16. Idéaux canoniques associés.

Cette détermination reste valable pour chaque facteur d'une décomposition de **M** en un produit d'idéaux dont les normes sont des puissances d'idéaux premiers différents (facteurs de la norme m). Ces facteurs sont par suite des puissances déterminées des $\mathbf{P}_i$, donc sont respectivement égaux aux idéaux $\mathbf{M}_i$, construits à priori.

Dans la décomposition maximum d'un idéal canonique **M**, on peut associer des systèmes de facteurs, de façon que les normes de leurs produits soient égales à des facteurs m_j, d'une décomposition, en produit, arbitrairement choisie, de la norme de **M**. Ceci est exprimé par la propriété complémentaire de décomposition d'un idéal canonique.

A toute *décomposition de la norme m*, d'un idéal canonique $\mathbf{M} = (m, \theta—c)$, en un *produit de nombres entiers* m_j, correspond une *décomposition de l'idéal* **M**, en un *produit d'idéaux canoniques*, de normes m_j et de racines égales —ou respectivement congrues, mod. m_j— à la racine c, de **M**:

$$m = \Pi m_j \quad \Rightarrow \quad (m, \ \theta—c) = \Pi(m_j, \ \theta—c).$$

16. Idéaux canoniques associés.

Définition. — Deux idéaux canoniques sont qualifiés **associés**, *relativement à une racine c*, lorsque cette racine c leur est commune et que *le produit de leurs normes est égal à* (la valeur absolue) $|F(c)|$:

$$\mathbf{M} = (m, \ \theta—c), \quad \mathbf{N} = (n, \ \theta—c); \qquad m \times n = |F(c)|.$$

Il est équivalent de dire que le *produit de ces deux idéaux canoniques, est égal à l'idéal principal* $(\theta—c)$:

$$\mathbf{M} \times \mathbf{N} = (\theta—c).$$

Le nombre entier positif $|F(c)|$ étant divisible par lui-même, il existe un idéal, de racine égale à c, qui l'a pour norme. Mais il est égal à l'idéal principal $(\theta—c)$, car d'après les propriétés des bases algébriques (multiplication, **12. 2**; simplification, **10. 1**):

$|F(c)| = |(\theta—c) \times (\theta'—c)| = (\theta—c) \times [\eta(\theta'—c)]$; [$\eta$ signe de $F(c)$],
$\Rightarrow (|F(c)|, \theta—c) = (\theta—c) \times [\eta(\theta'—c), 1] = (\theta—c) \times (1) = (\theta—c).$

(Cette égalité a déjà été signalée comme une application particulière de la construction d'une base canonique d'un idéal principal canonique; **11. 3**).

Ceci acquis, d'après la propriété de décomposition (**15. 3**), la première définition, donc $|F(c)| = m \times n$, entraîne:

$$(\theta—c) = (|F(c)|,\ \theta—c) = (m \times n,\ \theta—c)$$
$$= (m,\ \theta—c) \times (n,\ \theta—c) = \mathbf{M} \times \mathbf{N}.$$

Réciproquement la décomposition de $(\theta—c)$ en un produit de deux idéaux canoniques $\mathbf{M} \times \mathbf{N}$ entraîne la décomposition de sa norme $|F(c)|$ en le produit $m \times n$, de leurs normes (**13**).

Si deux idéaux canoniques **M** et **N** sont associés, relativement à une racine c, *les idéaux conjugués* $\mathbf{M}'$ *et* $\mathbf{N}'$ *sont associés, suivant la racine* (conjuguée pour chacune des normes), $c' = S—c$; car:

$$|F(c')| = |F(S—c)| = |F(c)| = m \times n$$
$$\Rightarrow \quad (m,\ \theta—c') \times (n,\ \theta—c') = (\theta—c').$$

Pour un idéal canonique $\mathbf{M} = (m,\ \theta—c)$, il y a une infinité d'idéaux associés, relativement à chaque entier $c + \lambda m$, racine de **M**.

Relativement à une racine c, il y a un nombre fini de couples d'idéaux associés, donnés par les diverses décompositions de $|F(c)|$ en un produit de deux nombres entiers positifs $m \times n$. Si $|F(c)|$ est un nombre premier, il n'y a qu'un seul couple trivial, formé des idéaux (1) et $(\theta—c)$.

16. 2. *Idéaux réfléchis.*

Définition. — *Un idéal canonique est* **réfléchi**, relativement à une racine c, *lorsqu'il est associé à un idéal égal*, relativement à cette racine —ou lorsque son carré est égal à l'idéal principal $(\theta—c)$— :

$$\{\mathbf{M} = (m,\ \theta—c),\quad m^2 = |F(c)|\} \quad \Leftrightarrow \quad \mathbf{M}^2 = (\theta—c).$$

L'idéal conjugué $\mathbf{M}'$ est alors réfléchi relativement à la racine (conjuguée) $c' = S—c$ [puisque $F(c') = F(c)$].

