Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 7 (1961)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LES CORPS QUADRATIQUES
Autor: Châtelet, A.
Kapitel: 30. Idéaux réduits remarquables.
DOI: https://doi.org/10.5169/seals-37125

LES CORPS QUADRATIQUES

par A. CHÂTELET

(suite et fin)

CHAPITRE V

LES CLASSES D'IDÉAUX DANS LES CORPS IMAGINAIRES — OU DE DISCRIMINANT NÉGATIF —

La considération des *idéaux réduits* (**25**), qui a permis de montrer que, dans tout corps quadratique, le nombre de classes d'idéaux est fini, permet, plus précisément, dans le cas d'un corps imaginaire (discriminant négatif), de déterminer compètement ces classes et, par suite de construire la « *structure de leur groupe* » (**23**).

30. Idéaux réduits remarquables.

On peut d'abord remarquer que, dans un *corps imaginaire*, dont le polynôme fondamental $F(x)$ ne prend que des valeurs positives:

la racine minimum $\bar{c}$, d'un idéal canonique (**7**), *est aussi celle qui donne à* $F(x)$ *la plus petite valeur.*

Toute autre racine de l'idéal considéré est un terme $\bar{c}+\lambda m$, de la progression arithmétique, dont la raison est la norme m, de l'idéal. Il suffit de former la différence:

$$F(\bar{c}+\lambda m)-F(\bar{c}) = \lambda m \times (2\bar{c}-S+\lambda m).$$

La valeur absolue $|2\bar{c}-S|$ étant au plus égale à m, la valeur entre parenthèses est nulle, ou du signe de l'entier λ; la différence est donc nulle, ou positive.

En dehors du cas trivial $\lambda = 0$, cette différence ne peut être nulle que pour des valeurs $+1$ ou -1, de λ; en outre:

$$|2\bar{c}-S| = m \quad \Leftrightarrow \quad |(S-\bar{c})-\bar{c}| = m;$$

les *zéros conjugués* (**5**) $\bar{c}$ et $\bar{c}' = S—\bar{c}$, définissent le même idéal qui est égal à son conjugué, —ou qui est *double* (**7**)— elles donnent aussi la même valeur (minimum) à $F(x)$.

Définitions. — Dans un corps imaginaire, *parmi les idéaux réduits* (**25**), on peut **remarquer**, ou appeler **remarquable**:

1° *un idéal qui est double* (**7**), qui est ainsi **réduit double**; il est égal à son conjugué et représente une *classe double*, égale à sa conjuguée, qui est aussi son inverse, en sorte que le carré de la classe est égal à la classe principale (**23**);

2° *un idéal qui est réfléchi* (**16**), qui est ainsi **réduit réfléchi**; il est équivalent de dire que c'est *un idéal réfléchi relativement à sa racine minimum:*

$$\mathbf{M}\times\mathbf{M} = (\theta—\bar{c}); \qquad F(\bar{c}) = m^2; \qquad |2\bar{c}—S| \leqslant m.$$

L'idéal conjugué $\mathbf{M}'$ est aussi réduit réfléchi (ou réfléchi relativement à sa racine minimum $S—\bar{c}$). Les deux idéaux, qui sont congrus, appartiennent à une même *classe double.*

Il est évident qu'un idéal (canonique) *réfléchi relativement à sa racine minimum* $\bar{c}$ est *réduit*, puisque le carré de sa norme n'est pas supérieur à $|F(c)|$. On peut vérifier que, d'une façon réciproque:

un idéal réduit qui n'est pas réfléchi relativement à sa racine minimum ne peut l'être relativement à tout autre racine.

Car sa norme m est alors inférieure à la norme $F(\bar{c})\colon m$, de l'idéal qui lui est associé, relativement à la racine minimum $\bar{c}$, elle l'est, à fortiori, pour tout idéal associé suivant une autre racine c, car, d'après la remarque précédente, $F(\bar{c})$ étant minimum:

$$F(c) \geqslant F(\bar{c}) \quad \Rightarrow \quad n = F(c)\colon m \geqslant F(\bar{c})\colon m > m.$$

On a indiqué la construction d'un *idéal double* (**21**), éventuellement *réduit* (**25**) et celle d'un *idéal réfléchi* (**16**). En les rapprochant pour un idéal réduit, dans le cas d'un corps imaginaire, on obtient une construction générale des *idéaux réduits remarquables.*

Théorème d'existence des idéaux réduits remarquables. Dans un corps quadratique, de discriminant D négatif, *les idéaux* *réduits remarquables sont associés* —ou correspondent biunivoquement— *aux décompositions de* $|D|$, s'il est impair, *ou de* $|D|: 4$, *en un produit de deux entiers positifs*, dans les conditions suivantes:

