PROCEEDINGS

of the

INTERNATIONAL CONFERENCE

on

CLASS NUMBERS AND FUNDAMENTAL UNITS

of

ALGEBRAIC NUMBER FIELDS

JUNE 24 – 28, 1986

KATATA, JAPAN

CYCLES D'ORDRE AU MOINS 16 DANS LE DEUX GROUPE DES CLASSES D'IDEAUX AU SENS STRICT DE CORPS QUADRATIQUES

par Pierre KAPLAN et Kenneth S. WILLIAMS

§ 1.- Introduction.

Les corps quadratiques que nous considérons dans ce travail sont des corps quadratiques dont le deux groupe des classes d'idéaux au sens strict a un 4-rang r_4 et un 8-rang r_8 égaux à 1 .

Soit donc $K = Q(\sqrt{m})$, où m n'a pas de diviseur carré, un tel corps quadratique, D son discriminant. On sait que le deux groupe des classes d'idéaux au sens strict de K est isomorphe au deux groupe C_2 du groupe des classes de formes quadratiques binaires $[a,b,c] = aX^2 + bXY + cY^2$ de discriminant $b^2 - 4ac = 4m$ (déterminant $\frac{b^2}{4} - ac = m$) , positives si $m < 0$.

Pour obtenir des conditions pour que le 16 rang r_{16} soit égal à 1 nous allons raisonner comme dans le travail [3], pages 315-317 et [4] § 1, dont nous reprenons les notations à partir d'ici, et auquel nous référons, en particulier à la proposition 1 de [4]. Il existe un caractère générique e_V (cf. [3], p. 316, c, α), $e_V \neq 1$, tel que les caractères des classes ambiguës soient exactement ceux vérifiant $e_V = 1$.

Si $m < 0$, soit h la forme ambiguë simple du genre principal distincte de la forme unité $f = [1,0,-m]$. Comme $r_8 = 1$, une des racines carrées h' de h est dans le genre principal, et $r_{16} = 1$ si, et seulement si, $e_V(h'') = 1$ où h'' désigne une racine carrée de h' . Nous déterminerons une forme h' , et nous pourrons évaluer $e_V(h'')$ comme $e_V(r)$ où r est un entier premier à $2m$ tel que r^2 soit représenté par h' .

Dans le cas où $m > 0$, soient h_1 , h_2 et h_3 les formes ambiguës simples du genre principal distinctes de f , et h_1' , h_2' , h_3' des racines carrées de ces formes, appartenant au genre principal. De telles formes existent car $r_8 = 1$. Soient h_1'' , h_2'' , h_3'' des racines carrées de ces formes. Alors $e_V(h_1'').e_V(h_2'').e_V(h_3'') = 1$ et $r_{16} = 1$ si, et seulement si, $e_V(h_1'') = e_V(h_2'') = e_V(h_3'') = 1$; sinon $r_{16} = 0$ et la forme h_i appartenant à la classe unité est celle telle que $e_V(h_i'') = 1$. Ici nous pourrons déterminer les formes h_i' , et, pour deux d'entre elles, évaluer $e_V(h_i'') = e_V(r_i)$ où r_i^2 est représenté par h_i' .

Dans certains cas, (par exemple $m = pq$, $p \equiv 1 \pmod 8$, $q \equiv -1 \pmod 4$) , nous ne pourrons évaluer qu'un seul nombre $e_V(h_i'')$, donc nous n'obtiendrons qu'un critère partiel. Il convient de noter que si il était possible de calculer les trois $e_V(h_i'')$ on obtiendrait une loi de réciprocité octique analogue à la loi de réciprocité biquadratique rationnelle.

Dans le paragraphe 2 nous déterminerons les formes h' , dans le paragraphe 3 nous préciserons les types de corps que nous considérons et déterminons le caractère e_V correspondant. Le paragraphe 4 contient les résultats les plus importants de ce travail, à savoir l'évaluation du caractère $e_V(h'')$ (théorèmes 1 et 2). Les paragraphes 5 et 6 suivants sont consacrés aux applications, respectivement aux corps imaginaires et réels. En particulier nous retrouvons, sous une forme généralisée et simplifiée tous les résultats obtenus par cette méthode dans les articles [5], [6] et [7] pour le cas où $r_2 = 1$.

§ 2.- Détermination d'une forme d'ordre 4 et d'une forme d'ordre 8.

Dans cette section nous ne supposons pas que $r_4 = 1$, mais nous supposons seulement $r_2 \geq r_4 \geq r_8 \geq 1$. Nous désignerons par P et Q deux entiers tels $P > 0$, $PQ = m$ et tels que la classe de la forme ambiguë

$$h = [P,0,-Q] \quad \text{ou} \quad h = \left[2P,2P,\frac{P-Q}{2}\right] \tag{2.1}$$

soit une puissance quatrième dans le groupe des classes de discriminant $4m$. Nous poserons $A = 1$ dans le premier cas et $A = 2$ dans le second cas, qui ne peut se produire que si $m \equiv -1 \pmod 4$.

