§1. Introduction

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):*