

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

**Artikel:** L'ARITHMÉTIQUE DES CORPS QUADRATIQUES  
**Autor:** Châtelet, Albert  
**Kapitel:** 11. Idéaux principaux.  
**DOI:** <https://doi.org/10.5169/seals-36338>

#### Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

#### Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

#### Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 16.01.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

On peut choisir notamment, comme il a été fait pour le théorème caractéristique (9.5), une base  $1\tau$ , des entiers. La modification de la base se borne alors à l'adjonction des  $h$  termes  $\tau \times \rho_i$ :

$$(\dots, \rho_i, \dots) = (\dots, \rho_i, \dots; \dots, \tau \times \rho_i, \dots)$$

Le système de  $2h$  termes est encore une base algébrique de **I**: d'une part tous ses termes, produits par des entiers du corps des termes de **I** appartiennent à **I**. D'autre part l'idéal engendré par cette nouvelle base contient tous les éléments des idéaux:

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

et notamment tous les termes  $\rho_i$ ; donc l'idéal **I**.

Reste à vérifier que cette base vérifie la condition caractéristique d'une base arithmétique. Les produits  $\gamma_j \times \tau$  pouvant être construits avec la base arithmétique  $\gamma_1 \gamma_2$ , on en conclut, pour chaque terme de la nouvelle base:

$$\begin{aligned} (\gamma_j \times \rho_i) \times \tau &= \rho_i \times (\gamma_j \times \tau) = \rho_i \times (x_j \times \gamma_1 + y_j \times \gamma_2) \\ &= x_j \times (\rho_i \times \gamma_1) + y_j \times (\rho_i \times \gamma_2) \end{aligned}$$

les  $x_j, y_j$  sont des nombres entiers, dépendant de  $j$  égal à 1 ou 2 et de  $i$  (de 1 à  $h$ ). Les produits par  $\tau$ , des termes de la nouvelle base, peuvent donc être effectivement construits par additions et soustractions, au moyen de ces termes eux-mêmes.

## 11. Idéaux principaux.

DÉFINITION (Rappel; 10.2). — *Un idéal fractionnaire est appelé **principal**, lorsqu'il peut être engendré par une base d'un seul élément  $\rho$ ; c'est-à-dire lorsqu'il est égal au produit par l'élément  $\rho$  de l'idéal unité (1).*

*L'élément  $\rho$  est une **base** (sous entendu algébrique) de l'idéal qui est lui-même désigné, comme il a été dit par:*

(ρ) abréviation de  $\rho \times (1)$ , ou  $\rho \times \mathbf{E}(0)$ .

*L'idéal nul est un idéal principal de base 0. Pour un idéal principal, non nul, toutes les bases sont égales aux produits de l'une*

*d'elles* (arbitraire) par les diviseurs de l'unité, du corps (3), qui peuvent se réduire à +1 et —1. Les valeurs absolues des normes de ces bases sont égales entre elles.

En particulier les bases de l'idéal unité (1), ou  $\mathbf{E}(\theta)$ , sont les diviseurs de l'unité.

La démonstration de cette propriété est analogue à celle qui établit la relation entre les bases arithmétiques de deux éléments. Pour que les idéaux principaux  $(\rho_1)$ ,  $(\rho_2)$  soient égaux, il faut et il suffit que la base de chacun d'eux appartienne à l'autre, ce qui est équivalent à leur inclusion réciproque:

$$\rho_2 = \xi_1 \times \rho_1 \quad \text{et} \quad \rho_1 = \xi_2 \times \rho_2; \quad \xi_1, \xi_2 \text{ entiers du corps.}$$

Il en résulte:

$$\rho_2 = (\xi_1 \times \xi_2) \times \rho_2 \Rightarrow \xi_1 \times \xi_2 = 1.$$

L'implication est obtenue en multipliant les deux membres de la première égalité par l'inverse de  $\rho_2$ , supposé non nul. Les entiers  $\xi_1$  et  $\xi_2$ , sont inverses l'un de l'autre, donc diviseurs de l'unité, (3). La condition est manifestement suffisante. En outre:

$$|N(\rho_1)| = |N(\rho_2) \times N(\xi_2)| = |N(\rho_2)|.$$

*Un idéal principal est qualifié rationnel lorsque l'une de ses bases est un élément rationnel q, du corps. Son facteur rationnel est égal à la valeur absolue de q, son facteur canonique est l'idéal unité.*

## 11. 2. Base canonique d'un idéal principal.

D'après la construction générale de 10. 4, on obtient des bases arithmétiques d'un idéal principal  $(\rho)$ , en multipliant par  $\rho$  des bases arithmétiques de (1):

$$\rho \times \gamma_1 \quad \rho \times \gamma_2; \quad \text{notamment: } \rho \quad \rho \times \tau.$$

Ces bases ayant deux termes sont *libres* (Th. de construction; 9. 1). Elles sont d'ailleurs déduites de l'une d'elles par des substitutions unimodulaires, puisqu'il en est ainsi des bases arithmétiques de  $\mathbf{E}(\theta)$ .

On peut utiliser cette construction pour obtenir la forme canonique d'un idéal principal.