Soit h' une racine carrée de h qui soit dans le genre principal. La forme h' représente proprement des nombres $Z \equiv 1 \pmod 4$. En effet ou bien $(-1)^{\frac{x-1}{2}}$ est parmi les caractères génériques, et $Z \equiv 1 \pmod 4$; ou bien $(-1)^{\frac{x-1}{2}}$ ne fait pas partie des caractères génériques, et on sait (cf. [1], § 229) qu'une forme de discriminant $4m$ représente des nombres Z donnant à $(-1)^{\frac{Z-1}{2}}$ la valeur 1 et des nombres Z donnant à $(-1)^{\frac{Z-1}{2}}$ la valeur -1 . On en déduit que l'équation

$$AZ^2 = PX^2 - QY^2 \tag{2.2}$$

a des solutions en entiers rationnels vérifiant :

(2.3) $$\begin{cases}(X,Y) = 1\ ,\ X > 0\ ,\ Z \equiv 1 \pmod 4\ ,\ Z > 0 \text{ si } m < 0\ ,\\ e(Z) = 1 \text{ pour tous les caractères génériques.}\end{cases}$$

Soient alors λ et μ tels que

(2.4) $$\lambda X - \mu Y = 1\ .$$

Appliquant la substitution linéaire de matrice $\begin{pmatrix} X & \mu \\ Y & \lambda \end{pmatrix}$ à la forme $[P,0,-Q]$ on obtient l'identité

(2.5) $$P(X\xi+\mu\eta)^2 - Q(Y\xi+\lambda\eta)^2 = AZ^2\xi^2 + 2b\xi\eta + c\eta^2$$

avec

(2.6) $$b = PX\mu - QY\lambda\ ,\quad c = P\mu^2 - Q\lambda^2\ .$$

Tenant compte de (2.2), (2.4) et (2.6) il vient

(2.7) $$bY = A\lambda Z^2 - pX\ ,\quad bX = A\mu Z^2 - qY\ .$$

L'équation (2.5) signifie que les formes $[P,0,-Q]$ et $[AZ^2,2b,c]$ sont équivalentes, donc

$$[P,0,-Q] \approx [AZ,2b,ZC]\ [Z,2b,AZc]$$
$$\approx [A,2b,Z^2C]\ [Z,2b,AZc]^2\ .$$

Composant avec la forme ambiguë $[A,2b,Z^2C]$ on trouve

$$h \approx [Z,2b,AZc]^2\ .$$

La forme $h' = [Z,2b,AZc]$ est donc la forme d'ordre 4 cherchée ; elle est dans le genre principal donc il existe des entiers x, y et r tels que

(2.8) $$r^2 = Zx^2 + 2bxy + AZcy^2$$

avec

(2.9) $$(x,y) = (r,2ZcPQ) = 1\ .$$

Ce nombre r est représenté par une racine quatrième h'' de la forme h, et nous voulons déterminer la valeur de $e_V(r)$ en fonction de P, Q, X, Y et Z.

Nous terminons cette section par quelques propriétés des nombres introduits jusqu'ici.

Les équations (2.7) et (2.8) montrent que $1 = \left(\frac{2bxy}{Z}\right) = \left(\frac{-2xyXYP}{Z}\right)$.

Comme $P > 0$, et que $Z \equiv 1 \pmod 4$ donne la valeur 1 aux caractères génériques, on a $\left(\frac{P}{Z}\right) = \left(\frac{Z}{P}\right) = 1$ d'où

$$(2.10) \qquad \left(\frac{Xx}{Z}\right) = \left(\frac{-2yY}{Z}\right) \; ; \; \left(\frac{Yx}{Z}\right) = \left(\frac{-2yX}{Z}\right) .$$

D'autre part, multipliant l'équation (2.8) par AZ on a

$$(2.11) \qquad AZr^2 = AZ^2x^2 + 2bxyAZ + c(AZy)^2 .$$

Appliquant l'identité (2.5) à (2.11) avec $\xi = x$, $\eta = AZy$ il vient

$$(2.12) \qquad AZr^2 = PS^2 - QT^2$$

avec

$$(2.13) \qquad S = Xx + \mu AZy \quad , \quad T = Yx + \lambda AZy .$$

Comme, d'après (2.9), on a $(x,AZy) = 1$ et que $\det\begin{pmatrix} X & \mu \\ Y & \lambda \end{pmatrix} = 1$ on voit que

$$(2.14) \qquad (S,T) = (S,AqZr) = (T,ApZr) = 1 .$$

Dans le cas où $D > 0$, c'est-à-dire $Q > 0$, nous aurons besoin d'une relation entre les signes de X , Z et Ty :

Lemme : Si $Q > 0$ et X est choisi > 0 , on ne peut avoir à la fois $Ty > 0$ et $Z < 0$.

Pour montrer ce lemme nous calculons $2QTy$. On a, d'après (2.13) et (2.6)

$$2QTy = 2Q(Yx+\lambda AZy)y = 2AQ\lambda Zy^2 + 2xy(A\mu Z^2 - bX) .$$

Remplaçons $2bxy$ par sa valeur tirée de (2.8). Il vient :

$$2QTy = Z\varphi(x,y) - Xr^2$$

où $\varphi(x,y)$ est la forme quadratique en x et y définie par

$$\varphi(x,y) = Xx^2 + 2A\mu Zxy + (2AQ\lambda + AcX)y^2 .$$

Le discriminant de $\varphi(x,y)$ est 4Δ avec

$$\Delta = A^2\mu^2Z^2 - X(2AQ\lambda+AcX) .$$

Remplaçant AZ^2 par $PX^2 - QY^2$ et c par $p\mu^2 - q\lambda^2$ et utilisant deux fois le fait que $\lambda X - \mu Y = 1$ on trouve facilement $\Delta = -AQ < 0$ ce qui montre que la forme $\varphi(x,y)$ est définie positive. Donc, si $Q > 0$ et X choisi > 0, alors on ne peut avoir à la fois $Ty > 0$ et $Z < 0$.

