25. Idéaux canoniques réduits.

En outre les éléments de $\mathbf{M}$ et de $\mathbf{M}_1$ se correspondent, en étant *représentés par les mêmes coefficients* (entiers rationnels) relativement aux bases correspondantes, $\alpha_1\ \beta_1$ et $\rho\times\alpha_1\ \rho\times\beta_1$.

Cette correspondance peut notamment être appliquée à des idéaux congrus, construits par l'intermédiaire d'idéaux associés:

$$\mathbf{M} = (m,\ \theta\text{—}c),\quad \mathbf{N} = (n,\ \theta\text{—}c);\qquad \mathbf{M}_1 = \mathbf{N}'.$$

La congruence de $\mathbf{M}_1$ à $\mathbf{M}$ est réalisée par le multiplicateur $(\theta\text{—}c)\colon n$. Appliqué à la base $(n,\ \theta'\text{—}c)$, de $\mathbf{M}_1$ il donnerait la base canonique de $\mathbf{M}$. Mais, appliqué à une base $(n,\ \theta\text{—}c_1)$, (où c_1 est une racine conjuguée de c, suivant le module n), il donne une base arithmétique libre de $\mathbf{M}_1$:

$$n\times[(\theta\text{—}c)\colon n] = (\theta\text{—}c),\quad [(\theta\text{—}c_1)\times(\theta\text{—}c)]\colon n$$

qui peut être différente de la base canonique, mais lui est arithmétiquement équivalente.

Dans l'exemple du tableau I, on peut considérer les idéaux associés:

$$\mathbf{M} = (3,\ \theta\text{—}1),\quad \mathbf{N} = (4,\ \theta\text{—}1),\qquad \mathbf{M}_1 = \mathbf{N}' = (4,\ \theta\text{—}2);$$

le multiplicateur de $\mathbf{M}_1$ étant $(\theta\text{—}1)\colon 4$, à la base choisie de $\mathbf{M}_1$, il fait correspondre:

$$4\times[(\theta\text{—}1)\colon 4] = \theta\text{—}1,\quad [(\theta\text{—}1)\times(\theta\text{—}2)]\colon 4 = \text{—}\theta\text{—}2.$$

On vérifie bien que ce couple d'éléments est bien arithmétiquement équivalent à la base canonique de $\mathbf{M}$:

$$\left\|\begin{matrix}\theta\text{—}1\\ \text{—}\theta\text{—}2\end{matrix}\right\| = \left\|\begin{matrix}0 & 1\\ \text{—}1 & \text{—}1\end{matrix}\right\| \times \left\|\begin{matrix}3\\ \theta\text{—}1\end{matrix}\right\|$$

25. Idéaux canoniques réduits.

THÉORÈME du nombre de classes d'idéaux. — Dans un corps quadratique, *le nombre de classes d'idéaux*, (mod. $\mathcal{R}$) —ou l'ordre du groupe quotient $\mathcal{G}|\mathcal{R}$— *est fini.*

Pour démontrer cette propriété, on peut ramener la construction des classes à celle d'idéaux canoniques particuliers, appelés *réduits*, pour lesquels on vérifie que:

1. Toute classe contient au moins un idéal réduit —ou *tout idéal canonique est congru à* (au moins) *un idéal réduit*— .

2. *Le nombre total d'idéaux* (canoniques) *réduits est fini.* Il en est, à fortiori, de même du nombre de classes, qui lui est au plus égal, et chacune d'elles ne renferme qu'un nombre fini d'idéaux réduits.

Le choix d'une définition d'un idéal réduit présente évidemment un certain caractère arbitraire; il est justifié, à posteriori, par la vérification des deux qualités précédentes.

Définition. — Un idéal canonique réduit, ou, par abréviation, *un* **idéal réduit**, *est un idéal canonique* $(m,\ \theta\text{—}\overline{c})$, *dont le carré de la norme est au plus égal à la valeur absolue du polynôme fondamental,* $|F(\overline{c})|$ pour la *racine minimum* $\overline{c}$ (de cet idéal):

$$|2\overline{c}\text{—}S| < m, \quad \text{ou bien} \quad 2\overline{c}\text{—}S = m; \qquad m^2 \leqslant |F(\overline{c})|.$$

Deux idéaux (canoniques) *conjugués* (**7**), *distincts*, dont les racines minimum sont $\overline{c}$ et $S\text{—}\overline{c}$ (**21**), *sont simultanément réduits*, puisque $F(\overline{c})$ et $F(S\text{—}\overline{c})$ sont égaux.

