14 bis. Sous groupe des idéaux principaux rationnels.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **6 (1960)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

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:

$$h \text{ entier positif:} \quad \mathbf{I}^h = \mathbf{I} \times \ldots \times \mathbf{I} \quad (h \text{ facteurs égaux});$$
$$\mathbf{I}^{-h} = (\mathbf{I}^{-1})^h = (\mathbf{I}^h)^{-1}; \quad \mathbf{I}^0 = (1).$$

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

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

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

Une classe $\mathcal{M}$ peut aussi être engendrée en multipliant un de ses idéaux (quelconque) par tous les idéaux de $\mathcal{Q}$ —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 **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 $\mathcal{M}_1$ et $\mathcal{M}_2$, 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 $\mathcal{M}_1\times\mathcal{M}_2$, constituée par les produits d'un de ses éléments (idéal) partous les nombres rationnels, non nuls —ou tous les idéaux de $\mathcal{Q}$— :

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

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* $\mathcal{M}_1\times\mathcal{M}_2$.

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; $\mathcal{M} \times \mathfrak{Q} = \mathcal{M}$.

Deux classes $\mathcal{M}$ et $\mathcal{M}'$ 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 $\mathcal{M}$ et $\mathcal{M}'$ 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.