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: 9. Bases arithmétiques d'un idéal.
DOI: https://doi.org/10.5169/seals-36338

8. 5. *Idéaux conjugués.*

Les définitions (constructive et axiomatique) de la conjugaison des idéaux canoniques s'étendent évidemment aux idéaux fractionnaires.

DÉFINITION. — *Deux idéaux fractionnaires sont appelés* **conjugués**, et sont désignés par une même lettre, avec et sans accent **I** et **I'**, lorsqu'ils ont des *facteurs rationnels égaux* et des *facteurs canoniques conjugués*:

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

Ils ont par suite des *bases canoniques conjuguées* (**2**).

Il est équivalent de dire (définition axiomatique) que *deux idéaux* (fractionnaires) *conjugués* sont constitués par des *éléments*, du corps, *respectivement conjugués* (**2**), construits d'ailleurs avec des coordonnées égales, relativement à des bases conjuguées.

$$\rho = \|x\ y\| \times \begin{Vmatrix} q \times m \\ q \times (\theta - c) \end{Vmatrix} \in \mathbf{I} \quad \Leftrightarrow \quad \rho' = \|x\ y\| \times \begin{Vmatrix} q \times m \\ q \times (\theta' - c) \end{Vmatrix} \in \mathbf{I}'.$$

Un idéal fractionnaire est **double**, lorsqu'il est égal à son conjugué. Il faut et il suffit que son facteur canonique soit double.

9. Bases arithmétiques d'un idéal.

La construction des éléments ρ, d'un idéal **I**, fractionnaire (ou canonique), par les valeurs d'une forme, dont le couple de générateurs est une *base canonique* et dont les valeurs des variables sont des nombres entiers est une généralisation de la construction des entiers du corps (**4**), ou des éléments du domaine $\mathbf{E}(\theta)$, qui est d'ailleurs un idéal trivial (unité).

On réalise encore ainsi une *représentation propre*, des éléments de l'idéal par les couples de nombres entiers, ou par les sommets d'un réseau de parallélogrammes.

Si l'idéal est entier —ou contenu dans $\mathbf{E}(\theta)$— on peut représenter l'idéal par un réseau contenu dans celui qui représente $\mathbf{E}(\theta)$.

Les parallélogrammes de ce sous-réseau (avec une frontière convenablement précisée) contiennent tous le même nombre de sommets du réseau primitif.

On est ainsi conduit à étendre aux idéaux la notion de *base arithmétique*, éventuellement *libre*, définie pour **E**(θ) (**4. 1**).

DÉFINITIONS. — *On appelle* **base arithmétique**, d'un idéal fractionnaire **I**, un système de h éléments ρ_i, de **I**, tel que *tout élément* ρ, de **I**, *soit égal à* (au moins) *une forme* (linéaire) *de ces termes* ρ_i, pour des valeurs des variables —ou des *multiplicateurs*— égales à des *nombres entiers*:

$$\rho = \Sigma z_i \times \rho_i; \quad i \text{ de } 1 \text{ à } h; \quad z_i \text{ nombres entiers.}$$

Il est équivalent de dire que tout élément de **I** peut être construit par additions et soustractions au moyen des termes de la base.

Une *base arithmétique*, d'un idéal **I**, non nul, *doit contenir au moins deux termes*, non nuls, car les éléments $x \times \rho_0$, construits avec un seul terme ρ_0 non nul, ne peuvent contenir le produit $\theta \times \rho_0$, qui d'après la troisième qualité de la définition axiomatique (**8. 2**) doit appartenir à l'idéal contenant ρ_0. Cette impossibilité résulte de l'implication déjà indiquée pour **E**(θ):

$$\{x \text{ nombre entier et } \rho_0 \neq 0\} \quad \Rightarrow \quad \theta \times \rho_0 - x \times \rho_0 = (\theta - x) \times \rho_0 \neq 0.$$

Une base arithmétique d'un idéal **I**, *est qualifiée* **libre**, lorsqu'elle définit une *représentation propre* des éléments ρ, de **I**, *par les systèmes de multiplicateurs* z_i, qui sont encore appelés les *coordonnées* des éléments ρ, relativement à cette base libre.

