INFRASTRUCTURE DES CLASSES AMBIGES D'IDÉAUX DES ORDRES DES CORPS QUADRATIQUES RÉELS

Autor(en): **Halter-Koch, Franz / Kaplan, Pierre / Williams, Kenneth S. / Yamamoto, Yoshihiko**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **37 (1991)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **23.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-58743

L'Enseignement Mathématique, t. 37 (1991), p. 263-292

INFRASTRUCTURE DES CLASSES AMBIGES D'IDÉAUX DES ORDRES DES CORPS QUADRATIQUES RÉELS

par Franz HALTER-KOCH, Pierre KAPLAN, Kenneth S. WILLIAMS[1]) et Yoshihiko YAMAMOTO

§ 1. INTRODUCTION

Soit O_D un ordre d'un corps quadratique réel K, de discriminant D. Le nombre D est un entier rationnel positif non carré congru à 1 ou 0 modulo 4. Chaque classe primitive d'idéaux C de O_D contient un nombre fini $l = l(C)$ d'idéaux réduits primitifs, et ces idéaux peuvent être rangés en une période. Le but de ce travail est d'étudier la structure, ce que D. Shanks appelle «l'infrastructure» ([8]), de cette période dans le cas où la classe C est une classe ambige, c'est-à-dire égale à sa conjuguée $\bar{C}$. Les notions évoquées ci-dessus sont soit définies dans notre précédent travail [7], auquel nous renvoyons le lecteur pour les détails et les démonstrations des faits exposés dans l'introduction, soit seront définies plus bas.

Après avoir rappelé au § 2 les résultats classiques concernant les idéaux ambiges primitifs réduits, résultats connus depuis Gauss ([1]) dans le langage des formes quadratiques binaires, puis déterminé le produit de deux idéaux ambiges réduits (Proposition 2), nous introduisons au § 3 une notion nouvelle, celle d'idéal symétrique, idéal nécessairement réduit, associé à certaines décompositions de D en somme de deux carrés. Ensuite nous déterminons le produit de deux idéaux symétriques (Proposition 4). Ceci fait, au § 4, après avoir montré qu'une classe ambige contient un idéal ambige réduit et un idéal symétrique quand $N(\varepsilon_D) = -1$, soit deux idéaux ambiges réduits ou deux idéaux symétriques quand $N(\varepsilon_D) = +1$ (Théorème 1), nous pouvons comparer modulo 4 la longueur l de la période d'une classe ambige C avec la longueur l_0 de la période de la classe principale.

Nous montrons aussi comment cette méthode permet d'obtenir une troisième démonstration du résultat de [6] qui dit que les longueurs

[1]) Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

modulo 4 des périodes des classes principales de discriminants D et $4D$ pour $D \equiv 1 \pmod 4$ sont égales si, et seulement si, $\varepsilon_{4D} = \varepsilon_D^3$ (Théorème 0). Mais le résultat le plus élégant de ce travail nous semble être le fait, inclus dans les Théorèmes 2 et 3, qu'un certain idéal symétrique S' construit d'une manière simple à partir d'un idéal symétrique donné S est toujours principal quand $N(\varepsilon_D) = -1$, toujours équivalent à S quand $N(\varepsilon_D) = +1$.

Nous indiquons maintenant les notations et résultats que nous allons utiliser. Si $a_1, a_2, \ldots, a_k$ sont des nombres entiers rationnels, nous désignerons par $(a_1, \ldots, a_k)$ le plus grand diviseur commun de ces nombres. Si A est un anneau commutatif unitaire et $\alpha_1, \ldots, \alpha_m$ des éléments de A, nous désignons respectivement sur $[\alpha_1, \ldots, \alpha_m]$ $(m \geqslant 2)$ le $\mathbf{Z}$-module et par $\langle \alpha_1, \ldots, \alpha_m \rangle$ $(m \geqslant 1)$ l'idéal (A-module) engendré par $\alpha_1, \ldots, \alpha_m$. Si φ est un nombre réel, $[\varphi]$ désigne la partie entière de φ. Le produit des idéaux $I = \langle \alpha_1, \ldots, \alpha_m \rangle$ et $J = \langle \beta_1, \ldots, \beta_n \rangle$ est l'idéal $IJ = \langle \alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_m\beta_n \rangle$. Enfin $a \mid b$ (respectivement $a \nmid b$) signifie que l'entier rationnel a divise (respectivement ne divise pas) l'entier rationnel b.

D'après [7], Proposition 1, les idéaux non nuls de O_D sont les $\mathbf{Z}$-modules $d\left[a, \dfrac{b+\sqrt{D}}{2}\right]$ où $4a \mid D - b^2$, et l'idéal I est déterminé par $|d|$, $|a|$ et $b \pmod{2a}$. Le nombre $|d^2a|$ est la norme de l'idéal I et sera noté $N(I)$. Sauf mention explicite du contraire, nous supposerons toujours d et $a > 0$ dans l'écriture $I = d\left[a, \dfrac{b+\sqrt{D}}{2}\right]$.

L'idéal I est *primitif* si $d = \left(a, b, \dfrac{D-b^2}{4a}\right) = 1$. Si l'idéal I est primitif, son conjugué $\bar{I}$ est primitif et $I\bar{I} = N(I)$.

Deux idéaux I et J de O_D sont équivalents (noté $I \sim J$), si il existe deux nombres α et β non nuls de O_D tels que $\alpha I = \beta J$. Parmi les classes définies par cette relation d'équivalence, celles contenant des idéaux primitifs forment un groupe fini que nous noterons C_D.

Considérons maintenant les idéaux primitifs réduits. Soit $I = \left[a, \dfrac{b+\sqrt{D}}{2}\right]$ un idéal primitif. Posons $\dfrac{D-b^2}{4a} = c$. On peut aussi écrire $I = a[1, \varphi]$ avec $\varphi = \dfrac{b+\sqrt{D}}{2a}$, et φ est déterminé modulo 1. L'idéal I est *réduit* si l'on peut

choisir b modulo $2a$, ou φ modulo 1, de manière que les trois conditions équivalentes suivantes soient réalisées

$$\varphi > 1 , \quad -1 < \bar{\varphi} < 0 , \tag{1.1}$$

$$0 < \sqrt{D} - b < 2a < \sqrt{D} + b , \tag{1.2}$$

$$0 < \sqrt{D} - b < 2c < \sqrt{D} + b . \tag{1.3}$$

Si l'idéal I est réduit et b choisi de façon à satisfaire (1.1), et donc (1.2) et (1.3), nous écrirons

$$I \equiv \{c, b, a\} . \tag{1.4}$$

L'idéal $\tilde{I}$ est l'idéal $\tilde{I} = \left[c, \dfrac{b + \sqrt{D}}{2}\right] \equiv \{a, b, c\}$.

L'ensemble fini des idéaux primitifs réduits d'une classe C primitive a $l = l(C)$ éléments qui peuvent être rangés dans une suite périodique de la manière suivante:

Si $I \equiv \{c, b, a\}$, l'idéal suivant I est $I' \equiv \{a, b', c'\}$ où

$$q = \left[\frac{b + \sqrt{D}}{2a}\right] , \quad b + b' = 2aq , \quad c' = \frac{D - b'^2}{4a} . \tag{1.5}$$

Comme I est réduit, $q = \left[q + \dfrac{-b + \sqrt{D}}{2a}\right] = \left[\dfrac{b' + \sqrt{D}}{2a}\right]$ si bien que l'idéal I précédant I' est défini à partir de I' symétriquement par

$$q = \left[\frac{b' + \sqrt{D}}{2a}\right] , \quad b + b' = 2aq , \quad c = \frac{D - b^2}{4a} . \tag{1.6}$$

Partant d'un idéal primitif réduit $I_0 = \left[a_0, \dfrac{b_0 + \sqrt{D}}{2}\right] \equiv \{a_{-1}, b_0, a_0\}$ le n-ème itéré par le procédé (1.5) de I_0 sera noté $I_n = \left[a_n, \dfrac{b_n + \sqrt{D}}{2}\right]$ $\equiv \{a_{n-1}, b_n, a_n\}$, de telle sorte que la période de I_0 est formée des idéaux $I_0, I_1, \ldots, I_{l-1}$ et que, pour tout $k \in \mathbf{Z}$, $I_{n+kl} = I_n$. De plus, pour tout n on a d'après (1.1), (1.2), (1.3) et [7:(2.12) et (5.5)]

$$I_n = \frac{a_n}{a_0}\left(\prod_{i=1}^{n}\varphi_i\right) I_0\ , \quad \operatorname{sgn}\left(N\left(\prod_{i=1}^{n}\varphi_i\right)\right) = (-1)^n\ ,$$

(1.7)

$$\varphi_n > 1\ , \quad \frac{a_n}{a_{n-1}}\,\varphi_n > 1\ .$$

Dans tout ce travail nous poserons

$$\bar{D} = \begin{cases} D\ , & \text{si} \quad D \equiv 1 \pmod 4\ , \\ \dfrac{D}{4}\ , & \text{si} \quad D \equiv 0 \pmod 4\ . \end{cases} \tag{1.8}$$

§2. Idéaux ambiges, idéaux ambiges primitifs réduits

Définition 1. Un idéal *ambige* est un idéal égal à son conjugué.

Lemme 1. i) *Les idéaux ambiges sont les* $\mathbf{Z}$*-modules de l'un des types suivants:*

$$A_1 = d\left[a, \frac{\sqrt{D}}{2}\right] \quad \textit{avec} \quad 4a \mid D\ ,$$

$$A_2 = d\left[a, \frac{a+\sqrt{D}}{2}\right] \quad \textit{avec} \quad 4a \mid D - a^2\ .$$

ii) *Si* $D \equiv 1 \pmod 4$ *il n'y a pas d'idéal ambige de type* A_1.

Démonstration. Dire que $I = d\left[a, \dfrac{b+\sqrt{D}}{2}\right]$ est ambige signifie que $\left[a, \dfrac{b+\sqrt{D}}{2}\right] = \left[a, \dfrac{-b+\sqrt{D}}{2}\right]$, donc que $b \equiv 0 \pmod a$, et I est du type A_1 ou A_2 suivant que $\dfrac{b}{a}$ est pair ou impair, ce qui démontre i), et ii) est clair.

