MÉMOIRES DE LA S. M. F.

PIERRE KAPLAN

Cycles d'ordre au moins 16 dans le 2-groupe des classes d'idéaux de certains corps quadratiques

Mémoires de la S. M. F., tome 49-50 (1977), p. 113-124

<http://www.numdam.org/item?id=MSMF_1977__49-50__113_0>

Calculateurs en Math. (1975 - LIMOGES)
Bull. Soc. math France
Mémoire 49-50, 1977, p. 113-124

CYCLES D'ORDRE AU MOINS 16 DANS LE 2-GROUPE DES CLASSES D'IDEAUX DE CERTAINS CORPS QUADRATIQUES

par Pierre KAPLAN

Introduction -

Soit (C_2^*) le 2-groupe des classes d'idéaux au sens étroit du corps quadratique $\mathbb{Q}(\sqrt{D})$ où D désigne un entier rationnel quadrat-frei. Soit R_n le 2^n-rang du groupe (C_2^*). Dans le travail précédent [3] (cf. aussi [2]), nous avons étudié le groupe (C_2^*) en le remplaçant par le groupe isomorphe (C_2), 2-groupe des classes de formes quadratiques binaires proprement primitives de déterminant D. Nous renvoyons à [3] pour les notations, rappels, conventions et résultats.

Les résultats les plus intéressants de [3] concernent le cas où $R_2 = 1$. Nous avons pu obtenir dans de nombreux cas des critères pour que $R_3 = 1$, et, simultanément, si $D > 0$ et $R_3 = 0$, déterminer les facteurs principaux, c'est-à-dire les diviseurs du discriminant du corps $\mathbb{Q}(\sqrt{D})$ représentés par la forme $X^2 - D Y^2$.

Dans ce travail, nous obtenons d'une part des critères pour que $R_4 = 1$ (et si $D > 0$ et $R_4 = 0$, nous déterminons les facteurs principaux) et d'autre part un algorithme très simple pour déterminer (C_2) quand $R_3 = 1$. L'algorithme s'applique aux cas où (C_2) est cyclique ($R_1 = R_2 = R_3 = 1$), et à ceux où $R_1 = 2$, $R_1 = R_2 = R_3 = 1$ quand D n'est pas somme de deux carrés. Parmi ces cas, ceux où on obtient des critères sont ceux où l'on connaît par une formule explicite au moins deux racines quatrièmes de la classe unité si $D > 0$, au moins une si $D < 0$.

Nous nous intéresserons surtout aux corps réels ($D > 0$), car la théorie et les résultats numériques obtenus sont plus intéressants dans ce cas.

Notations -

On désigne par p, π, ... des nombres premiers congrus à 1 modulo 4, par q... des nombres premiers congrus à -1 modulo 4.

Une forme quadratique binaire $A X^2 + 2 B X Y + C Y^2$ sera notée $[A, B, C]$, son déterminant $B^2 - A C$ noté D. Nous ne considérons que des formes " proprement primitives ", où le P.G.C.D. (A, 2 B, C) = 1. Deux formes f et f' sont équivalentes (notées : $f \sim f'$) si l'on passe de l'une à l'autre par une substitution linéaire de déterminant + 1. Les classes d'équivalence des formes de même déterminant D, positives si $D < 0$, forment un groupe (C) pour la " composition ", une forme composée de $[A, B, A' C]$ et $[A', B, A C]$ étant $[A A', B, C]$. Le groupe (C^*) des classes d'idéaux au sens étroit de $\mathbb{Q}(\sqrt{D})$ est isomorphe à (C) ou au quotient de (C) par un sous-groupe à 3 éléments, donc leurs 2-composantes (C_2^*) et (C_2) sont isomorphes.

On dit que l'entier m est représenté par la forme $g = [A, B, C]$ si il existe des entiers x et y tels que $m = A x^2 + 2 B x y + C y^2$ et cette représentation est dite propre si x et y sont premiers entre eux.

Nous noterons $h(D)$ le nombre de classes de formes proprement primitives de déterminant D, $h^*(D)$ le nombre des classes d'idéaux de $Q(\sqrt{D})$.

§ 1.- LA METHODE

Dans ce paragraphe, on suppose que le nombre D soit tel que le groupe (C_2) vérifie $R_1 \geq R_2 = 1$, c'est-à-dire tel que la méthode B de [3], § 1 s'applique : Il y a exactement une classe ambiguë A_o autre que la classe unité I dans le genre principal et il existe un diviseur propre V du nombre Δ tel que les genres des classes ambiguës soient ceux qui vérifient $e_v = 1$.

Alors $R_n = 1$ si, et seulement si, A_o est puissance 2^{n-1} d'une classe, c'est-à-dire si, et seulement si, il existe une suite de classes

$$A_o = H_1 , H_2 , \ldots, H_{n-1}$$

qui soient dans le genre principal et telles que $H_k = H_{k+1}^2$ $(k = 1 \ldots n-2)$.

Considérons une telle suite. Si $n > 2$, les racines carrées de A_o sont les classes $H_2 A$, celles qui sont dans le genre principal sont H_2 et $H_2 A_o$. Si $n > 3$, les racines quatrièmes de A_o sont les classes $H_3 A$ et $H_3 H_2 A$ et celles du genre principal sont H_3, $H_3 A_o$, $H_3 H_2$ et $H_3 H_2 A_o$ ...

On voit ainsi que les classes K telles que $K^2 = A_o$ sont les classes $A H_{n-1} \prod_{i=2}^{n-2} H_i^{\alpha_i}$, et que, parmi celles-ci, celles qui sont dans le genre principal sont $H_{n-1} \prod_{i=1}^{n-2} H_i^{\alpha_i}$, où les α_i sont 0 ou 1.

