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: 4. Bases arithmétiques des entiers d'un corps quadratique.
DOI: https://doi.org/10.5169/seals-36338

cyclique, d'ordre infini (puissances différentes, d'exposants entiers quelconques, d'un élément de base).

4. Bases arithmétiques des entiers d'un corps quadratique.

La construction des entiers du corps $\mathbf{R}(\theta)$ —ou des éléments du domaine $\mathbf{E}(\theta)$— peut être exprimée en disant qu'*ils sont engendrés, par additions et soustractions, au moyen des deux termes d'une base canonique*, indifféremment 1, θ ou 1, θ'.

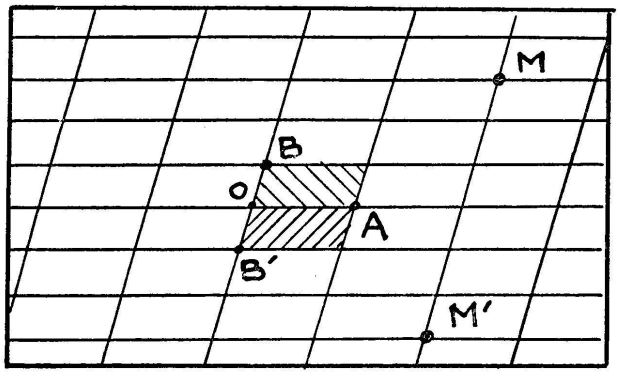
Un entier $\xi = x+y\theta$, de coordonnées x,y, nombres entiers, est égal à la somme de $|x|$ éléments égaux à $+1$, ou à -1 (suivant le signe de x), et de $|y|$ éléments égaux à θ, ou à $-\theta$ (suivant le signe de y). Le conjugué ξ' est obtenu de la même façon en remplaçant θ par θ'. En outre les coordonnées x,y sont déterminées, en particulier l'élément nul a pour coordonnées 0,0.

Cette *détermination* (et cette construction) peut être exprimée par l'un des deux énoncés suivants qui sont équivalents:

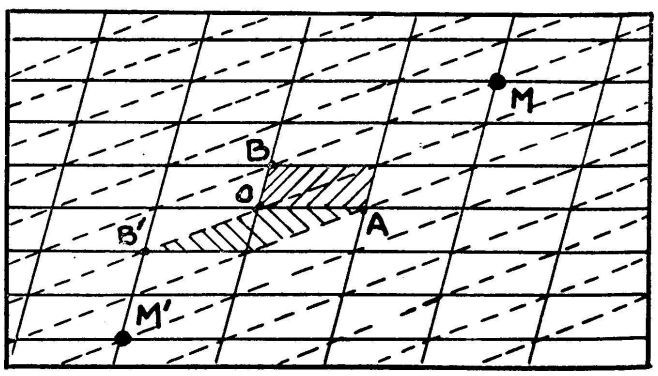
il y a une *correspondance biunivoque* entre les entiers ξ, du corps et les couples x,y de nombres entiers (qui en sont les coordonnées);

les entiers ξ sont *représentés proprement* par les points M, de coordonnées entières x,y, dans un plan, rapporté à deux vecteurs $\overrightarrow{OA}$ et $\overrightarrow{OB}$, non colinéaires, dont l'origine O représente l'élément nul et dont les extrémités A,B représentent les termes 1,θ de la base.