Pour un idéal (non nul), $\mathbf{I} = q \times (m, \theta - c)$, on constate que les bases arithmétiques de $h = 2$ termes, $\rho_1\ \rho_2$, sont encore les seules qui soient libres. En adoptant la disposition déjà indiquée pour l'idéal trivial **E**(θ), la construction d'un élément ρ, de **I**, défini par ses coordonnées $x\ y$, relativement à la base canonique, ou $z_1\ z_2$, relativement à la nouvelle base est exprimée par les produits matriciels

$$\rho = \|x\ y\| \times \begin{Vmatrix} q \times m \\ \\ q \times (\theta - c) \end{Vmatrix} \quad \text{ou} \quad \rho = \|z_1\ z_2\| \times \begin{Vmatrix} \rho_1 \\ \\ \rho_2 \end{Vmatrix}.$$

La construction de ces bases, et des coordonnées relatives, sont les mêmes que dans le cas particulier de l'idéal trivial.

THÉORÈME de construction des bases arithmétiques libres. — Pour un idéal fractionnaire, non nul, *toute base arithmétique, de deux termes*, est déduite d'une base canonique *par une substitution* (linéaire) *unimodulaire*; c'est-à-dire par multiplication par une matrice carrée $\overline{A}$ dont les termes sont des nombres entiers et le déterminant égal à $+1$ ou à -1.

Cette base est libre et *les coordonnées*, d'un élément de **I**, *relativement aux deux bases* (canonique et nouvelle) *sont liées par la substitution* (unimodulaire) *contragrédiente*; c'est-à-dire que les anciennes sont obtenues en multipliant les nouvelles (en ligne, si les bases sont en colonnes), par la même matrice $\overline{A}$:

$$\left\|\begin{matrix}\rho_1\\ \rho_2\end{matrix}\right\| = \overline{A}\times\left\|\begin{matrix}q\times m\\ q\times(\theta-c)\end{matrix}\right\| \quad \text{et} \quad \|x\ y\| = \|z_1\ z_2\|\times\overline{A}$$

$$\overline{A} = \left\|\begin{matrix}x_1 & y_1\\ x_2 & y_2\end{matrix}\right\| \qquad \begin{matrix}x_1,y_1;\ x_2,y_2 \text{ nombres entiers;}\\ x_1y_2-x_2y_1 = +1 \quad \text{ou} \quad -1.\end{matrix}$$

On peut aussi bien multiplier les anciennes coordonnées, disposées en colonne (comme les bases), à gauche, par la matrice $\widetilde{A}^{-1}$ *inverse de la transposée* de $\overline{A}$.

La démonstration de cette propriété, faite dans le cas de l'idéal trivial $\mathbf{E}(\theta)$, reste valable pour un idéal fractionnaire quelconque, non nul.

Il en résulte aussi, plus généralement, que deux bases arithmétiques, d'un idéal, et les coordonnées d'un élément, relativement à ces bases, sont liées par deux *substitutions unimodulaires contragrédientes*.

En particulier pour deux bases canoniques $(m,\ \theta-c)$; $(m,\ \theta'-c')$ dont les racines ont pour somme $c+c' = S-hm$, et pour les coordonnées x,y et x',y' d'un même élément relativement à ces bases, les substitutions sont explicitement:

$$\left\|\begin{matrix}m\\ \theta'-c'\end{matrix}\right\| = \left\|\begin{matrix}1 & 0\\ h & -1\end{matrix}\right\|\times\left\|\begin{matrix}m\\ \theta-c\end{matrix}\right\| \qquad \|x\ y\| = \|x'\ y'\|\times\left\|\begin{matrix}1 & 0\\ h & -1\end{matrix}\right\|$$

On peut aisément préciser les transformations des bases arithmétiques dans les deux opérations étudiées ci-dessus (**8. 4** et **8. 5**) sur les idéaux fractionnaires.