Ceci montre en particulier que, si $R_n = 1$, toute classe K d'ordre 2^{n-1} ou un diviseur peut, par composition avec une classe ambiguë, venir dans le genre principal, donc vérifie $e_v(K) = 1$.

La classe H_{n-1} étant dans le genre principal, soit H'_n une de ses racines carrées. Les racines 2^nèmes de A_o sont les classes $H'_n A \prod_{i=1}^{n-2} H_{i+1}^{\alpha_i}$, et, comme toutes les classes H_i sont dans le genre principal, on voit que $R_{n+1} = 1$ si, et seulement si, $e_v(H'_n) = 1$.

Si $D < 0$, le genre principal contient, outre la forme unité $[1, 0, -D]$, une seule forme ambiguë simple h et il existe une suite de formes $h_1 = h$, $h_2 , \ldots, h_{n-1}$ telles que $h_k \in H_k$, et, si h'_n est une racine carrée de h_{n-1} on a $R_{n+1} = 1$ si, et seulement si, $e_v(h'_n) = 1$.

Si $D > 0$, le genre principal contient, outre la forme f, trois formes ambiguës simples h_1, h_2, h_3, deux de ces formes étant dans la classe A_o et la troisième dans la classe I. Donc si $R_n = 1$, il existe trois suites de formes

$$h_{i,1} = h_i , h_{i,2} , h_{i,2} , \ldots, h_{i,n-1} \quad (i = 1, 2, 3),$$

du genre principal telles que $h_{i,k+1}^2 = h_{i,k}$. Soient $h'_{i,n}$ des racines carrées des formes $h_{i,n-1}$. Si, par exemple, c'est h_1 qui est équivalente à f, $h'_{i,n}$ est d'ordre 2^{n-1}, donc $e_v(h'_{1,n}) = 1$; en outre, les formes h_2 et h_3 sont équivalentes, donc $h'_{2,n}(h'_{3,n})^{-1}$ est d'ordre 2^{n-1}, donc $e_v(h'_{2,n}) = e_v(h'_{3,n})$ et par conséquent :

$$e_v(h'_{1,n}) \cdot e_v(h'_{2,n}) \cdot e_v(h'_{3,n}) = 1$$

En outre, $R_{n+1} = 1$ si, et seulement si, $e_v(H'_n) = 1$, c'est-à-dire ici, si et seulement si, $e_v(h'_{2,n}) = e_v(h'_{3,n}) = 1 = e_v(h'_{1,n})$. Sinon $R_{n+1} = 0$ et $e_v(h'_{1,n}) = 1$, $e_v(h'_{2,n}) = e_v(h'_{3,n}) = -1$. Ainsi les facteurs principaux sont déterminés. En résumé :

PROPOSITION 1 -

Soit D un entier quadrat-frei tel que les 2^k-rangs R_k du groupe (C_2) soient égaux à 1 pour $2 \leq k \leq n$; soit $e_v(A) = 1$ la relation vérifiée par les caractères des classes ambiguës.

a) Si $D < 0$, soient $f = [1, 0, -D]$ et h_1 les formes ambiguës simples du genre principal. Il existe des suites de formes $h_1, h_2, \ldots, h_{n-1}, h_n$ telles que $h_k = h_{k+1}^2$ $(1 \leq k < n)$. Quelle que soit la suite choisie, $R_{n+1} = 1$ si, et seulement si, $e_v(h_n) = 1$.

b) Si $D > 0$, soient $f = [1, 0, -D]$, h_1, h_2 et h_3 les formes ambiguës simples du genre principal. Il existe des triplets de suites de formes

$$h_{i,1} = h_i, h_{i,2}, \ldots, h_{i,n-1}, h_{i,n} \quad (i = 1, 2, 3),$$

telles que $h_{i,k} = h_{i,k+1}^2$ pour $1 \leq k < n$.

Quel que soit le triplet, on a $e_v(h_{1,n}) \cdot e_v(h_{2,n}) \cdot e_v(h_{2,n}) = 1$ et $R_{n+1} = 1$ si et seulement si, $e_v(h_{1,n}) = e_v(h_{2,n}) = e_v(h_{3,n}) = 1$. Sinon $R_{n+1} = 0$ et la forme h_i équivalente à f est celle telle que $e_v(h_{i,n}) = 1$

§ 2.- Calcul d'une racine carrée d'une forme du genre principal.

Soit $g = [A, B, C]$ une forme du genre principal de déterminant D. Soit m' un nombre premier à 2 D représenté par une racine carrée ϕ' de g. Le nombre m'^2 est représenté par g, donc il existe x' et y' tels que :

$$m'^2 = A x'^2 + 2 B x' y' + C y'^2$$

Divisant par le P.G.C.D. (x, y) de x et y, on obtient :

(1) $m^2 = A x^2 + 2 B x y + C y^2$, avec (2) : $(x, y) = (m, 2 D) = 1$.

Tout nombre m vérifiant (1) et (2) est premier coefficient d'une racine carrée de g. En effet m^2 est représenté proprement par g, donc g est équivalente à une forme $h = m^2, k, \ell$, où $D = k^2 - m^2 \ell$, et, comme m est premier à 2 D, m est premier à k, donc à 2 K et par conséquent h est proprement primitive, donc h et g ont pour racine carrée $\phi = m, k, \ell m$. Donc :

PROPOSITION 2 -

Soit g une forme du genre principal de déterminant D. Il existe des nombres m premiers à 2 D dont le carré m^2 est représenté proprement par g. Tout tel nombre m est premier coefficient d'une racine carrée ϕ de g.

