - 2bx'y']$ . L'égalité  $t^2 + mz^2 = 16s + 2f(x^2 + y^2)$  entraîne  $z \not\equiv 0 \pmod{p}$ . Soit  $p^{\lambda}$  la plus grande puissance de  $p$  qui divise  $a(x'^2 - y'^2) - 2bx'y'$ ; on a donc  $c = 2\ell + 1 + \lambda$ . L'hypothèse  $p$  inerte dans  $k/\mathbb{Q}$  entraîne  $\lambda = 0$ . En effet, on a l'identité  $m(x'^2 + y'^2)^2 = [a(x'^2 - y'^2) - 2bx'y']^2 + [b(x'^2 - y'^2) + 2ax'y']^2$ ; on sait que  $x'^2 + y'^2 \not\equiv 0 \pmod{p}$ ; si on avait  $a(x'^2 - y'^2) - 2bx'y' \equiv 0 \pmod{p}$ , alors  $m$  serait congru à un carré modulo  $p$ , et  $p$  serait décomposé dans  $k$ . On a donc  $c = 2\ell + 1$  et  $c$  est impair.

4) On peut remarquer que si  $s = +1$  et  $p$  ( $p \equiv 3 \pmod{4}$ ) est décomposé dans  $k/\mathbb{Q}$ , deux cas sont possibles:

ou bien  $t \not\equiv 0 \pmod{p}$  et alors  $c = 0$ ,

ou bien  $t \equiv 0 \pmod{p}$ ; alors  $c = 2\ell + 1 + \lambda$  et

$2(r + 2s) = p^{2\ell+1} [p^{2\ell+1+2\lambda} - (x'^2 + y'^2)mg']$  et  $e = 2\ell + 1$ ; donc  $\min(c, e)$  est impair.

(ii) On suppose que  $s = -1$  et que  $g = 4g'$ ,  $g'$  impair; alors:

1) 2 est inerte dans  $k/\mathbb{Q}$ : montrons que si  $g = 4g'$  et que si 2 est décomposé dans  $k/\mathbb{Q}$ , alors  $-1$  n'est pas norme dans  $K/k$ :

Soit  $\mathfrak{p}_2$  au-dessus de 2 dans  $k$ . Pour tout  $(\alpha, \beta) \in k^* \times k^*$ , on introduit le symbole de Hilbert  $(\alpha, \beta)_{\mathfrak{p}_2}$  et on rappelle que:

$$a) (\alpha\alpha', \beta)_{\mathfrak{p}_2} = (\alpha, \beta)_{\mathfrak{p}_2} (\alpha', \beta)_{\mathfrak{p}_2},$$

$$b) (\alpha, \beta\beta')_{\mathfrak{p}_2} = (\alpha, \beta)_{\mathfrak{p}_2} (\alpha, \beta')_{\mathfrak{p}_2},$$

c) pour que  $(\alpha, \beta)_{\mathfrak{p}_2} = 1$  il faut et il suffit que  $\beta$  soit une

normale locale en  $\mathfrak{p}_2$  dans l'extension  $k(\sqrt{\alpha})/k$ ,

$$d) (\alpha, \beta)_{\mathfrak{p}_2} (\beta, \alpha)_{\mathfrak{p}_2} = 1.$$

Soit  $\psi' = \frac{\psi^2}{4} = g' \sqrt{m} \frac{\sqrt{m+a}}{2} = g' \left[ \left( \frac{\sqrt{m+a}}{2} \right)^2 + \left( \frac{b}{2} \right)^2 \right]$ . Puisque 2 est décomposé dans  $k/\mathbb{Q}$ , on a  $m \equiv 1 \pmod{8}$ ; mais comme  $K$  est réel et que  $f = 4mg'$ , on obtient en appliquant I, §1, (ii) que  $g' \equiv 3 \pmod{4}$ ; donc d'après a), on a  $(-1, \psi')_{\mathfrak{p}_2} = (-1, g')_{\mathfrak{p}_2} = -1$ ; en vertu de d), on a donc  $(\psi', -1)_{\mathfrak{p}_2} = -1$ ; puisque  $K = k(\sqrt{\psi'})$ ,  $-1$  n'est pas norme dans  $K/k$ .

2) Montrons que  $c = 1$ : soit  $\epsilon_{\chi} = (t, z, x, y)$ ; on a  $\epsilon_{\chi}^{1+\sigma^2} = -1$ ; on a donc

$$t^2 + mz^2 = -16 + 8mg'(x^2 + y^2)$$

$$\text{et } tz = 4g'[a(x^2 - y^2) - 2bxy].$$

Les faits que  $\epsilon_{\chi}$  soit un entier et que  $tz \equiv 0 \pmod{4}$  entraînent que  $t$  et  $z$  sont pairs et que  $t/2$  et  $z/2$  sont de même parité. Il suffit donc de montrer qu'il est impossible que l'on ait  $t \equiv 0 \pmod{4}$  et  $z \equiv 0 \pmod{4}$ .