Il y a *équivalence* entre l'existence d'un couple d'idéaux canoniques, conjugués, réfléchis et une décomposition —ou

expression— du discriminant D, du corps. Elle est exprimée par les énoncés suivants qui sont réciproques et se distinguent suivant que la valeur $F(c)$ est positive ($+m^2$), ou négative ($-m^2$).

THÉORÈME d'existence d'idéaux réfléchis. — Dans un corps quadratique, de discriminant D:

1. Si D est *impair*, ou si $d = D:4$ est un *entier impair*, à toute décomposition de D en produit de deux nombres entiers, dont la différence est un multiple de 4, non nul:

$$D = u \times v; \quad u, v \text{ nombres entiers}; \quad v - u = 4m, \quad m \text{ entier} \neq 0;$$

correspond biunivoquement un couple d'idéaux réfléchis conjugués:

$$\left.\begin{array}{l} \mathbf{M} = (m, \theta - c)\ ,\ c = (u+S):2+m; \\ \mathbf{M}' = (m, \theta - c'),\ c' = (-v+S):2+m \end{array}\right\} c+c' = S \quad F(c) = F(c') = +m^2.$$

2. Si D est positif et *impair*; $S = -1$; à toute expression de D, comme somme de deux carrés (un pair et un impair)

$$D = a^2 + 4m^2; \quad a \text{ entier impair};$$

correspond biunivoquement un couple d'idéaux réfléchis conjugués:

$$\left.\begin{array}{l} \mathbf{M} = (m, \theta - c), \quad c = \quad (a-1):2 \\ \mathbf{M}' = (m, \theta - c'), \quad c' = -(a+1):2 \end{array}\right\} c+c' = -1, \ F(c) = (F(c') = -m^2.$$

2 *bis*. Si D est positif et $D:4 = d$ *entier pair*; $S = 0$; à toute expression de D en somme de carrés pairs:

$$D = a^2 + b^2; \quad a:2 = a', \quad b:2 = b' \text{ entiers impairs};$$

correspondent biunivoquement deux couples d'idéaux réfléchis conjugués:

$$\begin{array}{llll} \mathbf{M}_1 = (b', \theta - a'); & \mathbf{M}_1' = (b', \theta + a'); & F(a') = F(-a') = -b'^2 \\ \mathbf{M}_2 = (a', \theta - b'); & \mathbf{M}_2' = (a', \theta + b'); & F(b') = F(-b') = -a'^2 \end{array}$$

Pour vérifier ces propriétés, il est commode d'utiliser l'expression de $4F(c)$, qui donne une expression du discriminant D:

$$(2c-S)^2 - D = \pm 4m^2 \quad \Leftrightarrow \quad D = (2c-S)^2 \mp 4m^2.$$

Pour chaque cas, on établit d'abord la condition nécessaire: l'existence d'idéaux entraîne la décomposition et la nature de D; puis la condition suffisante: on calcule les expressions des idéaux réfléchis qui résultent de ces expressions de D.

1. $F(c)$ étant égal à $+m^2$, la valeur de D est:

$$D = (2c-S)^2-4m^2 = (2c-S-2m)\times(2c-S+2m);$$

c'est un produit de deux nombres entiers, dont la différence est égale à $4m$. Si $S = -1$, D est impair. Si $S = 0$ les deux facteurs sont simultanément doubles de nombres impairs, ou quadruples de nombres entiers. La deuxième circonstance est impossible, puisque D ne peut être multiple de 16; il est donc quadruple d'un nombre impair.

Réciproquement si D vérifie ces conditions nécessaires:

$$D = u\times v = (-v)\times(-u); \qquad v-u = (-u)-(-v) = 4m;$$

les systèmes d'équations en x:

$$\begin{aligned} 2x-S-2m &= u, \quad \text{ou} \quad -v \\ 2x-S+2m &= v, \quad \text{ou} \quad -u \end{aligned}$$

sont compatibles et ont pour solutions les valeurs c et c' indiquées.

2. $F(c)$ étant égal à $-m^2$, et $S = -1$, la valeur de D est:

$$D = (2c+1)^2+4m^2;$$

c'est bien une somme de carrés de deux nombres entiers, l'un pair l'autre impair; D est positif et congru à $+1$, mod. 4.

Réciproquement si D vérifie ces conditions nécessaires:

$$D = a^2+4m^2; \qquad a \text{ impair};$$

les équations en x:

$$2x+1 = a, \quad \text{ou} \quad -a$$

ont bien pour solutions les valeurs indiquées de c et c'.