Les entiers conjugués ξ, ξ' sont ainsi représentés respectivement par les points M, M', définis par les relations vectorielles (fig. 1)



S=0 ; x=2 y=3



S=-1 ; x=2 y=3

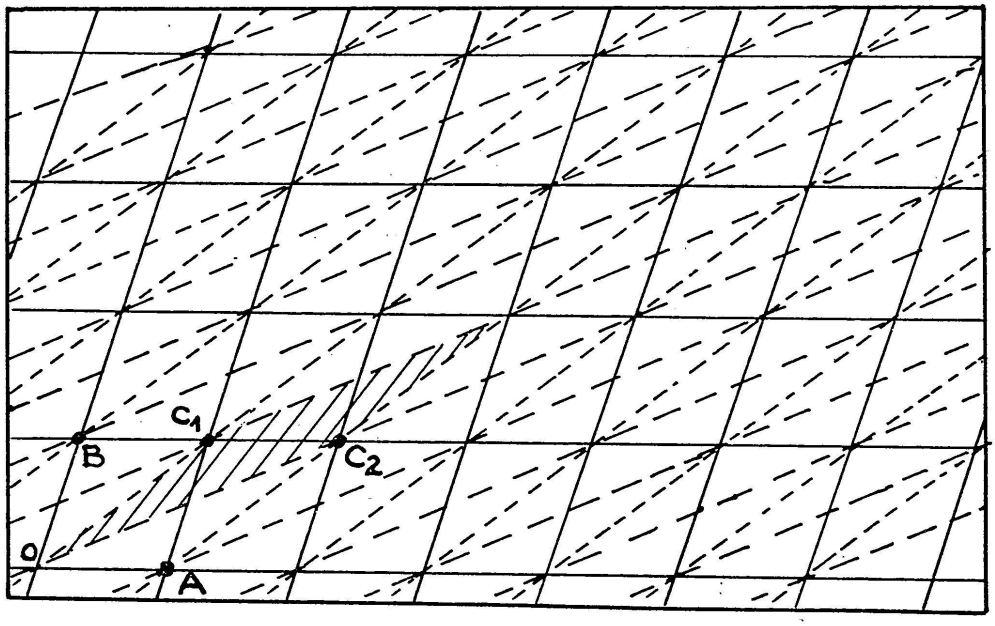
$$\overrightarrow{OM} = x.\overrightarrow{OA}+y.\overrightarrow{OB};\quad \overrightarrow{OM'} = x.\overrightarrow{OA}+y.\overrightarrow{OB'};$$
$$(\overrightarrow{OB'} = S.\overrightarrow{OA}-\overrightarrow{OB}).$$

Les points M,M' sont *symétriques obliquement*, parallèlement à la direction BB', relativement à la droite qui porte OA.

Dans cette représentation l'addition est manifestement conservée en ce sens que le point N représentant la *somme* $\eta = \xi_1+\xi_2$ [dans $\mathbf{E}(\theta)$], de deux entiers, représentés par les points M_1 et M_2 est défini par la *somme géométrique* des vecteurs $\overrightarrow{OM_1}$ et $\overrightarrow{OM_2}$:

$$\eta = \xi_1+\xi_2 \quad \Leftrightarrow \quad \overrightarrow{ON} = \overrightarrow{OM_1}+\overrightarrow{OM_2}.$$

Les points représentatifs M, de coordonnées entières, sont les sommets du *réseau de parallélogrammes* (fig. 2) construit avec les



vecteurs $\overrightarrow{OA}$ et $\overrightarrow{OB}$. On sait qu'un tel réseau peut être engendré par tout autre couple de vecteurs $\overrightarrow{OC_1}$ et $\overrightarrow{OC_2}$, à condition qu'ils forment un triangle non aplati qui ne contienne d'autres points du réseau que ses sommets O,C_1,C_2. Cette propriété qui sera établie arithmétiquement ci-dessous conduit à définir et à préciser d'autres générations du domaine $\mathbf{E}(\theta)$, par des couples d'entiers γ_1, γ_2 qui peuvent encore être appelés des *bases*, arithmétiques libres, de $\mathbf{E}(\theta)$.