On prouve alors le résultat suivant (cf. Gauss [1], §257-259):

Proposition 1. *Les idéaux ambiges primitifs et ambiges primitifs réduits sont donnés par le tableau suivant, où* $\bar{D}$ *est défini par (1.8):*

Discriminant	*Idéaux primitifs ambiges*	*+ réduits*
$D \equiv 1 \pmod 4$	$\left[a, \dfrac{a+\sqrt{D}}{2}\right]$, $a \mid D$, $\left(a, \dfrac{D}{a}\right) = 1$	$a < \sqrt{D}$
$D \equiv 4 \pmod{16}$ $D \equiv 8, 16, 24 \pmod{32}$	$[a, \sqrt{\bar{D}}]$, $a \mid \bar{D}$, $\left(a, \dfrac{\bar{D}}{a}\right) = 1$	$a < \sqrt{\bar{D}}$
$D \equiv 12 \pmod{16}$	$[a, \sqrt{\bar{D}}]$, $a \mid \bar{D}$, $\left(a, \dfrac{\bar{D}}{a}\right) = 1$	$a < \sqrt{\bar{D}}$
	$[2a, a+\sqrt{\bar{D}}]$, $a \mid \bar{D}$, $\left(a, \dfrac{\bar{D}}{a}\right) = 1$	
$D \equiv 0 \pmod{32}$	$[a, \sqrt{\bar{D}}]$, $a \mid \bar{D}$, $\left(a, \dfrac{\bar{D}}{a}\right) = 1$	$a < \sqrt{\bar{D}}$
	$[4a, 2a+\sqrt{\bar{D}}]$, $a \mid \dfrac{\bar{D}}{4}$, $\left(a, \dfrac{\bar{D}}{4a}\right) = 1$	$a < \dfrac{\sqrt{\bar{D}}}{2}$

Démonstration. Nous cherchons d'abord les idéaux primitifs ambiges. Soit I un tel idéal.

Si $D \equiv 1 \pmod 4$, $I = \left[a, \dfrac{a+\sqrt{D}}{2}\right]$ où $a \equiv 1 \pmod 2$, $4a \mid D - a^2$ et $\left(a, \dfrac{D-a^2}{4a}\right) = 1$. Alors $a \mid D$ et $\left(a, \dfrac{D}{a} - a\right) = \left(a, \dfrac{D}{a}\right) = 1$. Inversement si $a \equiv 1 \pmod 2$, $a \mid D$ et $\left(a, \dfrac{D}{a}\right) = 1$, on voit que $4a \mid D - a^2$ et $\left(a, \dfrac{D-a^2}{4a}\right) = 1$.

Si $D \equiv 0 \pmod 4$, tous les $\mathbf{Z}$-modules $\left[a, \dfrac{\sqrt{D}}{2}\right]$ avec $a \mid \dfrac{D}{4}$ et $\left(a, \dfrac{D}{4a}\right) = 1$ conviennent. Cherchons si il y en a du type $A_2 = \left[a, \dfrac{a+\sqrt{D}}{2}\right]$. Alors a est

pair et l'entier positif $a' = \frac{a}{2}$ doit vérifier

$$2a' \mid \bar{D} - a'^2, \quad \left(2a', \frac{\bar{D} - a'^2}{2a'}\right) = 1 . \tag{2.1}$$

ce qui entraîne $a' \mid \bar{D}$.

Si $\bar{D} \equiv 1 \pmod 2$, alors $a' \equiv 1 \pmod 2$ et la deuxième relation ne peut être vérifiée que pour $\bar{D} \equiv 3 \pmod 4$, c'est-à-dire $D \equiv 12 \pmod{16}$. Alors

$$2a' \mid \bar{D} - a'^2 \Leftrightarrow a' \mid \bar{D}$$

et si ceci est vrai

$$\left(2a', \frac{\bar{D} - a'^2}{2a'}\right) = 1 \Leftrightarrow \left(2a', \frac{\bar{D}}{a'} - a'\right) = 2 \Leftrightarrow \left(a', \frac{\bar{D}}{a'} - a'\right) = 1$$
$$\Leftrightarrow \left(a', \frac{\bar{D}}{a'}\right) = 1 .$$

Ceci nous donne la liste des idéaux primitifs ambiges pour $D \equiv 4$ et $12 \pmod{16}$.

Il reste donc à étudier les cas où $D \equiv 0 \pmod 8$. Alors (2.1) implique $a' = 2a''$ d'où $\bar{D} = 4D''$ et s'écrit donc ici

$$a'' \mid D'' - a''^2, \left(4a'', \frac{D'' - a''^2}{a''}\right) = 1$$

qui équivaut à

$$a'' \mid D'', \quad \left(4a'', \frac{D''}{a''} - a''\right) = 1 . \tag{2.2}$$

Mais (2.2) implique que $\frac{D''}{a''} \not\equiv a'' \pmod 2$, donc $D'' \equiv 0 \pmod 2$, soit $D \equiv 0 \pmod{32}$, et alors (2.2) équivaut à

$$a'' | D'', \quad \left(a'', \frac{D''}{a''}\right) = 1 ,$$

ce qui achève la démonstration de la liste des idéaux primitifs ambiges.

Pour trouver ceux qui sont réduits nous utilisons le

LEMME 2. *L'idéal* $I = a[1, \psi]$ *est réduit si, et seulement si,* $\psi + [-\bar{\psi}] > 1$.

Démonstration. On peut remplacer ψ par $\varphi = \psi + [-\bar{\psi}]$ qui vérifie $0 < -\bar{\psi} - [-\bar{\psi}] < 1$, c'est-à-dire $-1 < \bar{\varphi} < 0$, donc l'idéal I est réduit si, et seulement si, $\varphi = \psi + [-\bar{\psi}] > 1$, ce qu'il fallait démontrer.

Ceci étant, on voit que

$$\left[a, \frac{\sqrt{D}}{2}\right] \text{ est réduit } \Leftrightarrow \frac{\sqrt{D}}{2a} + \left[\frac{\sqrt{D}}{2a}\right] > 1 \Leftrightarrow a < \frac{\sqrt{D}}{2}$$

et que

$$\left[a, \frac{a+\sqrt{D}}{2}\right] \text{ est réduit } \Leftrightarrow \frac{\sqrt{D}+a}{2a} + \left[\frac{\sqrt{D}-a}{2a}\right] > 1$$

$$\Leftrightarrow \frac{\sqrt{D}}{2a} + \left[\frac{\sqrt{D}}{2a} - \frac{1}{2}\right] > \frac{1}{2} \Leftrightarrow \frac{\sqrt{D}}{2a} > \frac{1}{2} \Leftrightarrow a < \sqrt{D}$$

ce qui achève de démontrer la Proposition 1.

COROLLAIRE 1. *Si* $D \not\equiv 0 \pmod{32}$, *un idéal ambige primitif est déterminé par sa norme.*

Démonstration. Dans la deuxième colonne du tableau de la Proposition 1 à des normes distinctes correspondent des idéaux distincts.

COROLLAIRE 2. *Si* $D \equiv 0 \pmod{32}$, *soient* $t \geqslant 3$ *et* Δ *les entiers définis par*

$$\bar{D} = 2^t\Delta\,, \qquad \Delta \equiv 1 \pmod 2\,.$$

Les idéaux primitifs ambiges et primitifs ambiges réduits sont donnés par le tableau suivant, où a *désigne un entier tel que*

$$a > 0\,, \qquad a \mid \Delta\,, \qquad \left(a, \frac{\Delta}{a}\right) = 1\,.$$

Type	*Idéaux ambiges primitifs*	*+ réduits*
1	$[a, \sqrt{\bar{D}}]$	$a < \sqrt{\bar{D}}$
2	$[2^t a, \sqrt{\bar{D}}]$	$2^t a < \sqrt{\bar{D}}$
3	$[4a, 2a + \sqrt{\bar{D}}]$	$2a < \sqrt{\bar{D}}$
4	$[2^t a, 2^{t-1}a + \sqrt{\bar{D}}]$	$2^{t-1}a < \sqrt{\bar{D}}$

Démonstration. Le Corollaire 2 est une conséquence immédiate de la Proposition 1, cas où $D \equiv 0 \pmod{32}$.

Nous aurons aussi besoin du résultat suivant:

LEMME 3. *Soit* $I_0 = \left[a_0, \frac{ka_0 + \sqrt{D}}{2}\right] \equiv \{a_{-1}, ka_0, a_0\}$ *un idéal ambige primitif réduit,* I_1 *l'idéal suivant* I_0 *dans sa période. Alors* $I_1 = \rho_1 I_0$ *avec*

$$\rho_1 = \frac{ka_0 + \sqrt{D}}{2a_0}, \qquad \frac{\sqrt{D}}{a_0} - 1 < \rho_1 < \frac{\sqrt{D}}{a_0}. \tag{2.3}$$

Si $I_0 = (1)$ *alors* $\sqrt{D} - 1 < \rho_1 < \sqrt{D}$.

Démonstration. D'après (1.7) $I_1 = \frac{a_1}{a_0} \frac{ka_0 + \sqrt{D}}{2a_1} I_0 = \frac{ka_0 + \sqrt{D}}{2a_0} I_0$ et, comme l'idéal I_0 est réduit, $-1 < \frac{ka_0 - \sqrt{D}}{2a_0} < 0$, donc $\rho_1 = \frac{ka_0 + \sqrt{D}}{2a_0}$ $= \frac{\sqrt{D}}{a_0} + \frac{ka_0 - \sqrt{D}}{2a_0}$ vérifie les inégalités (2.3). Pour achever de démontrer le Lemme 3 il suffit de noter que $a_0 = 1$ si $I_0 = (1)$.

Définition 2. La *norme réduite* $N'(I)$ d'un idéal ambige primitif I est le nombre a du tableau de la Proposition 1 si $D \not\equiv 0 \pmod{32}$ et du tableau du Corollaire 2 si $D \equiv 0 \pmod{32}$.