Ce raisonnement donne une méthode pratique pour calculer une forme $\phi = [m, k, \ell\, m]$ racine carrée de $g = [A, B, C]$ quand on connait un carré représenté par g :

Soit $m^2 = A\,x^2 + 2\,B\,x\,y + C\,y^2$ avec $(x, y) = (m, 2\,D) = 1$

La substitution linéaire $\begin{pmatrix} x & \xi \\ y & \eta \end{pmatrix}$ étant choisie de déterminant 1, on trouve :

$$g \approx h = [m^2,\ A\,x\,\xi + B(x\,\eta + y\,\xi) + C\,y\,\eta,\ g(\xi, \eta)]$$

Donc : $k = A\,x\,\xi + B(x\,\eta + y\,\xi) + C\,y\,\eta$ et $\ell = g(\xi, \eta)$.

(On peut aussi calculer $|k|$ par la formule $k^2 = D + m^2\,\ell$.

Changer le signe de k revient à remplacer ϕ par ϕ^{-1}, qui est aussi racine carrée de g).

Si D est positif, on a intérêt, pour chercher les nombres m^2, à remplacer la forme $[A, B, C]$ par une forme équivalente $[A', B', C']$ dont les coefficients sont en valeur absolue inférieurs à $2\sqrt{D}$, par exemple en la réduisant au sens de la théorie des formes réduites indéfinies de Gauss. La première forme réduite trouvée vérifie (cf. [1], § 183) :

(1) $$|A'| < \sqrt{D}\ ,\quad 0 < B' < \sqrt{D}\ ,\quad |C'| < 2\sqrt{D}.$$

La première de ces équations (1) appliquée à une racine carrée de $[A, B, C]$ montre que $[A, B, C]$ représente des carrés $m^2 < D$.

D'autre part, si $|m| < \sqrt{D}$, on vérifie que si on impose à la forme $[m, k', \ell']$ où $k' = k + t\,m$ soit la condition : (2) $\sqrt{D} - |m| < k' < \sqrt{D}$, soit la condition (2') $|\sqrt{D} - k'| < \frac{|m|}{2}$, on obtient : $0 < k' < \frac{5}{3}\sqrt{D}$ et $|\ell'| < 2\sqrt{D}$.

Si on choisit $|m| < \sqrt{D}$, on voit donc qu'il est facile de trouver une racine carrée de $[A, B, C]$ dont les coefficients sont $< 2\sqrt{D}$.

Tous les exemples que nous avons calculés indiquent que une forme du genre principal dont les coefficients sont inférieurs à $2\sqrt{D}$ représente des carrés $< D$ pour des valeurs des indéterminées très petites, inférieures à $\sqrt[4]{D}$. Il serait très intéressant de démontrer cette conjecture.

§ 3.- Critères pour que (C_2) contienne un cycle d'ordre au moins 16 -

Cas où (C_2) est cyclique. $(R_1 = R_2 = R_3 = 1)$

a) Cas de $Q(\sqrt{2\,p})$: On a $p = a^2 + b^2 = u^2 + 2\,v^2 = 2\,e^2 - d^2$ (b impair). Ici

$$h_1 = \overline{f} = [-1, 0, 2\,p];\ h_2 = \overline{g} = [-2, 0, p];\ h_3 = g = [2, 0, -p]$$

$$h_{1,2} = \phi_{-1} = [a + b, a - b, -a - b];\ h_{2,2} = \phi_{-2} = [u, 2\,v, -2\,u];$$

$$h_{3,2} = \phi_2 = [d, 2\,e, d].$$

Comme $R_3 = 1$, les trois formes ϕ_i sont dans le genre principal. On obtient donc le critère suivant :

Critère 3.1.- Soient m_{-1}, m_{-2}, m_2 trois entiers premiers à 2 p dont les carrés sont représentés proprement par ϕ_{-1}, ϕ_{-2}, ϕ_2 respectivement. Alors :

a) Un ou trois des m_i est congru à ± 1 modulo 8

b) Si les trois m_i sont congrus à ± 1 modulo 8, $R_4 = 1$. Sinon $R_4 = 0$

c) Si un seul m_i est congru à ± 1 modulo 8, le i correspondant est facteur principal.

Remarque - Supposons que ϕ_i représente 1 (ou -1). Alors ϕ_i^2 représente 1, donc ϕ_i est ambiguë et appartient soit à $\mathcal{S}$, soit à $\mathcal{A}$. Si le facteur principal est -1, les deux formes $\phi_i = [a + b, a - b, -a - b]$ et $\phi_i' = [a - b, a + b, -a + b]$ ne peuvent pas être équivalentes, donc une est dans $\mathcal{A}$ et l'autre dans $\mathcal{S}$.

Si le facteur principal n'est pas -1, alors $[u, 2v, -2u]$ n'est pas équivalente à $[-u, 2v, 2u]$, ni $[d, 2e, 2d]$ à $[-d, 2e, -2d]$. Donc une de celles correspondant au facteur principal est dans $\mathcal{S}$:

Complément 1 : Pour que i soit facteur principal, il faut et il suffit que il existe une forme ϕ_i qui représente 1.

Exemples -

Etudions les plus petits exemples de corps $Q(\sqrt{2p})$ tels que $R_4 = 1 (p = 1217)$ et $R_5 = 1$ $(p = 12641)$.

a) $p = 1217 = 31^2 + 16^2 = 33^2 + 2.8^2 = 2.33^2 - 31^2$; $D = 2434$.

