15. Multiplication et décomposition des idéaux canoniques.

La multiplication est manifestement *associative* et *commutative* comme celle des idéaux (**12**).

La *classe unité* est le sous-groupe $\mathfrak{Q}$, ensemble des idéaux (q) principaux rationnels. Cet ensemble est manifestement une classe dont l'élément canonique est l'idéal unité (1); c'est un *élément neutre dans la multiplication* des classes; $\mathfrak{M} \times \mathfrak{Q} = \mathfrak{M}$.

Deux classes $\mathfrak{M}$ et $\mathfrak{M}'$ sont *conjuguées*, —ou chacune est conjuguée de l'autre— lorsqu'elles sont engendrées par deux éléments canoniques conjuguées **M** et **M'**. Chacune est constituée par l'ensemble des idéaux respectivement conjugués des idéaux de l'autre.

Deux classes conjuguées sont aussi *inverses* (au sens général de ce qualificatif), car leur produit est égal à la classe unité $\mathfrak{Q}$, son élément canonique étant $\mathbf{M} \times \mathbf{M}' = (1)$. Chacune des classes $\mathfrak{M}$ et $\mathfrak{M}'$ est auss iconstituée par l'ensemble des idéaux inverses des idéaux de l'autre $[q \times \mathbf{M}$ et $(qm)^{-1} \times \mathbf{M}']$.

De l'existence de l'inverse de toute classe, on peut déduire (raisonnement général **1. 2**), la possibilité et la détermination de la *division des classes*, ce qui comprend la détermination de la *classe neutre* et de l'*inverse* d'une classe. Le *quotient* de deux classes est d'ailleurs constitué par l'ensemble des quotients des idéaux de la classe dividende par ceux de la classe diviseur.

L'ensemble des classes d'idéaux, du groupe $\mathcal{G}_I$, relativement au sous-groupe $\mathfrak{Q}$, est, par conséquent aussi *un groupe multiplicatif abélien*. Il est appelé **groupe quotient** de $\mathcal{G}_I$ par $\mathfrak{Q}$ et noté $\mathcal{G}_I|\mathfrak{Q}$. Son existence, établie ici directement, est une propriété générale d'un groupe abélien, relativement à un sous-groupe.

15. Multiplication et décomposition des idéaux canoniques.

Les propriétés des congruences et notamment celles de la congruence fondamentale (**5** et **6**) permettent de donner des règles du calcul de la *multiplication des idéaux canoniques* (donc des classes, mod. Q) et, par suite, d'établir une *décomposition déterminée*, en un produit —ou sous forme d'un *monôme*— d'un idéal canonique.

15. 1. *Calcul pratique d'une multiplication d'idéaux canoniques.*

Il peut se ramener aux trois cas suivants.

1. Le *carré d'un idéal canonique* —double—, *dont la norme est un nombre premier* q, *diviseur du discriminant* D, *est l'idéal principal rationnel, de base* q:

$$\mathbf{Q} = (q,\ \theta\text{—}c);\quad q \text{ diviseur de } |D|;\qquad \mathbf{Q}^2 = \mathbf{Q}\times\mathbf{Q} = (q).$$

C'est une conséquence d'un cas particulier du théorème de la norme (**13**). Un idéal $\mathbf{Q}$, dont la norme q est diviseur de $|D|$, est égal à son conjugué —ou est double— (**7. 3**). Son carré étant ainsi égal au produit par son conjugué est égal à (q). Cette propriété, déjà signalée lorsque la norme est un entier quelconque, diviseur de $|D|$, est plus spécialement intéressante, pour le cas d'un nombre premier.

2. *Toute puissance*, d'exposant entier positif h, d'*un idéal canonique*, dont la norme est un nombre premier p, non diviseur de $|D|$, *est égale à un idéal canonique, de norme* p^h:

$$\mathbf{P} = (p,\ \theta\text{—}c_1);\qquad \mathbf{P}\times\ldots\times\mathbf{P} = \mathbf{P}^h = (p^h,\ \theta\text{—}c_h);$$

sa racine c_h est le zéro (défini mod. p^h), de la congruence fondamentale , mod. p^h, qui est congru à c_1, mod. p, et dont l'existence et le calcul effectif ont été établis par la résolution de congruences récurrentes du premier degré, mod. p (**6**).