Supposons donc que  $t = 4t'$  et  $z = 4z'$ ; on a alors

$$t'^2 + m z'^2 = -1 + mg' \frac{x^2 + y^2}{2}$$

$$\text{et } t'z' = g' \left[ a \frac{x^2 - y^2}{4} - b'xy \right], \text{ en posant } b = 2b'.$$

Il en résulte que  $x$  et  $y$  sont de même parité.

a) si  $x$  et  $y$  sont pairs, on pose  $x = 2x'$  et  $y = 2y'$ ;

alors on a

$$t'^2 + m z'^2 = -1 + 2mg'(x'^2 + y'^2)$$

$$\text{et } t'z' = g[a(x'^2 - y'^2) - 4b'x'y'].$$

(i) si  $x'$  et  $y'$  sont de parités différentes, alors  $t'^2 + m z'^2$  et  $t'z'$  sont impairs, ce qui est impossible;

(ii) si  $x'$  et  $y'$  sont de même parité,  $t'^2 + m z'^2 \equiv -1 \pmod{4}$ , ce qui est impossible.

b) si  $x$  et  $y$  sont impairs, alors  $\frac{x^2 - y^2}{2} \equiv 1 \pmod{4}$  et  $\frac{x^2 - y^2}{2} \equiv 0 \pmod{2}$ . Mais 2 est inerte dans  $k/\mathbb{Q}$ , ce qui entraîne  $m \equiv 5 \pmod{8}$  et  $b'$  impair; comme  $K$  est réel, il en résulte que  $g' \equiv 1 \pmod{4}$ ; on obtient donc  $t'^2 + z'^2 \equiv 0 \pmod{4}$  et  $t'z' \equiv b' \equiv 1 \pmod{2}$ , ce qui est impossible.

Soit  $\mathfrak{p}$  un nombre premier ramifié dans  $K/k$  et décomposé ou inerte dans  $k/\mathbb{Q}$ ; on rappelle que  $c = v_{\mathfrak{p}}(t)$  et  $e = v_{\mathfrak{p}}(sr + 2)$ . Les résultats démontrés dans les propositions 9 et 10 se résument dans le tableau suivant :

$p = 2$ $g = 4g'$	$s$	résultat ou commentaire sur $\min(c, e)$
déc.	+1	les 2 cas se rencontrent
inerte	+1	$c$ pair
déc.	-1	situation impossible
inerte	-1	$c = 1$

$p = 2$ $g = 8g'$	$s$	résultat ou commentaire sur $\min(c, e)$
déc.	+1	les 2 cas se rencontrent
inerte	+1	$c$ pair
déc.	-1	les 2 cas se rencontrent
inerte	-1	les 2 cas se rencontrent

$p \equiv 3 (4)$	$s$	résultat ou commentaire sur $\min(c, e)$
déc.	+1	les 2 cas se rencon- trent et $\min(c, e)$ est pair si et ssi $c = e = 0$
inerte	+1	$c = 0$
déc.	-1	situation impossible
inerte	-1	$c$ impair

$p \equiv 1 (4)$	$s$	résultat ou commentaire sur $\min(c, e)$
déc.	+1	pas d'exemples de $\min(c, e)$ pair
inerte	+1	$c = 0$
déc.	-1	les 2 cas se rencon- trent ; pas d'exemples de $\min(c, e)$ pair autre que $c = e = 0$
inerte	-1	$c = 0$

### III - TABLE NUMERIQUE.

La table suivante donne pour chaque extension  $K$  cyclique réelle de degré 4 de  $\mathbb{Q}$  et de conducteur inférieur à 4000 :

