CHAPITRE II DIVISIBILITÉ DES IDÉAUX

LES CORPS QUADRATIQUES

par A. CHÂTELET

(suite)

CHAPITRE II

DIVISIBILITÉ DES IDÉAUX

12. Multiplication des idéaux fractionnaires.

Entre les idéaux fractionnaires, d'un corps quadratique, on définit une opération, appelée *multiplication*, dont on vérifie qu'elle est déterminée, commutative et associative, et que l'opération inverse, appelée *division* est possible et déterminée, à l'exception de la division par un idéal nul.

DÉFINITION. — *Le* **produit** (résultat de la multiplication) *de deux idéaux*:

$$\mathbf{I} = (..,\rho_i,..), \quad i \text{ de } 1 \text{ à } h; \qquad \mathbf{J} = (..,\sigma_j,..), \quad j \text{ de } 1 \text{ à } k;$$

(définis par des bases algébriques (**10. 1**) de h et k générateurs), *est l'idéal*, désigné par $\mathbf{I}\times\mathbf{J}$, *dont une base algébrique est constituée par les produits mutuels des générateurs*, des idéaux multipliés:

$$\mathbf{I}\times\mathbf{J} = (..,\omega_{ij},..); \qquad \omega_{ij} = \rho_i \times \sigma_j, \quad \text{en nombre } h\times k.$$

Ce produit, qui est ainsi défini, est *déterminé*, c'est-à-dire indépendant des bases adoptées pour définir les idéaux multipliés.

C'est en effet l'ensemble des éléments du corps, de la forme:

$$\Sigma\xi_{ij}\times\omega_{ij} = \Sigma\xi_{ij}\times(\rho_i\times\sigma_j); \qquad \xi_{ij} \in \mathbf{E}(\theta);$$

(les ξ_{ij} étant des entiers arbitraires du corps). Cet ensemble est, par suite égal à l'ensemble des différences (et des sommes) mutuelles des produits de chaque élément de $\mathbf{I}$ par chaque élément de $\mathbf{J}$; ce qui est bien une construction indépendante des bases choisies.

La multiplication est manifestement *commutative*, comme celle des éléments du corps; elle s'étend à un nombre quelconque d'idéaux; elle est *associative*; car les générateurs d'un produit de trois idéaux peuvent s'écrire indifféremment:

$$\omega_{ijk} = (\rho_i \times \sigma_j) \times \tau_k = \rho_i \times (\sigma_j \times \tau_k).$$

La conjugaison conserve la multiplication: *le conjugué d'un produit* (d'idéaux) *est égal au produit des conjugués* (de ces idéaux)

$$(\mathbf{I} \times \mathbf{J})' = \mathbf{I}' \times \mathbf{J}'.$$

Il suffit en effet de définir $\mathbf{I}'$ et $\mathbf{J}'$ par les générateurs conjugués de ceux de $\mathbf{I}$ et $\mathbf{J}$; leurs produits mutuels seront les conjugués des générateurs de définition de $\mathbf{I} \times \mathbf{J}$.

12. 2. *Cas particuliers.*

Le *produit*, d'un idéal $\mathbf{I}$, *par un idéal principal* (ρ) est égal au *produit*, de $\mathbf{I}$, *par* (l'élément de) *la base* ρ (**8. 4**)

$$(\rho) \times \mathbf{I} = \rho \times \mathbf{I};$$

notamment:

$$(0) \times \mathbf{I} = (0); \quad (1) \times \mathbf{I} = 1 \times \mathbf{I} = \mathbf{I}; \quad (\rho) \times (\sigma) = \rho \times (\sigma) = (\rho \times \sigma).$$

L'*idéal unité* (1), ou $\mathbf{E}(\theta)$, est un *élément neutre* pour la multiplication, d'où son nom, on montre ci-dessous (**14**) que c'est le seul.

Le produit $\mathbf{I} \times \mathbf{F}$, *par un idéal entier* $\mathbf{F}$, *est inclus dans* $\mathbf{I}$, car les produits des générateurs de $\mathbf{I}$ par ceux de $\mathbf{F}$, qui sont des entiers du corps, appartiennent à $\mathbf{I}$ (3 de la condition caractéristique; **8. 2**).

Le produit de deux, ou plusieurs, *idéaux entiers* est un *idéal entier*, qui est *inclus dans chacun d'eux.*

12. 3. *Base arithmétique.*

On peut distinguer le cas d'idéaux définis par une base arithmétique (**9. 1**), c'est ce que précise l'énoncé:

Si, dans la multiplication de deux idéaux $\mathbf{I}$ et $\mathbf{J}$, dont les termes des bases sont ρ_i et σ_j, *l'un d'eux*, au moins, *est défini par*

une base arithmétique, les produits des générateurs $\rho_i \times \sigma_j$, *forment une base arithmétique*, du produit $\mathbf{I} \times \mathbf{J}$:

$$(\ldots,\rho_i,\ldots) \text{ arithmétique} \quad \Rightarrow \quad (\ldots,\rho_i \times \sigma_j,\ldots) \text{ arithmétique.}$$

Il suffit d'utiliser le théorème caractéristique (**9. 5**) des bases arithmétiques. En prenant une base 1 τ, de (1), l'hypothèse est exprimée par l'existence de nombres entiers z_{ir}, tels que:

$$\rho_i \times \tau = \Sigma z_{ir} \times \rho_r; \qquad \text{tout } i \text{ de 1 à } h; \qquad r \text{ de 1 à } h.$$

Cette même condition est alors remplie par les produits, car:

$$(\rho_i \times \sigma_j) \times \tau = (\rho_i \times \tau) \times \sigma_j = \Sigma z_{ir} \times (\rho_r \times \sigma_j); \qquad r \text{ de 1 à } h; \quad \text{tous } i,j.$$

On a déjà utilisé, en fait, un cas particulier de cette construction, en formant une base arithmétique d'un idéal défini par une base algébrique (**10. 4**) (notamment d'un idéal principal, **11. 2**); il est égal à son produit par l'idéal (1), qui peut être défini par une base arithmétique de deux termes $\gamma_1\ \gamma_2$, de sorte que:

$$(\ldots,\rho_i,\ldots) = (\gamma_1,\ \gamma_2) \times (\ldots,\rho_i,\ldots) = (\ldots,\gamma_1 \times \rho_i, \gamma_2 \times \rho_i,\ldots).$$

C'est la base, qui a été justifiée par un raisonnement direct.

Un autre cas particulier d'une telle multiplication est donnée par la forme canonique d'un idéal (**8. 1**), ce qu'expriment les égalités:

$$q \times (m,\ \theta\text{—}c) = (q) \times (m,\ \theta\text{—}c) = (q \times m,\ q \times (\theta\text{—}c)).$$

L'idéal est égal au produit de l'idéal principal (q), de base q, par l'idéal canonique, de base arithmétique m, θ—c, d'où la base arithmétique $q \times m$, $q \times (\theta\text{—}c)$.