$\phi_{-2} = [-33, 15, 66]$ représente 1 pour (1, -1), donc -2 est facteur principal.

$\phi_{-1} = [47, 15, -47]$ représente 81 pour (2, 1), donc $h_2 \geq 16$; comme $81 = 3^4$ une racine quatrième de ϕ_{-1} est $[3, \ldots, \ldots]$ qui n'est pas dans le genre principal, donc $h_2 = 16$.

($\phi_2 = [31, 66, 62]$ représente 15^2 pour (1, 1), d'où $h_2 \geq 16$).

b) $p = 12641 = 79^2 + 80^2 = 33^2 + 2.76^2 = 2.105^2 - 97^2$; $D = 25282$.

$\phi_{-1} = [1, \ldots, -1]$ représente 1, donc -1 est facteur principal.

$\phi_{-2} = [97, 210, 194]$ représente 39^2 pour (1, -4), donc $h_2 \geq 16$.

Montrons sur cet exemple comment déterminer h_2 (cf. § 2).

Toute substitution linéaire de matrice $\begin{pmatrix} 1 & \xi \\ -4 & \eta \end{pmatrix}$ et de déterminant 1 transforme ϕ_2 en $\phi_2' = [39^2, X, \phi_2(\xi, \eta)]$; $\xi = 0$, $\eta = 1$ donne donc :

$$\phi_2' = [39^2, X, 194], \text{ d'où } X^2 = D + 39^2.194 = 320356 = 566^2.$$

Une racine carrée de ϕ_2 est donc $[39, 566, \ldots] = \psi'_2$.

Avant de chercher un carré représenté par ψ'_2, on a intérêt à modifier le second coefficient modulo 39, de manière à le rendre le plus possible voisin de $\sqrt{D} \approx 159$: $\psi'^2 \sim \psi_2 = [39, 176, c]$ avec $c = \frac{176^2 - D}{39} = 146$. on trouve que

$\psi''_2 = [39, 176, 146]$ représente 81 pour (1, 2). Donc ψ''_2 est puissance 4^e, d'une forme $[3, \ldots, \ldots]$, donc n'est pas une puissance huitième, donc $h_2 = 32$.

De même, $\phi_{-2} = [-33, 138, 66]$ représente 73^2 pour (1, 7). On trouve comme racine carrée " réduite " $[73, 176, 78]$ qui représente 33^2 pour (1, 2), puis comme racine quatrième $[33, 167, 79]$ qui représente 117^2 pour (5, 6). Comme $117 \equiv 5 \pmod 8$, ϕ_{-2} est une puissance 8^e, mais pas 16^e, donc on retrouve que $h_2 = 32$.

Nous avons pu calculer, en programmant la méthode des § 1 et 2, la valeur de h_2 pour $Q(\sqrt{2p})$ où $p < 2.10^6$ ([5]).

Les plus petites valeurs de p telles que $h_2 = 2^n$ sont :

$h_2 = 8$: $p = 113$ $D = 226$

$h_2 = 16$: $p = 1217$ $D = 2434$

$h_2 = 32$: $p = 12641$ $D = 25282$

$h_2 = 64$: $p = 27953$ $D = 55906$

$h_2 = 128$: $p = 206081$ $D = 4121162$

$h_2 = 256$ pour $p = 1408961$, $p = 1410977$ et $p = 1566449$.

On peut conjecturer qu'il existe des nombres premiers p tels que le 2-groupe (C_2^*) des classes de $Q(\sqrt{2p})$ soit un cycle $C(2^n)$ d'ordre 2^n arbitrairement grand. Comme à chaque étape il y a une chance sur deux pour que chaque m_i soit $\equiv \pm 1 \pmod 8$, on peut même penser que, parmi les nombres premiers, la densité de ceux pour lesquels $(C_2^*) = C(\geq 2^{n+1})$ est $\frac{1}{4^n}$.

On peut faire des conjectures analogues pour chaque type de D (par exemple $5p$, $3p$, $-p$) que nous étudierons (pour $D < 0$, il faut remplacer $\frac{1}{4}$ par $\frac{1}{2}$ dans l'expression des densités).

b) Cas de $Q(\sqrt{\pi p})$ où $h(-\pi) = 2$ ($\pi = 5, 13, 37$) :

Posons $\pi = \alpha^2 + \beta^2$ et $p = a^2 + b^2$ avec β et b pairs. On a $R_2 = 1$ si, et seulement si $(\frac{p}{\pi}) = 1$ et alors les formes h_1, h_2 et h_3 sont

$$h_1 = -1, 0, \pi p, \quad h_2 = -\pi, 0, p, \quad h_3 = \pi, 0, p$$

En outre $(\frac{-\pi}{p}) = (\frac{p}{\pi}) = 1$ montre que p est représenté par une classe du genre principal de déterminant $-\pi$, donc par la classe principale, c'est-à-dire que $p = x^2 + \pi y^2$.