Corollaire : Définissons les trois nombres $\alpha, \beta, \gamma = \pm 1$ par

$$(2.15) \qquad \alpha = \begin{cases} -1 \text{ si } T \text{ et } Z < 0 \\ +1 \text{ sinon} \end{cases}, \quad \beta = \begin{cases} -1 \text{ si } Z \text{ et } y < 0 \\ +1 \text{ sinon} \end{cases}, \quad \gamma = \operatorname{sgn} Z .$$

Alors pour $m > 0$ et $X > 0$ on a :

$$(2.16) \qquad \alpha\beta\gamma = 1 .$$

Remarque : Si $m < 0$, $\alpha = \beta = \gamma = 1$, car $Z > 0$.

§ 3.- Détermination du caractère e_V.

Dans toute la suite de ce travail P désignera un nombre positif n'ayant pas de diviseur congru à 3 modulo 4.
Nous allons maintenant décrire les cas où notre méthode s'applique.

Proposition 1 : On suppose $m = PQ$, avec $Q \equiv 1 \pmod 4$ si $P \not\equiv 1 \pmod 8$. Si la forme ambiguë $[P,0,-Q]$ est dans le genre principal, alors $r_4 \geq 1$ et toute la classe ambiguë vérifie

$$e_p(A) = 1 .$$

Proposition 2 : On suppose $m = -s$, avec $s \equiv 1 \pmod 8$, $s > 0$ tel que tous les facteurs premiers de s soient congrus à 1 modulo 4. Alors $r_4 \geq 1$ et toute classe ambiguë A vérifie

$$e_2(A) = 1 .$$

Corollaire : Si $r_4 = 1$ alors $V = P$ dans le cas de la proposition 1 et $V = 2$ dans celui de la proposition 2.

Démonstrations : Pour démontrer la proposition 2 il suffit de remarquer que, quelle que soit la décomposition $-m = P'Q'$, $P' > 0$, $Q' > 0$ on a

$$P' \equiv Q' \equiv \frac{P'+Q'}{2} \equiv 1 \pmod 4$$

et que la forme ambiguë $\left[2,2,\frac{1+PQ}{2}\right]$ est dans le genre principal.

Il reste à prouver la proposition 1.
Considérons d'abord le cas où P est impair. Les classes ambiguës contiennent des formes $a = \pm [P'Q',0,P''Q'']$, avec

$$P'P'' = P \quad , \quad Q'Q'' = Q \quad , \quad P' > 0 \quad , \quad P'' > 0$$

et, dans le cas où $Q \equiv 3 \pmod 4$, le composé de a avec la forme $b_0 = \left[2,2,\frac{1-PQ}{2}\right]$, pour laquelle $e_P(b_0) = \left(\frac{2}{P}\right) = 1$. Calculons $e_P(a)$. On a

$$e_P(a) = \left(\frac{P'Q'}{P''}\right)\left(\frac{P''Q''}{P'}\right) = \left(\frac{P'}{P''}\right)\left(\frac{P''}{P'}\right)\left(\frac{Q'}{P''}\right)\left(\frac{Q''}{P'}\right) = \left(\frac{Q'}{P''}\right)\left(\frac{Q''}{P'}\right) .$$

Changeant éventuellement les notations on peut supposer $Q' \equiv 1 \pmod 2$ et

$$e_P(a) = \left(\frac{P''}{Q'}\right)\left(\frac{Q''}{P'}\right) = \left(\frac{P'}{Q'}\right)\left(\frac{Q''}{P'}\right) = \left(\frac{Q'}{P'}\right)\left(\frac{Q''}{P'}\right) = 1$$

car $\left(\frac{P'P''}{Q'}\right) = \left(\frac{Q'Q''}{P'}\right) = 1$ puisque $[P,0,-Q]$ est dans le genre principal.

Considérons maintenant le cas où $P = 2P_1$, P_1 étant impair.
Alors, par hypothèse, $Q \equiv 1 \pmod 4$, donc, puisque la forme $[2P_1,0,-Q]$ est dans le genre principal, $Q \equiv 1 \pmod 8$. Une classe ambiguë contient une forme $a = \pm [2P'Q',0,-P''Q'']$ avec

$$P'P'' = P_1 \quad , \quad Q'Q'' = Q \quad , \quad P' \text{ et } P'' > 0 .$$

On trouve alors, comme $\left(\frac{2P'P''}{Q''}\right) = 1$:

$$e_{2P}(a) = \left(\frac{2}{P''Q''}\right)\left(\frac{P''Q''}{P'}\right)\left(\frac{2P'Q'}{P''}\right) = \left(\frac{2}{Q''}\right)\left(\frac{Q''}{P'}\right)\left(\frac{Q'}{P''}\right) = \left(\frac{2}{Q''}\right)\left(\frac{P'}{Q''}\right)\left(\frac{Q'}{P''}\right)$$

$$= \left(\frac{P''}{Q''}\right)\left(\frac{Q'}{P''}\right) = \left(\frac{Q}{P''}\right) = 1 .$$

§ 4.- Evaluation du caractère e_V pour une forme d'ordre 8.