- 1) le conducteur  $f$  de  $K$ ,
- 2) la décomposition en facteurs premiers de  $f$ , notée déc. prim. ,
- 3) le conducteur  $m$  du sous-corps quadratique  $k$  de  $K$ ,
- 4) les entiers  $a$  et  $b$  ( $a, b > 0, b$  pair) tels que  $m = a^2 + b^2$ ,
- 5) la norme  $s_0$  dans  $k/\mathbb{Q}$  du générateur  $\epsilon_0$  de  $E_k$ ,
- 6) la norme  $s$  dans  $K/k$  du générateur  $\epsilon_x$  de  $E_x$ ,
- 7)  $t = \epsilon_x + \epsilon_x^\sigma + \epsilon_x^{\sigma^2} + \epsilon_x^{\sigma^3}$  (le signe de  $\epsilon_x$  est choisi de manière à ce que  $t$  soit positif),
- 8)  $r = \epsilon_x \epsilon_x^\sigma + \epsilon_x \epsilon_x^{\sigma^2} + \epsilon_x \epsilon_x^{\sigma^3} + \epsilon_x^\sigma \epsilon_x^{\sigma^2} + \epsilon_x^\sigma \epsilon_x^{\sigma^3} + \epsilon_x^{\sigma^2} \epsilon_x^{\sigma^3}$ ,
- 9) l'indice  $Q_K = (|E_K| : |E_x| \oplus |E_k|)$  (égal à 1 ou 2),
- 10) l'indice  $h_x = (|E_x| : |F_x|)$ ,
- 11) le nombre de classes  $h_0$  de  $k$  (ce dernier est suivi du symbole \* lorsqu'une classe non triviale de  $k$  devient principale dans  $K$ ),
- 12) le nombre de classes  $h$  de  $K$  (on a  $h = \frac{Q_K}{2} h_0 h_x$ ).

f	déc.	prim.	m	a	b	s <sub>o</sub>	s	t	r	Q <sub>K</sub>	h <sub>x</sub>	h <sub>o</sub>	h
15		3.5	5	1	2	-1	-1	3	-1	1	2	1	1
16		16	8	2	2	-1	-1	4	-6	2	1	1	1
17		17	17	1	4	-1	-1	1	-6	2	1	1	1
20		4.5	5	1	2	-1	-1	2	-6	1	2	1	1
35		5.7	5	1	2	-1	-1	7	9	1	2	1	1
39		3.13	13	3	2	-1	+1	9	19	1	2	1	1
40		8.5	5	1	2	-1	-1	8	-6	1	2	1	1
41		41	41	5	4	-1	-1	5	-6	2	1	1	1
48		16.3	8	2	2	-1	-1	12	26	1	2	1	1
52		4.13	13	3	2	-1	-1	6	-6	1	2	1	1
55		5.11	5	1	2	-1	+1	11	31	1	2	1	1
65		5.13	65	7	4	-1	-1	7	-6	1	2	2*	2
65		5.13	65	1	8	-1	-1	72	254	1	2	2*	2
73		73	73	3	8	-1	-1	184	-2050	2	1	1	1
80		16.5	40	6	2	-1	-1	12	-326	1	2	2*	2
80		16.5	40	2	6	-1	-1	12	-6	1	2	2*	2
80		16.5	8	2	2	-1	-1	28	-6	2	2	1	2
85		5.17	17	1	4	-1	-1	152	-1026	2	2	1	2
87		3.29	29	5	2	-1	-1	39	23	1	2	1	1
89		89	89	5	8	-1	-1	136	-30978	2	1	1	1
91		7.13	13	3	2	-1	-1	7	-19	1	2	1	1
95		5.19	5	1	2	-1	+1	19	-59	1	2	1	1
97		97	97	9	4	-1	-1	9	-6	2	1	1	1
104		8.13	13	3	2	-1	-1	72	826	1	2	1	1
111		3.37	37	1	6	-1	+1	33	-179	1	2	1	1
112		16.7	8	2	2	-1	+1	28	166	1	2	1	1
113		113	113	7	8	-1	-1	8528	101694	2	1	1	1
115		5.23	5	1	2	-1	-1	23	-21	1	2	1	1
116		4.29	29	5	2	-1	-1	10	-6	1	2	1	1
120		8.3.5	5	1	2	-1	-1	12	-46	1	4	1	2