Pour un *idéal double*, la norme m étant diviseur du discriminant, d'après la valeur de la racine minimum indiquée ci-dessus (**21**), la condition de réduction est équivalente, suivant les cas à:

$$\overline{c} = 0: \qquad m^2 \leqslant |F(0)|, \quad \text{ou} \quad 4m^2 \leqslant |D|;$$

$$2\overline{c}\text{—}S = m; \quad 4m^2 \leqslant |m^2\text{—}D|; \qquad \begin{cases} 3m^2 \leqslant |D|; & D < 0 \\ 5m^2 \leqslant D; & D > 0. \end{cases}$$

L'*idéal unité* $(1,\ \theta\text{—}0)$ *est manifestement réduit.*

1. Pour tout idéal canonique **M**, *on peut construire*, au moins *un idéal congru, qui soit réduit.*

On peut raisonner par récurrence sur la norme. La construction est triviale si **M** vérifie les conditions de réduction; il est congru à lui-même.

La construction est encore évidente s'il existe une racine c, de l'idéal, pour laquelle $|F(c)| = m$. Alors l'idéal est principal (**11**):

$$(m,\ \theta—c) = (|F(c)|,\ \theta—c) = (\theta—c);$$

il est congru à l'idéal unité qui est réduit.

La construction existe pour la valeur 1, de la norme, puisque l'idéal est alors l'idéal unité, qui est réduit. Il suffit d'établir, par récurrence, qu'*un idéal canonique*, qui ne vérifie pas les deux constructions triviales précédentes, *est congru à un idéal canonique, de norme plus petite.*

Un tel idéal, a, au moins, une racine c (notamment sa racine minimum) telle que:

$$m^2 > |F(c)| \quad \text{et} \quad m < |F(c)|.$$

L'idéal $\mathbf{N} = (n, \theta—c)$, de norme $|F(c)| : m = n$, qui lui est associé, vérifie les conditions de comparaison:

$$1 < n = |F(c)| : m < m.$$

Or l'idéal **M** est congru à l'idéal $\mathbf{N}'$ conjugué de **N** (**22**), dont la norme n est bien inférieure à m.

Si la racine c est minimum pour **N**, cet idéal et son conjugué $\mathbf{N}'$ sont réduits, et la récurrence est terminée.

2. *Les conditions de réduction entraînent une limitation des racines minimum*, donc aussi des normes des idéaux réduits, dont le nombre est, par suite, fini.

Cette limitation est exprimée par la comparaison (générale):

$$(2\bar{c}—S)^2 \leqslant |F(\bar{c})|;$$

qui est équivalente, suivant le signe du discriminant D, à:

$$\begin{array}{lllll} D > 0: & F(\bar{c}) < 0; & 5(2\bar{c}—S)^2 \leqslant D\ ; & \text{et} & 4m^2 \leqslant D\ ; \\ D < 0: & & 3(2\bar{c}—S)^2 \leqslant |D|; & \text{et} & 3m^2 \leqslant |D|. \end{array}$$

La condition générale résulte immédiatement de l'élimination de m entre les conditions de réduction.

Si D est *positif*, les valeurs de c qui rendent $F(c)$ *positif* ne vérifient pas cette condition, car:

$$4F(c) = (2c—S)^2—D \quad \Rightarrow \quad (2c—S)^2 > 4F(c) > F(c).$$

Pour les valeurs de c qui rendent $F(c)$ *négatif*, l'expression du polynôme entraîne l'équivalence:

$$4(2c—S)^2 \leqslant 4|F(c)| = D—(2c—S)^2 \Leftrightarrow 5(2c—S)^2 \leqslant D.$$

En outre:

$$4m^2 \leqslant D—(2c—S)^2 \leqslant D \Rightarrow 4m^2 \leqslant D.$$

Si D est négatif, l'expression du polynôme, dont la valeur est toujours positive, entraîne l'équivalence:

$$4(2c—S)^2 \leqslant 4F(c) = (2c—S)^2+|D| \Leftrightarrow 3(2c—S)^2 \leqslant |D|;$$

en outre:

$$4m^2 \leqslant (2c—S)^2+|D| \leqslant m^2+|D| \Rightarrow 3m^2 \leqslant |D|.$$