A partir d'ici nous supposons que $r_4 = r_8 = 1$. Nous démontrons ici les résultats les plus importants de ce travail.

Théorème 1 : Soit $m = PQ$ une décomposition de m telle que $Q \equiv 1 \pmod 4$ si $P \not\equiv 1 \pmod 8$. On suppose que la forme ambiguë $h = [P,0,-Q]$ est une puissance quatrième. Alors l'équation $Z^2 = PX^2 - QY^2$ a des solutions vérifiant (2.3). Pour toute telle solution, toute racine quatrième h'' de h vérifie

$$(4.1) \qquad e_p(h'') = \left(\frac{Z}{P}\right)_4 \left(\frac{2X'}{Z}\right) \quad \text{avec} \quad X' = \begin{cases} X & , \text{ si } X \text{ est impair,} \\ \frac{X}{2} & , \text{ si } X \text{ est pair.} \end{cases}$$

Remarque : Si X est pair alors $P \equiv 1 \pmod 8$, $Q \equiv 3 \pmod 4$.

Théorème 2 : Soit $m = -PQ$ où P et $Q > 0$, où tous les facteurs premiers de m sont congrus à 1 modulo 4 et où $PQ \equiv 1 \pmod 8$. On suppose que la forme $h = [P,0,Q]$ ou bien $h = \left[2P,2P,\frac{P+Q}{2}\right]$ est une puissance quatrième et l'on pose $A = 1$ dans le premier cas, $A = 2$ dans le deuxième.
Alors l'équation $AZ^2 = PX^2 + QY^2$ a des solutions satisfaisant à (2.3) et pour toute telle solution toute racine quatrième h'' de h vérifie

$$(4.2) \qquad e_2(h'') = e_{PQ}(h'') = \left(\frac{Z}{PQ}\right)_4 \left(\frac{2XY}{Z}\right) .$$

Démonstrations : Pour ces deux théorèmes nous allons montrer, sans faire d'hypothèse sur les valeurs de r_4 et de r_8 , qu'il existe une racine quatrième h'' de h satisfaisant à (4.1) ou (4.2). D'après [4], proposition 1, cela suffit pour démontrer les théorèmes 1 et 2.

Démonstration du théorème 1 :
a) Cas où $P \equiv 1 \pmod 4$. Posons $Y = 2^k Y_1$, $T = 2^n T_1$, $y = 2^{n'} y_1$, où $Y_1 \equiv T_1 \equiv y_1 \equiv 1 \pmod 2$.
Nous partons des deux équations

$$(4.3) \qquad Z^2 = PX^2 - QY^2 \quad ; \quad Zr^2 = PS^2 - QT^2 .$$

De la première de ces équations nous déduisons

$$1 = \left(\frac{Z}{P}\right) = \left(\frac{-Q}{P}\right)\left(\frac{Y}{P}\right) = \left(\frac{-Q}{P}\right)_4 \left(\frac{2}{P}\right)^k \left(\frac{Y_1}{P}\right) = \left(\frac{Q}{P}\right)_4 \left(\frac{2}{P}\right)^{k+1} .$$

Comme $P \equiv 1 \pmod 8$ si Q est pair on a $k = 1$ si X est impair et $P \equiv 5 \pmod 8$ donc :

(4.4) $$\left(\frac{Q}{P}\right)_4 = \varepsilon \quad \text{avec} \quad \varepsilon = 1 \quad \text{si} \quad X \quad \text{est impair,} \quad \varepsilon = \left(\frac{2}{P}\right) \quad \text{si} \quad X \quad \text{est pair.}$$

Ceci étant la deuxième équation (4.3) nous donne

(4.5) $$\left(\frac{r}{P}\right)\left(\frac{Z}{P}\right)_4 = \left(\frac{-Q}{P}\right)_4\left(\frac{T}{P}\right) = \varepsilon\left(\frac{2T}{P}\right) .$$

Appliquant la loi de réciprocité quadratique et les équations (2.12), (2.15), (2.19) il vient successivement

$$\left(\frac{2T}{P}\right) = \left(\frac{2}{P}\right)^{n+1}\left(\frac{T_1}{P}\right) = \left(\frac{2}{P}\right)^{n+1}\left(\frac{P}{T_1}\right) = \left(\frac{2}{P}\right)^{n+1}\left(\frac{Z}{T_1}\right) = \alpha\left(\frac{2}{P}\right)^{n+1}\left(\frac{T_1}{Z}\right) = \alpha\left(\frac{2}{P}\right)^{n+1}\left(\frac{2}{Z}\right)^{n}\left(\frac{T}{Z}\right)$$

$$= \alpha\left(\frac{2}{P}\right)^{n+1}\left(\frac{2}{Z}\right)^{n}\left(\frac{Yx}{Z}\right) = \alpha\left(\frac{2}{P}\right)^{n+1}\left(\frac{2}{Z}\right)^{n}\left(\frac{-2yX}{Z}\right) = \alpha\left(\frac{2}{P}\right)^{n+1}\left(\frac{2}{Z}\right)^{n+1}\left(\frac{-1}{|Z|}\right)\left(\frac{y}{Z}\right)\left(\frac{X}{Z}\right)$$

$$= \alpha\gamma\left(\frac{2}{P}\right)^{n+1}\left(\frac{2}{Z}\right)^{n+n'+1}\left(\frac{y_1}{Z}\right)\left(\frac{X}{Z}\right) = \alpha\beta\gamma\left(\frac{2}{P}\right)^{n+1}\left(\frac{2}{Z}\right)^{n+n'+1}\left(\frac{Z}{y_1}\right)\left(\frac{X}{Z}\right) .$$

Tenant compte de (2.7) et de (2.15) on obtient

(4.6) $$\left(\frac{r}{P}\right)\left(\frac{Z}{P}\right)_4 = \varepsilon\left(\frac{2}{P}\right)^{n+1}\left(\frac{2}{Z}\right)^{n+n'+1}\left(\frac{X}{Z}\right) .$$

Maintenant nous distinguons quatre cas suivant les parités de X et de T .