f	déc.	prim.	m	a	b	s <sub>0</sub>	s	t	r	Q <sub>K</sub>	h <sub>X</sub>	h <sub>0</sub>	h
136	8.17	17	1	4	-1	-1	16	-6	1	4	1	2	
137	137	137	11	4	-1	-1	11	-6	2	1	1	1	
143	11.13	13	3	2	-1	-1	33	-2099	1	2	1	1	
145	5.29	145	9	8	-1	+1	236	4646	1	2	4*	4	
145	5.29	145	1	12	-1	+1	54	151	1	2	4*	4	
148	4.37	37	1	6	-1	-1	246	-1190	1	2	1	1	
155	5.31	5	1	2	-1	+1	31	91	1	2	1	1	
159	3.53	53	7	2	-1	-1	39	365	1	2	1	1	
176	16.11	8	2	2	-1	-1	44	90	1	2	1	1	
183	3.61	61	5	6	-1	+1	57	-1763	1	2	1	1	
185	5.37	185	13	4	-1	-1	13	-6	1	2	2*	2	
185	5.37	185	11	8	-1	-1	5008	6654	1	2	2*	2	
193	193	193	7	12	-1	-1	903	12346	2	1	1	1	
195	3.5.13	13	3	2	-1	+1	9	-59	1	4	1	2	
195	3.5.13	5	1	2	-1	-1	33	59	1	4	1	2	
203	7.29	29	5	2	-1	+1	112	3022	1	2	1	1	
204	4.3.17	17	1	4	-1	+1	38	210	1	4	1	2	
205	5.41	41	5	4	-1	-1	200	9342	1	4	1	2	
208	16.13	104	10	2	-1	-1	396	1658	1	2	2*	2	
208	16.13	104	2	10	-1	-1	20	-6	1	2	2*	2	
208	16.13	8	2	2	-1	-1	124	2490	2	2	1	2	
212	4.53	53	7	2	-1	-1	14	-6	1	10	1	5	
215	5.43	5	1	2	-1	-1	172	174	1	2	1	1	
221	13.17	17	1	4	-1	+1	208	-13730	1	4	1	2	
232	8.29	29	5	2	-1	-1	184	2778	1	2	1	1	
233	233	233	13	8	-1	-1	203752	-5852034	2	1	1	1	
235	5.47	5	1	2	-1	-1	47	519	1	2	1	1	
240	16.3.5	40	6	2	-1	+1	36	166	1	4	2	4	
240	16.3.5	40	2	6	-1	+1	36	-314	1	4	2	4	
240	16.3.5	8	2	2	-1	-1	12	-166	1	4	1	2	

f	déc. prim.	m	a	b	s <sub>0</sub>	s	t	r	Q <sub>K</sub>	h <sub>x</sub>	h <sub>0</sub>	h
241	241	241	15	4	-1	-1	15	-6	2	1	1	1
244	4. 61	61	5	6	-1	-1	654	-16598	1	2	1	1
247	13. 19	13	3	2	-1	-1	19	59	1	2	1	1
255	3.5. 17	85	9	2	-1	+1	21	-419	1	4	2	4
255	3.5. 17	85	7	6	-1	+1	21	91	1	4	2	4
255	3.5. 17	5	1	2	-1	-1	33	-91	1	4	1	2
257	257	257	1	16	-1	-1	382352	1054120446	2	1	3	3
259	7. 37	37	1	6	-1	+1	329	20319	1	2	1	1
260	4.5. 13	13	3	2	-1	-1	318	-1046	1	4	1	2
260	4.5. 13	5	1	2	-1	-1	58	-6	1	4	1	2
265	5. 53	265	11	12	-1	-1	198	259	1	2	2*	2
265	5. 53	265	3	16	-1	-1	3512	-7426	1	2	2*	2
272	16. 17	136	10	6	+1	+1	132	-538	2	2	2	4
272	16. 17	136	6	10	+1	+1	1220	-24474	2	2	2	4
272	16. 17	8	2	2	-1	+1	68	-410	1	4	1	2
280	8.5. 7	5	1	2	-1	-1	28	114	1	4	1	2
281	281	281	5	16	-1	-1	86760	-241666	2	1	1	1
295	5.59	5	1	2	-1	+1	59	-179	1	2	1	1
296	8. 37	37	1	6	-1	-1	24	-6	1	2	1	1
299	13. 23	13	3	2	-1	+1	4117	-8535	1	2	1	1
303	3. 101	101	1	10	-1	-1	141	701	1	2	1	1
304	16. 19	8	2	2	-1	-1	532	20826	1	2	1	1
305	5. 61	305	17	4	+1	-1	17	-6	1	4	2*	4
305	5. 61	305	7	16	+1	-1	688	-193986	1	4	2*	4
312	8. 3. 13	13	3	2	-1	+1	108	-410	1	4	1	2
313	313	313	13	12	-1	-1	726	-273881	2	1	1	1
319	11. 29	29	5	2	-1	-1	77	255	1	2	1	1
327	3. 109	109	3	10	-1	+1	105	2731	1	2	1	1
328	8. 41	41	5	4	-1	-1	36	-2302	2	4	1	4
335	5. 67	5	1	2	-1	-1	67	69	1	2	1	1