L'égalité est triviale pour $h = 1$ et il suffit de la vérifier par récurrence sur cet exposant. En la supposant vraie pour h—1, l'entier c_h est, d'après sa détermination, congru à c_{h-1}, mod. p^{h-1} et à c_1, mod. p; c'est donc aussi une racine des idéaux $\mathbf{P}^{h-1}$ et $\mathbf{P}$, qui peuvent être définis par les bases (canoniques):

$$\mathbf{P}^{h-1} = (p^{h-1},\ \theta\text{—}c_h).\qquad \mathbf{P} = (p,\ \theta\text{—}c_h).$$

On forme une base (arithmétique) de leur produit en multipliant les termes de ces deux bases:

$$\mathbf{P}^h = \mathbf{P}\times\mathbf{P}^{h-1} = (p^h,\quad p\times(\theta\text{—}c_h),\quad p^{h-1}\times(\theta\text{—}c_h),\quad (\theta\text{—}c_h)^2).$$

L'élément $(\theta\text{—}c_h)^2$ peut être exprimé (par la formule de Taylor):

$$(\theta\text{—}c_h)^2 = \text{—}\dot{F}(c_h)\times(\theta\text{—}c_h)\text{—}F(c_h).$$

En transportant cette expression dans la base obtenue, on peut supprimer $F(c_h)$ qui est multiple de p^h (**10. 1**) d'où:

$$\mathbf{P}^h = (p^h,\ p(\theta—c_h),\ p^{h-1}(\theta—c_h),\ —\dot{F}(c_h)\times(\theta—c_h)).$$

Mais c_h étant zéro simple, de $F(x)$, mod. p, la dérivée $\dot{F}(c)$ est un nombre entier, premier avec p, et il existe des nombres entiers u et v tels que:

$$u\times p+v\times\dot{F}(c_h) = 1$$
$$\Rightarrow\quad u\times[p(\theta—c_h)]+v[\dot{F}(c_h)\times(\theta—c_h)] = (\theta—c_h).$$

Il en résulte que $\mathbf{P}^h$, ainsi défini, contient p^h et $(\theta—c_h)$ donc l'idéal canonique $(p^h,\ \theta—c_h)$; mais inversement cet idéal contient les quatre termes de la base définissant $\mathbf{P}^h$ et il lui est égal.

Cette propriété et ce calcul, comme les précédents, sont encore valables pour la puissance d'un idéal canonique, dont la norme est un entier quelconque, non diviseur du discriminant.

3. *Le produit de deux idéaux canoniques*:

$$\mathbf{M}_1 = (m_1,\ \theta—c_1),\qquad \mathbf{M}_2 = (m_2,\ \theta—c_2),$$

dont les normes m_1 et m_2 sont des nombres entiers (positifs) *premiers entre eux*, *est* égal à *un idéal canonique*, de norme $m_1\times m_2$:

$$\mathbf{M}_1\times\mathbf{M}_2 = (m_1\times m_2,\ \theta—c);\quad \{c\equiv c_1\ (m_1)\ \text{ et }\ c\equiv c_2\ (m_2)\}$$

sa racine c est l'entier, déterminé, mod. $(m_1\times m_2)$, qui est congru, à la fois, à c_1, mod. m_1 et à c_2, mod. m_2; il est ainsi zéro de la congruence fondamentale, mod. $(m_1\times m_2)$, ainsi qu'il a été établi et calculé par la résolution d'une congruence du premier degré (**6**).