On a $R_3 = 1$, si, et seulement si $(\frac{p}{\pi})_4 = (\frac{\pi}{p})_4 = 1$. Alors on a : $(\frac{p}{\pi})_4 \times (\frac{\pi}{p})_4 = 1$; mais on sait que si $\pi \equiv 5 \pmod 8$ et $p = x^2 + \pi y^2$, $(-1)^y = (\frac{\pi}{p})_4 \times (\frac{p}{\pi})_4$, donc y est pair et x est impair (cf. [3], § 13). Donc $h_{2,1} = \phi_{-\pi} = [x, \pi y, -\pi x]$ est une racine carrée de h_2. On sait que $\phi_{-1} = h_{1,2} = [a\alpha + b\beta, a\beta - b\alpha, -a\alpha - b\beta]$ est une racine carrée de h_{-1}, donc avec les notations et hypothèses ci-dessus :

Critère 3.2.- Soit π tel que $h(-\pi) = 2$ et p tel que $(\frac{p}{\pi})_4 = (\frac{\pi}{p})_4 = 1$. Soient m_{-1} et $m_{-\pi}$ des nombres premiers à $2\pi p$ dont les carrés soient représentés proprement par ϕ_{-1} et $\phi_{-\pi}$ respectivement.

(C_2) $(\pi p) = C(\geq 16)$ si, et seulement si, $(\frac{m_{-1}}{\pi}) = (\frac{m_{-\pi}}{\pi}) = 1$

Si $(\frac{m_{-1}}{\pi}) = 1$ et $(\frac{m_{-\pi}}{\pi}) = -1$, -1 est facteur principal.

Si $(\frac{m_{-1}}{\pi}) = -1$ et $(\frac{m_{-\pi}}{\pi}) = 1$, $-\pi$ est facteur principal

Si $(\frac{m_{-1}}{\pi}) = (\frac{m_{-\pi}}{\pi}) = -1$, π est facteur principal

Exemples où $\pi = 5 = 1 + 2^2$:

a) $p = 461 = 19^2 + 10^2 = 21^2 + 5.2^2$; $D = 5p = 2305$

$\phi_{-1} = [1, 48, -1]$, donc -1 est facteur principal

$\phi_{-\pi} = [21, 10, +105]$ représente 64 pour $(1, -1)$, donc une racine carrée est $[16, \ldots, \ldots]$ et une racine quatrième de $\phi_{-\pi}$ est $[8, \ldots, \ldots]$; $(\frac{8}{5}) = -1$, donc $h_2(2305) = 16$. Le nombre 2305 est le plus petit $D > 0$ tel que $(C_2) = C(\geq 16)$.

b) $p = 7841 = 79^2 + 40^2 = 81^2 + 5.16^2$; $D = 39205$

$\phi_{-1} = [1, \ldots, -1]$, donc -1 est facteur principal

$\phi_{-\pi} = [9^2, \ldots, \ldots]$, donc $(C_2) = C(\geq 16)$. Une racine quatrième de $\phi_{-\pi}$ est $[3, \ldots, \ldots]$ est $(\frac{3}{5}) = -1$, donc $h_2 = 16$.

Exemple où $\pi = 37 = 1 + 6^2$: $p = 149 = 7^2 + 10^2 = 1^2 + 37.2^2$; $D = 5513$

Ici, $x = 1$, donc -1 est facteur principal ($\phi_{-\pi}$ représente 1).

$\phi_1 = [53, 52, -53] \approx [-53, 54, 49]$; $(\frac{7}{37}) = (\frac{37}{7}) = (\frac{2}{7}) = 1$, donc $(C_2) = C(\geq 16)$. (On remarque que $75^2 - 5513 = 112 = 7.4^2$, donc une racine carrée de l'inverse de ϕ_{-1} est $[4^2, \ldots, \ldots]$, donc une racine quatrième de ϕ_{-1}^{-1} est $[8, \ldots, \ldots]$ et $(\frac{8}{37}) = -1$, donc $h_2 = 16$.

c) Cas de $Q(\sqrt{\pi p})$ où $h(-\pi) = 4$. ($\pi = 17, 73, 97, 193$. Il est probable que ce sont les seuls) :

Le cas à étudier est celui où $(\frac{p}{\pi})_4 = (\frac{\pi}{p})_4 = 1$. La théorie de [3], § 13, montre que, comme $(\frac{p}{\pi})_4 (\frac{\pi}{p})_4 = 1$, p est représenté par $[1, 0, \pi]$ et cette représentation $p = x^2 + \pi y^2$ est unique. Mais ici, on ne peut connaître la parité de x et il y a des cas où x est pair ($\pi = 17$, $p = 157 = 2^2 + 17.3^2$) et des cas où x est impair ($\pi = 17$, $p = 149 = 9^2 + 17.2^2$).

a) Si x est impair, le raisonnement du § 2 s'applique.

b) Si x est pair, la forme $[x, \pi y, -\pi x]$ est " improprement primitive ". Considérons le groupe (C_1) des classes de formes $\{A, B, C\} = AX^2 + BXY + CY^2$ où $B^2 - 4AC = D$; on sait que la formule de composition est la même : $\{A, B, A'C\}\{A', B, AC\} = \{AA', B, C\}$, donc $\{\frac{x}{2}, \pi y, -\pi \frac{x}{2}\}^2$ représente $-\pi$

et si $D = A^2 + B^2$, $\{\frac{B}{2}, A, -\frac{B}{2}\}^2$ représente -1. La proposition 0 de [3] est aussi vraie, mais il n'y a que des formes du second type {B, B, E}; les formes ambiguës simples représentant $-\pi$ et -1 sont $\{-\pi, -\pi, \frac{p-\pi}{4}\}$ et $\{-1, -1, \frac{p\pi - 1}{4}\}$. La théorie des genres est vraie et on trouve :