Ceci acquis, pour obtenir les idéaux réduits, en utilisant le tableau des valeurs de $F(c)$, pour c entier croissant à partir de 0, on peut:

I. *Déterminer la limite* r des entiers, à partir de laquelle la condition de limitation n'est plus vérifiée, c'est-à-dire telle que

$$(2c—S)^2 > |F(c)| \Leftrightarrow c \geqslant r;$$

ce qui est équivalent, suivant le signe de D, à:

$$D > 0: \quad 5(2c—S)^2 > D \Leftrightarrow c \geqslant r;$$
$$D < 0: \quad 3(2c—S)^2 > |D| \Leftrightarrow c \geqslant r.$$

II. Pour les valeurs entières de c, limitées par:

$$0 \leqslant c < r;$$

chercher les diviseurs m (entiers positifs) des valeurs $F(\overline{c})$, tels que

$$(2\overline{c}—S) \leqslant m \leqslant |F(\overline{c})|: m.$$

III. A *chaque couple d'entiers* $\overline{c}$ *et* m, ainsi obtenus, *correspond*

1° si m est diviseur du discriminant D, un *idéal double réduit*:

$$(m, \ \theta—\overline{c}), \quad 2\overline{c}—S = 0 \quad \text{ou} \quad m.$$

2° si m n'est pas diviseur de D, *deux idéaux réduits conjugués*, différents:

$$(m, \ \theta—\overline{c}), \quad (m, \ \theta—\overline{c'}); \quad \overline{c'} = S—\overline{c}.$$

On peut remplacer la racine minimum négative $\overline{c'}$ par la plus petite racine positive $\overline{c'}+m = m+S-\overline{c}$.

Exemple 1 (tableau I). — Dans le corps de discriminant $D = -39$, la valeur de r, déterminée par comparaison avec $|D|$ est 2:

$$3.(2\times 1+1)^2 = 27 < 39 < 3.(2\times 2+1)^2 = 75.$$

Il suffit de chercher les diviseurs de $F(0) = 10$ et de $F(1) = 12$, qui vérifient les conditions de réduction (compris entre $2c+1$ et la racine carrée de $|F(c)|$). On obtient deux idéaux doubles, de normes 1 et 3 (diviseurs de 39):

$$(1,\ \theta-0),\qquad (3,\ \theta-1)$$

et deux idéaux conjugués distincts, de norme 2:

$$(2,\ \theta-0)\qquad (2,\ \theta+1) = (2,\ \theta-1).$$

Il y a quatre idéaux réduits différents, donc au plus quatre classes, on vérifie ci-dessous que c'est effectivement le nombre de classes.

Exemple 2 (tableau II) — Dans le corps de discriminant $D = +60$ la valeur de r est 2:

$$5\times(2\times 1)^2 = 20 < 60 < 5\times(2\times 2)^2 = 80.$$

Il suffit de chercher les diviseurs de $|F(0)| = 15$ et de $|F(1)| = 14$, qui vérifient les conditions de réduction. On obtient ainsi trois idéaux doubles, de normes 1, 3, 2 (diviseurs de 60):

$$(1,\ \theta-0),\qquad (3,\ \theta-0),\qquad (2,\ \theta-1).$$

Il y a au plus trois classes; on vérifie ci-dessous qu'il n'y en a que deux, la classe principale contenant l'idéal de norme 1, d'ailleurs égal à (1) et une classe double contenant les deux idéaux de normes 3 et 2 (dont on peut vérifier qu'ils sont congrus).

26. Propriétés générales des groupes de classes d'idéaux.

Certaines relations entre les classes d'idéaux, d'un corps quadratique, sont des applications de propriétés générales des groupes abéliens d'ordre fini qu'on va indiquer sommairement [1]).

---

[1]) Ces propriétés sont exposées et démontrées dans de nombreux ouvrages. Je me permets de citer: *Arithmétique et Algèbre modernes*, ch. II, § 5 et 7; ch. III, n° 35 (1954 et 1955), ou, pour plus de développements: *Les groupes abéliens finis* (1925).