D'après sa détermination c est aussi racine de $\mathbf{M}_1$ et de $\mathbf{M}_2$, qui peuvent être mis sous les formes canoniques:

$$\mathbf{M}_1 = (m_1,\ \theta—c),\qquad \mathbf{M}_2 = (m_2,\ \theta—c).$$

On peut encore former une base arithmétique de leur produit en multipliant les termes de ces deux bases:

$$\mathbf{M}_1\times\mathbf{M}_2 = (m_1\times m_2,\quad m_1\times(\theta—c),\quad m_2\times(\theta—c),\quad (\theta—c)^2).$$

Mais m_1 et m_2 étant premiers entre eux, on peut trouver des entiers u_1 et u_2 tels que:

$$u_1 \times m_1 + u_2 \times m_2 = 1$$
$$\Rightarrow \quad u_1 \times [m_1(\theta - c)] + u_2 \times [m_2(\theta - c)] = (\theta - c).$$

On peut alors raisonner comme précédemment: le produit $\mathbf{M}_1 \times \mathbf{M}_2$ ainsi défini, contient $m_1 \times m_2$ et $(\theta - c)$, donc l'idéal canonique indiqué dans l'énoncé; mais cet idéal contient les quatre termes de la base définissant le produit, à qui il est donc égal.

Cette troisième propriété s'étend à un produit, d'un nombre fini h d'idéaux canoniques, dont les *normes* sont des nombres entiers, *premiers entre eux*, deux à deux. Ceci est évident par récurrence sur h; la propriété étant vraie pour un produit de $h-1$ idéaux, le reste, avec adjonction d'un idéal supplémentaire, dont la norme qui était première avec la norme de chacun des idéaux précédents est première avec le produit de ces normes qui est égale à la norme du produit des $h-1$ premiers idéaux.

15. 2. *Composition d'idéaux canoniques.*

On peut rassembler les propriétés précédentes en un premier énoncé.

Théorème de composition. — *Pour qu'un produit* d'idéaux canoniques dont les normes sont des nombres premiers, *soit égal à un idéal canonique*, il faut et il suffit que *si plusieurs de ces idéaux ont une même norme p* (supérieure à 1) *ils aient aussi pour racine un même zéro simple de la congruence fondamentale*, mod. *p*. En particulier, pour tout nombre premier p, diviseur du discriminant, il ne peut exister, dans le produit qu'un idéal, au plus, dont la norme soit égale à ce diviseur.

La condition est *suffisante*: dans un produit d'idéaux qui la vérifie, on peut associer chaque système de h_i idéaux, de même norme p_i, qui, ayant une même racine, mod. p, sont égaux; leur produit (partiel) est une puissance, qui, d'après la construction 2 est égale à un idéal canonique, dont la norme m_i est égale à la puissance $p_i^{h_i}$; cette construction est triviale si $h_i = 1$, notamment si p_i

est diviseur du discriminant. On forme ainsi un produit d'idéaux canoniques, dont les normes m_i, puissances de nombres premiers p_i, différents, sont des nombres premiers entre eux deux à deux. La construction 3 permet alors de former un idéal canonique, égal à ce produit, dont la norme est le produit des normes m_i et dont la racine c est respectivement congrue à chacune des racines c_i, mod. p_i.

La condition est *nécessaire*: un produit de h idéaux canoniques, dont les normes sont des nombres premiers, ne peut être égal à un idéal canonique, s'il contient au moins un couple de facteurs, de même norme p, et dont les racines sont des zéros différents c,c'; ou un zéro double (c congru à c') de la congruence fondamentale, mod. p.

Car le produit peut alors être mis sous la forme:

$$\mathbf{I} = \mathbf{I}_1 \times (p,\ \theta\text{—}c) \times (p,\ \theta\text{—}c');$$

le premier terme $\mathbf{I}_1$ s'il n'est pas égal à (1), [pour $h = 2$], est égal au produit des h—2 facteurs différents du couple; c'est en tous cas un *idéal entier* (produit d'idéaux entiers), donc de la forme $a \times \mathbf{M}$, produit d'un facteur rationnel entier $a \geqslant 1$, par un idéal canonique $\mathbf{M}$, peut être égal à (1). Les deux derniers facteurs étant conjugués (éventuellement égaux, si c est racine double, congru à c'), leur produit est égal à l'idéal principal (p). Le produit $\mathbf{I}$ est ainsi égal à:

$$\mathbf{I} = a \times \mathbf{M} \times (p) = (a \times p) \times \mathbf{M};$$

ce ne peut être un idéal canonique puisqu'il a un facteur rationnel $a \times p$ entier, supérieur à 1 ($p > 1$).