Critère 3.3.- Soient π tel que $h(-\pi) = 4$ et p tel que $(\frac{p}{\pi})_4 = (\frac{\pi}{p})_4 = 1$. Alors (C_2) $(p\pi) = C(\geq 8)$ et $p = x^2 + \pi y^2$. Si x est impair, posons $\phi_{-1} = [a\alpha + b\beta, a\beta - b\alpha, -a\alpha - b\beta]$, $\phi_{-\pi} = [x, \pi y, -\pi x]$. Si x est pair, posons : $\phi_{-1} = \{\frac{a\beta - b\alpha}{2}, a\alpha + b\beta, -\frac{a\beta - b\alpha}{2}\}$, $\phi_{-\pi} = \{\frac{x}{2}, \pi y, -\pi\frac{x}{2}\}$. Soient m_{-1} et $m_{-\pi}$ des entiers premiers à 2p dont les carrés sont représentés par ϕ_{-1} et $\phi_{-\pi}$ respectivement. Alors :

1) $(C_2) = C(\geq 16)$ si, et seulement si, $(\frac{m_{-1}}{\pi}) = (\frac{m_{-\pi}}{\pi}) = +1$. Sinon $(C_2) = C(8)$.

2) Si $(\frac{m_{-1}}{\pi}) = 1$, $(\frac{m_{-\pi}}{\pi}) = -1$, -1 est facteur principal

3) Si $(\frac{m_{-1}}{\pi}) = -1$, $(\frac{m_{-\pi}}{\pi}) = 1$, $-\pi$ est facteur principal

4) Si $(\frac{m_{-1}}{\pi}) = (\frac{m_{-\pi}}{\pi}) = -1$, π est facteur principal.

En outre on démontre comme le complément 1, pour les cas où $h(-\pi) = 2$ ou 4, le complément 2 : Pour que -1 (respectivement $-\pi$) soit facteur principal, il faut et il suffit qu'il existe une forme ϕ_{-1} (respectivement $\phi_{-\pi}$) qui représente 1. Exemples avec $\pi = 17 = 1 + 4^2$; $D = 17p$, $p = a^2 + b^2$ (b impair) :

On a $R_3 = 1$ si $(\frac{p}{17}) = (\frac{p}{17})_4 = 1$, donc $p \equiv \pm 1$ ou ± 4 (mod. 17) et si $(\frac{a + 4b}{17}) = 1$.

a) $p = 149$, $D = 2433$. On a $p = 149 = 9^2 + 17.2^2 = 7 + 10^2 \equiv -4$ (mod. 17) et $(\frac{7 + 40}{17}) = (\frac{-4}{17}) = 1$. Donc $R_3 = 1$.

$\phi_{-17} = [9, 34, -153]$. Comme $(\frac{3}{17}) = (\frac{17}{3}) = -1$, -17 n'est pas facteur principal et $R_4 = 0$.

$\phi_{-1} = [47, 18, -47]$ ou bien $[33, 38, -33]$. La première représente 36 pour (1, 1), donc une de ses racines carrées est $[12, \ldots, \ldots]$; $(\frac{12}{17}) = -1$, donc -1 n'est pas facteur principal, donc 17 est facteur principal.

b) $p = 157$, $D = 2669$. On a $p = 157 = 2^2 + 17.3^2 = 11^2 + 6^2 \equiv 4$ (mod. 17) et $(\frac{11 + 24}{17}) = (\frac{1}{17}) = 1$. Donc $R_3 = 1$.

$\phi_{-17} = \{1, 51, -17\}$, donc -17 est facteur principal.

$\phi_{-1} = \{25, 13, -25\}$ ou bien $\{19, 35, -19\}$. Comme $(\frac{5}{17}) = -1$, $R_4 = 0$

c) $p = 613$, $D = 10421$. On a $p = 613 = 1 + 17.6^2 = 17^2 + 18^2 \equiv 1$ (mod. 17) $(\frac{17 + 4.18}{17}) = (\frac{72}{17}) = (\frac{2}{17}) = 1$. Donc $R_3 = 1$.

$\phi_{-1} = [55, 89, -55]$ ou bien $[89, 55, -89]$

On trouve que $[55, 89, -55]$ représente $625 = 5^4$ pour $(2, 5)$.

Donc $R_4 = 1$, et, comme $(\frac{5}{17}) = (\frac{17}{5}) = (\frac{2}{5}) = -1$, $R_5 = 0$, donc $h_2 = 16$.

§ 4.- Critère pour que (C_2) contienne un cycle d'ordre au moins 16. Cas où $R_1 = 2$, $R_2 = R_3 = 1$ et où D n'est pas somme de deux carrés.

Il y a alors trois caractères génériques, dont un et un seul a sa valeur invariante par changement de signe; ce caractère est e_v.

Soient h_1, h_2, h_3 les trois formes ambiguës simples (autres que f) du genre principal; aucune d'elles n'est $\overline{f} = [-1, 0, D]$. Soient $h_{1,2}$, $h_{2,2}$, $h_{3,2}$ des racines carrées de h_1, h_2, h_2. Comme $R_3 = 1$, on a :

$$e_v(h_{1,2}) = e_v(h_{2,2}) = e_v(h_{3,2}) = 1.$$

Les deux autres caractères génériques sont égaux, et changent de signe si on change le signe de la forme, donc, changeant éventuellement les signes des formes $h_{i,2}$ (ce qui revient à les composer avec $\overline{f}$), on peut les choisir dans le genre principal.

Supposons que l'on connaisse explicitement des formes $h_{i,2}$ pour deux des trois valeurs de i, disons $i = 1$ et $i = 2$. On obtient, en appliquant la proposition 1 pour $n = 3$ et la proposition 2 :

Critère 4.0.- Soient m_i $(i = 1, 2)$ des nombres premiers à 2 D tels que m_i^2 ou $-m_i^2$ soit représenté proprement par $h_{i,2}$

On a $R_4 = 1$ si, et seulement si $e_v(m_1) = e_v(m_2) = 1$.

