Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 37 (1991)

Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

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

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

Kapitel: §2. Idéaux ambiges, idéaux ambiges primitifs réduits

DOI: https://doi.org/10.5169/seals-58743

$$(1.7)\qquad \begin{gathered} I_n = \frac{a_n}{a_0}\left(\prod_{i=1}^{n} \varphi_i\right) I_0 \ , \quad \operatorname{sgn}\left(N\left(\prod_{i=1}^{n} \varphi_i\right)\right) = (-1)^n \ , \\ \varphi_n > 1 \ , \quad \frac{a_n}{a_{n-1}}\, \varphi_n > 1 \ . \end{gathered}$$

Dans tout ce travail nous poserons

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

§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 **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

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

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

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

qui équivaut à

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

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*

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

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

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

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

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

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

Démonstration. D'après (1.7) $I_1 = \dfrac{a_1}{a_0}\dfrac{ka_0 + \sqrt{D}}{2a_1} I_0 = \dfrac{ka_0 + \sqrt{D}}{2a_0} I_0$ et, comme l'idéal I_0 est réduit, $-1 < \dfrac{ka_0 - \sqrt{D}}{2a_0} < 0$, donc $\rho_1 = \dfrac{ka_0 + \sqrt{D}}{2a_0}$ $= \dfrac{\sqrt{D}}{a_0} + \dfrac{ka_0 - \sqrt{D}}{2a_0}$ 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*

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

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

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

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 $d_0d_1 > \sqrt{D}$ on trouve par le même calcul

$$\left[d_0d_1, \frac{d_0d_1+\sqrt{D}}{2}\right]\left[dd', \frac{dd'+\sqrt{D}}{2}\right] = \left[D, \frac{D+\sqrt{D}}{2}\right] = \sqrt{D}\,.$$

Multipliant par l'idéal primitif $\dfrac{I_0I_1}{d}$ on obtient

$$\left[dd', \frac{dd'+\sqrt{D}}{2}\right] = \frac{\sqrt{D}\,I_0I_1}{dd_0d_1}$$

ce qui démontre la Proposition 2 avec $r = \dfrac{1}{dd_0d_1}$, $J = \left[dd', \dfrac{dd'+\sqrt{D}}{2}\right]$.

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,

$$\frac{1}{2d}\,[2D_0, D_0+\sqrt{\bar{D}}]\,[2D_1, D_1+\sqrt{\bar{D}}] = [d_0d_1, \sqrt{\bar{D}}]\,,$$

d'où $r = \dfrac{1}{2d}$, $J = [d_0d_1, \sqrt{\bar{D}}]$, si $d_0d_1 < \sqrt{\bar{D}}$, et

$$\frac{1}{d}\,[2D_0, D_0+\sqrt{\bar{D}}]\,[D_1, \sqrt{\bar{D}}] = [2d_0d_1, d_0d_1+\sqrt{\bar{D}}]\,,$$

d'où $r = \dfrac{1}{d}$, $J = [2d_0d_1, d_0d_1+\sqrt{\bar{D}}]$, si $d_0d_1 < \sqrt{\bar{D}}$.

Puis, si $d_0d_1 > \sqrt{\bar{D}}$, on obtient respectivement $r = \dfrac{1}{2dd_0d_1}$, $J = [dd', \sqrt{\bar{D}}]$ et $r = \dfrac{1}{dd_0d_1}$, $J = [2dd', dd'+\sqrt{\bar{D}}]$.

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*

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

et un nombre rationnel r *dépendant de* I_0 *et* I_1 *tel que l'idéal* J *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	$2^t d_0d_1 < \sqrt{\bar{D}}$	$2^t d_0d_1 > \sqrt{\bar{D}}$
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