Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 6 (1960)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LES CORPS QUADRATIQUES
Autor: Châtelet, A.
Kapitel: 17. Idéaux premiers.
DOI: https://doi.org/10.5169/seals-36339

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 $\mathbf{P}_i$:

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