9. 2. *Multiplication d'un idéal par un élément.*

Si deux idéaux fractionnaires se déduisent l'un de l'autre par multiplication par un élément non nul (**8. 4**):

$$\mathbf{J} = \lambda \times \mathbf{I} \quad \text{et} \quad \mathbf{I} = \mu \times \mathbf{J}; \qquad \lambda \times \mu = 1$$

il en est de même de leurs bases arithmétiques libres (de 2 termes)

$$\begin{aligned} &\rho_1\ \rho_2 \text{ base de } \mathbf{I} \quad \Rightarrow \quad \lambda \times \rho_1 \ \ \lambda \times \rho_2 \text{ base de } \mathbf{J} \\ &\sigma_1\ \sigma_2 \text{ base de } \mathbf{J} \quad \Rightarrow \quad \mu \times \sigma_1 \ \ \mu \times \sigma_2 \text{ base de } \mathbf{I}. \end{aligned}$$

En particulier les bases arithmétiques libres d'un idéal sont égales aux produits par son facteur rationnel des bases arithmétiques libres de son facteur canonique. Dans ce cas les bases canoniques sont conservées, ce qui n'est pas vrai dans le cas général d'une multiplication par un élément non rationnel.

9. 3. *Idéaux conjugués et base matricielle.*

Pour *deux idéaux* fractionnaires *conjugués* **I** et **I'** (**8. 5**), *les bases arithmétiques libres* (de deux éléments) *sont respectivement conjuguées. Les coordonnées* de deux éléments conjugués ρ, de **I** et ρ' de **I'**, relativement à ces bases respectives, *sont égales*:

$$\rho = \|z_1\ z_2\| \times \left\| \begin{matrix} \rho_1 \\ \rho_2 \end{matrix} \right\| \in \mathbf{I} \quad \Leftrightarrow \quad \rho' = \|z_1\ z_2\| \times \left\| \begin{matrix} \rho'_1 \\ \rho'_2 \end{matrix} \right\| \in \mathbf{I}'.$$

On peut considérer simultanément des couples d'idéaux conjugués **I** et **I'**, et les couples d'éléments conjugués ρ de **I** et ρ' de **I'**. On appelle alors **base matricielle**, du couple **I**, **I'**, une matrice carrée constituée par des bases arithmétiques libres conjuguées, éventuellement canoniques, des idéaux du couple.

Un *couple d'éléments conjugués* ρ de **I** et ρ' de **I'** est alors défini par *un couple de nombres entiers* $z_1\ z_2$, qui sont ses *coordonnées*, *rela-*

tivement à la base matricielle; et l'équivalence des égalités précédentes peut être exprimée par une seule égalité matricielle:

$$\|\rho\ \rho'\| = \|z_1\ z_2\| \times \begin{Vmatrix} \rho_1 & \rho_1' \\ \rho_2 & \rho_2' \end{Vmatrix} = \|x\ y\| \times \begin{Vmatrix} q\times m & q\times m \\ q\times(\theta - c) & q\times(\theta' - c) \end{Vmatrix}$$

9. 4. *Bases arithmétiques surabondantes.*

Relativement à une base arithmétique, dont le nombre h, de termes, est supérieur à 2, *la représentation*, des éléments, *n'est plus propre* et *la base n'est plus libre.*

On exprime les termes de la base, au moyen d'une base arithmétique libre, de deux éléments, qui peut être canonique:

$$\rho_i = a_i\times\gamma_1 + b_i\times\gamma_2; \qquad i \text{ de } 1 \text{ à } h; \qquad a_i,\ b_i \text{ nombres entiers.}$$

Les propriétés usuelles des équations linéaires homogènes montrent qu'il est possible de trouver des nombres entiers u_i, non tous nuls, tels que:

$$\{\Sigma u_i\times a_i = 0 \text{ et } \Sigma u_i\times b_i = 0\} \Rightarrow \Sigma u_i\times\rho_i = 0.$$

Il en résulte que si un élément ρ, de l'idéal est construit, au moyen de la base avec un système de multiplicateurs z_i, il l'est aussi avec tous les systèmes $z_i+\lambda u_i$ (λ nombre entier arbitraire), car:

$$\rho = \Sigma z_i\times\rho_i \Rightarrow \Sigma(z_i+\lambda u_i)\times\rho_i = \Sigma z_i\times\rho_i + \lambda\times\Sigma u_i\times\rho_i = \rho.$$

On exprime ces propriétés en disant que: *les termes* —ou les générateurs— de la base *sont dépendants* (il existe entre eux une relation); ou que *la base arithmétique est surabondante* (on peut construire une base d'un nombre moindre de termes).