1) X <u>impair et</u> T <u>pair</u>, ce qui est toujours le cas si $Q \equiv 1$ ou $2 \pmod 4$
Ici $\varepsilon = 1$; de plus, si $\left(\frac{2}{Z}\right) \neq \left(\frac{2}{P}\right)$, où alors Q est impair, on a $n = 1$ et de plus, si $Z \equiv 5 \pmod 8$ les équations (4.3) montrent que $T \not\equiv Y \pmod 4$ donc, comme $T = Yx + \lambda Zy$, $y \equiv 2 \pmod 4$ et $n' = 1$.
Tenant compte de tout ceci on trouve

$$\left(\frac{r}{P}\right) = \left(\frac{Z}{P}\right)_4\left(\frac{2X}{Z}\right)$$

ce qui démontre le théorème 1 pour $P \equiv 1 \pmod 4$, $Q \equiv 1$ ou $2 \pmod 4$.

2) X <u>et</u> T <u>impairs</u>.
Ici $\varepsilon = 1$, $n = n' = 0$ donc on obtient

$$\left(\frac{r}{P}\right) = \left(\frac{Z}{P}\right)_4\left(\frac{2}{P}\right)\left(\frac{2X}{Z}\right) .$$

3) X pair et T impair.
Ici $\varepsilon = \left(\frac{2}{P}\right)$, $n = 0$, et comme μ et $S = Xx + \mu Zy$ sont pairs on voit que y est pair et que $S - X \equiv y \pmod 4$.
L'équation (4.6) s'écrit donc

$$\left(\frac{r}{P}\right)\left(\frac{Z}{P}\right)_4 = \left(\frac{2}{Z}\right)^{n'}\left(\frac{2X}{Z}\right) .$$

Les équations (4.3) nous donnent

$$Z - 1 \equiv P(S^2 - X^2) \pmod 8$$

ce qui montre que $n' = 1$ si, et seulement si $Z \equiv 5 \pmod 8$ donc

$$\left(\frac{r}{P}\right) = \left(\frac{Z}{P}\right)_4\left(\frac{X}{Z}\right) .$$

4) X et T pairs.
Ici $\varepsilon = \left(\frac{2}{P}\right)$, $n' = 0$, et la congruence $Z \equiv P - QT^2 \pmod 8$ montre que $\left(\frac{2}{Z}\right) \neq \left(\frac{2}{P}\right)$ si, et seulement si, $n = 1$. Donc

$$\left(\frac{r}{P}\right) = \left(\frac{Z}{P}\right)_4\left(\frac{2}{P}\right)^{n+2}\left(\frac{2}{Z}\right)^{n+2}\left(\frac{2X}{Z}\right) = \left(\frac{Z}{P}\right)_4\left(\frac{2}{P}\right)\left(\frac{X}{Z}\right)$$

ce qui démontre le théorème 1 dans le cas où $P \equiv 1 \pmod 8$, $Q \equiv 3 \pmod 4$.

b) Cas où $P = 2P'$ avec $P' \equiv 1 \pmod 4$, $Q \equiv 1 \pmod 4$.
Comme les formes $[2P',0,-Q]$ et $[Z,b,Zc]$ sont dans le genre principal on a $Z \equiv Q \equiv 1 \pmod 8$. Ici nous partons des deux équations

(4.7) $$Z^2 = 2P'X^2 - QY^2 \quad , \quad Zr^2 = 2P'S^2 - QT^2 .$$

Utilisant la première nous obtenons

$$1 = \left(\frac{Z}{P'}\right) = \left(\frac{-Q}{P'}\right)_4\left(\frac{Y}{P}\right) = \left(\frac{Q}{P'}\right)_4\left(\frac{2}{P'}\right)\left(\frac{2}{Y}\right) = \left(\frac{Q}{2P'}\right)_4$$

la dernière égalité étant la traduction de la congruence

$$1 \equiv 2P' - QY^2 \pmod{16} .$$

De même considérant la deuxième équation (4.7) modulo 16 et modulo P on a :

$$\left(\frac{2}{r}\right) = \left(\frac{Z}{2}\right)_4\left(\frac{2}{T}\right)\left(\frac{Q}{2}\right)_4\left(\frac{2}{P^r}\right) \quad ; \quad \left(\frac{r}{P^r}\right) = \left(\frac{Z}{P^r}\right)_4\left(\frac{-Q}{P^r}\right)_4\left(\frac{T}{P^r}\right)$$

d'où résulte, en multipliant et en appliquant la loi de réciprocité quadratique,

$$e_P(r) = \left(\frac{Z}{P}\right)_4\left(\frac{Q}{P}\right)_4\left(\frac{2}{T}\right)\left(\frac{T}{P^r}\right) = \left(\frac{Z}{P}\right)_4\left(\frac{P}{T}\right) .$$