13. Propriétés des normes.

On va étudier, plus spécialement, la multiplication d'idéaux, mis sous leur forme canonique, et en déduire des propriétés des normes, qui justifient leur définition, donnée ci-dessus, à priori (**8. 1**).

THÉORÈME des normes. — *Le produit de deux idéaux conjugués est égal à l'idéal principal rationnel, dont une base est leur norme commune* (nombre rationnel positif, défini **8. 1**):

$$\mathbf{I}\times\mathbf{I}' = (\text{norme de } \mathbf{I}) \quad \text{ou} \quad (N(\mathbf{I})).$$

La norme d'un produit d'idéaux est égal au *produit de leurs normes*

$$\text{norme } (\mathbf{I}\times\mathbf{J}) = \text{norme de } \mathbf{I} \times \text{norme de } \mathbf{J}.$$

On peut établir d'abord la première propriété, pour un idéal canonique:

$$\mathbf{M} = (m,\ \theta\text{—}c), \qquad \mathbf{M}' = (m,\ \theta'\text{—}c);$$

une base (arithmétique) du produit $\mathbf{M}\times\mathbf{M}'$ est formée du produit des générateurs:

$$\mathbf{M}\times\mathbf{M}' = (m^2,\ m\times(\theta\text{—}c),\ m\times(\theta'\text{—}c),\ (\theta\text{—}c)\times(\theta'\text{—}c)).$$

Le dernier terme est égal à l'entier rationnel $F(c) = \pm m\times n$, de sorte que m peut être mis en facteur commun:

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

L'idéal $\mathbf{E}_1$ contient les éléments suivants qui sont des entiers rationnels:

$$m, \quad n, \quad \theta\text{—}c+\theta'\text{—}c = S\text{—}2c \equiv c'\text{—}c, \pmod{m},$$

où c' est zéro conjugué de c, de la congruence fondamentale, mod. m. On vérifie qu'ils sont premiers entre eux, en constatant qu'un nombre premier p ne peut les diviser simultanément. Il suffit de se borner à un diviseur p, de m, il divise les entiers $F(c)$, et $F(c')$ qui sont divisibles par m. Alors, *ou bien* p ne divise pas le discriminant du corps, les zéros c et c' de la congruence fondamentale sont distincts et p ne divise pas $c'\text{—}c$. *Ou bien*, il y a une racine double c et c' étant congrus, mod. p; mais alors p^2 ne divise pas $|F(c)| = m\times n$ et p ne divise pas n (propriétés de la congruence fondamentale **4** et **5**).

L'idéal $\mathbf{E}_1$ engendré par des entiers algébriques est entier, comme il contient trois entiers rationnels premiers entre eux, il contient leur p.g.c.d., qui est 1; il contient donc tous les entiers du corps et il est égal à $\mathbf{E}(\theta)$, ou à (1). Donc:

$$\mathbf{M}\times\mathbf{M}' = (m)\times(1) = (m).$$

Le cas général en résulte immédiatement, par application de la *commutativité* et de l'*associativité* de la multiplication:

$$\mathbf{I} = (q)\times(m,\ \theta\text{—}c), \quad \mathbf{I}' = (q)\times(m,\ \theta'\text{—}c);$$
$$\mathbf{I}\times\mathbf{I}' = (q)\times(q)\times(m,\ \theta\text{—}c)\times(m,\ \theta'\text{—}c) = (q^2)\times(m) = (q^2m).$$

La seconde propriété se déduit immédiatement de la première:

$$\text{Norme de } \mathbf{I}\times\mathbf{J} = (\mathbf{I}\times\mathbf{J})\times(\mathbf{I}'\times\mathbf{J}') = (\mathbf{I}\times\mathbf{I}')\times(\mathbf{J}\times\mathbf{J}') = [N(\mathbf{I})]\times[N(\mathbf{J})].$$

Le *carré d'un idéal double* **G** —égal à son conjugué, (**7**)— *est égal à l'idéal principal rationnel*, dont une base est la norme de **G**:

$$\mathbf{G} = q\times(g,\ \theta\text{—}c) = q\times(g,\ \theta'\text{—}c) = \mathbf{G}' \Rightarrow \mathbf{G}^2 = \mathbf{G}\times\mathbf{G}' = (q^2\times g).$$

Les cas particuliers indiqués pour la multiplication entraînent des cas particuliers et des conséquences du théorème des normes.

La *norme d'un idéal principal* (ρ) *est égale à la valeur absolue* $|N(\rho)|$, de la norme de ρ [égale pour les diverses bases possibles, (**11. 1**)], [ceci a déjà été établi par un raisonnement direct pour un idéal canonique, (**11. 3**)]

$$(\rho)\times(\rho') = (\text{norme de } \rho) \Rightarrow \text{norme de } (\rho) = |\text{norme de } \rho|.$$

En particulier la norme d'un *idéal principal rationnel* (q) est égale à q^2.

Un idéal entier **F** *contient sa norme*, puisque son idéal conjugué **F'** étant aussi entier, chacun d'eux contient $\mathbf{F}\times\mathbf{F}'$.

Il n'y a qu'*un idéal entier, de norme* 1, qui est l'*idéal unité*. Car un tel idéal étant contenu dans (1) et contenant (1), lui est égal.

14. Division des idéaux fractionnaires.

DÉFINITION. — *Deux idéaux*, non nuls, *sont* **inverses** —ou chacun d'eux est l'inverse de l'autre— *lorsque leur produit est égal à l'idéal unité* (1).

Les normes d'idéaux inverses sont des nombres inverses, puisque leur produit est égal à la norme de l'idéal (1). Cette remarque, jointe à l'expression du produit de deux idéaux conjugués (**13**), conduit à la construction d'idéaux inverses.