9. 5. *Construction d'une forme canonique.*

On peut préciser des conditions pour que des éléments d'un corps quadratique, en nombre h constituent une base arithmétique d'un idéal (fractionnaire). On peut alors construire sa forme canonique (**8. 1** et **8. 2**) par des opérations d'arithmétique élémentaire (sur des nombres rationnels).

THÉORÈME caractéristique d'une base arithmétique. — Dans un corps quadratique $\mathbf{R}(\theta)$, dont une base des entiers

est 1τ, *pour qu'un système, de h éléments* ρ_i, *soit une base arithmétique d'un idéal* **I**, il faut et il suffit: que les h produits $\rho_i \times \tau$ puissent être construits, par additions et soustractions au moyen des termes ρ_i; c'est-à-dire qu'*il existe* (au moins) un système de h^2 *nombres entiers* z_{ij}, tel que:

$$\rho_i \times \tau = \Sigma z_{ij} \times \rho_j; \qquad j \text{ de } 1 \text{ à } h \text{ dans } \Sigma; \qquad \text{égalités } i \text{ de } 1 \text{ à } h.$$

On peut prendre τ égal à θ, ou à θ', ou, plus généralement à $\pm\theta+e$; e nombre entier arbitraire.

La condition est *nécessaire*: Si l'ensemble $\mathbf{I}_0$, construit avec les ρ_i est un idéal, il doit contenir les produits des ρ_i par tout entier du corps (**8. 2**) et, notamment, par τ.

La condition est *suffisante*. L'ensemble $\mathbf{I}_0$ vérifie bien les trois conditions de la définition axiomatique (**8. 2**): 1° il contient les sommes et les différences de ses éléments; 2° les facteurs rationnels de ses éléments:

$$\rho = \Sigma x_i \times \rho_i; \qquad x_i \text{ nombres entiers};$$

sont limités inférieurement; ils sont au moins égaux au p.g.c.d. des facteurs rationnels des ρ_i. Pour vérifier 3, il suffit de former le produit d'un élément ρ par un entier arbitraire du corps $a+b\tau$; (a,b nombres entiers):

$$(\Sigma x_i \times \rho_i) \times (a+b\tau) = \Sigma(x_i a) \times \rho_i + \Sigma[\Sigma(x_i b z_{ij})] \times \rho_j.$$

C'est bien une forme des h termes ρ_j, avec des multiplicateurs:

$$x_i a + \Sigma(x_j b z_{ij}) \text{ nombres entiers.}$$

Le théorème est trivial si les ρ_i sont tous nuls, la condition est manifestement remplie, l'idéal engendré est l'*idéal nul.*

Si non, on peut vérifier (à nouveau, voir **9. 1**), que *la base ne peut se réduire à un seul terme*: $\rho_1 = r_1 + s_1\theta$, car en prenant le produit par θ, la condition est exprimée par:

$$(r_1+s_1\theta) \times (\theta) = z \times (r_1+s_1\theta) \qquad \text{ou} \qquad \begin{cases} zr_1+Ns_1 & = 0 \\ r_1+(S-z)s_1 & = 0. \end{cases}$$

Ces égalités considérées comme des équations linéaires et homogènes en r_1 et s_1 ne peuvent avoir que des solutions nulles, puisque leur déterminant

$$N-z(S-z) = z^2-Sz+N$$

ne peut être nul, pour z égal à un nombre entier (**1**).

Pour un idéal **I**, non nul, défini par une base arithmétique, dont les termes, en nombre h, au moins égal à 2, sont exprimés par leurs coordonnées r_i et s_i, relativement à une base canonique du corps $\mathbf{R}(\theta)$:

$$\rho_i = r_i + s_i\theta; \quad i \text{ de 1 à } h; \quad r_i, s_i \text{ nombres rationnels;}$$

la forme canonique peut être obtenue par les constructions suivantes.

1. *Le facteur rationnel* q, de **I**, *est égal au p.g.c.d. positif des multiplicateurs* s_i (deuxièmes coordonnées des ρ_i), qui ne sont pas tous nuls.

2. *Le facteur canonique* **M**, *de* $\mathbf{I} = q \times \mathbf{M}$, a pour *base arithmétique* les h quotients:

$$\alpha_i = \rho_i \times q^{-1} = a_i + b_i\theta; \quad [a_i = r_i \times q^{-1}, \quad b_i = s_i \times q^{-1}],$$

qui sont des entiers du corps.

