31. Détermination des idéaux réduits.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **7 (1961)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.09.2024**

Aux décompositions $420 = u \times (4v)$ correspondent les *idéaux réduits doubles*, de normes 1, 3, 5, 7, et de racine minimum 0.

Exemple 3: Dans le corps de discriminant (tableau XVIII):

$$-440 = (+8) \times (+5) \times (-11),$$

les seules décompositions auxquelles correspondent des idéaux réduits remarquables sont:

$$1 \times (4 \times 110), \quad 2 \times (4 \times 55), \quad 5 \times (4 \times 22), \quad 10 \times (4 \times 11),$$

qui donnent les idéaux doubles, de normes 1, 2, 5, 10, et de racine minimum 0.

31. Détermination des idéaux réduits.

Dans un corps imaginaire les idéaux canoniques réduits représentent les classes, *presque proprement.*

Théorème de la détermination des idéaux réduits — Dans un corps quadratique imaginaire, *une classe d'idéaux contient:* soit *un et un seul idéal* (canonique) *réduit*; soit (exceptionnellement) *deux idéaux réduits conjugués*, qui sont alors *réduits réfléchis.*

On a établi l'existence, dans chaque classe, d'au moins un idéal (canonique) réduit (**25**):

$$\mathbf{M} = (m, \quad \theta - \bar{c}); \qquad |2\bar{c} - S| \leqslant m \leqslant |F(\bar{c})| : m.$$

Il reste à chercher dans quelles conditions un idéal $\mathbf{N} = \mathbf{M} \times (\rho)$, congru à $\mathbf{M}$ —ou dans la même classe— peut être aussi réduit. On peut mettre l'élément ρ, et, par suite l'idéal principal (ρ) sous sa forme canonique (**3** et **11**), d'où:

$$\mathbf{N} = \mathbf{M} \times (u + v\theta) \times q = (m, \theta - \bar{c}) \times (u + v\theta) \times q;$$

u, v nombres entiers premiers entre eux.

Le produit $\mathbf{M} \times (u + v\theta)$ est un idéal entier; en développant et explicitant son expression, on obtient des générateurs d'une base arithmétique libre:

$$(m, \theta - \bar{c}) \times (u + v\theta) = (mu + mv\theta, \quad (-\bar{c}u - vN) + [u + v(S - \bar{c})]\theta).$$

Le facteur rationnel de cet idéal m_1, est égal au p.g.c.d. des coefficients de θ, dans ces générateurs, il divise leur combinaison:

$$m[u+v(S-\bar{c})]-mv(S-\bar{c}) = mu;$$

divisant mu et mv, il divise m, puisque u,v sont premiers entre eux.

Pour que **N** soit canonique, il faut que le produit $m_1 \times q$ soit égal à 1, et sa norme n est égale à:

$$n = N(\mathbf{N}) = N(\mathbf{M}) \times N(u+v\theta) \times N(q) = m \times N(u+v\theta) \times m_1^{-2}.$$

On peut minorer $N(u+v\theta)$, en supposant v non nul:

$$4N(u+v\theta) = (2u+vS)^2+v^2|D| \geqslant v^2|D|;$$

d'où une minoration de la norme n, de **N**:

$$4n \geqslant m \times v^2 \times |D| \times m_1^{-2} \quad \Rightarrow \quad 4mn \geqslant (m : m_1)^2 \times v^2 \times |D|.$$

Pour que **M** et **N**, qui sont canoniques, soient tous deux réduits, il faut que leurs normes vérifient les limitations:

$$3m^2 \leqslant |D| \quad \text{et} \quad 3n^2 \leqslant |D| \quad \Rightarrow \quad 3mn \leqslant |D|;$$

ce qui entraîne:

$$4|D| \geqslant 12mn \geqslant 3(m : m_1)^2 \times v^2 \times |D| \quad \Rightarrow \quad 4 \geqslant 3(m : m_1)^2 \times v^2.$$

Comme $m : m_1$ et v sont des entiers, ils doivent être tous deux de valeur absolue égale à 1; donc $m = m_1$ et on peut prendre $v = 1$.