THÉORÈME des idéaux inverses. — Deux idéaux dont les normes sont des nombres inverses et dont les facteurs canoniques sont des idéaux conjugués:

$$\mathbf{I}_1 = q_1 \times (m,\ \theta\text{—}c), \quad \mathbf{I}_2 = q_2 \times (m,\ \theta'\text{—}c); \quad (q_1^2 m) \times (q_2^2 m) = 1$$

sont des *idéaux inverses.*

La vérification est immédiate. D'après cette propriété, tout idéal **I**, non nul, a (au moins) un *inverse*, qui, suivant une notation usuelle est désigné par une *puissance* d'*exposant* —1:

$$\mathbf{I} = q \times (m,\ \theta\text{—}c) \quad \Rightarrow \quad \mathbf{I}^{-1} = (q \times m)^{-1} \times (m,\ \theta'\text{—}c).$$

Un raisonnement, dont le caractère général a déjà été rappelé (**1. 2**), permet de déduire de cette existence la possibilité et la détermination de la *division* (opération inverse de la multiplication) des idéaux, ce qui comprend notamment la *détermination* —ou l'unicité— de l'*idéal unité* et de l'*inverse d'un idéal.*

THÉORÈME de la division des idéaux. — Etant donnés: un idéal **D**, appelé *dividende* et un idéal **I**, non nul, appelé *diviseur*; *il existe un et un seul idéal* **J**, appelé *quotient* de **D** par **I**, dont le produit par le diviseur **I** est égal au dividende **D**.

Le quotient d'un idéal, non nul, *par lui-même*, est égal à l'*idéal unité* (1), qui est, par suite le seul idéal neutre (**12. 2**) pour la multiplication.

Le quotient de l'idéal (1), par un idéal **I**, non nul, est l'*idéal* $\mathbf{I}^{-1}$ (construit par le théorème précédent), qui est, par suite, le seul idéal inverse de **I**.

Le *quotient*, d'un idéal **D** par un idéal **I**, non nul, est égal au produit de **D** par $\mathbf{I}^{-1}$ —inverse de **I**— :

$$\mathbf{I} \times \mathbf{I}^{-1} = (1) \begin{cases} \mathbf{I} \times \mathbf{J} = \mathbf{I} & \Leftrightarrow \quad \mathbf{J} = (1); \\ \mathbf{I} \times \mathbf{J} = (1) & \Leftrightarrow \quad \mathbf{J} = \mathbf{I}^{-1}; \\ \mathbf{I} \times \mathbf{J} = \mathbf{D} & \Leftrightarrow \quad \mathbf{J} = \mathbf{D} \times \mathbf{I}^{-1}. \end{cases}$$

La dernière équivalence est obtenue en multipliant les deux membres de l'égalité de gauche par $\mathbf{I}^{-1}$, ou les deux membres de l'égalité de droite par **I**. La première et la seconde équivalence sont de conséquences de la dernière.

La construction de l'*inverse* (déterminé) d'*un idéal* **I**, non nul, est équivalente à la *multiplication de son conjugué* **I'** *par l'inverse de leur norme commune.*

Cette règle est applicable à un idéal défini par une base (algébrique ou arithmétique), son inverse est défini par la base obtenu en multipliant les conjugués des éléments de la base de **I** par l'inverse de la norme de **I**. Pour un idéal principal, ceci donne une expression évidente par elle-même:

$$(\rho)^{-1} = (\rho' : N(\rho)) = \rho' \times (\rho^{-1} \times \rho'^{-1}) = (\rho^{-1}).$$

L'existence et les propriétés de la multiplication et de la division des idéaux, non nuls, peuvent être (partiellement) exprimées en disant que:

Les idéaux (fractionnaires) *non nuls*, d'un corps quadratique $\mathbf{R}(\theta)$, constituent un **groupe multiplicatif abélien** —ou commutatif— . Il sera, en général, désigné par $\mathcal{G}(\theta)$, ou simplement $\mathcal{G}$.

Ce groupe contient notamment les *puissances d'exposants entiers* (quelconques) de chacun de ses éléments, définies (suivant les notations usuelles) par les formules:

$$h \text{ entier positif:} \quad \mathbf{I}^h = \mathbf{I} \times \ldots \times \mathbf{I} \quad (h \text{ facteurs égaux});$$
$$\mathbf{I}^{-h} = (\mathbf{I}^{-1})^h = (\mathbf{I}^h)^{-1}; \quad \mathbf{I}^o = (1).$$

Ces puissances vérifient manifestement les règles usuelles de calcul:

$$\mathbf{I}^h \times \mathbf{I}^k = \mathbf{I}^{h+k}; \quad (\mathbf{I}^h)^k = \mathbf{I}^{h \times k}; \quad h,k \text{ entiers quelconques.}$$

Le groupe contient, par suite, les *monômes*, ou produits de puissances, $\mathbf{I}_1^{h1} \times \mathbf{I}_2^{h2} \times ..$, dont les règles de calcul sont également usuelles

14 bis. Sous groupe des idéaux principaux rationnels.

Dans le groupe $\mathcal{G}(\theta)$, la famille des idéaux principaux rationnels (q) (**11**) constitue un sous-groupe, qui sera noté $\mathfrak{Q}$, **isomorphe** au groupe multiplicatif des nombres rationnels positifs q.

Par isomorphisme, il faut entendre que la multiplication et la division des idéaux (q) sont obtenues par les opérations, de même nom, sur les nombres positifs q (ce qui est évident):

$$(q_1)\times(q_2) = (q_1\times q_2); \qquad (q)^{-1} = (q^{-1}).$$

Une **classe** $\mathfrak{M}$, **mod.** $\mathfrak{Q}$, *est l'ensemble des* (idéaux) *produits d'un même idéal canonique* $\mathbf{M}$, *par tous les idéaux du sous-groupe* $\mathfrak{Q}$ —ou l'ensemble de tous les idéaux, dont le facteur canonique est $\mathbf{M}$— :

$$\mathfrak{M}: \quad (q)\times\mathbf{M} = q\times\mathbf{M}; \qquad q \text{ nombres rationnels non nuls.}$$

Les classes $\mathfrak{M}$ constituent une *répartition* du groupe $\mathfrak{G}$; tout idéal, non nul, appartient à une classe et une seule: celle qui est définie par son facteur canonique.

Une classe $\mathfrak{M}$ peut aussi être engendrée en multipliant un de ses idéaux (quelconque) par tous les idéaux de $\mathfrak{Q}$ —ou par tous les éléments rationnels— :

$$(q)\times(q_0\times\mathbf{M}) = (q\times q_0)\times\mathbf{M}; \qquad q\times\mathbf{M} = (q\times q_0^{-1})\times(q_0\times\mathbf{M}).$$

L'idéal $\mathbf{M}$ est le seul idéal de la classe qui soit canonique; c'est donc un élément remarquable de cette classe, d'où son nom.

Les classes se *multiplient* (et se *divisent*) entre elles.