Si $e_v(m_i) = 1$ et $e_v(m_2) = -1$, h_1 est équivalente à f.

Si $e_v(m_1) = e_v(m_2) = -1$, h_3 est équivalente à f.

A) Ce critère s'applique aux cas $D = 3p$, $6p$, $22p$, $7p$. Etudions le cas $D = 3p$ en détails :

Cas de $D = 3p$ (cf. [3], § 5, théorème B_2 et son corollaire) :

Comme $R_3 = 1$, on a $p = u^2 + 2v^2 = x^2 + 3y^2 \equiv 1 \pmod{24}$ avec $u + v \equiv \pm 1$ et $x \equiv \pm 1 \pmod{12}$. Les caractères génériques sont $e_p = e_v$, e_3 et $e_2 = (\frac{-1}{m})$ les formes ambiguës simples du genre principal sont :

$$h_1 = g = [-3, 0, p], \quad h_2 = [-2, 1, \frac{3p-1}{2}], \quad h_3 = h_1 h_2$$

On connaît explicitement les formes :

$$h_{1,2} = [x, 3y, -3x], \quad h_{2,2} = [u + v, u - 2v, -2(u + v)].$$

Choisissons les signes de x, u et v de façon que $x \equiv u + v \equiv 1 \pmod{4}$. Les formes $h_{1,2}$ et $h_{2,2}$ sont des formes ψ_{-3} et ψ_{-2} du genre principal et on trouve :

Critère 4.1.- Soient m_{-3} et m_{-2} des entiers premiers à 2 D dont les carrés sont représentés proprement par ψ_{-3} et ψ_{-2} respectivement.

a) $\kappa_4 = 1$ si, et seulement si, $m_{-3} \equiv \pm 1$ et $m_{-2} \equiv \pm 1$ (mod. 12)

b) Si $m_{-3} \equiv \pm 1$ et $m_{-2} \equiv \pm 3$ (mod. 12), -3 est facteur principal

Si $m_{-3} \equiv \pm 3$ et $m_{-2} \equiv \pm 1$ (mod. 12), -2 est facteur principal

Si $m_{-3} \equiv \pm 3$ et $m_{-2} \equiv \pm 3$ (mod. 12, 6 est facteur principal

B) Cas de $D = \pi q$ tel que $h(\pi) = 1$:

On sait que (cf. [3], § 5) pour $D = \pi q$, on a $R_1 = 2$ et $R_2 = 1$, si, et seulement si $\pi \equiv 1$ (mod. 8) et $(\frac{q}{\pi}) = 1$

D'autre part dans de très nombreux cas (80 % environ), le nombre de classes d'idéaux au sens strict de $Q(\sqrt{\pi})$ est égal à 1, et si $\pi \equiv 1$ (mod. 8), ce nombre est égal au nombre $h(\pi)$ des classes de formes proprement primitives de déterminant π.

Nous supposons donc que π est un nombre premier donné tel que $\pi \equiv 1$ (mod. 8) et $h(\pi) = 1$ et nous étudions les groupes (C_2) pour $D = \pi q$ où $q \equiv -1$ (mod. 4) est tel que $(\frac{q}{\pi}) = 1$.

B_1) Cas de $D = \pi q$ où $q \equiv 3$ (mod. 8) : On a :

$$\pi = u^2 + 2v^2 \; ; \; q = w^2 + 2z^2 = -x^2 + \pi y^2$$

où x est toujours impair. Les formes ambiguës simples du genre principal sont :

$$f,\ g = [\pi,\ 0,\ -q],\ \bar{h} = \left[-2,\ 1,\ \frac{p\,q\,-1}{2}\right],\ g\,\bar{h}$$

Posons : $\psi_\pi = [x,\ \pi y,\ \pi x]$ et $\psi_{-2} = [u z + v w,\ u w - 2 v z,\ -2(u z + v w)]$

On a : $\psi_\pi^2 = g$ et $\psi_{-2}^2 = \bar{h}$. Donc $(\frac{q}{\pi})_4 = (\frac{x}{\pi})$ et $R_3 = 1$ si, et seulement si $(\frac{u z + v w}{\pi}) = (\frac{x}{\pi}) = 1$. Supposons que cela soit et choisissons les signes de façon que $u z + v w \equiv x \equiv 1$ (mod. 4); les formes ψ_π et ψ_{-2} sont dans le genre principal; soient m_π et m_{-2} des entiers dont les carrés sont représentés proprement par ψ_π et ψ_{-2} respectivement :

Critère 4.2.- $R_4 = 1$ si, et seulement si, $(\frac{m_\pi}{\pi}) = (\frac{m_{-2}}{\pi}) = 1$

Si $(\frac{m_\pi}{\pi}) = 1$ et $(\frac{m_{-2}}{\pi}) = -1$, π est facteur principal.

Si $(\frac{m_\pi}{\pi}) = -1$ et $(\frac{m_{-2}}{\pi}) = 1$, -2 est facteur principal

Si $(\frac{m_\pi}{\pi}) = (\frac{m_{-2}}{\pi}) = -1$, $-2\,\pi$ est facteur principal

B_2) Cas de $D = \pi q$ où $q \equiv -1$ (mod. 8) : on a :

$$\pi = 2e^2 - d^2 \; ; \; q = 2r^2 - s^2 = -x^2 + \pi y^2$$

Les formes ambiguës simples du genre principal sont :

$$f,\ g = [\pi,\ 0,\ -q],\ h = \left[2,\ 1,\ \frac{1 - \pi\,q}{2}\right],\ g\,h$$

Posons $\psi_\pi = [x,\ \pi y,\ \pi x]$, $\psi_2 = [e s + d r,\ 2 e r + d s,\ 2(e s + d r)]$.