La relation entre **N** et **M** devient ainsi:

$$\mathbf{N} \times (m) = \mathbf{M} \times (\theta+u); \quad \text{et} \quad F(-u) = N(\theta+u) = m \times n.$$

On peut mettre l'idéal principal $(\theta+u)$ sous forme canonique et diviser les deux membres par **M** [on a vu (**13**) que $(m) = \mathbf{M} \times \mathbf{M}'$]; on obtient:

$$\mathbf{N} \times \mathbf{M}' = (m \times n, \quad \theta+u) = (m, \quad \theta \times u) \times (n, \quad \theta+u).$$

La racine $-u$, doit être aussi une de racine $\mathbf{M}'$, c'est-à-dire est congrue mod. m, au zéro $\bar{c}' = S-\bar{c}$. L'idéal **N** est égal au deuxième facteur (du dernier membre) et $-u$ est congru, mod. n, à sa racine minimum $\bar{c}_1$. Les limitations des racines minimum des idéaux réduits (**25** et remarque de **29**) entraînent les comparaisons:

$$m^2 \leqslant F(\bar{c}') \leqslant F(-u); \quad n^2 \leqslant F(\bar{c}_1) \leqslant F(-u); \quad m \times n \leqslant F(-u).$$

Mais la dernière comparaison est une égalité; il en est donc de même des premières et:

$$m^2 = F(\bar{c}') = F(-u) = F(\bar{c}_1) = n^2 \quad \Rightarrow \quad -u = \bar{c}' = \bar{c}_1.$$

L'idéal **N** est égal au conjugué **M**$'$, de l'idéal **M**, en sorte que **M** et **M**$'$, qui sont congrus, sont réfléchis relativement aux racines minimum $\bar{c}$ et $\bar{c}'$. Leur congruence est explicitée (**24**) par:

$$(\theta-\bar{c}) = \mathbf{M}^2 \qquad (\theta-\bar{c}') = \mathbf{M}'^2;$$

ou

$$\mathbf{M}'\times(\theta-\bar{c}) = \mathbf{M}\times(m) \qquad \mathbf{M}\times(\theta-\bar{c}') = \mathbf{M}'\times(m).$$

On trouve bien le cas d'exception signalé et seulement ce cas. Le cas trivial de la congruence de **M** avec lui-même a été écarté en supposant v non nul, dans l'expression de ρ.

En conséquence: *pour obtenir les classes d'idéaux*, d'un corps quadratique imaginaire, *il suffit de construire les idéaux canoniqies réduits*, ce qui peut être fait par l'algorithme suivant:

on utilise le *tableau des valeurs* $F(c)$, du polynôme fondamental du corps, pour les valeurs entières de c, croissantes de 0 jusqu'à la limite r, exclue, pour laquelle $3\times(2c-S)^2$ devient supérieur la valeur absolue $|D|$, du discriminant.

On retient chaque décomposition:

$$F(c) = m\times n; \qquad (2c-S) \leqslant m \leqslant n,$$

en un produit de deux facteurs (entiers) au moins égaux à $2c-S$. *Le premier facteur* (au plus égal au second) *m est la norme de deux idéaux conjugués réduits:*

$$(m,\ \theta-c), \quad (m,\ \theta-c'); \qquad c+c' = S.$$

Si m est *diviseur de* $|D|$, ces deux idéaux sont égaux à un *idéal double*, de racine minimum c, qui définit une *classe double.*

Si les deux facteurs sont égaux:

$$m = n \quad \text{et} \quad F(c) = F(c') = m^2,$$

les deux idéaux sont *réfléchis*, ils sont congrus et définissent une seule *classe double.*

Tableau IX.

CLASSES d'idéaux et Structure de leur GROUPE.

$F(x) = x + x^2 + 58$; $D = -231 = (-3)\times(-7)\times(-11)$; $r = 4$.