2 *bis*. La valeur de $F(c)$ étant $-m^2$, et $S = 0$, la valeur de D est:

$$D = (2c)^2+4m^2, \quad \text{ou} \quad d = D:4 = c^2+m^2;$$

$d = D:4$ ne pouvant être congru, mod. 4, ni à $+1$, ni à 0, c et m sont impairs et $D:4$ est double d'un nombre impair [D multiple de 8].

Réciproquement si D remplit ces conditions il existe bien les deux couples d'idéaux indiqués.

En particulier, les décompositions triviales $D = 1 \times D$, si $d \equiv 1$, (mod. 4), et $D = 2 \times 2d$, si $d \equiv 3$, (mod. 4), correspondent à des couples d'idéaux conjugués réfléchis:

$$D = 1-4N; \qquad F(x) = x^2+x+N;$$
$$F(-N) = F(N-1) = N^2;$$
$$D = 4d \ (d \text{ impair}); \qquad F(x) = x^2-d;$$
$$F[\pm(d+1):2)] = [(d-1):2]^2.$$

Un idéal, de norme m peut être réfléchi relativement à deux racines c et c', donnant à $F(x)$ des valeurs égales et par conséquent conjuguées. Cet idéal est alors égal à son conjugué —ou est double— et:

$$c-c' = \lambda m; \quad 2c-S = \lambda m;$$
$$D = \lambda^2 m^2 \pm 4m^2 = (\lambda^2 \pm 4) \times m^2; \quad (\lambda \text{ entier})$$

comme D ne peut pas avoir de facteur carré, cette circonstance ne se produit que pour l'*idéal unité*, de norme 1 et pour des corps quadratiques, de discriminant $D = \lambda^2 \pm 4$. Pour les premières valeurs des discriminants, ce sont:

D	$F(x)$	$c = (S+\lambda):2)$	$c' = (S-\lambda):2$	$F(c) = F(c')$
—4	x^2+1	0	0	+1
—3	x^2+x+1	0	—1	+1
+5	x^2+x-1	0	—1	—1
id.	id.	1	—2	+1
+8	x^2-2	1	—1	—1
12	x^2-3	2	—2	+1
13	x^2+x-3	1	—2	—1
.....	.....	.....	.....	.....

On pourrait aussi rechercher des idéaux réfléchis relativement à deux racines, qui donnent à $F(x)$ des valeurs opposées $+m^2$ et $-m^2$; c'est le cas pour $F(x) = x^2+x-1$, pour lequel l'idéal (1) est réfléchi

relativement aux racines 0 et —1, +1 et —2. Cette circonstance semble présenter moins d'intérêt pour les études faites ci-dessous.

17. Idéaux premiers.

Les propriétés de décomposition des idéaux canoniques peuvent être comprises dans une théorie plus générale (au moins en apparence) de la décomposition des idéaux fractionnaires, analogue à la théorie de la décomposition des nombres fractionnaires, en arithmétique ordinaire. On utilise à cet effet la notion d'*idéaux premiers.*

DÉFINITION. — Par extension du vocabulaire arithmétique usuel, *un idéal entier* **P** *est appelé* **premier**, *lorsque sa seule décomposition en un produit de deux idéaux entiers est sa multiplication par l'idéal unité*:

$$\{\mathbf{P} = \mathbf{I}\times\mathbf{J},\quad \mathbf{I} \text{ et } \mathbf{J} \text{ entiers}\} \Leftrightarrow \{\mathbf{I} = (1) \quad ou \quad \mathbf{J} = (1)\}.$$

THÉORÈME des idéaux premiers. — Dans un corps quadratique $\mathbf{R}(\theta)$, de polynôme fondamental $F(x)$, les *idéaux premiers* sont:

1. *Les idéaux principaux rationnels* (q), de norme q^2, dont la base q: est un nombre premier, pour lequel *la congruence fondamentale est impossible* —ou qui n'est diviseur d'aucune valeur $F(c)$, pour c entier—. Ils sont appelés **idéaux premiers, du second degré.**

2. Les *idéaux canoniques* $(p,\ \theta—c)$, dont *la norme p est un nombre premier* et dont la racine c est un zéro de $F(x)$, mod. p. Ils sont appelés **idéaux premiers, du premier degré.**

Tout idéal entier, mis sous forme canonique $q\times\mathbf{M}$, est un produit de deux idéaux entiers, l'un canonique **M**, l'autre principal rationnel (q). Il ne peut être premier que si l'un des deux facteurs est égal à l'idéal unité (1), soit qu'il soit principal rationnel, égal à $(q)\times(1)$; soit qu'il soit canonique, égal à $(1)\times\mathbf{M}$. On va examiner successivement ces deux cas.