PROPOSITION 2. *Soit* $D \not\equiv 0 \pmod{32}$. *Soient* I_0 *et* I_1 *deux idéaux ambiges primitifs de normes réduites* D_0 *et* D_1 *respectivement.*

Il existe quatre entiers positifs d, d_0, d_1, d' *premiers entre eux deux à deux tels que*

$$\bar{D} = dd_0d_1d', \qquad D_0 = dd_0, \qquad D_1 = dd_1$$

et un nombre rationnel r *dépendant de* I_0 *et* I_1 *tel que l'idéal*

$$J = \begin{cases} rI_0I_1, & N'(J) = d_0d_1, \quad \text{si} \quad d_0d_1 < \sqrt{\bar{D}}, \\ r\sqrt{\bar{D}}I_0I_1, & N'(J) = dd', \quad \text{si} \quad d_0d_1 > \sqrt{\bar{D}}, \end{cases}$$

soit un idéal ambige primitif réduit.

L'idéal J *est égal à (1) si, et seulement si,* $I_0 = I_1$.

Démonstration. D'après la Proposition 1 et la Définition 2 on a

$$\bar{D} = D_0 D_0' = D_1 D_1' \quad \text{avec} \quad (D_0, D_0') = (D_1, D_1') = 1 .$$

Définissons d, d_0 et d_1 par

$$D_0 = d d_0 , \quad D_1 = d d_1 , \quad (d_0, d_1) = 1 .$$

On voit qu'il existe d' tel que $D_1' = d_0 d'$ d'où $D_0' = d_1 d'$ et donc

$$\bar{D} = d d_0 d_1 d' \quad \text{avec} \quad (d d_0, d_1 d') = (d d_1, d_0 d') = 1$$

ce qui prouve que les nombres d, d_0, d_1, d' sont premiers entre eux deux à deux.

Supposons d'abord $D \equiv 1 \pmod 4$. Alors $I_0 = \left[D_0, \dfrac{D_0 + \sqrt{D}}{2} \right]$, $I_1 = \left[D_1, \dfrac{D_1 + \sqrt{D}}{2} \right]$ et, effectuant le produit, on trouve

$$\frac{I_0 I_1}{d} = \left\langle d d_0 d_1 , \frac{d d_0 d_1 + d_1 \sqrt{D}}{2} , \frac{d d_0 d_1 + d_0 \sqrt{D}}{2} , \frac{d_0 d_1 \left(\dfrac{d + d'}{2} \right) + \left(\dfrac{d_0 + d_1}{2} \right) \sqrt{D}}{2} \right\rangle .$$

Comme $(d_0, d_1) = 1$ et $\dfrac{d_0 + d_1}{2} \equiv \dfrac{d + d'}{2} \pmod 2$ on voit que $\dfrac{I_0 I_1}{d}$ est un idéal ambige entier sans diviseur rationnel, et, comme tout nombre de $\dfrac{I_0 I_1}{d}$ s'écrit $\dfrac{k d_0 d_1 + l \sqrt{D}}{2}$ où $l, k \in \mathbf{Z}$, on voit que tout entier rationnel de $\dfrac{I_0 I_1}{d}$ est multiple de $d_0 d_1$.

D'autre part $d d_0 d_1$ et $\left(\dfrac{d - d'}{2} \right) d_0 d_1$ appartiennent à $\dfrac{I_0 I_1}{d}$, donc $N\left(\dfrac{I_0 I_1}{d} \right) = d_0 d_1$, ce qui, comme $(d_0 d_1, d d') = 1$, prouve par la Proposition 1 que $\dfrac{I_0 I_1}{d} = \left[d_0 d_1, \dfrac{d_0 d_1 + \sqrt{D}}{2} \right]$ et que $\dfrac{I_0 I_1}{d}$ est ambige et primitif.

Si $d_0 d_1 < \sqrt{D}$, $\dfrac{I_0 I_1}{d}$ est réduit donc on satisfait à la Proposition 2 en posant

$$J = \frac{I_0 I_1}{d} , \quad r = \frac{1}{d} .$$

Si $d_0 d_1 > \sqrt{D}$ on trouve par le même calcul

$$\left[d_0 d_1, \frac{d_0 d_1 + \sqrt{D}}{2}\right]\left[dd', \frac{dd' + \sqrt{D}}{2}\right] = \left[D, \frac{D + \sqrt{D}}{2}\right] = \sqrt{D}\,.$$

Multipliant par l'idéal primitif $\frac{I_0 I_1}{d}$ on obtient

$$\left[dd', \frac{dd' + \sqrt{D}}{2}\right] = \frac{\sqrt{D} I_0 I_1}{d d_0 d_1}$$

ce qui démontre la Proposition 2 avec $r = \frac{1}{d d_0 d_1}$, $J = \left[dd', \frac{dd' + \sqrt{D}}{2}\right]$.

Le cas où $D \equiv 0 \pmod 4$, quand les idéaux I_0 et I_1 sont du type A_1, est analogue, en plus simple, et on trouve le même résultat.

Si $D \equiv 12 \pmod{16}$ on trouve, par un calcul analogue, quand au moins un des idéaux I_0, I_1 est du type A_2,

$$\frac{1}{2d}\,[2D_0, D_0 + \sqrt{\bar{D}}]\,[2D_1, D_1 + \sqrt{\bar{D}}] = [d_0 d_1, \sqrt{\bar{D}}]\,,$$

d'où $r = \frac{1}{2d}$, $J = [d_0 d_1, \sqrt{\bar{D}}]$, si $d_0 d_1 < \sqrt{\bar{D}}$, et

$$\frac{1}{d}\,[2D_0, D_0 + \sqrt{\bar{D}}]\,[D_1, \sqrt{\bar{D}}] = [2d_0 d_1, d_0 d_1 + \sqrt{\bar{D}}]\,,$$

d'où $r = \frac{1}{d}$, $J = [2d_0 d_1, d_0 d_1 + \sqrt{\bar{D}}]$, si $d_0 d_1 < \sqrt{\bar{D}}$.

Puis, si $d_0 d_1 > \sqrt{\bar{D}}$, on obtient respectivement $r = \frac{1}{2d d_0 d_1}$, $J = [dd', \sqrt{\bar{D}}]$

et $r = \frac{1}{d d_0 d_1}$, $J = [2dd', dd' + \sqrt{\bar{D}}]$.

Ces calculs montrent que $J = (1)$ si, et seulement si, $d_0 = d_1 = 1$ et si les idéaux I_0 et I_1 sont de même type, donc si $I_0 = I_1$. Ceci achève de prouver la Proposition 2.

PROPOSITION 2'. *Soit* $D \equiv 0 \pmod{32}$, *et soient* t *et* Δ *les entiers définis au Corollaire 2.*

Soient I_0 *et* I_1 *deux idéaux ambiges primitifs de normes réduites* D_0 *et* D_1 *respectivement. Il existe quatre entiers positifs* d, d_0, d_1, d', *premiers*

entre eux deux à deux, tels que

$$\Delta = dd_0d_1d', \quad D_0 = dd_0, \quad D_1 = dd_1,$$

et un nombre rationnel r *dépendant de* I_0 *et* I_1 *tel que l'idéal* J *défini ci-dessous soit un idéal ambige primitif* réduit.

Types de I_0 *et* I_1 *(Corollaire 2)*	$J = rI_0I_1$	$J = r\sqrt{\bar{D}}I_0I_1$
du même type	$d_0d_1 < \sqrt{\bar{D}}$	$d_0d_1 > \sqrt{\bar{D}}$
1 *et* 2, 3 *et* 4	$2^td_0d_1 < \sqrt{\bar{D}}$	$2^td_0d_1 > \sqrt{\bar{D}}$
2 *et* 3, 1 *et* 4	$2^{t-1}d_0d_1 < \sqrt{\bar{D}}$	$2^{t-1}d_0d_1 > \sqrt{\bar{D}}$
1 *et* 3, 2 *et* 4	$2d_0d_1 < \sqrt{\bar{D}}$	$2d_0d_1 > \sqrt{\bar{D}}$

L'idéal J *est égal à (1) si, et seulement si,* $I_0 = I_1$.

Démonstration. La Proposition 2′ se démontre comme la Proposition 2. On calcule les produits d'idéaux primitifs ambiges réduits des dix différentes combinaisons de types en fonction des nombres d_0 et d_1. Si le produit obtenu n'est pas réduit, on le multiplie par l'idéal «complémentaire» pour obtenir un idéal réduit.

§3. IDÉAUX SYMÉTRIQUES

Définition 3. Soit $I = \left[a, \dfrac{b+\sqrt{D}}{2}\right]$ un idéal et $c = \dfrac{D-b^2}{4a}$. L'idéal I est *symétrique* si l'on peut choisir $b > 0$ dans sa classe modulo $2a$ de façon que $a = c$.

Définition 4. a) Une *représentation* de $\bar{D}$ comme somme de deux carrés est un couple (M, N) d'entiers > 0 tels que $(M, N) = 1, M^2 + N^2 = \bar{D}$ et $M \equiv 1 \pmod 2$.

b) Soit $\bar{D} = M^2 + N^2$ une représentation de $\bar{D}$. L'idéal symétrique primitif

$$S = \begin{cases} \left[\frac{N}{2}, \frac{M+\sqrt{D}}{2}\right], & \text{si} \quad D \equiv 1 \pmod 4, \\ [M, N+\sqrt{\bar{D}}], & \text{si} \quad D \equiv 0 \pmod 4, \end{cases}$$

est dit *associé* à la représentation (M, N) de $\bar{D}$.

PROPOSITION 3. i) *Tout idéal symétrique est réduit.*

ii) *Les idéaux symétriques primitifs sont les idéaux associés aux représentations de* $\bar{D}$.

Démonstration. i) On voit facilement que les relations $D = b^2 + 4a^2$, $a > 0, b > 0$ impliquent (1.2).

ii) Soit $I = \left[a, \frac{b+\sqrt{D}}{2}\right]$ un idéal symétrique. On a donc $D = b^2 + 4a^2$, $b > 0$, et I est primitif si, et seulement si, $(a, b) = 1$.