Le produit de deux classes $\mathfrak{M}_1$ et $\mathfrak{M}_2$, d'éléments canoniques $\mathbf{M}_1$ et $\mathbf{M}_2$ est l'ensemble des produits de chaque élément de l'une par chaque élément de l'autre. Cet ensemble est encore une classe, notée $\mathfrak{M}_1\times\mathfrak{M}_2$, constituée par les produits d'un de ses éléments (idéal) partous les nombres rationnels, non nuls —ou tous les idéaux de $\mathfrak{Q}$— :

$$\mathfrak{M}_1\times\mathfrak{M}_2: \quad (q_1\times\mathbf{M}_1)\times(q_2\times\mathbf{M}_2) = (q_1\times q_2)\times(\mathbf{M}_1\times\mathbf{M}_2);$$

Les nombres $q_1\times q_2$ peuvent prendre, comme q_1 et q_2 toutes les valeurs rationnelles, non nulles. L'idéal $\mathbf{M}_1\times\mathbf{M}_2$ n'est pas nécessairement canonique, mais *son facteur canonique est l'élément canonique de* $\mathfrak{M}_1\times\mathfrak{M}_2$.

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

(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.

1. Pour que l'idéal principal rationnel (q) soit premier, *il faut* que sa base q soit un nombre premier; si non la décomposition de q en un produit $q_1 \times q_2$, de deux entiers différents de 1, entraînerait celle de l'idéal (q) en un produit $(q_1) \times (q_2)$ de deux idéaux principaux, entiers, différents de (1).

D'après la propriété de la norme d'un produit (**13** et **15. 3**), l'idéal principal (q), de norme q^2 ne peut être décomposé, comme le nombre entier q^2, qu'en un produit de deux idéaux entiers, soit de normes 1 et q^2, soit de normes q et q. Pour que cette seconde circonstance soit impossible, *il faut et il suffit* qu'il n'y ait pas d'idéal, de norme q, c'est-à-dire *que la congruence fondamentale soit impossible*, mod. q.

2. Pour qu'un idéal canonique $(m, \theta—c)$ soit premier, il *faut* que sa norme soit un nombre premier, sinon la décomposition de m en plusieurs facteurs premiers, entraînerait la décomposition de **M** en un produit d'idéaux canoniques, donc entiers, différents de (1); en raison du théorème de décomposition (**15. 3**).

Cette condition est *suffisante*, car d'après la propriété de la norme d'un produit, l'idéal **M** ne peut alors être que le produit de deux idéaux entiers, de normes égales à 1 et p, c'est-à-dire de l'idéal unité et de lui-même.

On peut compléter la construction des idéaux premiers, du premier degré, par des propriétés de décomposition de leur norme m, ou, plus exactement de l'idéal principal rationnel (m) qui l'a pour base.

Si, pour un nombre premier p, qui n'est pas diviseur du discriminant D, *la congruence fondamentale est possible*, le polynôme $F(x)$ a deux zéros c, c', conjugués, incongrus, mod. p. Il y a deux idéaux premiers, de norme p, différents; ils sont conjugués (**13**) et leur produit est égal à *l'idéal principal* (p), qui *est ainsi décomposable*, dans $\mathbf{R}(\theta)$:

$$(p) = (p, \theta—c) \times (p, \theta—c') = (p, \theta—c) \times (p, \theta'—c)$$
$$= (p, \theta'—c') \times (p, \theta—c').$$

Pour un nombre premier p qui est *diviseur de* D, la congruence fondamentale est possible, mais $F(x)$ n'a qu'un zéro double c. Il n'y a qu'un idéal premier; de norme p; il est *double* —ou égal

à son conjugué— et son carré est égal à l'*idéal principal* (p), qui *est*, encore, *décomposable dans* $\mathbf{R}(\theta)$:

$$(p) = (p,\ \theta\text{—}c)\times(p,\ \theta\text{—}c) = (p,\ \theta\text{—}c)^2.$$

Les puissances (**14**) d'exposant entier positif h, des idéaux premiers, qui, dans le langage de l'algèbre moderne, sont appelés **idéaux primaires**, ont, suivant les cas, les formes canoniques suivantes:

$(q)^h = (q^h)$; $\quad F(x) \equiv 0,\ (\text{mod. } q)$; impossible;

$(p,\ \theta\text{—}c)^h = (p^h,\ \theta\text{—}c_h)$; $\quad p$ premier avec D; $\ c_h \equiv c,\ (\text{mod. } p)$.

$\left.\begin{array}{l}(p,\ \theta\text{—}c)^{2h} = (p^h);\\ (p,\ \theta\text{—}c)^{2h+1} = p^h\times(p,\ \theta\text{—}c)\end{array}\right\}$ p diviseur de D.

Les inverses de ces idéaux, ou les *puissances d'exposant négatif* (**14**) sont:

$(q)^{-h} = (q^{-h})$; $\quad (p,\ \theta\text{—}c)^{-h} = p^{-h}\times(p^h,\ \theta'\text{—}c_h)$;

$\left.\begin{array}{l}(p,\ \theta\text{—}c)^{-2h} = (p^{-h});\\ (p,\ \theta\text{—}c)^{-2h-1} = p^{-h-1}\times(p,\ \theta'\text{—}c)\end{array}\right\}$ p diviseur de D.

La propriété de *décomposition*, unique —ou déterminée—, d'un nombre rationnel en un *produit de puissances* (d'exposants entiers, non nuls, positifs ou négatifs) *de nombres premiers*, s'étend, mutatis mutandis, aux idéaux fractionnaires et premiers d'un corps quadratique.

Théorème de décomposition des idéaux fractionnaires. — Dans un corps quadratique $\mathbf{R}(\theta)$, *un idéal fractionnaire*, non nul, *est égal à un produit déterminé*, à l'ordre près des facteurs, *de puissances*, d'exposants entiers non nuls (positifs ou négatifs), *d'idéaux premiers différents.*

Pour un *idéal canonique* $\mathbf{M}$ —ou entier et de facteur rationnel égal à 1— on a établi ci-dessus (**15. 3**) sa décomposition en un produit de puissances d'idéaux canoniques, dont les normes sont des nombres premiers différents, et qui sont par conséquent premiers.

Pour un *idéal principal* (q), on peut d'abord décomposer le nombre rationnel q, mis éventuellement sous sa forme irréductible, en un produit de puissances de nombres premiers différents:

$$q = (\Pi p_i^{hi})\times(\Pi q_j^{kj}); \qquad h_i,\ k_j \text{ entiers non nuls.}$$

On distingue les nombres premiers q_j, qui sont normes d'idéaux principaux premiers (congruence fondamentale impossible) et les nombres premiers p_j qui sont normes d'idéaux canoniques. On en déduit la décomposition:

$$(q) = [\Pi(q_j)^{kj}] \times \Pi[(p_i, \theta - c_i)^{hi} \times (p_i, \theta' - c_i)^{hi}].$$

Pour un *idéal fractionnaire*, mis sous forme canonique:

$$\mathbf{I} = q \times (m, \theta - c) = (q) \times (m, \theta - c);$$

on décompose les deux facteurs, comme il vient d'être dit, on forme le produit des deux décompositions, on associe éventuellement les puissances d'un même idéal, dont on additionne les exposants; on supprime ceux dont l'exposant devient ainsi nul.

