18 bis. Utilisation du plus grand commun diviseur.

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:

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