Si $D \equiv 1 \pmod 4$, b est impair donc $I = \left[\frac{N}{2}, \frac{M+\sqrt{D}}{2}\right]$ où $N = 2a$, $M = b$ et $(N, M) = (2a, b) = 1$. Inversement, si $D = M^2 + N^2$, $(M, N) = 1$ et $M \equiv 1 \pmod 2$, alors $\left[\frac{N}{2}, \frac{M+\sqrt{D}}{2}\right]$ est un idéal symétrique et primitif.

Si $D \equiv 0 \pmod 4$, b est pair, donc a impair et $\frac{D}{4} = M^2 + N^2$ avec $M = a \equiv 1 \pmod 2$ $N = \frac{b}{2}$, *et* $I = [M, N+\sqrt{\bar{D}}]$ avec $(M, N) = \left(a, \frac{b}{2}\right) = 1$.

Inversement si $\frac{D}{4} = M^2 + N^2$ avec $(M, N) = 1$, $M \equiv 1 \pmod 2$ alors $[M, N+\sqrt{\bar{D}}]$ est un idéal symétrique, et primitif car $(2N, M) = (N, M) = 1$.

Nous allons étudier les représentations de $\bar{D}$ dans les Lemmes 4 et 5 puis en déduire une propriété importante des idéaux symétriques associés.

LEMME 4. a) *Les discriminants* D *tels que l'anneau* O_D *contienne des idéaux symétriques primitifs sont les nombres* D *tels que*

(3.1) $\bar{D} = 2^s p_1^{s_1} \dots p_k^{s_k}$, $s = 0$ *ou* 1, p_i *premier* $\equiv 1 \pmod 4$.

b) *Soit* l *le nombre des diviseurs premiers distincts de* $\bar{D}$. *Le nombre des représentations de* $\bar{D}$ *comme somme de deux carrés est* 2^{l-1}.

c) *Le nombre des idéaux primitifs symétriques est* 2^{l-1}.

d) *Le nombre des idéaux ambiges primitifs réduits est* 2^{l-1}, *et la norme de tout tel idéal divise* $\bar{D}$.

Démonstration. D'après la Proposition 3 les nombres D sont les nombres tels que $\bar{D}$ est somme de deux carrés premiers entre eux, ce qui prouve (3.1). D'après [9], Satz 52, le nombre des décompositions de $\bar{D}$ en somme de deux carrés premiers entre eux est 2^{k-1}; chaque décomposition donne une représentation si $s = 0$ et deux représentations si $s = 1$, ce qui prouve b), et c) résulte de la Proposition 3, ii).

Comme $D \equiv 1 \pmod 4$ ou $D \equiv 4 \pmod{16}$ ou $D \equiv 8 \pmod{32}$, le tableau de la Proposition 1 montre d).

LEMME 5. *Soit* D *un discriminant tel que* $\bar{D}$ *soit représentable comme somme de deux carrés. Soit, d'une part,* $\bar{D} = M^2 + N^2$ *une représentation de* D *et, d'autre part, une décomposition* $\bar{D} = D_1 D_2$ *en deux facteurs* $D_1 > 0$ *et* $D_2 > 0$ *premiers entre eux. Alors il existe un couple* unique *de représentations* $D_1 = a_1^2 + b_1^2, D_2 = a_2^2 + b_2^2$ *et* un *signe* $\theta = \pm 1$ *tels que*

$$M = |a_1 a_2 - \theta b_1 b_2|, \quad N = |a_1 b_2 + \theta a_2 b_1|.$$

Démonstration. Nous supposerons D_1 impair. Soient l_1 et l_2 le nombre des diviseurs premiers de D_1 et D_2 respectivement. D'après le Lemme 4 le nombre des représentations de D_1 est 2^{l_1-1} celui de D_2 est 2^{l_2-1}. Prenant un couple de représentations $D_1 = a_1^2 + b_1^2, D_2 = a_2^2 + b_2^2$ et un signe $\theta = \pm 1$ nous obtenons

$$\bar{D} = |a_1 a_2 - \theta b_1 b_2|^2 + |a_2 b_1 + \theta a_1 b_2|^2 \tag{3.2}$$

de $2^{l_1-1+l_2-1+1} = 2^{l-1}$ manières différentes.

Pour démontrer le Lemme 5 il suffit de montrer que nous obtenons ainsi les 2^{l-1} représentations de $\bar{D}$, c'est-à-dire que nous avons bien des représentations de $\bar{D}$ au sens de la Définition 4 et qu'elles sont distinctes.

Comme $a_1 \equiv a_2 \equiv 1 \pmod 2$ et que $b_1 \equiv 0 \pmod 2$ on voit que $a_1 a_2 - \theta b_1 b_2$ est impair.

D'autre part, dans l'anneau $Z[i]$, on a

$$(a_1 + ib_1)(a_2 + i\theta b_2) = (a_1 a_2 - \theta b_1 b_2) + i(a_2 b_1 + \theta a_1 b_2). \tag{3.3}$$

Comme ni $a_1 + ib_1$, ni $a_2 + ib_2$ n'a de diviseur rationnel et que $(a_1^2 + b_1^2, a_2^2 + b_2^2) = 1$ on voit que $(a_1 a_2 - \theta b_1 b_2, a_2 b_1 + \theta a_1 b_2) = 1$, et donc que $M = |a_1 a_2 - \theta b_1 b_2|$, $N = |a_2 b_1 + \theta a_1 b_2|$ est une représentation de $\bar{D}$. Il

reste à démontrer que les 2^{l-1} représentations ainsi obtenues sont distinctes. Supposons donc que l'on ait

$$|a_1a_2 - \theta b_1b_2| = |a_1'a_2' - \theta' b_1'b_2'|, \quad |a_2b_1 + \theta a_1b_2| = |a_2'b_1' + \theta' a_1'b_2'|,$$

où (a_1', b_1') *et* (a_2', b_2') sont des représentations de D_1 et D_2 respectivement. Ceci signifie que l'une des quatre égalités suivantes est vraie:

$$(a_1 + ib_1)(a_2 + i\theta b_2) = \begin{cases} (a_1' + ib_1')(a_2' + i\theta' b_2') \\ -(a_1' + ib_1')(a_2' + i\theta' b_2') \\ (a_1' - ib_1')(a_2' - i\theta' b_2') \\ -(a_1' - ib_1')(a_2' - i\theta' b_2') \end{cases}$$

Les troisième et quatrième égalités ne peuvent pas être vérifiées car les deux membres n'ont pas les mêmes facteurs irréductibles dans $\mathbf{Z}[i]$. On voit donc que $a_1 + ib_1$ et $a_1' + ib_1'$ sont associés et, tenant compte des parités et des signes de a_1, b_1, a_1', b_1', on a $a_1 + ib_1 = a_1' + ib_1'$ d'où $a_2 + i\theta b_2 = \pm (a_2' + i\theta' b_2')$ ce qui, tenant compte des signes de a_2, b_2, a_2', b_2', montre que $\theta = \theta'$ et $a_2 + i\theta b_2 = a_2' + i\theta b_2'$, et achève la démonstration du Lemme 5.

Grâce à ce Lemme 5 nous pouvons obtenir le résultat le plus profond de ce travail:

PROPOSITION 4. *Soit* D *un discriminant tel que l'anneau* O_D *contienne des idéaux primitifs symétriques. Soit* $\bar{D} = M^2 + N^2$ *une représentation de* $\bar{D}$ *et* $\bar{D} = D_1D_2$ *une décomposition de* $\bar{D}$ *en deux facteurs premiers entre eux.*

Soient $D_1 = a^2 + b^2, D_2 = c^2 + d^2$ *et* $\theta = \pm 1$ *les représentations de* D_1 *et* D_2 *et le nombre* θ *bien déterminés par le Lemme 5 tels que* $M = |ac - \theta bd|, N = |ad + \theta bc|$. *Alors* $m = |ac + \theta bd|, n = |ad - \theta bc|$ *est une représentation de* $\bar{D}$, *et posant*

$$(3.4) \quad \begin{cases} I = \left[D_1, \dfrac{D_1 + \sqrt{D}}{2}\right], \quad S = \left[\dfrac{N}{2}, \dfrac{M + \sqrt{D}}{2}\right], \quad S' = \left[\dfrac{n}{2}, \dfrac{m + \sqrt{D}}{2}\right], \\ \quad si \quad D \equiv 1 \pmod 4, \\ I = [D_1, \sqrt{\bar{D}}], \quad S = [M, N + \sqrt{\bar{D}}], \quad S' = [m, n + \sqrt{\bar{D}}], \\ \quad si \quad D \equiv 0 \pmod 4 \end{cases}$$

on a

$$SS' = \left(\frac{\gamma}{D_1}\right) I \tag{3.5}$$

où γ *est un nombre de* O_D *qui vérifie*

$$\operatorname{sgn} N(\gamma) = \operatorname{sgn}(abD_2 - cdD_1)\,, \tag{3.6}$$

$$\begin{cases} \left(\dfrac{M+\sqrt{D}}{2}\right)\left(\dfrac{m+\sqrt{D}}{2}\right) = \dfrac{\gamma^2}{D_1}\,, & \text{si} \quad D \equiv 1 \pmod 4\,, \\ (N+\sqrt{D})\,(n+\sqrt{D}) = \dfrac{\gamma^2}{D_1}\,, & \text{si} \quad D \equiv 0 \pmod 4\,. \end{cases} \tag{3.7}$$

Démonstration. Supposons $D \equiv 1 \pmod 4$. Alors on voit que

$$4SS' = \begin{cases} [ad+bc,\, ac-bd+\sqrt{D}]\;[ad-bc,\, ac+bd+\sqrt{D}]\,, & \text{si } ac > bd\,, \\ [ad+bc,\, bd-ac+\sqrt{D}]\;[ad-bc,\, ac+bd+\sqrt{D}]\,, & \text{si } ac < bd\,. \end{cases} \tag{3.8}$$