Il nous reste à calculer $\left(\frac{P}{T}\right)$. On trouve successivement

$$\left(\frac{P}{T}\right) = \left(\frac{Z}{T}\right) = \alpha\left(\frac{T}{Z}\right) = \alpha\left(\frac{Yx}{Z}\right) = \alpha\left(\frac{-2yX}{Z}\right) = \alpha\gamma\left(\frac{yX}{Z}\right) = \alpha\gamma\left(\frac{y_1X}{Z}\right)$$

$$= \alpha\beta\gamma\left(\frac{X}{Z}\right) = \left(\frac{2X}{Z}\right)$$

ce qui montre que $e_P(r) = \left(\frac{Z}{P}\right)_4\left(\frac{2X}{Z}\right)$ et achève la démonstration du théorème 1.

Démonstration du théorème 2 :

Dans les deux cas nous obtenons l'équation (2.2) sous la forme

(4.8) $$AZ^2 = PX^2 + QY^2$$

où X, Y, Z satisfont aux conditions (2.3). En particulier Z est positif et $\equiv 1 \pmod 4$. Le nombre r satisfait à

(2.8) $$r^2 = Zx^2 + 2bxy + AZcy^2 ,$$

Ici nous multiplions par Z pour obtenir

(4.9) $$Zr^2 = S^2 + PQy^2 \quad \text{avec} \quad S = Zx + by .$$

Les nombres $S = 2^nS_1$ et $y = 2^ry_1$, où S_1 et y_1 sont impairs, sont de parités différentes, et on voit que $n + r = 1$ si, et seulement si, $Z \equiv 5 \pmod 8$. Calculons $e_2(r) = e_{PQ}(r)$. Utilisant la loi de réciprocité quadratique et les équations (4.9), (2.6) et (2.8) il vient successivement

$$e_{PQ}(r) \times \left(\frac{Z}{PQ}\right)_4 = \left(\frac{S}{PQ}\right) = \left(\frac{S_1}{PQ}\right) = \left(\frac{PQ}{S_1}\right) = \left(\frac{Z}{S_1}\right) = \left(\frac{S_1}{Z}\right) = \left(\frac{2}{Z}\right)^n\left(\frac{S}{Z}\right) = \left(\frac{2}{Z}\right)^n\left(\frac{by}{Z}\right)$$

$$= \left(\frac{2}{Z}\right)^n\left(\frac{bY^2y}{Z}\right) = \left(\frac{2}{Z}\right)^n\left(\frac{-pXYy}{Z}\right) = \left(\frac{2}{Z}\right)^{n+r}\left(\frac{XY}{Z}\right)\left(\frac{y_1}{Z}\right) = \left(\frac{2XY}{Z}\right)$$

ce qui achève de démontrer le théorème 2.

§ 5.- Applications aux corps quadratiques imaginaires.

Dans toute la suite de ce travail $p, p', \dots, p_1, p_2, \dots, p_i \dots$ désigneront des nombres premiers $\equiv 1 \pmod 4$, $q, q', \dots, q_1, q_2, \dots, q_i \dots$ des nombres premiers $\equiv 3 \pmod 4$.
Quand $m < 0$ nous poserons $m = -s$, avec $s > 0$.
Du théorème 1 nous déduisons le critère

Critère 1 : Soit $Q(\sqrt{-s})$ un corps quadratique imaginaire tel que $r_4 = r_8 = 1$ et tel que la forme ambiguë simple du genre principal soit $[P,0,Q]$, avec $PQ = s$, où $P > 0$ n'est divisible par aucun nombre premier congru à 3 modulo 4 et où $Q \equiv 1 \pmod 4$ si $P \not\equiv 1 \pmod 8$.
Alors l'équation $Z^2 = PX^2 + QY^2$ a des solutions où $(X,Y) = 1$ où $Z > 0$ donne la valeur 1 à tous les caractères génériques et où $Z \equiv 1 \pmod 4$. Pour toute telle solution

$$(5.1) \qquad r_{16} = 1 \Leftrightarrow \left(\frac{Z}{P}\right)_4 \left(\frac{2X'}{Z}\right)$$

où $X' = X$ si X est impair, $X' = \frac{X}{2}$ si X est pair.

Ce critère s'applique en particulier aux cas suivants :

α) $s = 2p_1 \dots p_n$ où $p_i \equiv 1 \pmod 4$,
où les p_i sont non résidus quadratiques les uns des autres et où $n = 1, 2$ où un nombre impair ≥ 3, avec $P = p_1 \dots p_n$, $Q = 2$ donc X est impair et $Z \equiv 1 \pmod 8$. On sait alors que $r_4 = 1$, et $r_8 = 1$ si, et seulement si, $\left(\frac{2}{P}\right)_4 = 1$. Si l'on remarque que $P = U^2 - 2V^2$ on retrouve le critère, démontré dans [6] pour le cas $n = 1$, à savoir :