L'existence de cette décomposition peut aussi être établie directement comme conséquence de la définition des idéaux premiers et de la constitution du *groupe* G_I des idéaux non nuls (**14**). Le raisonnement est analogue à celui qui est fait ordinairement pour les nombres rationnels et entiers.

La démonstration de la détermination de la décomposition faite pour les nombres rationnels, par comparaison de deux décompositions et par récurrence sur le nombre de facteurs (de l'une d'elles) s'étend de même à la décomposition des idéaux.

18. Divisibilité des idéaux.

On peut étendre aux idéaux (d'un corps quadratique) les propriétés usuelles de la *divisibilité* des nombres fractionnaires et entiers, de l'arithmétique élémentaire.

Pour comparer plusieurs idéaux fractionnaires **A**, **B**, ..., on peut utiliser un système de h idéaux premiers $\mathbf{P}_i$, comprenant tous ceux qui figurent dans une *décomposition* (**17**) de (au moins) un des idéaux considérés. On peut alors introduire dans ces décompositions, les puissances d'exposant nul (donc égales à l'idéal unité) de ceux des $\mathbf{P}_i$ qui n'y figuraient pas. Chacun des idéaux considérés est ainsi égal à un produit de puissances des h idéaux $\mathbf{P}_i$:

$$\mathbf{A} = \Pi \mathbf{P}_i^{a_i}; \quad \mathbf{B} = \Pi \mathbf{P}_i^{b_i}; \ldots \quad a_i, b_i, \ldots \text{ nombres entiers};$$

et ils sont ainsi caractérisés par les systèmes de h exposants a_i; b_i;.

Leurs *produits*, ou leurs quotients, sont obtenus en *additionnant*, ou en retranchant, les exposants, de même indice:

$$(\Pi \mathbf{P}_i^{a_i}) \times (\Pi \mathbf{P}_i^{b_i}) = \Pi \mathbf{P}_i^{a_i+b_i}; \qquad (\Pi \mathbf{P}_i^{a_i}) : (\Pi \mathbf{P}_i^{b_i}) = \Pi \mathbf{P}_i^{a_i-b_i}.$$

Pour qu'un idéal, ainsi représenté, soit *entier*, il faut et il suffit qu'*aucun des exposants ne soit négatif*:

$$\{\Pi \mathbf{P}_i^{a_i} \text{ idéal entier}\} \Leftrightarrow \{a_i \geqslant 0, \text{ tout } i\}.$$

DÉFINITION. — *Un idéal* (fractionnaire) **M** *est* **divisible** *par un idéal* **D**, non nul, —ou est **multiple** de **D**— lorsqu'il *est égal au produit de* **D** *par un idéal entier* —ou lorsque *le quotient* $\mathbf{M} \times \mathbf{D}^{-1}$ *est un idéal entier*— :

$$\{\mathbf{M} = \mathbf{D} \times \mathbf{Q}, \quad \mathbf{Q} \subset (1)\} \quad \text{ou} \quad \mathbf{M} \times \mathbf{D}^{-1} \subset (1).$$

Deux idéaux fractionnaires **M** et **D** étant représentés par leurs décompositions avec un même système d'idéaux premiers $\mathbf{P}_i$, pour que **M** *soit divisible par* **D**, il faut et il suffit que *ses exposants soient au moins égaux à ceux de* **D**, de même indice:

$$\{(\Pi \mathbf{P}_i^{m_i}) \text{ divisible par } (\Pi \mathbf{P}_i^{d_i})\} \Leftrightarrow \{m_i \geqslant d_i; \quad \text{tout } i\}$$

En particulier un *idéal premier* est diviseur d'un *idéal entier* lorsqu'il figure dans sa décomposition (avec un exposant non nul). Il est diviseur d'un produit d'idéaux entiers, si et seulement si il est diviseur de l'un d'eux (au moins).

De la condition de divisibilité, on déduit (comme pour la divisibilité des nombres fractionnaires) la formation du **plus grand commun diviseur** et du **plus petit multiple commun,** d'un système d'idéaux fractionnaires, décomposés en produits de puissances d'un même système d'idéaux premiers:

$$\mathbf{U} = \Pi \mathbf{P}_i^{u_i}; \quad \mathbf{V} = \Pi \mathbf{P}_i^{v_i}; \ \ldots; \qquad u_i, v_i, \ldots \text{ entiers};$$

$$\text{p.g.c.d. } (\mathbf{U},\mathbf{V},\ldots) = \Pi \mathbf{P}_i^{\text{minimum } (u_i,v_i,\ldots)};$$

$$\text{p.p.c.m. } [\mathbf{U},\mathbf{V},\ldots] = \Pi \mathbf{P}_i^{\text{maximum } (u_i,v_i,\ldots)}.$$

On peut en déduire des relations mutuelles; en particulier leur *corrélation* peut être exprimée par la construction:

l'inverse du p.g.c.d. (ou du p.p.c.m.) *est égal au p.p.c.m.* (ou au p.g.c.d.) des inverses.

On peut aussi énoncer des propriétés caractéristiques, corrélatives, en utilisant une définition préalable.

DÉFINITION. — *Des idéaux* (fractionnaires) *sont* **premiers entre eux** (dans leur ensemble) *lorsque leur p.g.c.d. est égal à l'idéal unité.*

Il est équivalent de dire qu'ils sont entiers et qu'il n'y a aucun facteur premier commun à leurs décompositions, avec un exposant non nul.

On vérifie immédiatement, en utilisant les systèmes d'exposants que: *pour qu'un idéal fractionnaire*:

$$\mathbf{D} \text{ soit p.g.c.d.} \quad \text{ou} \quad \mathbf{M} \text{ soit p.p.c.m.}$$

d'un système d'idéaux fractionnaires $\mathbf{F}_i$, *il faut et il suffit que les quotients*:

$$\mathbf{F}_i \times \mathbf{D}^{-1} \quad \text{ou} \quad \mathbf{M} \times \mathbf{F}_i^{-1},$$

soient premiers entre eux (dans leur ensemble).

18 bis. Utilisation du plus grand commun diviseur.

On peut définir et établir les notions de *divisibilité* en suivant le même ordre que celui qui est couramment employé en Arithmétique élémentaire et qui a été étendu par DEDEKIND aux idéaux des corps de nombres algébriques.

On peut définir d'abord et directement la divisibilité des idéaux fractionnaires par l'une des propriétés caractéristiques suivantes, dont l'équivalence résulte de l'existence de l'inverse d'un idéal non nul.