On a $\psi_\pi^2 = g$ et $\psi^2 = h$. Donc $(\frac{q}{\pi})_4 = (\frac{x}{\pi})$ et $R_3 = 1$ si, et seulement si $(\frac{e\,s + d\,r}{\pi}) = (\frac{x}{\pi}) = 1$.

Supposons que cela soit et que les signes soient tels que $e\,s + d\,r \equiv x \equiv 1 \pmod{.}$

Soient m_π et m_2 des entiers dont les carrés sont représentés par ψ_π et ψ_2 respectivement. Alors :

Critère 4.3.- $R_4 = 1$ si, et seulement si $(\frac{m_\pi}{\pi}) = (\frac{m_2}{\pi}) = 1$

Si $(\frac{m}{\pi}) = 1$ et $(\frac{m_2}{\pi}) = -1$, π est facteur principal.

Si $(\frac{m_\pi}{\pi}) = -1$ et $(\frac{m_2}{\pi}) = 1$, 2 est facteur principal

Si $(\frac{m_\pi}{\pi}) = (\frac{m_2}{\pi}) = -1$, $2\,\pi$ est facteur principal.

Exemples avec $\pi = 17$; $u = 3$, $v = 2$ et $e = 3$, $d = 1$.

a) $q = 659 \equiv 3 \pmod{8}$; $D = 11203$; $(\frac{659}{17}) = (\frac{19}{17}) = (\frac{2}{17}) = 1$

$659 = 9^2 + 2.17^2 = -87^2 + 17.22^2$: $w = y$, $z = 17$, $x = 87$, $y = 22$.

$(\frac{u\,z + v\,w}{17}) = (\frac{18}{17}) = 1$; $(\frac{x}{17}) = (\frac{87}{17}) = (\frac{2}{17}) = 1$. Donc $R_3 = 1$.

$\psi_\pi = [87, 374, \ldots] \approx [87, 113, 18]$ qui représente -11^2 pour $(1, -1)$

$\psi_{-2} = [69, 41, -138] \approx [69, 110, 13]$ qui représente 27^2 pour $(2, 1)$

Donc -34 est facteur principal et $R_4 = 0$.

b) $q = 191 \equiv -1 \pmod{8}$, $D = 3247$; $(\frac{191}{17}) = (\frac{21}{17}) = 1$

$191 = 2.10^2 - 3^2 = -81 + 17.4^2$: $r = 10$, $s = 3$, $x = 9$, $y = 4$

$(\frac{x}{17}) = (\frac{9}{17}) = 1$ et $(\frac{e\,s + d\,r}{17}) = (\frac{9 + 10}{17}) = 1$, donc $R_3 = 1$

$\psi_\pi = [9, \ldots, \ldots]$ et $(\frac{3}{17}) = -1$, donc $R_4 = 0$

$\psi_2 = [-1, \ldots, \ldots]$, donc 2 est facteur principal.

c) Cas où $D = D = 2\,\pi\,q$, avec $h(\pi) = 1$:

Ici on voit aussi que $2\,q$ est représenté par une classe de déterminant π mais on voit, modulo 8, que $2\,q$ n'est pas représenté par $[-1, 0, \pi]$. Donc $2\,q$ est représenté par la classe improprement primitive de déterminant π, autrement dit, q est représenté par la classe de $\{-1, -1, \frac{\pi - 1}{4}\}$.

Ceci ne permet pas d'obtenir explicitement de racine carrée de forme ambiguë simple, donc on ne peut avoir des résultats analogues à ceux du cas $D = \pi\,q$.

§ 5.- Cas des corps imaginaires.

Donnons un exemple des résultats que l'on peut obtenir :

Soit $D = -p$, où $p \equiv 1 \pmod{8}$

On sait que (C_2) est cyclique, $h_2 \equiv 0 \pmod{4}$ $(R_1 = R_2 = 1)$ et que $p = 2\,e^2 - d^2$. En outre $h_2 \equiv 0 \pmod{8}$ si, et seulement si $|e| \equiv 1 \pmod{4}$.

Alors les formes $\phi = [|e|, d, 2\,|e|]$ sont dans le genre principal positif de

déterminant $-p$ et $h_2 \equiv 0 \pmod{16}$ si, et seulement si, tout nombre m premier à $2p$ dont le carré est représenté par une forme ϕ vérifie $|m| \equiv 1 \pmod{4}$.

BIBLIOGRAPHIE

[1] C.F. GAUSS.- Disquisitiones Arithmeticae.

[2] P. KAPLAN.- Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-sous-groupe des classes est cyclique et réciprocité biquadratique Journal of the Mathematical Society of Japan.- 25 (1973), p. 596-608.

[3] P. KAPLAN.- Sur le 2-groupe des classes d'idéaux des corps quadratiques, I et II.- Journal für die reine und angew. Math. 283-284 (1976), p. 313-363

[4] P. KAPLAN.- Cours d'arithmétique.- U.E.R. de Mathématiques.- Université de Nancy.

[5] P. KAPLAN et C. SANCHEZ.- Table des 2-groupe des classes d'idéaux de $\mathbb{Q}(\sqrt{2p})$ pour $p < 2.10^6$.- U.E.R. de Mathématiques, Université de Nancy I (1974).

P. KAPLAN
10, allée Jacques Offenbach
54420 SAULXMES les NANCY