15. 3. *Décomposition des idéaux canoniques.*

De la propriété précédente, résulte une propriété, en quelque sorte inverse.

Théorème de décomposition. — *Un idéal canonique* $\mathbf{M} = (m,\ \theta\text{—}c)$ *est, d'une seule façon, décomposable en* —ou égal à— :

1° *un produit d'idéaux canoniques* $\mathbf{P}_i$, dont les normes sont des *nombres premiers* p_i; qui peuvent être répartis en produits partiels, respectivement de h_i idéaux égaux:

$$\mathbf{M} = \Pi[\mathbf{P}_i \times \ldots \times \mathbf{P}_i] = \Pi \mathbf{P}_i^{hi}; \qquad \mathbf{P}_i = (p_i,\ \theta\text{—}c_i);$$

Il est équivalent de dire que **M** est égal à un *monôme* (**14**) des idéaux $\mathbf{P}_i$. Cette décomposition est, en quelque sorte, *maximum.*

2° *un produit d'idéaux canoniques* $\mathbf{M}_i$, dont les normes m_i sont des *puissances*, d'exposant entier positif h_i, *de nombres premiers* p_i *différents*:

$$\mathbf{M} = \Pi \mathbf{M}_i; \quad \mathbf{M}_i = (m_i, \ \theta - c_I); \quad m_i = p_i^{hi}.$$

Les nombres premiers p_i, en valeur et en nombre —ou leurs puissances m_i— sont les facteurs de la décomposition (déterminée) du nombre entier m, norme de l'idéal **M**.

Les racines c_i, de $\mathbf{P}_i$; ou c_I, de $\mathbf{M}_i$; sont respectivement congrus à la racine c, de **M**, mod. p_i, ou module m_i.

La racine c, de l'idéal **M** étant zéro de la congruence fondamentale, mod. m, ce module m ne peut contenir de facteur premier q, du discriminant D, à une puissance supérieure à 1 (première condition de possibilité de la congruence, pour un module composé; **6**).

Cette racine c est alors, à fortiori, zéro de la congruence, pour tout diviseur de m, notamment pour les facteurs p_i; elle définit donc des idéaux canoniques:

$$\mathbf{P}_i = (p_i, \ \theta - c_i); \quad c_i \equiv c, \quad (\text{mod. } p_i).$$

Le théorème précédent montre alors que le produit des $\mathbf{P}_i$ ainsi construits, est égal à **M**; ou en constitue une *décomposition*, qui peut être qualifiée *maximum.* En groupant les facteurs égaux, on en constitue un *monôme de puissances* qui peut être remplacé par le produit des facteurs $\mathbf{M}_i$, de norme $m_i = p_i^{hi}$, égaux à ces puissances.

La décomposition (maximum) est *déterminée* —ou unique— . Si un idéal canonique **M** est égal à un produit d'idéaux canoniques dont les normes sont des nombres premiers p_i, d'une part sa norme m étant égale au produit des normes, les p_i sont, en valeur et en nombre, les facteurs premiers de la décomposition (déterminée) du nombre entier m.

D'autre part, en raison de la condition nécessaire du théorème de composition, dans ce produit, les idéaux d'une même norme p doivent être réduits à un seul si p est diviseur du discriminant, sinon ils doivent avoir une même racine, congrue, mod. p_i, à la racine c, de **M**; ils sont donc respectivement égaux aux idéaux $\mathbf{P}_i$, construits à priori.

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