Considérant d'abord le cas où $ac > bd$ on trouve

$$\begin{aligned} 4SS' = \langle\, & a^2d^2 - b^2c^2,\, (ad+bc)\,(ac+bd+\sqrt{D})\,, \\ & (ad-bc)\,(ac-bd+\sqrt{D}),\, a^2c^2 - b^2d^2 + D + 2ac\sqrt{D}\,\rangle\,. \end{aligned} \tag{3.9}$$

Posons

$$\gamma' = \frac{D_1 c + a\sqrt{D}}{2}\,, \quad \gamma'' = \frac{D_1 d + b\sqrt{D}}{2}\,, \quad \gamma', \gamma'' \in O_D\,. \tag{3.10}$$

On vérifie par un calcul aisé que

$$b^2c^2 - a^2d^2 = \frac{4N(\gamma')}{D_1}\,, \quad a^2d^2 - b^2c^2 = \frac{4N(\gamma'')}{D_1}\,, \tag{3.11}$$

$$\begin{aligned} a^2c^2 - b^2d^2 + D + 2ac\sqrt{D} &= \frac{4\gamma'^2}{D_1}\,, \\ b^2d^2 - a^2c^2 + D + 2bd\sqrt{D} &= \frac{4\gamma''^2}{D_1}\,, \end{aligned} \tag{3.12}$$

$$\begin{aligned} (ad+bc)\,(ac+bd+\sqrt{D}) &= \frac{4\gamma'\gamma''}{D_1}\,, \\ (ad-bc)\,(ac-bd+\sqrt{D}) &= \frac{4\gamma'\bar{\gamma}''}{D_1}\,, \end{aligned} \tag{3.13}$$

si bien que l'on a

$$SS' = \left(\frac{\gamma'}{D_1}\right) \langle \gamma', \bar{\gamma}', \gamma'', \bar{\gamma}'' \rangle \ . \tag{3.14}$$

Si $ac < bd$ il suffit de changer le rôle des paires (a, c) et (b, d) et l'on trouve

$$SS' = \left(\frac{\gamma''}{D_1}\right) \langle \gamma', \bar{\gamma}', \gamma'', \bar{\gamma}'' \rangle \ . \tag{3.15}$$

Considérons maintenant l'idéal entier ambige sans diviseur rationnel $J = \langle \gamma', \gamma'', \bar{\gamma}', \bar{\gamma}'' \rangle$.

La définition (3.10) de γ' et γ'' montre que tout nombre de J s'écrit $\dfrac{xD_1 + y\sqrt{D}}{2}$ où $x, y \in \mathbf{Z}$ avec $x \equiv y \pmod 2$, donc tout entier rationnel de J est multiple de D_1. D'autre part $\gamma' + \bar{\gamma}' = cD_1$ et $\gamma'' + \bar{\gamma}'' = dD_1$ appartiennent à J et aussi D_1, donc $N(J) = D_1$. Mais, d'après le Lemme 1, I est le seul idéal ambige sans diviseur rationnel de norme D_1, donc $J = I$.

On obtient (3.5) en posant $\gamma = \gamma'$ si $ac > bd$, $\gamma = \gamma''$ si $ac < bd$. Mais, d'après (3.11), on voit que

$$\operatorname{sgn} N(\gamma) = \begin{cases} \operatorname{sgn}(bc - ad) \ , & \text{si} \quad ac - bd > 0 \ , \\ \operatorname{sgn}(ad - bc) \ , & \text{si} \quad ac - bd < 0 \ , \end{cases}$$

ce qui signifie que

$$\operatorname{sgn} N(\gamma) = \operatorname{sgn}[(ac - bd)\,(bc - ad)] = \operatorname{sgn}(ab D_2 - cd D_1)$$

ce qui est (3.6), et (3.7) se voit en comparant (3.8) et (3.12), ce qui achève la démonstration quand $D \equiv 1 \pmod 4$.

Considérons maintenant le cas où $D \equiv 0 \pmod 4$. La démonstration de (3.14) et (3.15) est semblable, il suffit de supprimer le facteur 4 dans (3.8), de permuter c et d, de supprimer les facteurs 2 des dénominateurs de (3.10), et de remplacer D par $\bar{D}$ si bien que (3.14) et (3.15) sont vraies avec

$$\gamma' = D_1 d + a\sqrt{\bar{D}} \ , \quad \gamma'' = D_1 c + b\sqrt{\bar{D}} \ . \tag{3.16}$$

Ici aussi il faut montrer que $J = \langle \gamma', \gamma'', \bar{\gamma}', \bar{\gamma}'' \rangle$ est égal à I. On voit, comme plus haut, que tout entier rationnel de J est multiple de D_1, et aussi que $2cD_1$, $2dD_1$ et $(bd - ac)D_1$ sont dans J, ce qui, comme $(c, d) = 1$, $a \equiv c \equiv 1 \pmod 2$ et $bd \equiv 0 \pmod 2$ prouve que $N(J) = D_1$, et, d'après la Proposition 1, prouve que $J = I$. La démonstration de (3.6) et (3.7) est la même que celle pour le cas $D \equiv 1 \pmod 4$ ce qui achève la démonstration de la Proposition 4.

§4. CLASSES AMBIGES

Définition 5. Une classe C d'idéaux de O_D est *ambige* si elle est égale à sa conjuguée $\bar{C}$, c'est-à-dire si tout idéal I de C est équivalent à son conjugué $\bar{I}$.

PROPOSITION 5. *Les classes ambiges primitives sont les éléments d'ordre 2 du groupe C_D des classes primitives d'idéaux de O_D.*

Démonstration. D'après [7] (Proposition 2, Définitions 3 et 4) toute classe C du groupe C_D des classes primitives vérifie $C\bar{C} = 1$, donc $C^2 = 1$ si, et seulement si, $C = \bar{C}$, ce qu'il fallait démontrer.

PROPOSITION 6. *Une classe d'idéaux C de O_D est ambige si, et seulement si, sa période est formée de couples d'idéaux $I \equiv \{c, b, a\}$ et $\tilde{I} \equiv \{a, b, c\}$.*

Démonstration. Soit $I = \left[a, \frac{b + \sqrt{D}}{2}\right]$ un idéal, $c = \frac{D - b^2}{4a}$. On sait ([7], Corollary 2) que $\left[a, \frac{b + \sqrt{D}}{2}\right] \sim \left[c, \frac{-b + \sqrt{D}}{2}\right]$. Donc la classe de I est ambige si, et seulement si, $\left[a, \frac{b + \sqrt{D}}{2}\right] \sim \left[c, \frac{b + \sqrt{D}}{2}\right]$. La Proposition 6 s'obtient en considérant les idéaux réduits de C.

PROPOSITION 7. *La classe d'un idéal symétrique est ambige.*

Démonstration. Soit $S = \left[a, \frac{b + \sqrt{D}}{2}\right]$ un idéal symétrique où b est choisi de façon que $a = c$. D'après [7], Corollaire 2, on voit que $S \sim \left[a, \frac{-b + \sqrt{D}}{2}\right]$, ce qui prouve la Proposition 7.

THÉORÈME 1. *Soit C une classe ambige primitive de O_D dont la période contient l idéaux réduits primitifs.*

Si $N(\varepsilon_D) = -1$ le nombre l est impair et la période de C contient un *idéal ambige et* un *idéal symétrique. La numérotation des idéaux de la période de C peut être choisie de façon que ces idéaux soient respectivement I_0 (ambige) et $I_{\frac{l+1}{2}}$ (symétrique).*

Si $N(\varepsilon_D) = 1$ *le nombre* l *est pair et la période de* C *contient soit* deux *idéaux ambiges, soit* deux *idéaux symétriques. La numérotation des idéaux de la période de* C *peut être choisie de façon que ces deux idéaux soient* I_0 *et* $I_{\frac{l}{2}}$.

Démonstration. Nous considérons une classe ambige dont la période a pour longueur l, contenant les idéaux $I_0 \equiv \{c, b, a\}$ et $I_n \equiv \{a, b, c\}$. Nous distinguons le cas α) où n est impair ($n = 2m + 1$) et le cas β) où n est pair ($n = 2m$).

α) On a $I_0 \equiv \{c, b, a\}$, $I_{2m+1} \equiv \{a, b, c\}$.

Tenant compte de (1.5) et (1.6) on trouve que

$$I_m \equiv \{C, B, A\}\,, \qquad I_{m+1} \equiv \{A, B, C\}$$

ce qui prouve que $A \mid B$ et que $I_m = \left[A, \dfrac{B + \sqrt{D}}{2}\right]$ est un idéal ambige.

D'autre part

$$I_l = I_0 \equiv \{c, b, a\}\,, \qquad I_{2m+1} \equiv \{a, b, c\}\,.$$

Donc, pour tout $k \geqslant 0$

$$I_{l-k} \equiv \{P, Q, R\}\,, \qquad I_{2m+1+k} \equiv \{R, Q, P\}\,.$$

Si l *est impair,* l'équation $l - k = 2m + 1 + k$ admet pour solution $k = \dfrac{l-1}{2} - m$, et on voit que l'idéal $I_{l-k} = I_{m+\frac{l+1}{2}} \equiv \{P, Q, P\}$ est symétrique. Changeant la numérotation on voit que I_0 est ambige et $I_{\frac{l+1}{2}}$ symétrique.

Si l *est pair,* l'équation $l - k = 2m + 1 + k + 1$ admet pour solution $k = \dfrac{l}{2} - m - 1$, donc $I_{2m+k+1} = I_{m+\frac{l}{2}}$ est un idéal ambige. Donc, changeant la numérotation, I_0 et $I_{\frac{l}{2}}$ sont des idéaux ambiges.

β) On a

$$I_0 \equiv \{c, b, a\}\,, \qquad I_{2m} \equiv \{a, b, c\}\,.$$

Tenant compte de (1.5) et (1.6) on voit que I_m est un idéal symétrique.

En outre

$$I_0 = I_l \equiv \{c, b, a\}\ , \qquad I_{2m} \equiv \{a, b, c\}$$

donc, pour tout $k \geqslant 0$,

$$I_{l-k} = \{P, Q, R\}\ , \qquad I_{2m+k} = \{R, Q, P\}\ .$$

Si l est impair, l'équation $l - k = 2m + k + 1$ admet pour solution $k = \dfrac{l-1}{2} - m$ ce qui montre que l'idéal $I_{m+\frac{l-1}{2}}$ est ambige.