Décomposition de $\lvert D\rvert$		*Idéal réduit*
$\lvert D\rvert = u\times v$; $u \leqslant v$, impairs ou $\lvert D\rvert : 4 = (u:2)\times(v:2)$ $u:2 \leqslant v:2$, impairs	$3u \leqslant v$	$m=u$; $\bar{c} = (u+S):2$ $(m,\ \theta-\bar{c})$ *double.*
	$3u \geqslant v$	$m = (v+u):4$; $\bar{c} = (v-u-2S):4$ $(m,\ \theta-\bar{c})$ *réfléchi.*
$\lvert D\rvert = u\times(4v)$; $u \leqslant v$:		$m=u$; $(m,\ \theta-0)$ *double.*

Tout *idéal double réduit* est obtenu en prenant, pour sa norme m, un diviseur convenable de $|D|$. La limitation de m (**25**) et la valeur de la racine minimum $\bar{c}$ (**21**) sont données, suivant les cas, par:

$$\begin{array}{lllll} S=-1; & |D| = m\times v; & m,\ v \text{ impairs}; & \bar{c} = (m-1):2 & 3m^2 \leqslant |D|; \\ S=0; & |D| = 2u\times 2v; & u,\ v \text{ impairs}; & m=2u;\ \bar{c}=\mathrm{u}; & 3m^2 \leqslant |D|; \\ S=0; & |D| = m\times 4v, & & \bar{c}=0 & 4m^2 \leqslant |D|. \end{array}$$

Ce sont bien les circonstances de l'énoncé.

Tout idéal réfléchi, relativement à une racine c, est obtenu (**16**) par une décomposition du discriminant (négatif) en un produit de deux entiers, dont un négatif:

$$D = (-u)+v; \quad v-(-u) = v+u, \quad \text{multiple de } 4.$$

Ceci exige que $|D|$ soit impair, ou quadruple d'un nombre impair $N = |d|$ [les nombres entiers $|D|$ et N congrus à -1, mod. 4]. Ce sont les deux premiers cas de l'énoncé. La norme m et la racine c sont données par:

$$4m = v+u; \quad 2\times(2c-S) = v-u.$$

Pour que la racine c soit minimum, ce qui est la condition de réduction, il faut et il suffit que:

$$2\times(v-u) = 4\times(2c-S) \leqslant 4m = (v+u) \quad \Leftrightarrow \quad v \leqslant 3u.$$

La valeur $u = 1$ constitue un cas particulier trivial de la première décomposition; il lui correspond l'idéal unité $(1,\ \theta-0)$. L'idéal est *réduit double*; si

$$1 = u = 3v; \quad [D = (-1)\times 3 = -3; \quad F(x) = x^2+x+1]$$

l'idéal unité est, à la fois, *double et réfléchi.*

Dans le cas de $|D|$ pair, à la décomposition triviale $|D| = 1\times 4v$, correspond encore l'idéal unité, qui est *réduit double.*

Exemple 1. — Dans le corps de discriminant:

$$D = -231 = (-3)\times(-7)\times(-11),$$

dent les calculs sont indiqués dans le tableau IX, aux décompositions:

$$|D| = 1\times 231, \quad 3\times 77, \quad 7\times 33,$$

dont le premier facteur u, est inférieur au tiers du second, correspondent les *idéaux réduits doubles* [norme u, racine minimum $(u-1): 2$]:

$$(1,\ \theta-0), \quad (3,\ \theta-1), \quad (7,\ \theta-3).$$

A la décomposition 11×21, correspond l'*idéal réduit réfléchi* [norme $(11+21): 4 = 8$; racine minimum $(21-11-2): 4 = 2$]:

$$(8,\ \theta-2); \quad F(2) = 8^2; \quad (8,\ \theta-2)^2 = (\theta-2).$$

Exemple: 2. — Dans le corps (tableau XVIII), de discriminant:

$$D = -420 = (-4)\times(-3)\times(+5)\times(-7),$$

aux décompositions de $|D|: 4 = 105$, correspondent les idéaux réduits remarquables:

3×35: idéal double $(6,\ \theta-3)$; $[m = 2\times 3, \quad \bar{c} = 3]$
5×21: id. $(10,\ \theta-5)$; $[m = 2\times 5, \quad \bar{c} = 5]$
7×15: idéal réfléchi $(11,\ \theta-4)$; $[m = (7+15): 2,$
$\bar{c} = (15-7): 2]$.

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:

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