L'idéal **M** est divisible par l'idéal **D**, *si le quotient* $\mathbf{M} \times \mathbf{D}^{-1}$ *est un idéal entier* (inclus dans l'idéal unité (1));

ou *si* **M** (ensemble d'éléments du corps) *est inclus dans* **D** **(10. 3)**

$$\mathbf{M} \times \mathbf{D}^{-1} \subset (1) \quad \Leftrightarrow \quad \mathbf{M} \subset \mathbf{D}.$$

On passe d'une inclusion à l'autre en multipliant les deux membres par **D** (inclusion de gauche), ou par $\mathbf{D}^{-1}$ (inclusion de droite).

Il en résulte immédiatement la réciprocité de la divisibilité des inverses:

$$\mathbf{M} \text{ divisible par } \mathbf{D} \quad \Leftrightarrow \quad \mathbf{D}^{-1} \text{ divisible par } \mathbf{M}^{-1};$$

car ces deux propriétés sont équivalentes (d'après la première définition de la divisibilité) à $\mathbf{M}\times\mathbf{D}^{-1} = (\mathbf{D}^{-1})\times(\mathbf{M}^{-1})^{-1}$ idéal entier.

On déduit de la deuxième définition, que *le plus grand commun diviseur*, qui est par suite *le plus petit ensemble contenant commun* (**10. 3**), d'idéaux définis par des bases algébriques, a une base formée par la réunion de ces bases:

$$\text{p.g.c.d. } ((..,\rho_i,..),(..,\sigma_j,..), \ldots) = (..,\rho_i,\ldots,\sigma_j, \ldots).$$

Les idéaux $(..,\rho_i,..)$, $(..,\sigma_j,..)$, ... sont inclus dans l'idéal construit qui en est donc un diviseur commun. En outre tout diviseur commun de ces idéaux contient les éléments de leurs bases, donc l'idéal qui a pour base leur réunion et qui est bien le plus petit idéal contenant commun.

On peut alors définir le *p.p.c.m.* en passant par l'intermédiaire des inverses, en application de la réciprocité de leur divisibilité:

$$\mathbf{M} = \text{p.p.c.m. } [\mathbf{F}_1, \mathbf{F}_2, ..] \quad \Leftrightarrow \quad \mathbf{M}^{-1} = \text{p.g.c.d. } (\mathbf{F}_1^{-1}, \mathbf{F}_2^{-1}, \ldots).$$

On peut envisager le p.g.c.d. (donc aussi le p.p.c.m.) comme une *opération* sur les idéaux; elle est *interne*, *associative* et *commutative*. *La multiplication est distributive* relativement à cette opération:

$$\mathbf{H}\times[\text{p.g.c.d. } (..,\mathbf{F}_i,..)] = \text{p.g.c.d. } (..,\mathbf{H}\times\mathbf{F}_i,..).$$

La définition d'un système d'idéaux premiers entre eux, reste la même et la relation entre p.g.c.d. et multiplication peut se faire par l'intermédiaire de la *propriété fondamentale de l'arithmétique*, qui reste valable pour des idéaux entiers:

on ne change pas le p.g.c.d. de deux idéaux entiers, quand on multiplie par un idéal premier avec l'autre.

Ceci résulte de la suite d'égalités, où **I** est un idéal entier et **A** et **B** des idéaux (entiers) premiers entre eux; les parenthèses désignant les p.g.c.d.:

$$(\mathbf{A},\ \mathbf{B}\times\mathbf{I}) = (\mathbf{A},\ \mathbf{A}\times\mathbf{I},\ \mathbf{B}\times\mathbf{I}) = (\mathbf{A},\ (\mathbf{A},\ \mathbf{B})\times\mathbf{I}) = (\mathbf{A},\ \mathbf{I}).$$

On établit ensuite les propriétés des idéaux conjugués et des normes, sans utiliser à nouveau les idéaux canoniques, mais seulement la construction des idéaux inverses; puis l'existence des *idéaux premiers*, c'est-à-dire les idéaux entiers dont les seuls diviseurs sont triviaux.

Enfin on en déduit l'existence et la détermination de la décomposition d'un idéal entier en produit d'idéaux premiers, puis l'existence et la détermination de la décomposition d'un idéal fractionnaire en un produit de puissances (d'exposants non nuls) d'idéaux premiers différents.

19. Corps (et domaine) principal.

Le qualificatif *principal* a déjà été utilisé pour désigner un idéal (**11**), lorsqu'il peut être engendré par une base algébrique d'un seul élément, défini au produit près par un diviseur de l'unité. On l'utilise aussi pour qualifier ceux des corps qui ne contiennent pas d'autres idéaux.

DÉFINITION. — *Un corps* $\mathbf{R}(\theta)$ [*ainsi que son domaine des entiers* $\mathbf{E}(\theta)$], *est appelé* **principal**, *lorsque tous ses idéaux*, fractionnaires, *sont principaux.*

Au moins dans un corps principal, il peut être commode d'appeler **facteur**, *un élément* ρ, *défini au produit près par un diviseur de l'unité*; [dans les corps imaginaires, à l'exception de $\mathbf{R}(i)$ et de $\mathbf{R}(j)$, un diviseur est ainsi un élément, défini, au produit près par $+1$ ou -1, ou, en abrégé, *au signe près*].

Dans un corps principal, un idéal fractionnaire est ainsi caractérisé par, ou *est associé à un facteur*, qui en constitue une base. La multiplication, et la division par un idéal non nul, sont équivalentes aux opérations de même nom sur les facteurs associés (**12** et **14**):

$$(\rho)\times(\sigma) = (\rho\times\sigma); \qquad (\rho):(\sigma) = (\rho:\sigma).$$

On peut vérifier que les éléments de base des idéaux étant des facteurs, c'est-à-dire étant définis au produit près par des diviseurs de l'unité ε, il en est de même des résultats des opérations:

$$\rho_1 = \sigma_1\times\varepsilon_1 \quad \text{et} \quad \rho_2 = \sigma_2\times\varepsilon_2$$
$$\Rightarrow \quad \rho_1\times\rho_2 = (\sigma_1\times\sigma_2)\times(\varepsilon_1\times\varepsilon_2); \qquad \rho_1:\rho_2 = (\sigma_1:\sigma_2)\times(\varepsilon_1:\varepsilon_2).$$

ε_1 et ε_2 étant des diviseurs de l'unité, c'est-à-dire étant des entiers algébriques, en même temps que leurs inverses, il en est de même de leur produit et de leur quotient (**3**).

Pour qu'un corps soit principal, il suffit que ses idéaux premiers du premier degré [canoniques] soient principaux; il en est toujours ainsi des idéaux premiers du second degré (p), qui sont en outre rationnels. Il en est par suite de même de tous les idéaux fractionnaires qui sont des produits des idéaux premiers et de leurs inverses.

