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: §3. Idéaux symétriques

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: 02.07.2025

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

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	$2^t d_0d_1 < \sqrt{\bar{D}}$	$2^t d_0d_1 > \sqrt{\bar{D}}$
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

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

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 $I = \left[a, \dfrac{b+\sqrt{D}}{2}\right]$ 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 $I = \left[\dfrac{N}{2}, \dfrac{M+\sqrt{D}}{2}\right]$ 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 $\left[\dfrac{N}{2}, \dfrac{M+\sqrt{D}}{2}\right]$ est un idéal symétrique et primitif.

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

Inversement si $\dfrac{D}{4} = M^2 + N^2$ 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) $\quad \bar{D} = 2^s p_1^{s_1} \dots p_k^{s_k}, \quad s = 0$ *ou* $1, \quad p_i$ *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*

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

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*

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

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

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

$$\gamma' = \frac{D_1c + a\sqrt{D}}{2}\ , \qquad \gamma'' = \frac{D_1d + b\sqrt{D}}{2}\ , \qquad \gamma', \gamma'' \in O_D\ . \tag{3.10}$$

On vérifie par un calcul aisé que

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

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

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

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

$$\operatorname{sgn} N(\gamma) = \operatorname{sgn}[(ac - bd)(bc - ad)] = \operatorname{sgn}(abD_2 - cdD_1)$$

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

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

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.