f	déc.	prim.	m	a	b	s <sub>0</sub>	s	t	r	Q <sub>K</sub>	h <sub>x</sub>	h <sub>0</sub>	h
336	16.3.7	8	2	2	-1	+1	28		-954	1	4	1	2
337	337	337	9	16	-1	-1	16768		69515006	2	1	1	1
340	4.5.17	85	9	2	-1	-1	18		-6	1	4	2	4
340	4.5.17	85	7	6	-1	-1	1038		-6806	1	4	2	4
340	4.5.17	5	1	2	-1	-1	18		-1366	1	4	1	2
353	353	353	17	8	-1	-1	2047232		104113539006	2	1	1	1
355	5.71	5	1	2	-1	+1	71		211	1	2	1	1
357	3.7.17	17	1	4	-1	-1	1344		267710	1	4	1	2
365	5.73	73	3	8	-1	-1	768		-371	2	2	1	2
368	16.23	8	2	2	-1	+1	92		550	1	2	1	1
371	7.53	53	7	2	-1	+1	49		-471	1	2	1	1
377	13.29	377	19	4	+1	-1	19		-6	1	4	2*	4
377	13.29	377	11	16	+1	-1	5752		13566	1	4	2*	4
395	5.79	5	1	2	-1	+1	79		-9719	1	2	1	1
401	401	401	1	20	-1	-1	80		-8427	2	1	5	5
403	13.31	13	3	2	-1	-1	124		-370	1	2	1	1
404	4.101	101	1	10	-1	-1	646		-33942	1	2	1	1
407	11.37	37	1	6	-1	+1	33		-475	1	2	1	1
408	8.3.17	17	1	4	-1	+1	64		414	1	4	1	2
409	409	409	3	20	-1	-1	246		8583	2	1	1	1
415	5.83	5	1	2	-1	-1	913		7389	1	2	1	1
420	4.3.5.7	5	1	2	-1	-1	42		-166	1	8	1	4
424	8.53	53	7	2	-1	-1	728		-6	1	2	1	1
427	7.61	61	5	6	-1	-1	105		-677	1	10	1	5
433	433	433	17	12	-1	-1	10242		21211	2	1	1	1
435	3.5.29	29	5	2	-1	+1	25		93	1	8	1	4
435	3.5.29	5	1	2	-1	+1	29		201	1	8	1	4
436	4.109	109	3	10	-1	-1	522		-6	1	2	1	1
440	8.5.11	5	1	2	-1	+1	44		-794	1	4	1	2
445	5.89	89	5	8	-1	-1	47		-6	2	4	1	4



f	déc.	prim.	m	a	b	s <sub>0</sub>	s	t	r	Q <sub>K</sub>	h <sub>x</sub>	h <sub>0</sub>	h
447	3.149	149	7	10	-1	-1	27	-1645	1	2	1	1	
449	449	449	7	20	-1	-1	13289	581898	2	1	1	1	
455	5.7.13	13	3	2	-1	-1	903	-7481	1	4	1	2	
455	5.7.13	5	1	2	-1	-1	7	-201	1	4	1	2	
457	457	457	21	4	-1	-1	21	-6	2	5	1	5	
464	16.29	232	14	6	-1	-1	396	27834	1	2	2*	2	
464	16.29	232	6	14	-1	-1	77556	5783290	1	2	2*	2	
464	16.29	8	2	2	-1	-1	164	-6	2	2	1	2	
471	3.157	157	11	6	-1	+1	153	-779	1	2	1	1	
476	4.7.17	17	1	4	-1	+1	38	-470	1	4	1	2	
481	13.37	481	15	16	-1	-1	13344	63486	1	2	2*	2	
481	13.37	481	9	20	-1	-1	124	-487	1	2	2*	2	
485	5.97	97	9	4	-1	-1	7154808	-873377731586	2	2	1	2	
488	8.61	61	5	6	-1	-1	200	7802	1	2	1	1	
492	4.3.41	41	5	4	-1	+1	898	6402	1	4	1	2	
493	17.29	17	1	4	-1	-1	2365192	-451940994	2	2	1	2	
496	16.31	8	2	2	-1	+1	2108	-20090	1	2	1	1	
505	5.101	505	21	8	+1	+1	39596	100272806	2	2	4	8	
505	5.101	505	19	12	+1	+1	711	5056	2	2	4	8	
515	5.103	5	1	2	-1	-1	103	-1131	1	2	1	1	
519	3.173	173	13	2	-1	-1	147	-1909	1	2	1	1	
520	8.5.13	65	7	4	-1	+1	56	526	1	8	2	8	
520	8.5.13	65	1	8	-1	-1	32	-6	1	8	2	8	
520	8.5.13	13	3	2	-1	-1	72	-6	1	4	1	2	
520	8.5.13	5	1	2	-1	-1	72	-2086	1	4	1	2	
521	521	521	11	20	-1	-1	940	-104727	2	1	1	1	
528	16.3.11	8	2	2	-1	-1	924	6074	1	4	1	2	
533	13.41	41	5	4	-1	-1	2776976	-68932000962	2	2	1	2	
535	5.107	5	1	2	-1	-1	107	-21291	1	2	1	1	
543	3.181	181	9	10	-1	+1	720	7246	1	2	1	1	