$$(5.2) \qquad r_{16} = 1 \Leftrightarrow \left(\frac{U}{P}\right)_4 .$$

β) $s = 2p_1 \dots p_n q$ avec $p_i \equiv -q \equiv 1 \pmod 8$, $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_i}{q}\right) = -1$, et $n = 0$ (alors $s = 2q$), 1 ou un nombre pair. Alors $r_4 = 1$, $P = 2$, et on a $r_8 = 1$ si, et seulement si $\frac{s}{2} \equiv 1 \pmod{16}$. ([3], proposition B_9').
Le critère 1 donne une condition pour que $r_{16} = 1$, que l'on peut particulariser en remarquant que $\frac{s}{2} = U^2 - 2V^2$, où (cf. [6], p. 205) l'on peut choisir $U \equiv 1 \pmod{16}$, d'où le critère démontré pour $n = 0$ dans [6] :

$$r_{16} = 1 \Leftrightarrow \left(\frac{V}{U}\right) = 1 .$$

γ) $s = p_1 \dots p_n q$ avec $\left(\frac{q}{p_i}\right) = 1$, $\left(\frac{p_i}{p_j}\right) = -1$, $n = 1, 2$ ou un nombre impair.
Alors $r_4 = 1$, $P = p_1 \dots p_n$, $Q = -q \equiv 1 \pmod 4$, $r_8 = 1$ si, et seulement si $\left(\frac{-q}{p}\right)_4 = 1$ ([3], proposition B'_{18}), et critère 1 donne une condition pour que $r_{16} = 1$, qui est, pour le cas où $n = 1$ ($r_2 = 1$) , celle de [7].

Le critère 1 s'applique aussi à plusieurs cas où $r_2 = 2$, $r_4 = r_8 = 1$.

δ) $s = pp'$ ou $s = 2pp'$, $p \equiv 1$, $p' \equiv 5 \pmod 8$, $\left(\frac{p}{p'}\right) = 1$, $P = p$.
Les critères pour que $r_8 = 1$ sont les propositions B'_3 et B'_6 de [ ]. Dans le cas $s = pp'$ un calcul simple montre que, si $r_8 = 1$, $(-1)^X = -\left(\frac{p}{p'}\right)_4$, ce qui détermine la parité de X .

δ') $s = pp'q$ où exactement un des symboles de Legendre $\left(\frac{p}{q}\right)\left(\frac{p'}{q}\right), \left(\frac{p'}{p}\right)$ vaut -1 , et on a, respectivement $P = p', p, pp'$ (cf. [3], propositions B'_7 , B'_8)

$s = 2pq$ où $p \equiv 1$, $q \equiv 3 \pmod 8$, $\left(\frac{p}{q}\right) = 1$, $P = p$

$s = 2pq$ où $p \equiv 5$, $q \equiv -1 \pmod 8$, $\left(\frac{p}{q}\right) = 1$, $P = 2p$.

Du théorème 2 nous déduisons

Critère 2 : Soit $Q(\sqrt{-s})$ un corps quadratique imaginaire tel que $s \equiv 1 \pmod 8$, que tous les facteurs premiers de s soient congrus à 1 modulo 4 et tel que $r_4 = r_8 = 1$.
Alors exactement une des équations

$$AZ^2 = PX^2 + QY^2 \quad , \quad A = 1 \text{ ou } 2 \quad , \quad s = PQ$$

a des solutions X, Y, Z vérifiant (2.2) et, pour toute telle solution

$$r_{16} = 1 \Leftrightarrow \left(\frac{Z}{s}\right)_4 \left(\frac{2XY}{Z}\right) = 1 .$$

Ce critère s'applique aux cas suivants :

α_2) $s = p_1 \dots p_n$ où $p_i \equiv 1 \pmod 8$, $\left(\frac{p_i}{p_j}\right) = -1$, $n = 1, 2$ ou un nombre impair (cf. [3], propositions B'_2, B'_{16}), avec $A = 2$, $P = 1$, $Q = s$. Comme $s = 2g^2 - h^2$, on retrouve le critère de [6] pour $n = 1$, à savoir

$$r_{16} = 1 \Leftrightarrow \left(\frac{g}{s}\right)_4 \left(\frac{2h}{g}\right) .$$

δ_2) $s = pp'$ avec $p \equiv p' \equiv 5 \pmod 8$, avec $P = p$ et $A = 1$ ou 2 suivant que $\left(\frac{p}{p'}\right) = 1$ ou -1 (cf. [3], propositions B'_1, B'_4).

§ 6.- Application à des corps quadratiques réels.

Nous obtenons un critère général, correspondant au théorème B_1 de [3] :

Critère 3 : Soit $Q(\sqrt{m})$ un corps quadratique réel tel que le nombre m n'a pas de diviseur premier congru à 3 modulo 4 , et tel que $r_4 = r_8 = 1$. Alors il existe exactement une décomposition $m = PQ$ telle que les équations

$$Z^2 = PX^2 - QY^2 \quad , \quad Z'^2 = QX'^2 - PY'^2$$

aient des solutions vérifiant (2.3). Les nombres

$$\alpha = \left(\frac{Z}{P}\right)_4\left(\frac{2X}{Z}\right) \quad , \quad \beta = \left(\frac{Z'}{Q}\right)_4\left(\frac{2X'}{Z'}\right)$$

ne dépendent que de m et $r_{16} = 1$ si, et seulement si, $\alpha = \beta = 1$. Sinon P , Q ou -1 est facteur principal suivant que $(\alpha,\beta) = (1,-1)$, $(-1,1)$ ou $(-1,-1)$.

Ce critère inclut le cas où $r_2 = 1$ traité déjà dans [4]. Mais grâce au lemme 1, qui permet de travailler avec des nombres Z négatifs, nous avons pu le formuler et le démontrer de manière plus élégante. On peut vérifier directement que la formulation de [4] et le critère 3 sont équivalents.