Changeant la numérotation on voit que I_0 est ambige et $I_{\frac{l+1}{2}}$ symétrique.

Si l est pair, l'équation $l - k = 2m + k$ admet pour solution $k = \dfrac{l}{2} - m$, donc l'idéal $I_{m+\frac{l}{2}}$ est symétrique. Donc, changeant la numérotation, on voit que I_0 et $I_{\frac{l}{2}}$ sont symétriques.

En résumé nous voyons que l'on peut choisir la numérotation dans la période pour que:

Si l est impair, I_0 est ambige, $I_{\frac{l+1}{2}}$ symétrique,

Si l est pair, I_0 et $I_{\frac{l}{2}}$ sont ambiges, ou bien symétriques.

Il reste à montrer que la période de C ne contient pas d'autre idéal ambige ou symétrique que ceux que nous venons de trouver.

Si $I_0 \equiv \{c, ka, a\}$ et $I_x \equiv \{C, KA, A\}$ $(0 < x < l)$ sont ambiges, on a $I_{x+1} \equiv \{A, KA, C\}$ et, d'après (1.5) et (1.6), on a $I_0 = I_{2x}$, donc $x = \dfrac{l}{2}$.

Si $I_0 \equiv \{c, ka, a\}$ est ambige et $I_x = \{A, B, A\}$ $(0 < x < l)$ est symétrique, on voit que $I_{x-k} = \tilde{I}_{x+k}$ $(k \geqslant 0)$, donc $I_0 = \tilde{I}_{2x}$, donc $I_1 = \tilde{I}_0 = I_{2x}$ et $I_0 = I_{2x-1}$, donc $x = \dfrac{l+1}{2}$.

Si $I_0 \equiv \{A, B, A\}$ et $I_x \equiv \{C, D, C\}$ sont symétriques $(0 < x < l)$, on voit que $I_0 = I_{2x}$ donc $x = \dfrac{l}{2}$.

Pour achever la démonstration du Théorème 1 il suffit de remarquer que $N(\varepsilon_D) = (-1)^l$.

COROLLAIRE 3. a) *Il existe des classes ambiges ne contenant pas d'idéal ambige si, et seulement si,* $N(\varepsilon_D) = +1$ *et* D *est somme de deux carrés premiers entre eux.*

b) *Le nombre de ces classes est égal à celui des classes ambiges contenant deux idéaux ambiges.*

Démonstration. Le Corollaire 3 est une conséquence immédiate du Théorème 1, de la Proposition 7 et du Lemme 4, c) et d).

Remarque. La méthode que nous avons utilisée pour établir le Théorème 1 est celle que Gauss utilise pour étudier les classes ambiges de formes quadratiques binaires ([1], § 187) et, dans le cas où $D = 4p$, p premier $\equiv 1 \pmod 4$, montrer que la période de la classe principale permet de décomposer p en somme de deux carrés car elle contient les formes symétriques $\pm ax^2 + 2bxy \mp ay^2$ où $p = a^2 + b^2$ avec $a \equiv 1 \pmod 2$ ([1], § 165).

Le Théorème 1 lui-même, exprimé dans le langage des formes quadratiques binaires, se trouve dans [4] (Théorème 1, p. 172).

Dans le cas où D n'a pas de diviseur carré, le Corollaire 3 a) est établi d'une autre manière dans [5] (Corollaire 1), et est équivalent au Satz 107 du Bericht de Hilbert ([2]).

Nous pouvons maintenant comparer modulo 4 la longueur de la période d'une classe ambige non principale avec la longueur de la période de la classe principale, en combinant le Théorème 1 avec les Propositions 2 et 4. Nous commençons par le cas où $N(\varepsilon_D) = -1$.

THÉORÈME 2. *Soit* D *un discriminant tel que* $N(\varepsilon_D) = -1$, l_0 *la longueur de la période la classe principale. Soit* C *une classe ambige primitive non principale d'idéal ambige* I *de norme* D_1 *tel que* $\bar{D} = D_1 D_2$, *et d'idéal symétrique* S *associé à la représentation* (M, N) *de* $\bar{D}$. *Soient* a, b, c, d *les entiers positifs et* S' *l'idéal symétrique définis à partir de* D_1, M *et* N *comme dans la Proposition 4, et soit* l *la longueur de la période de* C.

Alors l'idéal S' est principal, *et*

$$(4.1) \qquad \begin{cases} l \equiv l_0 \pmod 4, & \text{si} \quad cdD_1 - abD_2 > 0 \\ l \equiv l_0 + 2 \pmod 4, & \text{si} \quad cdD_1 - abD_2 < 0. \end{cases}$$

Démonstration. Comme les idéaux I et S sont équivalents, (3.5) montre que l'idéal S' est principal.

Plus précisément, posant $S = \alpha I$ avec $1 < \alpha \leqslant \varepsilon_D$, on voit que $S' = \left(\frac{\gamma}{\alpha D_1}\right)$. D'autre part soit α_0 tel que $S' = (\alpha_0)$ avec $1 < \alpha_0 \leqslant \varepsilon_D$. Le Lemme 3 montre que, en fait,

$$\sqrt{D} - 1 < \alpha_0 \leqslant \varepsilon_D .$$

Comme l'idéal ambige I est réduit et non principal on a $1 < D_1 < D_2$ (Proposition 1), ce qui entraîne $\sqrt{D_2} < \sqrt{D} - 1$ si $D \equiv 1 \pmod 4$ et $2\sqrt{D_2} < \sqrt{D} - 1$ si $D \equiv 0 \pmod 4$. Les définitions (3.10) et (3.15) de γ montrent que, comme $D_1 < D_2$, on a

$$\begin{cases} 1 < \dfrac{\gamma}{D_1} < \sqrt{D_2} , & \text{si} \quad D \equiv 1 \pmod 4 , \\ 1 < \dfrac{\gamma}{D_1} < 2\sqrt{D_2} , & \text{si} \quad D \equiv 0 \pmod 4 , \end{cases}$$

ce qui montre, comme $1 < \alpha \leqslant \varepsilon_D$, que

$$\frac{1}{\varepsilon_D} < \frac{\gamma}{\alpha D_1} < \sqrt{D} - 1 < \alpha_0 \leqslant \varepsilon_D .$$

Comme $\alpha_0 \equiv \dfrac{\gamma}{\alpha D_1} \pmod{\times \varepsilon_D}$ on voit que $\alpha_0 = \dfrac{\gamma \varepsilon_D}{\alpha D_1}$ et, comme $N(\varepsilon_D) = -1$,

$$\operatorname{sgn}(N(\alpha)) = -\operatorname{sgn}(N(\alpha_0))\operatorname{sgn}(N(\gamma))$$

ce qui, tenant compte de (1.7), (3.6) et du Théorème 1, prouve (4.1) et achève la démonstration du Théorème 2.

Nous considérons maintenant le cas où $N(\varepsilon_D) = +1$, et nous commençons par traiter le cas où $D \not\equiv 0 \pmod{32}$.

THÉORÈME 3. *Soit D un discriminant tel que $D \not\equiv 0 \pmod{32}$ et $N(\varepsilon_D) = +1$.*

a) *Soit C une classe ambige non principale primitive contenant deux idéaux ambiges I_0 et I_1 de normes réduites respectives D_0 et D_1 et soient d, d_0 et d_1 les nombres bien déterminés tels que*

$$D_0 = dd_0 , \quad D_1 = dd_1 , \quad (d_0, d_1) = 1 .$$

Alors

$$(4.2)\qquad \begin{cases} l \equiv l_0 \pmod 4\,, & \text{si} \quad d_0 d_1 < \sqrt{\bar{D}}\,, \\ l \equiv l_0 + 2 \pmod 4\,, & \text{si} \quad d_0 d_1 > \sqrt{\bar{D}}\,. \end{cases}$$

b) *Soit* I *l'idéal ambige réduit principal et* $\neq (1)$, *de norme* D_1', *et soit* $D_2' = \dfrac{\bar{D}}{D_1'}$. *Soit* C *une classe ambige non principale contenant les deux idéaux symétriques* S *et* S'. *Alors* S' *s'obtient à partir de* S *et* I *par (3.4). De plus*

$$(4.3)\qquad \begin{cases} l \equiv l_0 \pmod 4\,, & \text{si} \quad cdD_1' - abD_2' > 0\,, \\ l \equiv l_0 + 2 \pmod 4\,, & \text{si} \quad cdD_1' - abD_2' < 0\,. \end{cases}$$

Démonstration.

a) Nous appliquons la Proposition 2. Comme $I_0 \neq I_1$ et $I_0 \sim I_1$, on voit que l'idéal J est $\neq (1)$ et principal.

Posant $J = (\alpha_0)$ et $I_1 = \alpha I_0$, on trouve l'égalité d'idéaux:

$$(\alpha_0) = \begin{cases} (r\alpha N(I_0))\,, & \text{si} \quad d_0 d_1 < \sqrt{\bar{D}}\,, \\ (r\alpha N(I_0))\sqrt{\bar{D}}\,, & \text{si} \quad d_0 d_1 > \sqrt{\bar{D}}\,, \end{cases}$$

ce qui, compte tenu de ce que $N(\sqrt{\bar{D}}) = -\bar{D}$ et $N(\varepsilon_D) = +1$, prouve (4.2).

b) Posant $I = (\alpha_0)$ et $N(S) = s$, la relation (3.5) implique

$$S' = \frac{\gamma}{D_1' s}\,\alpha_0 \bar{S} = \frac{\gamma}{D_1' s^2}\,\alpha_0 \beta S$$

où, d'après [7] Corollary 2, $\beta = \dfrac{-M + \sqrt{D}}{2}$ ou $\beta = -N + \sqrt{\bar{D}}$ suivant que $D \equiv 1$ ou $D \equiv 0 \pmod 4$, et donc $N(\beta) < 0$. Ceci, compte tenu de ce que $N(\varepsilon_D) = +1$ et de (3.6), prouve (4.3) et achève la démonstration du Théorème 3.