f	déc.	prim.	m	a	b	s <sub>0</sub>	s	t	r	Q <sub>K</sub>	h <sub>x</sub>	h <sub>0</sub>	h
545	5. 109	545	23	4	+1	-1	-1	23	-6	1	4	2*	4
545	5. 109	545	17	16	+1	-1	-1	89248	-1079106	1	4	2*	4
551	19. 29	29	5	2	-1	-1	-1	19	-93	1	10	1	5
555	3. 5. 37	37	1	6	-1	+1	+1	144	1486	1	4	1	2
555	3. 5. 37	5	1	2	-1	-1	-1	87	179	1	4	1	2
559	13. 43	13	3	2	-1	+1	+1	43	-475	1	2	1	1
560	16. 5. 7	40	6	2	-1	-1	-1	8988	-24806	1	4	2	4
560	16. 5. 7	40	2	6	-1	-1	-1	28	-166	1	4	2	4
560	16. 5. 7	8	2	2	-1	+1	+1	196	-3194	1	4	1	2
561	3. 11. 17	17	1	4	-1	-1	-1	33	266	1	4	1	2
565	5. 113	113	7	8	-1	-1	-1	53	-6	2	2	1	2
569	569	569	13	20	-1	-1	-1	794	11943	2	1	1	1
577	577	577	1	24	-1	-1	-1	123975327936	1811572719932719870	2	1	7	7
580	4. 5. 29	29	5	2	-1	-1	-1	10	-1398	1	8	1	4
580	4. 5. 29	5	1	2	-1	-1	-1	58	234	1	8	1	4
583	11. 53	53	7	2	-1	+1	+1	1859	-94811	1	2	1	1
584	8. 73	73	3	8	-1	+1	+1	2624	-194466	1	4	1	2
591	3. 197	197	1	14	-1	-1	-1	141	2555	1	2	1	1
592	16. 37	296	14	10	-1	-1	-1	2196	-44998	1	2	2*	2
592	16. 37	296	10	14	-1	-1	-1	98100	-44998	1	2	2*	2
592	16. 37	8	2	2	-1	-1	-1	124	-7110	2	2	1	2
593	593	593	23	8	-1	-1	-1	12350873232	916333584446	2	1	1	1
595	5. 7. 17	85	9	2	-1	+1	+1	21	-79	1	4	2	4
595	5. 7. 17	85	7	6	-1	+1	+1	3591	8251	1	4	2	4
595	5. 7. 17	5	1	2	-1	-1	-1	203	1269	1	4	1	2
596	4. 149	149	7	10	-1	-1	-1	130050	88202	1	2	1	1
601	601	601	5	24	-1	-1	-1	2319607080	62904850679592574	2	1	1	1
611	13. 47	13	3	2	-1	-1	-1	40749	-2594351	1	2	1	1
615	3. 5. 41	205	13	6	+1	+1	+1	496	-4914	2	4	2	8
615	3. 5. 41	205	3	14	+1	+1	+1	119	-609	2	4	2	8

f	déc. prim.	m	a	b	s <sub>0</sub>	s	t	r	Q <sub>K</sub>	h <sub>x</sub>	h <sub>o</sub>	h
615	3.5.41	5	1	2	-1	-1	87	-211	1	8	1	4
617	617	617	19	16	-1	-1	5172152	-118264365954	2	1	1	1
624	16.3.13	104	10	2	-1	-1	228	410	1	4	2	4
624	16.3.13	104	2	10	-1	-1	228	-52006	1	4	2	4
624	16.3.13	8	2	2	-1	-1	84	410	1	4	1	2
628	4.157	157	11	6	-1	-1	13614	13258330	1	2	1	1
629	17.37	17	1	4	-1	-1	1208	-7554	2	10	1	10
635	5.127	5	1	2	-1	-1	1397	205869	1	2	1	1
641	641	641	25	4	-1	-1	25	-6	2	5	1	5
655	5.131	5	1	2	-1	+1	2096	257806	1	2	1	1
656	16.41	328	18	2	-1	+1	324	5254	1	8	4*	16
656	16.41	328	2	18	-1	-1	36	-6	1	8	4*	16
656	16.41	8	2	2	-1	-1	292	7866	2	4	1	4
660	4.3.5.11	5	1	2	-1	+1	44	306	1	8	1	4
663	3.13.17	221	11	10	+1	-1	33	215	1	8	2	8
663	3.13.17	221	5	14	+1	-1	84	878	1	8	2	8
663	3.13.17	13	3	2	-1	+1	17	-189	1	8	1	4
667	23.29	29	5	2	-1	+1	1127	30427	1	2	1	1
671	11.61	61	5	6	-1	-1	44	-1714	1	2	1	1
673	673	673	23	12	-1	-1	182151	-3768806	2	1	1	1
680	8.5.17	85	9	2	-1	-1	10728	-19046	1	4	2	4
680	8.5.17	85	7	6	-1	-1	152	2714	1	4	2	4
680	8.5.17	17	1	4	-1	+1	64	-674	1	8	1	4
680	8.5.17	5	1	2	-1	-1	152	-6	1	4	1	2
685	5.137	137	11	4	-1	-1	87989472	4078448894	2	2	1	2
687	3.229	229	15	2	-1	+1	51063	1289047	1	2	3	3
688	16.43	8	2	2	-1	-1	1204	-35430	1	2	1	1
689	13.53	689	25	8	+1	+1	186988	7708884774	2	2	4	8
689	13.53	689	17	20	+1	+1	958	6207	2	2	4	8
692	4.173	173	13	2	-1	-1	26	-6	1	10	1	5