Si le nombre m a des diviseurs premiers congrus à 3 modulo 4 nous ne pourrons trouver qu'un résultat partiel, car nous ne pouvons calculer qu'une seule des valeurs $e_V(h_i)$ $(i = 1,2,3)$. Nous allons traiter deux exemples.

Exemple 1 : $m = pq$, $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 4$, $\left(\frac{p}{q}\right) = 1$.
Ici on sait que $r_2 = 2$, $r_4 = 1$, et l'on peut prendre $h_1 = [p,0,-q]$, $h_2 = \left[2\varepsilon,2,\varepsilon\frac{1-pq}{2}\right]$ où $\varepsilon = \left(\frac{2}{q}\right)$. On connaît les conditions pour que $r_8 = 1$ (cf. [3], théorèmes B_3 et B_4).
Supposons que $r_8 = 1$. Alors, considérant h_1 , on voit que $V = p$ et que l'équation $Z^2 = pX^2 - qY^2$ a des solutions vérifiant (2.3) ; de plus on peut choisir X impair. En effet, considérant les formes de discriminant $-4q$ on voit que l'équation $pX_1^2 = Z_1^2 + qY_1^2$ a des solutions où X_1 est une puissance de p et $(X_1,Y_1) = 1$. Ceci montre que Z_1 est le premier coefficient d'une racine carrée de h_1 , donc, comme $r_8 = 1$, $e_p(Z_1) = 1$, donc $e_q(Z_1)$ $e_2(Z_1) = 1$,

et, comme ici $e_q(Z_1) = \left(\frac{Z_1}{q}\right)$ et $e_2(Z_1) = (-1)^{\frac{Z_1-1}{2}}$ changent de signe avec Z_1 on voit que, en choisissant convenablement le signe de Z_1 on peut supposer que X_1, Y_1, Z_1 satisfait à (2.3), et X_1 est impair. On trouve donc le résultat suivant :

Critère 4 : Soit $m = pq$ avec $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 4$ $\left(\frac{p}{q}\right) = 1$ tels que $r_8 = 1$. Alors l'équation $Z^2 = pX^2 - qY^2$ a des solutions satisfaisant à (2.3) où X est impair. Pour toute telle solution on a

$$r_{16} = 1 \text{ où } p \text{ est facteur principal} \Leftrightarrow \left(\frac{Z}{p}\right)_4 \left(\frac{2X}{Z}\right) = 1 .$$

Remarque 1 : Par voie analytique on peut obtenir ([5]) dans ce cas :

$r_{16} = 1$ ou p est facteur principal $\Leftrightarrow h(-pq) + h(-p) \equiv 0 \pmod{16}$

où $h(m)$ désigne le nombre des classes d'idéaux de $Q(\sqrt{m})$.

Cas $m = 2pq$ (cf. [3], théorèmes B_4 et B_5).
Procédant de la même manière on obtient le

Critère 5 : Soit $m = 2pq$ ou $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 4$, $\left(\frac{p}{q}\right) = 1$, d'où $r_4 = 1$. Supposons en outre $r_8 = 1$. Alors l'équation $Z^2 = pX^2 - 2qY^2$ a des solutions vérifiant (2.3) et, pour toute telle solution,

$$r_{16} = 1 \text{ où } p \text{ est facteur principal} \Leftrightarrow \left(\frac{Z}{p}\right)_4 \left(\frac{2X}{Z}\right) = 1 .$$

Remarque 2 : Les critères 4 et 5 s'appliquent aussi aux cas plus généraux $m = Pq$ et $m = 2Pq$ où P est produit de nombres premiers $p_i \equiv 1 \pmod 8$, non résidus quadratiques les uns des autres mais résidus quadratiques de q, et où le nombre n des p_i est $1, 2$ ou un nombre impair. Si $n > 1$ on ne peut pas montrer que l'équation $Z^2 = PX^2 - qY^2$ a des solutions vérifiant (2.2) où X est impair.

Bibliographie

[1] C.F. Gauss, Disquisitiones Arithmeticae.

[2] K. Hardy, P. Kaplan et K.S. Williams, Divisibilité par 16 du nombre des classes au sens strict des corps quadratiques réels dont le deux groupe des classes est cyclique. Osaka J. of Math., 23 (1986), à paraître.

[3] P. Kaplan,Sur le deux groupe des classes d'idéaux des corps quadratiques. Journal für die reine une angew. Math. 283/284 (1976), pp. 313-363.

[4] P. Kaplan,Cycles d'ordre au moins 16 dans le deux groupe des classes d'idéaux de certains corps quadratiques. Bull. Soc. Math. France, Mémoire 49-50 (1977), pp. 113-124.

[5] P. Kaplan et K.S. Williams, Congruences for the class numbers of the fields $Q(\sqrt{\pm pq})$ with p and q odd primes. Preprint.

[6] P.A. Leonard and K.S. Williams, On the divisibility of the class numbers of $Q(\sqrt{-p})$ and $Q(\sqrt{-2p})$ by 16. Canad. Math. Bull. 25 (1982), 200-206.

[7] P.A. Leonard and K.S. Williams, On the divisibility of $Q(\sqrt{-pq})$ by 16. Proceedings of the Edinburgh Mathematical Society 26 (1983), 221-231.