Dans un corps principal, la théorie de la divisibilité est analogue à celle du corps des nombres fractionnaires (définis au signe près). Les définitions et les propriétés peuvent être énoncées indifféremment pour les idéaux, ou pour les facteurs associés.

Un facteur α, ou l'idéal (α) est *entier*, si α est un entier du corps [appartenant à $\mathbf{E}(\theta)$].

Un facteur μ *est divisible par un facteur* δ, ou l'idéal (μ) est divisible par l'idéal (δ), *si* $\mu \times \delta^{-1}$ *est un entier du corps.*

Un facteur entier π, est **premier**, lorsqu'il est la base d'un idéal (π) qui est premier; il est équivalent de dire que *le facteur* π *n'a que des diviseurs entiers triviaux*: le facteur 1 (ensemble des diviseurs de l'unité) et le facteur π lui-même (produits d'une de ses valeurs par les diviseurs de l'unité).

On peut alors prendre comme *propriété essentielle* de la divisibilité, le théorème de la décomposition d'un idéal (**17**), en remplaçant idéal par facteur (associé).

Dans un corps principal, *un facteur non nul*, non présumé entier, *est égal à un produit déterminé* (à l'ordre près des facteurs) de *puissances de facteurs premiers différents*, avec des exposants non nuls (positifs et négatifs).

On indique ci-dessous la construction des corps quadratiques principaux, au moins pour des valeurs limitées du discriminant. On donne sommairement ici quelques propriétés arithmétiques de l'un d'entre eux, particulièrement remarquable $\mathbf{R}(i)$, (ensemble des nombres imaginaires à coefficients rationnels). Ces propriétés peuvent être exprimées dans le langage général de la divisibilité mais elles peuvent aussi être interprétées comme des propriétés des nombres entiers rationnels et de leurs expressions possibles en sommes de deux carrés.

20. Corps R(i) et domaine des entiers de Gauss.

Le corps quadratique $\mathbf{R}(i)$, caractérisé par le polynôme fondamental:

$$F(x) = x^2+1; \quad D = -4;$$

peut être obtenu, par *adjonction* au corps des nombres rationnels, du symbole i, qui se comporte comme un élément dont le carré est égal à —1; (**1**). C'est l'ensemble des expressions, ou des éléments:

$$\rho = r+si, \quad \text{ou} \quad \rho = q\times\alpha, \quad \alpha = x+yi;$$

r,s nombres rationnels, *coefficients* de ρ; q, p.g.c.d. positif de r,s, *facteur rationnel* de ρ; x,y nombres entiers premiers entre eux, coefficients de α, *entier canonique* du corps (**3**).

Deux *éléments conjugués* se déduisent l'un de l'autre en changeant i en $-i$ (**2**):

$$\rho = r+si \quad \Leftrightarrow \quad \rho' = r-si;$$

(ce sont, au sens général de la théorie des nombres complexes, des *imaginaires conjuguées*).

Les *entiers* (algébriques) du corps (**3**) sont donnés par des coefficients entiers rationnels (ou ont un diviseur rationnel entier); ils sont appelés **entiers de Gauss** (qui a étudié leur arithmétique); ils sont engendrés par la *base arithmétique libre* $1\ i$ (canonique).

Les diviseurs de l'unité (déjà indiqués; **3**) sont quatre éléments d'un groupe (cyclique d'ordre 4):

$$i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = +1.$$

On peut représenter géométriquement les éléments $r+si$, du corps $\mathbf{R}(i)$, par les points d'un plan, de coordonnées, r,s, relativement à deux axes rectangulaires. Des éléments conjugués sont représentés par des points symétriques relativement à l'axe réel (dont le vecteur unité représente le « symbole » 1).

Les points représentatifs des entiers sont les sommets d'un quadrillage de côtés parallèles aux axes et dont les côtés sont de longueur 1.

Les produits d'un élément par les quatre diviseurs de l'unité sont représentés par les sommets d'un carré, dont le centre est l'origine (représentant 0) et dont les solmets sont déduits de l'un d'eux par des rotations autour de cette origine, d'angles:

$$\pi : 2, \quad 2\times(\pi : 2) = \pi; \qquad 3\times(\pi : 2), \quad 4\times(\pi : 2) = 2\pi.$$

Pour étudier la *congruence fondamentale* (**5**), relativement à un *module premier* impair p, on peut considérer le corps des entiers, définis mod. p, ou, plus exactement le *groupe* des $p-1$ entiers non nuls [1]). Ce groupe est *cyclique*, c'est-à-dire engendré par les puissances d'un entier générateur convenable g, dont la puissance d'exposant $p-1$ est congrue à $+1$ et dont celle d'exposant $(p-1):2$ est égale à -1. [On sait qu'il y a ainsi $\varphi(p-1)$ générateurs possible, appelés *racines primitives.*]

Si $p-1$ n'est pas divisible par 4; -1 n'est pas congru à un carré; la congruence n'a pas de solution.

Sinon, c'est-à-dire si p est congru à $+1$, mod. 4, la congruence a deux solutions simples, qui sont congrues aux puissances de g, d'exposants $(p-1):4$ et $[3(p-1)]:4$; ce sont d'ailleurs des nombres opposés, mod. p.

Pour le *module* 2, la congruence a une solution double qui est 1, ce nombre annule en effet x^2+1 et $2x$, mod. p [1]).

Pour un *module composé* m (**6**), la congruence a des solutions si, et seulement si, le module m est le produit ou le double d'un produit de s puissances de nombres premiers, dont chacun est congru à $+1$, mod. 4; il y a alors 2^{s-1} couples de solutions conjuguées.

Ces considérations permettent de construire les idéaux canoniques du corps (**7**) qui sont:

$$(m, \ i-c); \qquad c^2+1 \equiv 0, \quad (\text{mod. } m).$$

On en déduit les expressions des idéaux ou des facteurs premiers du corps, ou du domaine $\mathbf{E}(i)$:

1. *Le nombre* 2 *est égal au produit de deux éléments conjugués* $1+i$ et $1-i$; qui sont égaux, au produit près par un diviseur de

1) L'étude de ce groupe est faite dans tous les Traités de Théorie élémentaire des Nombres.

l'unité donc sont deux bases possibles d'un même *idéal principal*, qui est *premier*; le facteur 2 est le carré d'un *facteur* premier.

2. *Un nombre premier q impair, congru à* —1, mod. 4, est la base d'un *idéal principal*; qui est *premier*; q est un *facteur* premier.

3. *Un nombre premier p impair, congru à* +1, mod. 4, est égal au *produit de deux idéaux principaux, conjugués*, qui sont *premiers*; p est produit de deux facteurs premiers.

