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

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 28.11.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

est clair.

(1.7)
$$I_n = \frac{a_n}{a_0} \left(\prod_{i=1}^n \varphi_i \right) I_0 , \quad \operatorname{sgn} \left(N \left(\prod_{i=1}^n \varphi_i \right) \right) = (-1)^n ,$$

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

Dans tout ce travail nous poserons

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

§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 **Z**-modules de l'un des types suivants:

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

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

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

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

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
$D \equiv 1 \pmod{4}$	$\left[a, \frac{a+\sqrt{D}}{2}\right], \ a \mid D, \ \left(a, \frac{D}{a}\right) = 1$	$a < \sqrt{D}$
$D \equiv 4 \pmod{16}$ $D \equiv 8, 16, 24 \pmod{32}$	$[a,\sqrt{\bar{D}}], a \bar{D}, \left(a,\frac{\bar{D}}{a}\right)=1$	$a < \sqrt{\bar{D}}$
$D \equiv 12 \pmod{16}$	$[a, \sqrt{\bar{D}}], a \bar{D}, \left(a, \frac{\bar{D}}{a}\right) = 1$ $[2a, a + \sqrt{\bar{D}}], a \bar{D}, \left(a, \frac{\bar{D}}{a}\right) = 1$	$a<\sqrt{ar{D}}$
$D \equiv 0 \pmod{32}$	$[a, \sqrt{\bar{D}}], a \bar{D}, \left(a, \frac{\bar{D}}{a}\right) = 1$	$a < \sqrt{\bar{D}}$
	$[4a, 2a + \sqrt{\overline{D}}], a \frac{\overline{D}}{4}, (a, \frac{\overline{D}}{4a}) = 1$	$a < \frac{\sqrt{\bar{D}}}{2}$

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

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

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

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

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

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

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

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 (mod 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

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

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

$$a^{\prime\prime}|D^{\prime\prime},\;\left(a^{\prime\prime},\frac{D^{\prime\prime}}{a^{\prime\prime}}\right)=1$$
,

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

Ceci étant, on voit que

$$\left[a, \frac{\sqrt{D}}{2}\right]$$
 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

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

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

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

Туре	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	$[4a,2a+\sqrt{ar{D}}]$	$2a < \sqrt{\bar{D}}$
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

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

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

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

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

$$J = egin{cases} rI_0I_1 \;, & N'(J) = d_0d_1 \;, & si & d_0d_1 < \sqrt{ar{D}} \;, \ r\sqrt{ar{D}}I_0I_1 \;, & N'(J) = dd' \;, & si & d_0d_1 > \sqrt{ar{D}} \;, \end{cases}$$

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

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

Définissons d, d_0 et d_1 par

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

On voit qu'il existe d' tel que $D'_1 = d_0 d'$ d'où $D'_0 = d_1 d'$ et donc

$$\bar{D} = dd_0d_1d'$$
 avec $(dd_0, d_1d') = (dd_1, d_0d') = 1$

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 $I_0 = \left[D_0, \frac{D_0 + \sqrt{D}}{2}\right]$,

 $I_1 = \left[D_1, \frac{D_1 + \sqrt{D}}{2} \right]$ et, effectuant le produit, on trouve

$$\frac{I_0I_1}{d} = \left\langle dd_0d_1, \frac{dd_0d_1 + d_1\sqrt{D}}{2}, \frac{dd_0d_1 + d_0\sqrt{D}}{2}, \frac{d_0d_1\left(\frac{d+d'}{2}\right) + \left(\frac{d_0+d_1}{2}\right)\sqrt{D}}{2} \right\rangle.$$

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

D'autre part dd_0d_1 et $\left(\frac{d-d'}{2}\right)d_0d_1$ appartiennent à $\frac{I_0I_1}{d}$, donc $N\left(\frac{I_0I_1}{d}\right)$ = d_0d_1 , ce qui, comme (d_0d_1,dd') = 1, prouve par la Proposition 1 que $\frac{I_0I_1}{d} = \left[d_0d_1,\frac{d_0d_1+\sqrt{D}}{2}\right]$ et que $\frac{I_0I_1}{d}$ est ambige et primitif.

Si $d_0d_1 < \sqrt{D}$, $\frac{I_0I_1}{d}$ est réduit donc on satisfait à la Proposition 2 en posant

$$J = \frac{I_0 I_1}{d} \; , \quad \ r = \frac{1}{d} \; . \label{eq:J}$$

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 $\frac{I_0I_1}{d}$ 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 $r = \frac{1}{dd_0d_1}$, $J = \left[dd', \frac{dd' + \sqrt{D}}{2}\right]$.

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

$$rac{1}{d} \left[2D_0, D_0 + \sqrt{ar{D}} \right] \left[D_1, \sqrt{ar{D}} \right] = \left[2d_0d_1, d_0d_1 + \sqrt{ar{D}} \right],$$

d'où $r = rac{1}{d}$, $J = \left[2d_0d_1, d_0d_1 + \sqrt{ar{D}} \right]$, si $d_0d_1 < \sqrt{ar{D}}$.

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

et
$$r = \frac{1}{dd_0d_1}$$
, $J = [2dd', dd' + \sqrt{\bar{D}}]$.

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

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

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)	$J = rI_0I_1$	$J=r\sqrt{ar{D}}I_0I_1$
du même type 1 et 2, 3 et 4 2 et 3, 1 et 4 1 et 3, 2 et 4	$d_0d_1<\sqrt{ar{D}} \ 2^td_0d_1<\sqrt{ar{D}} \ 2^{t-1}d_0d_1<\sqrt{ar{D}} \ 2d_0d_1<\sqrt{ar{D}} \ 2d_0d_1<\sqrt{ar{D}}$	$d_0d_1>\sqrt{ar{D}}$ $2^td_0d_1>\sqrt{ar{D}}$ $2^{t-1}d_0d_1>\sqrt{ar{D}}$ $2d_0d_1>\sqrt{ar{D}}$

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 $I = \left[a, \frac{b+\sqrt{D}}{2}\right]$ un idéal et $c = \frac{D-b^2}{4a}$. 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