c	$F(c)$	Idéaux réduits	Classe	Calculs
-4	70	»		$(7, \theta+4) = (\mathbf{7}, \theta-3)$
-3	64	»		$(8, \theta+3) \sim (\mathbf{8}, \theta-2)$
-2	$\mathbf{6}\times 10$ $\mathbf{5}\times 12$ $\mathbf{4}\times 15$	$(\mathbf{6}, \theta+2)$ $(\mathbf{5}, \theta+2)$ $(\mathbf{4}, \theta+2)$	$= \mathbf{I}\times\mathbf{J}$ $\sim \mathbf{I}^4\times\mathbf{J}$ $= \mathbf{I}^2$	$(\mathbf{2}, \theta-0)\times(\mathbf{3}, \theta-1) = (\mathbf{6}, \theta+2)$ $(\mathbf{2}, \theta-0)^2 = (\mathbf{4}, \theta+2)$ $(3, \theta+2) = (\mathbf{3}, \theta-1)$
-1	$\mathbf{2}\times 29$	$(\mathbf{2}, \theta+1)$	$\sim \mathbf{I}^5$	
0	$\mathbf{1}\times 58$ $\mathbf{2}\times 29$	$(\mathbf{1}, \theta-0)$ $(\mathbf{2}, \theta-0)$	$= (1)$ $= \mathbf{I}$	
$+1$	$\mathbf{3}\times 20$ $\mathbf{4}\times 15$ $\mathbf{5}\times 12$ $\mathbf{6}\times 10$	$(\mathbf{3}, \theta-1)$ $(\mathbf{4}, \theta-1)$ $(\mathbf{5}, \theta-1)$ $(\mathbf{6}, \theta-1)$	$= \mathbf{J}$ $\sim \mathbf{I}^4$ $\sim \mathbf{I}^2\times\mathbf{J}$ $\sim \mathbf{I}^5\times\mathbf{J}$	 $(\mathbf{2}, \theta+1)^2 = (\mathbf{4}, \theta-1)$ $(\mathbf{4}, \theta+2)\times(\mathbf{3}, \theta-1) = (12, \theta+2) \sim (\mathbf{5}, \theta-1)$
$+2$	$\mathbf{8}\times 8$	$(\mathbf{8}, \theta-2)$	$= \mathbf{I}^3$	$(\mathbf{2}, \theta-0)^3 = (\mathbf{8}, \theta-2)$; $(\mathbf{2}, \theta-0)^6 \sim (1)$
$+3$	$\mathbf{7}\times 10$	$(\mathbf{7}, \theta-3)$	$\sim \mathbf{I}^3\times\mathbf{J}$	$(\mathbf{8}, \theta-2)\times(\mathbf{3}, \theta-1) = (24, \theta-10) \sim (\mathbf{7}, \theta+11)$ $= (\mathbf{7}, \theta-3)$
10	$168 = 7\times 24$			

GROUPE: $\mathbf{I}^x\times\mathbf{J}^y$; x, mod. 6; y, mod. 2; ordre 12.
ou: $(\mathbf{I}^2)^x\times(\mathbf{I}^3)^y\times\mathbf{J}^z$; x, mod. 3; y, z, mod. 2.

Dans tout autre cas, les deux idéaux réduits sont distincts et définissent *deux classes conjuguées.*

Les classes ainsi engendrées sont différentes et *ce sont toutes les classes du corps.*

Exemples. — Le tableau IX indique les calculs pour le corps de discriminant —231; le rang est $r = 4$. Pour c compris entre 0 et 3 inclus, on a inscrit les décompositions $F(c) = m \times n$, en deux facteurs au moins égaux à $2c+1$ et devant chacune l'idéal $(m, \theta - c)$, dont la norme est le facteur au plus égal à l'autre. Dans le tableau prolongé en deçà de 0, on a inscrit les idéaux conjugués $(m, \theta - c')$.

Il y a cinq idéaux réduits remarquables: trois idéaux doubles, de normes **1**, **3**, **7**, qui définissent des classes doubles; un couple d'idéaux réfléchis, de norme **8**, qui définissent une même classe double. Enfin quatre couples d'idéaux conjugués, de normes 2, 4, 5, 6, définissant des couples de classes conjuguées. En tout:

$$4+2\times 4 = 12 \text{ classes.}$$

D'autres tableaux de ce même chapitre donnent encore des exemples de calcul d'idéaux réduits et de classes d'idéaux dans des corps quadratiques imaginaires.

Le tableau XI concerne des corps qui ne contiennent qu'une seule classe et, par suite, sont *principaux.*

Les tableaux XII et XIV concernent des corps dont le discriminant est premier; ils n'ont donc que le seul idéal réduit remarquable (1) et des couples d'idéaux réduits conjugués; en tout un nombre impair de classes.

Les tableaux XV, XVII, XVIII concernent des corps dont le discriminant est composé, pair ou impair.

32. Répartition des idéaux dans les classes.

Les idéaux réduits d'un corps imaginaire et les classes qu'ils définissent étant ainsi calculés, on peut répartir, dans ces classes, les idéaux canoniques donnés par le tableau des valeurs du polynôme fondamental (**21**). Il suffit d'appliquer le calcul de récurrence indiqué ci-dessus (**25**).