3. *Une racine* c, *de l'idéal canonique* **M**, est obtenue, en appliquant aux a_i (premières coordonnées des α_i) les multiplicateurs qui permettent de construire le p.g.c.d., au moyen des s_i:

$$q = \Sigma u_i \times s_i \quad \Rightarrow \quad \Sigma u_i \times a_i = -c; \quad u_i \text{ nombres entiers.}$$

4. *La norme* m, de **M**, est égale au *p.g.c.d. positif des* h *entiers rationnels*, appartenant à **M**:

$$[\alpha_i - b_i \times (\theta - c)] = a_i + b_i c; \quad i \text{ de 1 à } h.$$

En prenant τ égal à θ, les conditions que doivent vérifier les générateurs ρ_i sont exprimées par:

$$(r_i + s_i\theta) \times \theta = \Sigma z_{ij}(r_j + s_j\theta) \quad \Leftrightarrow \quad \begin{cases} -Ns_i = \Sigma z_{ij} \times r_j \\ r_i \times Ss_i = \Sigma z_{ij} \times s_j. \end{cases}$$

Les deuxièmes relations montrent que les s_i ne sont pas tous nuls si non, il en serait de même des r_i et par suite des ρ_i.

1. Les s_i ont donc un p.g.c.d. positif q (nombre rationnel) et ces mêmes relations montrent qu'il est diviseur des r_i. En conséquence, il existe des systèmes de nombres entiers u_i et des nombres entiers a_i et b_i, tels que:

$$\Sigma u_i \times s_i = q; \quad s_i = q \times b_i, \quad r_i = q \times a_i.$$

Pour les éléments de **I**:

$$\rho = r+s\theta = \Sigma x_i \times \rho_i = q\times(\Sigma x_i \times a_i)+q\times(\Sigma x_i \times b_i)\times\theta,$$

les multiplicateurs s sont des multiples de q et le minimum de leurs valeurs absolues est q, effectivement atteint, pour les valeurs u_i, des x_i. C'est la construction qui a été donnée (**8.1**) du *facteur rationnel.*

2. Les quotients:

$$\rho\times q^{-1} = \Sigma x_i \times \rho_i \times q^{-1} = \Sigma x_i \times \alpha_i,$$

constituent un ensemble d'entiers du corps, engendrés par les h termes α_i, qui vérifient les conditions du théorème, car:

$$\rho_i \times \tau = \Sigma z_{ij} \times \rho_j \quad \Rightarrow \quad \alpha_i \times \tau = \Sigma z_{ij} \times \alpha_j.$$

C'est donc un idéal **M**, facteur canonique de $\mathbf{I} = q\times\mathbf{M}$, et qui est, par suite, un *idéal canonique.*

D'ailleurs, d'après la construction précédente, le facteur rationnel de **M** est égal au p.g.c.d. des $b_i = s_i \times q^{-1}$, qui est égal à 1.

3. Le p.c.g.d. q, des s_i, ayant été exprimé avec des multiplicateurs u_i, on les utilise pour construire un nombre entier c,

$$\Sigma u_i \times a_i = -c \quad \Leftrightarrow \quad \Sigma u_i \times (a_i+b_i\theta) = \theta - c.$$

L'élément $\theta - c$ appartient à **M** et c est bien une racine.

4. On peut alors former les entiers rationnels de **M**, en retranchant, de chaque élément, un élément convenable de **M**, de façon à annuler le multiplicateur de θ:

$$\Sigma x_i \times (a_i+b_i\theta) - \Sigma x_i \times b_i \times (\theta - c) = \Sigma x_i \times (a_i+b_i c).$$

La norme m, de **M**, qui est la plus petite valeur absolue de ces entiers est égale au p.g.c.d. positif des h nombres entiers $a_i+b_i c$ et elle est effectivement atteinte, pour des valeurs convenables des x_i.

On vérifie aisément qu'un changement de multiplicateurs u_i, dans l'expression de q, et par suite de c, remplace cette racine par un des termes de la progression $c+\lambda m$ (λ nombre entier), (**5**).