f	déc.	prim.	m	a	b	s <sub>o</sub>	s	t	r	Q <sub>K</sub>	h <sub>x</sub>	h <sub>o</sub>	h
695	5.139	5.139	5	1	2	-1	+1	8479	-67139	1	2	1	1
696	8.3.29	8.3.29	29	5	2	-1	-1	996	2546	1	4	1	2
697	17.41	17.41	697	21	16	-1	-1	1008728	6670705406	2	2	6	12
697	17.41	17.41	697	11	24	-1	-1	4262578248	9591637246	2	2	6	12
697	17.41	17.41	41	5	4	-1	-1	866	-2097	2	2	1	2
697	17.41	17.41	17	1	4	-1	-1	169	-6	2	2	1	2
703	19.37	19.37	37	1	6	-1	-1	1197	-145797581	1	2	1	1
707	7.101	7.101	101	1	10	-1	-1	1071	-2329	1	2	1	1
712	8.89	8.89	89	5	8	-1	+1	352	-12098	1	4	1	2
715	5.11.13	5.11.13	13	3	2	-1	-1	33	189	1	4	1	2
715	5.11.13	5.11.13	5	1	2	-1	+1	121	-1619	1	4	1	2
724	4.181	4.181	181	9	10	-1	-1	9126	-973062	1	2	1	1
728	8.7.13	8.7.13	13	3	2	-1	-1	84	-110	1	20	1	10
740	4.5.37	4.5.37	37	1	6	-1	-1	198	8874	1	4	1	2
740	4.5.37	4.5.37	5	1	2	-1	-1	198	2954	1	4	1	2
745	5.149	5.149	745	27	4	+1	-1	27	-6	1	4	2*	4
745	5.149	5.149	745	13	24	+1	-1	13567432	12792427774	1	4	2*	4
748	4.11.17	4.11.17	17	1	4	-1	+1	106	754	1	4	1	2
752	16.47	16.47	8	2	2	-1	+1	75388	-247034	1	2	1	1
755	5.151	5.151	5	1	2	-1	+1	1661	57831	1	2	1	1
760	8.5.19	8.5.19	5	1	2	-1	+1	76	1366	1	4	1	2
761	761	761	761	19	20	-1	-1	4410	-8377	2	1	3	3
763	7.109	7.109	109	3	10	-1	+1	105	551	1	2	1	1
767	13.59	13.59	13	3	2	-1	-1	7611	-139847285	1	2	1	1
769	769	769	769	25	12	-1	-1	31008	-4241810	2	1	1	1
776	8.97	8.97	97	9	4	-1	-1	10176	2976730	1	4	1	2
780	4.3.5.13	4.3.5.13	65	7	4	-1	+1	74	786	1	8	2	8
780	4.3.5.13	4.3.5.13	65	1	8	-1	+1	334	-774	1	8	2	8
785	5.157	5.157	785	23	16	-1	-1	1552528	-35925666306	1	2	6*	6
785	5.157	5.157	785	1	28	-1	-1	583	-18846	1	2	6*	6