La vérification de la propriété de 2 est immédiate:

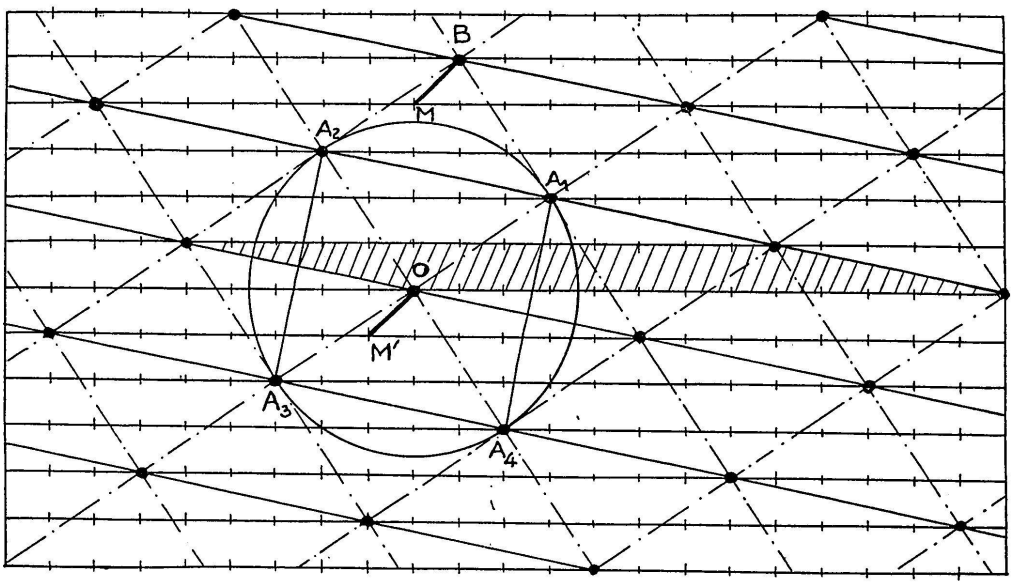
$$2 = (1+i)\times(1-i) = -i\times(1+i)^2.$$

Un nombre premier q, congru à —1, mod. 4, ne peut être la norme d'un idéal canonique; l'idéal principal (q) n'a donc pas de diviseur (entier) sauf lui-même et l'idéal unité.

Un nombre premier p, congru à +1, mod. 4, est la norme commune de deux idéaux canoniques, dont les racines sont deux zéros conjugués c,c', du polynôme x^2+1, considéré mod. p. L'idéal principal (p) en est le produit et chacun d'eux est premier:

$$(p) = (p,\ i-c)\times(p,\ i-c'); \qquad c+c' \equiv 0, \pmod{p}.$$

Reste à montrer que ces deux idéaux sont *principaux*, ceci résulte des propriétés générales, exposées ci-dessous sur les *idéaux réduits*. On peut en donner une démonstration directe par des considérations géométriques sur le *quadrillage* des points représentant les entiers du corps.



Les éléments de l'idéal $(p, i—c)$ sont les entiers algébriques exprimés par:

$$x \times p + y \times (i—c) = (xp—yc) + yi; \qquad x,y \text{ entiers rationnels.}$$

Les points représentatifs sont dans le quadrillage (de tous les entiers) l'ensemble **P** des sommets du réseau de parallélogrammes engendré par les vecteurs joignant l'origine 0 aux points de coordonnées $(p,0)$ et $(—c,1)$. Parmi les points de **P**, on peut distinguer ceux qui sont les plus proches de l'origine (de distance au moins égale à 1). Il en existe au moins 4 (A_1,A_2,A_3,A_4), à une même distance r, représentant des entiers:

$$a+bi, \quad —b+ai = (a+bi) \times i,$$
$$—a—bi = (a+bi) \times i^2, \quad b—ai = (a+bi) \times i^3;$$

ils forment un carré de centre 0. A l'intérieur du cercle circonscrit à ce carré (circonférence exclue) il n'y a pas de point de **P**. (La figure représente les entiers de l'idéal $(13, i—5)$; le point A_1, représente $3+2i = 13+2 \times (i—5)$.)

On peut alors vérifier que le réseau de parallélogrammes peut être engendré par deux vecteurs successifs OA_1 et OA_2, en constatant que le parallélogramme OA_1BA_2 construit avec ces deux vecteurs ne renferme pas de point de **P**. Effectivement un tel point M, étant à l'extérieur du cercle de centre 0 et de rayon r, ne pourrait être que dans le triangle BA_1A_2, et il serait à une distance de B inférieure à r, ce qui est impossible pour une raison évidente de translation, car le point M' extrémité du vecteur OM' équipolent à BM serait à une distance de 0 inférieure à r, tout en appartenant à **P**.

Les points A_1 et A_2 représentent donc des éléments d'une base arithmétique libre de l'idéal et l'élément p est égal à une expression linéaire, à coefficients entiers rationnels x, y:

$$p = x \times (a+bi) + y \times (—b+ai) \quad \Leftrightarrow \quad 0 = xb+ya \text{ et } p = xa—yb.$$

Mais p étant premier, la dernière relation exige que a, b d'une part, x, y d'autre part sont premiers entre eux. De plus, ni a, ni b ne sont nuls; car les idéaux $(bi, —b)$ et (a, ai) sont des idéaux principaux rationnels. L'avant-dernière relation exige donc que:

$$x = a \text{ ou } —a, \quad y = —b \text{ ou } b; \qquad p = a^2+b^2.$$

La dernière relation exprime que p est décomposable en un produit de deux entiers du corps; définis au produit près par des diviseurs de l'unité:

$$p = (a+bi)(a-bi) = (-b+ai)(-b-ai)$$
$$= (-a-bi)(-a+bi) = (b-ai)(b+ai).$$

Ces entiers sont les générateurs d'idéaux conjugués; les propriétés des produits d'idéaux montrent que ces idéaux principaux ont pour norme p et pour racines c et c', solutions de la congruence fondamentale, avec la correspondance:

$$a+bc \equiv 0, \quad a-bc' \equiv 0, \quad (\text{mod. } p).$$

Les propriétés générales de la congruence fondamentale permettent alors d'affirmer la propriété générale suivante:

un *facteur rationnel* m, est décomposable dans $\mathbf{R}(i)$ en un *produit de deux facteurs algébriques conjugués*, ou l'*entier positif* m *est égal à une somme de deux carrés* (de nombres entiers) si et seulement si il est égal au produit ou au double du produit de s puissances de nombres congrus à $+1$, mod. 4; il y a alors 2^{s-1} *décompositions en somme de deux carrés*, différentes (sans distinctoin d'ordre).

(A suivre)