THÉORÈME de la forme canonique d'un idéal principal. — Pour un idéal principal  $(\rho)$ , de base  $\rho$ , élément du corps:

1. *Le facteur rationnel de l'idéal est égal au facteur rationnel de (l'élément de) la base  $\rho$ :*

$$(\rho) = (r+s\theta) = q \times \mathbf{M}, \quad \mathbf{M} \text{ canonique}; \quad q = \text{p.g.c.d. } (r, s).$$

2. Le *facteur canonique  $\mathbf{M}$*  est égal à l'idéal principal  $(\alpha)$ , dont une base  $\alpha$  est l'*entier canonique* du corps égal au quotient de  $\rho$  par le facteur  $q$ :

$$\mathbf{M} = (\alpha); \quad \alpha = a+b\theta; \quad \{a = r \times q^{-1}, \quad b = s \times q^{-1}\}.$$

En explicitant la construction d'une base arithmétique avec la base 1  $\tau = \theta - S$ , de (1), on obtient:

$$\rho \times 1 = r+s\theta, \quad \rho \times (\theta - S) = -(rS + sN) + r\theta.$$

Le facteur rationnel est bien égal au p.g.c.d. positif de  $r, s$  qui sont multiplicateurs de  $\theta$ .

Le facteur canonique en résulte, sa base  $a+b\theta$  est un entier canonique, puisque les multiplicateurs  $a, b$  sont premiers entre eux.

On retrouve bien ainsi la forme canonique d'un idéal principal rationnel, de base  $q = q+0 \times \theta$ :

$$(q) = |q| \times (1, \theta) = |q| \times (1).$$

### 11. 3. Idéal principal canonique.

De ce théorème, on déduit immédiatement les propriétés caractéristiques:

Pour qu'un idéal principal  $(\alpha)$  soit *entier*, il faut et il suffit que sa base  $\alpha$  soit un *entier du corps*.

Pour qu'il soit un *idéal canonique* (à fortiori entier), il faut et il suffit que sa base soit un *entier canonique du corps*.

$$(\alpha) \text{ canonique} \Leftrightarrow \alpha \text{ canonique.}$$

Pour calculer une base canonique d'un idéal principal, il suffit de chercher la norme et une racine de son facteur canonique  $\mathbf{M}$ , qui est un idéal canonique. En appliquant la construction générale de 10. 3, on obtient les propriétés suivantes.

THÉORÈME de la base canonique d'un idéal principal canonique. — Pour un idéal principal canonique:

$(a+b\theta)$ ;  $a, b$  (nombres entiers) premiers entre eux;

1. *Une racine c est donnée par l'expression:*

$$c = -(aa' + Sab' + Nbb'); \quad ba' - ab' = +1.$$

2. *La norme m est égale à la valeur absolue de la norme de (l'élément de) la base  $\alpha$ :*

$$m = |N(\alpha)| = |a^2 + Sab + Nb^2|.$$

L'existence des nombres entiers  $a'$ ,  $b'$  résulte de ce que  $a, b$  sont premiers entre eux; ces quatre nombres forment une matrice carrée unimodulaire, qui permet de construire une base arithmétique libre de (1):

$$\begin{vmatrix} a & b \\ a' & b' \end{vmatrix} \times \begin{vmatrix} 1 \\ \theta' \end{vmatrix} = \begin{vmatrix} a + b\theta' = \alpha' \\ a' + b'\theta' = \beta' \end{vmatrix}$$

On en déduit une base arithmétique de l'idéal  $(\alpha)$ :

$$(\alpha) = (\alpha \times \alpha', \quad \alpha \times \beta') \quad \begin{cases} \alpha \times \alpha' = N(\alpha) = a^2 + Sab + Nb^2 \\ \alpha \times \beta' = (aa' + Sab' + Nbb') + \theta. \end{cases}$$

Mais cette base est canonique puisque son premier terme est un entier rationnel et que le second est de la forme  $\theta - c$ . On obtient bien les expressions de l'énoncé.

En calculant la valeur  $F(c)$ , pour le nombre  $c$ , on obtient:

$$F(c) = (a^2 + Sab + Nb^2) \times (a'^2 + Sa'b' + Nb'^2);$$

elle est bien divisible par  $m$ .

On peut aussi vérifier que le nombre  $c$  n'est défini qu'à l'addition près d'un multiple de  $m$ , les nombres  $a'$  et  $b'$  n'étant eux-mêmes définis qu'à l'addition près d'équimultiples de  $a$  et  $b$ .

On aurait pu aussi utiliser une base arithmétique:

$$a + b\theta, \quad (a + b\theta) \times (\theta - S) = -(Sa + Nb) + a\theta;$$

on obtient la valeur de  $c$  par le calcul:

$$(a+b\theta) \times a' + [-(Sa+Nb)+a\theta] \times (-b') = (aa'+Sab'+Nb^2) + \theta.$$

On obtient la norme en prenant le p.g.c.d. des nombres:

$$\begin{aligned} a \times (ba'-ab') + c \times b &= -b' \times (a^2 + Sab + Nb^2) \\ -(Sa+Nb) \times (ba'-ab') + c \times a &= -a' \times (a^2 + Sab + Nb^2). \end{aligned}$$

Dans le cas particulier d'une base  $a+\theta$ , le calcul se simplifie ( $a'=1, b'=0$ ), la racine est égale à  $-a$  et la norme à  $F(-a)$ , ce qui peut être exprimé par la forme canonique:

$$(\theta-c) = (|F(c)|, \theta-c); \quad [\text{d'ailleurs } F(c) = (\theta-c) \times (\theta'-c)].$$

(A suivre)