Nous pouvons maintenant donner le résultat dont l'observation a été le point de départ de ce travail.

COROLLAIRE 4. *Soit* $D = 8q$, *où* $q = p^s$ *avec* p *premier* $\equiv 1 \pmod 4$ *et* $s \geqslant 1$. *Il y a deux classes ambiges, la classe principale* C_0 *et une autre* C, *et les longueurs de leurs périodes vérifient*

$$(4.4)\qquad l \equiv l_0 + 2 \pmod 4\,.$$

Démonstration. Les idéaux ambiges primitifs réduits sont (1) et $[2, \sqrt{2q}]$ donc, avec les notations du Théorème 1 si $N(\varepsilon_D) = -1$ et du Théorème 2 si $N(\varepsilon_D) = +1$, on a $D_1 = 2 = 1^2 + 1^2$ et $D_2 = q = c^2 + d^2$ où c et $d > 0$ sont bien définis par $c \equiv 1 \pmod 2$, si bien que ici

$$cdD_1 - abD_2 = 2cd - (c^2 + d^2) = -(c-d)^2 < 0$$

ce qui, tenant compte de (4.1) si $N(\varepsilon_D) = -1$ et de (4.3) si $N(\varepsilon_D) = +1$ prouve (4.4).

Maintenant nous étudions le cas où $D \equiv 0 \pmod{32}$.

THÉORÈME 4. *Soit D un discriminant tel que $D \equiv 0 \pmod{32}$. Soit C une classe ambige non principale primitive contenant deux idéaux ambiges I_0 et I_1 de normes réduites respectives D_0 et D_1 et soient d, d_0 et d_1 les nombres bien déterminés tels que*

$$D_0 = dd_0\,, \quad D_1 = dd_1\,, \quad (d_0, d_1) = 1\,.$$

Alors les classes modulo 4 de l et l_0 vérifient

Types de I_0 et I_1 (Corollaire 2)	$l \equiv l_0 \pmod 4$	$l \equiv l_0 + 2 \pmod 4$
du même type	$d_0 d_1 < \sqrt{D}$	$d_0 d_1 > \sqrt{D}$
1 *et* 2, 3 *et* 4	$2^t d_0 d_1 < \sqrt{D}$	$2^t d_0 d_1 > \sqrt{D}$
2 *et* 3, 1 *et* 4	$2^{t-1} d_0 d_1 < \sqrt{D}$	$2^{t-1} d_0 d_1 > \sqrt{D}$
1 *et* 3, 2 *et* 4	$2 d_0 d_1 < \sqrt{D}$	$2 d_0 d_1 > \sqrt{D}$

Démonstration. La démonstration du Théorème 4 est semblable à la démonstration du Théorème 3, a).

COROLLAIRE 5. *Soit $D = 2^{t+2}q$ avec $t \geqslant 3, q = p^s, p$ premier impair, $s \geqslant 1$. Il y a deux classes ambiges, la classe principale C_0 et une autre C. On a*

(4.5) $\qquad l \equiv l_0 \pmod 4\,, \quad si \quad q < 2^{t-2} \quad ou\ si \quad q > 2^t\,.$

(4.6) $\qquad l \equiv l_0 + 2 \pmod 4\,, \quad si \quad 2^{t-2} < q < 2^t\,.$

Démonstration. Le Corollaire 2 montre qu'il y a trois idéaux ambiges primitifs réduits non principaux.

Si $2^{t-2} < q < 2^t$ le Corollaire 2 montre que ces idéaux sont $[q, \sqrt{D}]$, $[4, 2+\sqrt{D}]$ et $[2^t, 2^{t-1}+\sqrt{D}]$. Pour toute combinaison de deux de ces idéaux on vérifie facilement que c'est la condition pour que $l \equiv l_0 + 2 \pmod 4$ du Théorème 4 qui est vérifiée, ce qui prouve (4.6). La démonstration de (4.5) est analogue.

Remarque. Si $D = 32q$ $(t = 3)$, (4.5) est vrai pour $q > 8$ et (4.6) pour $q = 3, 5, 7$.

Exemple 1 (Corollaire 4).

$$D = 40 = 8 \times 5\,, \qquad N(\varepsilon_D) = -1\,, \qquad l_0 = 1\,, \qquad l = 3$$
$$D = 136 = 8 \times 17\,, \qquad N(\varepsilon_D) = +1\,, \qquad l_0 = 4\,, \qquad l = 6\,.$$

Pour terminer cette section nous donnons deux exemples numériques, l'un du Théorème 2 où $N(\varepsilon_D) = -1$ et l'autre du Théorème 3 où $N(\varepsilon_D) = +1$.

Exemple 2 (Théorème 2).

$$D = 12325 = 25 \times 17 \times 29\,, \qquad N(\varepsilon_D) = -1\,.$$

Il y a quatre classes ambiges, C_0 (principale), C_1, C_2 et C_3 et nous donnons pour chacune l'idéal ambige réduit, l'idéal symétrique et la longueur, obtenus par réduction ([7], § 5).

$$C_0 : \left[1, \frac{111+\sqrt{D}}{2}\right] \sim \left[1, \frac{111+\sqrt{D}}{2}\right]; \qquad l_0 = 1\,.$$

$$C_1 : \left[17, \frac{85+\sqrt{D}}{2}\right] \sim \left[27, \frac{97+\sqrt{D}}{2}\right]; \qquad l_1 = 5\,.$$

$$C_2 : \left[25, \frac{75+\sqrt{D}}{2}\right] \sim \left[53, \frac{33+\sqrt{D}}{2}\right]; \qquad l_2 = 7\,.$$

$$C_3 : \left[29, \frac{87+\sqrt{D}}{2}\right] \sim \left[39, \frac{79+\sqrt{D}}{2}\right]; \qquad l_3 = 5\,.$$

Nous vérifions le Théorème 2 pour la classe C_2.

$$D_1 = 25 = 3^2 + 4^2\,, \qquad D_2 = 17.29 = 13^2 + 18^2 = 3^2 + 22^2\,.$$

On trouve que $33 = 4.18 - 3.13$. Donc $a = 3$, $b = 4$, $c = 13$, $d = 18$. Ensuite, changeant le signe, on trouve $4.18 + 3.13 = 111$, ce qui montre que $S' = \left[1, \frac{111+\sqrt{D}}{2}\right] \in C_0$. Enfin

$$cdD_1 - abD_2 = 13.18.25 - 3.4.17.29 = -66 < 0$$

donc $l_2 \equiv l_0 + 2 \pmod 4$, ce qui est vrai.

Exemple 3 (Théorème 3):

$$D = 5525 = 25.13.17\,, \quad N(\varepsilon_D) = +1\,.$$

Les quatre idéaux ambiges réduits se répartissent dans les deux classes C_0 (principale) et C_1 ainsi

$$C_0 : \left[1, \frac{73 + \sqrt{D}}{2}\right] \sim \left[25, \frac{25 + \sqrt{D}}{2}\right]; \quad l_0 = 4\,.$$

$$C_1 : \left[13, \frac{65 + \sqrt{D}}{2}\right] \sim \left[17, \frac{51 + \sqrt{D}}{2}\right]; \quad l_1 = 6\,.$$

Vérifions le Théorème 3 a) pour C_1. On a $D_0 = 13$, $D_1 = 17$, donc $d_0 = 13$, $d_1 = 17$ et $d_0 d_1 > \sqrt{D}$ donc $l_1 \equiv l_0 + 2 \pmod 4$, ce qui est vrai.

Vérifions le Théorème 3 b). On a

$$D_1' = 25 = 3^2 + 4^2\,, \quad D_2' = 13.17 = 11^2 + 10^2 = 5^2 + 14^2\,,$$
$$D = 41^2 + 62^2 = 73^2 + 14^2 = 71^2 + 22^2 = 7^2 + 74^2\,,$$

et on trouve deux classes ambiges contenant les idéaux symétriques:

$$C_2 : \left[37, \frac{7 + \sqrt{D}}{2}\right] \sim \left[7, \frac{73 + \sqrt{D}}{2}\right]; \quad l_2 = 4\,.$$

$$C_3 : \left[31, \frac{41 + \sqrt{D}}{2}\right] \sim \left[11, \frac{71 + \sqrt{D}}{2}\right]; \quad l_3 = 6\,.$$

On a donc $a = 3$, $b = 4$.

Pour la classe C_2, $7 = 4.10 - 3.11$ et $73 = 4.10 + 3.11$, donc $c = 11$, $d = 10$ et

$$cdD_1' - abD_2' = 11.10.25 - 3.4.13.17 = 98 > 0$$

donc $l_2 \equiv l_0 \pmod 4$, ce qui est vrai.

Pour la classe C_3, $41 = 4.14 - 3.5$, $71 = 4.14 + 3.5$, donc $c = 5$, $d = 14$ et

$$cdD_1' - abD_2' = 5.14.25 - 3.4.13.17 = -902 < 0$$

donc $l_3 \equiv l_0 + 2 \pmod 4$, ce qui est vrai.

§5. Troisième démonstration du Théorème 0 ([6], [3]).

Cette démonstration n'utilise pas les Propositions 2 et 4. En revanche nous aurons besoin de la Proposition suivante, qui est une conséquence immédiate des résultats de [7] et du Théorème 1.