f	déc.	prim.	m	a	b	s <sub>0</sub>	s	t	r	Q <sub>k</sub>	h <sub>x</sub>	h <sub>0</sub>	h
788	4.197	197	1	14	-1	-1	84654		-1576006	1	2	1	1
793	13.61	793	27	8	+1	+1	531436		58694694	2	2	4	8
793	13.61	793	3	28	+1	+1	126		799	2	2	4	8
795	3.5.53	53	7	2	-1	-1	597		49019	1	4	1	2
795	3.5.53	5	1	2	-1	-1	597		1319	1	4	1	2
807	3.269	269	13	10	-1	-1	597		-2965	1	2	1	1
808	8.101	101	1	10	-1	-1	40		-6	1	10	1	5
809	809	809	5	28	-1	-1	1964		-26703	2	1	1	1
815	5.163	5	1	2	-1	-1	7987		7989	1	2	1	1
816	16.3.17	136	10	6	+1	+1	412		-1626	2	4	2	8
816	16.3.17	136	6	10	+1	+1	412		-549978	2	4	2	8
816	16.3.17	8	2	2	-1	-1	84		-550	1	8	1	4
820	4.5.41	205	13	6	+1	+1	3604		-7374	2	4	2	8
820	4.5.41	205	3	14	+1	+1	324		-13934	2	4	2	8
820	4.5.41	5	1	2	-1	-1	164		-494	1	8	1	4
831	3.277	277	9	14	-1	+1	1104		117454	1	2	1	1
835	5.167	5	1	2	-1	-1	1503		299099	1	2	1	1
840	8.3.5.7	5	1	2	-1	-1	168		-166	1	8	1	4
848	16.53	424	18	10	-1	-1	34860		-1814726	1	2	2*	2
848	16.53	424	10	18	-1	-1	756		-10182	1	2	2*	2
848	16.53	8	2	2	-1	-1	14084		-50886	2	2	1	2
851	23.37	37	1	6	-1	-1	161		5729	1	2	1	1
857	857	857	29	4	-1	-1	29		-6	2	5	1	5
861	3.7.41	41	5	4	-1	-1	26040		13937534	1	4	1	2
865	5.173	865	17	24	-1	-1	26225902848		1231211742575614	1	2	2*	2
865	5.173	865	9	28	-1	-1	147		-6	1	2	2*	2
871	13.67	13	3	2	-1	-1	201		4089	1	2	1	1
872	8.109	109	3	10	-1	-1	147672		-2765990	1	2	1	1
876	4.3.73	73	3	8	-1	+1	142		-870	1	8	1	4
879	3.293	293	17	2	-1	-1	1431		7319	1	2	1	1

f	déc.	prim.	m	a	b	s <sub>0</sub>	s	t	r	Q <sub>K</sub>	h <sub>K</sub>	h <sub>0</sub>	h
880	16.5.11	40	6	2	-1	-1	572	794	1	4	2	4	
880	16.5.11	40	2	6	-1	-1	1188	-4575206	1	4	2	4	
880	16.5.11	8	2	2	-1	-1	4268	-6246	1	4	1	2	
881	881	881	25	16	-1	-1	12780000	-4335869698	2	1	1	1	
884	4.13.17	221	11	10	+1	+1	412	-878	2	4	2	8	
884	4.13.17	221	5	14	+1	+1	412	-64526	2	4	2	8	
884	4.13.17	13	3	2	-1	-1	306	-38486	1	8	1	4	
888	8.3.37	37	1	6	-1	+1	588	85846	1	4	1	2	
895	5.179	5	1	2	-1	+1	179	-22019	1	2	1	1	
899	29.31	29	5	2	-1	-1	1953	187769	1	2	1	1	
901	17.53	17	1	4	-1	-1	4008616	1546110	2	4	1	4	
904	8.113	113	7	8	-1	+1	448	-4514	1	8	1	4	
905	5.181	905	29	8	+1	+1	1225004	9412006	2	2	4	8	
905	5.181	905	11	28	+1	+1	539	45256	2	2	4	8	
912	16.3.19	8	2	2	-1	-1	228	-454	1	4	1	2	
915	3.5.61	61	5	6	-1	+1	65	-177	1	8	1	4	
915	3.5.61	5	1	2	-1	+1	61	-429	1	8	1	4	
916	4.229	229	15	2	-1	-1	30	-6	1	10	3	15	
920	8.5.23	5	1	2	-1	-1	2668	-44526	1	4	1	2	
923	13.71	13	3	2	-1	-1	1415811	-361688411	1	2	1	1	
929	929	929	23	20	-1	-1	15426	-10255237	2	1	1	1	
935	5.11.17	85	9	2	-1	-1	33	79	1	20	2	20	
935	5.11.17	85	7	6	-1	-1	33	-7401	1	4	2	4	
935	5.11.17	5	1	2	-1	+1	319	-3819	1	4	1	2	
937	937	937	19	24	-1	-1	135508908763696536	77894251248871873020670	2	1	1	1	
944	16.59	8	2	2	-1	-1	236	474	1	10	1	5	
949	13.73	73	3	8	-1	-1	111	-6	2	2	1	2	
951	3.317	317	11	14	-1	-1	1407	311	1	2	1	1	
952	8.7.17	17	1	4	-1	+1	2104	-96146	1	4	1	2	
953	953	953	13	28	-1	-1	2044	-260175	2	1	1	1	