Proposition 7. *Soit D un discriminant tel que $N(\varepsilon_D) = -1$, C une classe ambige primitive dont l'idéal ambige réduit est I de norme D_1 et dont l'idéal symétrique est $S = \left[R, \frac{Q+\sqrt{D}}{2}\right]$, et soit $\alpha \in K^\times$ tel que*

$$S = \alpha I, \quad 1 < \alpha \leqslant \varepsilon_D . \tag{5.1}$$

Alors

$$\varepsilon_D \left(\frac{Q+\sqrt{D}}{2}\right) = \alpha^2 D_1 . \tag{5.2}$$

Démonstration. Soit P la période de C. Nous utilisons les notations du Théorème 1 et de [7], (5.3) à (5.5), et numérotons les idéaux de P de manière que $I = I_0 \equiv \{a_{-1}, b_0, a_0\}$, $S = I_\lambda \equiv \{a_{\lambda-1}, b_\lambda, a_\lambda\}$ avec $a_{\lambda-1} = a_\lambda$. D'après [7], (6.4) et (5.3) nous avons

$$\varepsilon_D = \varphi_1 \dots \varphi_{\lambda-1}\varphi_\lambda\varphi_{\lambda+1} \dots \varphi_l , \quad l = 2\lambda - 1 , \tag{5.3}$$

où

$$\varphi_k = \frac{b_k + \sqrt{D}}{2a_k} \quad (k \in \mathbf{Z}) .$$

Comme I_λ est un idéal symétrique on a $b_{\lambda+k} = b_{\lambda-k}$ et $a_{\lambda-1-k} = a_{\lambda+k}$ pour tout $k \in \mathbf{Z}$ si bien que

$$\varphi_{\lambda+k} = \varphi_{\lambda-k} \frac{a_{\lambda-k}}{a_{\lambda-k-1}} . \tag{5.4}$$

Utilisant (5.4) pour $k = 1, \dots, \lambda - 1$ dans (5.3) on trouve, comme $a_\lambda = a_{\lambda-1}$,

$$\varepsilon_D = (\varphi_1 \dots \varphi_{\lambda-1})^2 \varphi_\lambda \frac{a_\lambda}{a_0} . \tag{5.5}$$

D'après [7], (5.5) et Proposition 8, $\alpha = \frac{a_\lambda}{a_0}\varphi_1 \dots \varphi_\lambda$ vérifie (5.1), si bien que (5.5) s'écrit $\varepsilon_D \varphi_\lambda = \alpha^2 \frac{a_0}{a_\lambda}$, ce qui, comme $a_\lambda \varphi_\lambda = \frac{Q + \sqrt{D}}{2}$ et $a_0 = D_1$ prouve (5.2).

Nous considérons maintenant un discriminant $D \equiv 1 \pmod 4$ tel que $N(\varepsilon_D) = -1$. On sait que, suivant le cas, $\varepsilon_{4D} = \varepsilon_D$ ou ε_D^3. D'autre part il existe un homomorphisme θ du groupe C_{4D} sur le groupe C_D ([7], Theorem 1) qui envoie la classe de l'idéal primitif $[a, b + \sqrt{D}]$, où $ab \equiv 1 \pmod 2$, sur la classe de $\left[a, \frac{b + \sqrt{D}}{2}\right]$. Avec ces notations nous avons

THÉORÈME 0 ([6], Theorem, [3], Theorem 5). *Soit* $D \equiv 1 \pmod 4$ *un discriminant tel que* $N(\varepsilon_D) = -1$, C *une classe ambige primitive de discriminant* $4D$. *Soit* l *la longueur de la période de* C *et* l' *celle de la période de* $\theta(C)$. *Alors*

$$l \equiv l' \pmod 4, \quad \text{si} \quad \varepsilon_{4D} = \varepsilon_D^3,$$
$$l \equiv l' + 2 \pmod 4, \quad \text{si} \quad \varepsilon_{4D} = \varepsilon_D.$$

Démonstration. Nous considérons une classe primitive ambige C de O_{4D} et son image $\theta(C)$ par l'homomorphisme θ de C_{4D} sur C_D.

La période de C contient l'idéal ambige $I_0 = [a, \sqrt{D}]$ où, d'après la Proposition 1, $a \equiv 1 \pmod 2$, $a \mid D$ et $a < \sqrt{D}$. Comme $I_0 = [a, a + \sqrt{D}]$ la classe $\theta(C)$ contient l'idéal $J_0 = \left[a, \frac{a + \sqrt{D}}{2}\right]$, qui est ambige et réduit car $a \mid D$ et $a < \sqrt{D}$. L'idéal J_0 est donc l'idéal ambige réduit de $\theta(C)$.

D'autre part la période de C contient l'idéal symétrique $I_\lambda = [M, N + \sqrt{D}]$ où $D = M^2 + N^2$ avec $M \equiv 1 \pmod 2$ et $(M, N) = 1$. On voit que $I_\lambda = [M, (M+N) + \sqrt{D}]$ et, comme $M + N \equiv 1 \pmod 2$, l'idéal $J = \left[M, \frac{M + N + \sqrt{D}}{2}\right]$ est un idéal de $\theta(C)$. Or on a

$$\frac{D - (M+N)^2}{4M} = \frac{M^2 + N^2 - (M+N)^2}{4M} = -\frac{N}{2}.$$

Donc, d'après [7], Corollary 2,

$$J \sim \left[-\frac{N}{2}, \frac{-M-N+\sqrt{D}}{2}\right] = \left[\frac{N}{2}, \frac{-M+\sqrt{D}}{2}\right].$$

Mais, comme $\theta(C)$ est une classe ambige, $J \sim \left[\frac{N}{2}, \frac{M+\sqrt{D}}{2}\right]$, donc l'idéal $\left[\frac{N}{2}, \frac{M+\sqrt{D}}{2}\right]$ est l'idéal symétrique J_μ de $\theta(C)$.

Posant $I_\lambda = \alpha I_0$ avec $1 < \alpha \leqslant \varepsilon_{4D}$ et $J_\mu = \beta J_0$ avec $1 < \beta \leqslant \varepsilon_D$ nous trouvons d'après (5.2)

$$\varepsilon_D \varepsilon_{4D} \left(\frac{M+\sqrt{D}}{2}\right)(N+\sqrt{D}) = a^2\alpha^2\beta^2 .$$

Notant que $\varepsilon_{4D} = \varepsilon_D$ ou ε_D^3 et que

$$\left(\frac{M+\sqrt{D}}{2}\right)(N+\sqrt{D}) = \left(\frac{M+N+\sqrt{D}}{2}\right)^2 \tag{5.6}$$

nous obtenons, en prenant la racine carrée de nombres réels positifs,

$$a\alpha\beta = \begin{cases} \varepsilon_D^2 \left(\dfrac{M+N+\sqrt{D}}{2}\right), & \text{si} \quad \varepsilon_{4D} = \varepsilon_D^3 , \\ \varepsilon_D \left(\dfrac{M+N+\sqrt{D}}{2}\right), & \text{si} \quad \varepsilon_{4D} = \varepsilon_D . \end{cases}$$

Comme la norme $N\left(\frac{M+N+\sqrt{D}}{2}\right) = \frac{MN}{2} > 0$ et $N(\varepsilon_D) = -1$ on voit que $N(\alpha\beta) > 0$, c'est-à-dire $\lambda \equiv \mu \pmod 2$, si, et seulement si, $\varepsilon_{4D} = \varepsilon_D^3$, ce qui démontre le Théorème 0.

Remarque. Ce qui, dans cette démonstration, joue le rôle de la Proposition 4 est l'égalité (5.6).

On peut démontrer de manière analogue (4.1) à partir de (3.7) et (5.2), sans utiliser (3.5), *après* avoir montré que S' est principal de la manière suivante:

Nous supposons $D \equiv 0 \pmod 4$, le cas $D \equiv 1 \pmod 4$ est analogue. Avec les notations de la Proposition 4 et du Théorème 2 on écrit (5.2) pour la classe C et pour la classe principale respectivement.

$$\varepsilon_D(N+\sqrt{D}) = \alpha^2 D_1$$

et $$\varepsilon_D(n + \sqrt{D}) = \alpha_0^2 .$$

Multipliant et tenant compte de (3.7) on obtient

(5.7) $$\varepsilon_D^2 \frac{\gamma^2}{D_1} = \alpha^2 \alpha_0^2 D_1 .$$

Comme tous les nombres intervenant dans (5.7) sont positifs, on a

$$\varepsilon_D \gamma = \alpha \alpha_0 D_1$$

ce qui, au vu de (3.6), donne (4.1) en comparant les signes des normes des deux membres.

Remerciements. Les auteurs remercient le Professeur Hideo Wada (Université Sophia, Tokyo, Japon) pour ses remarques qui leur ont permis de parfaire leur texte.

BIBLIOGRAPHIE

[1] GAUSS, C.F. *Disquisitiones Arithmeticae.* Traduction française, Librairie Blanchard (1979). Traduction allemande dans *Untersuchungen über höhere Arithmetik,* Chelsea Publishing Co., New York (1965).

[2] HILBERT, D. *Die Theorie der Algebraischen Zahlkörper.* Werke I, Springer (1932).

[3] ISHII, N., P. KAPLAN and K.S. WILLIAMS. On Eisenstein's problem. *Acta Arithmetica 54* (1990), 323-345.

[4] KAPLAN, P. *Cours d'Arithmétique.* U.E.R. de Mathématiques, Université de Nancy 1, tome 3 (1973).

[5] —— Comparaison des 2-groupes des classes d'idéaux au sens large et au sens étroit d'un corps quadratique réel. *Proc. Japan Acad. 50* (1974), 688-693.

[6] KAPLAN, P. and K.S. WILLIAMS. Pell's equation $X^2 - mY^2 = -1, -4$ and continued fractions. *Journal of Number Theory 23* (1986), 169-182.

[7] KAPLAN, P. and K.S. WILLIAMS. The distance between ideals in the orders of a real quadratic field. *L'Enseignement Mathématique 36* (1990), 321-358.
[8] SHANKS, D. The infrastructure of a real quadratic field and its applications. *Proc. (1972), Number Theory Conference,* Boulder, Colorado (1972), 217-224.
[9] SCHOLZ, A. und B. SCHOENEBERG. *Einführung in die Zahlentheorie.* Walter de Gruyter, Berlin and New York (1973).

(Reçu le 29 janvier 1991)

Franz Halter-Koch

Institut für Mathematik
Karl-Franzens-Universität
Halbärthgasse 1/1
A-8010 Graz, Autriche

Pierre Kaplan

Département de Mathématiques
Université de Nancy 1
B.P. 239
F-54506 Vandoeuvre-lès-Nancy Cedex, France

Kenneth S. Williams

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada KIS 5B6

Yoshihiko Yamamoto

Department of Mathematics
Faculty of Science
Osaka University
Toyonaka, Osaka, Japon