4. 1: *Bases arithmétiques libres.*

DÉFINITIONS. — *On appelle* **base arithmétique**, du domaine des entiers du corps **E**(θ), *un système de h entiers* γ_i, tel que *tout entier* ξ, du corps *soit égal à* (au moins) *une forme* de ces termes γ_i, pour des *multiplicateurs* —ou des valeurs des variables— égaux à des nombres entiers:

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

Il est équivalent de dire que tout entier ξ peut être construit, au moins d'une façon, par additions et soustractions, au moyen des termes de la base: il est obtenu en additionnant les h sommes de $|z_i|$ éléments égaux à $+\gamma_i$, ou à $-\gamma_i$, suivant le signe de z_i. Les bases canoniques sont manifestement des bases arithmétiques, de deux termes.

Une base arithmétique doit contenir au moins deux termes, non nuls, car les éléments $x \times \gamma_0$, construits avec un seul terme γ_0, non nul, ne peuvent contenir le produit $\theta \times \gamma_0$, qui est encore un entier du corps, puisque:

x nombre entier et $\gamma_0 \neq 0 \Rightarrow \theta \times \gamma_0 - x \times \gamma_0 = (\theta - x) \times \gamma_0 \neq 0.$

Une base arithmétique est qualifiée **libre**, lorsque *chaque entier* ξ *n'est égal qu'à une seule* (valeur de la) *forme*, en sorte qu'elle définit une *représentation propre* des entiers ξ par les systèmes de h multiplicateurs z_i, qui sont alors appelés (sans ambiguité) les *coordonnées* de ξ, *relativement à cette base libre.*

On va d'abord étudier les bases formées de $h = 2$ termes $\gamma_1\ \gamma_2$, dont on constate que ce sont les seules qui soient libres. On disposera ces termes en colonne; les multiplicateurs ou variables étant en ligne, de sorte que la construction d'un entier peut être exprimée par le produit matriciel:

$$\xi = z_1 \times \gamma_1 + z_2 \times \gamma_2 = \| z_1\ z_2 \| \times \left\| \begin{matrix} \gamma_2 \\ \\ \gamma_2 \end{matrix} \right\|.$$

THÉORÈME de construction des bases arithmétiques libres —Dans **E**(θ), *toute base arithmétique, de deux termes*, est obtenue en *multipliant* une base canonique (en colonne), à gauche, *par une*

matrice carrée $\overline{A}$ *à termes entiers* (rationnels), et de *déterminant égal à* $+1$ *ou à* -1.

Cette base est libre et les coordonnées $x\ y$, d'un entier, relativement à la base canonique, sont obtenues en multipliant, à droite, par la même matrice, les coordonnées $z_1\ z_2$, de cet entier, relativement à la nouvelle base, disposées en ligne:

$$\left\|\begin{matrix}\gamma_1\\ \gamma_2\end{matrix}\right\| = \overline{A}\times\left\|\begin{matrix}1\\ 0\end{matrix}\right\|; \quad \text{et} \quad \|x\ y\| = \|z_1\ z_2\|\times\overline{A}$$

Le théorème comporte deux propositions particllement réciproques: d'une part: *toute nouvelle base arithmétique*, de deux termes $\gamma_1\ \gamma_2$, *est obtenue par une telle multiplication.*

Les entiers (du corps) γ_1, γ_2 peuvent être construits avec 1 et θ, ce qui peut s'exprimer par une égalité matricielle: multiplication par une matrice $\overline{A}$, dont les termes sont des nombres entiers:

$$\begin{matrix}\gamma_1 = x_1+y_1\theta\\ \gamma_2 = x_2+y_2\theta\end{matrix} \quad \text{ou} \quad \left\|\begin{matrix}\gamma_1\\ \gamma_2\end{matrix}\right\| = \overline{A}\times\left\|\begin{matrix}1\\ \theta\end{matrix}\right\|; \quad \overline{A} = \left\|\begin{matrix}x_1\ y_1\\ x_2\ y_2\end{matrix}\right\|$$

Mais les entiers 1 et θ doivent pouvoir être construits, d'une façon analogue, en multipliant (à gauche) la nouvelle base par une matrice convenable $\overline{B}$, dont les termes sont aussi des nombres entiers; On en déduit:

$$\left\|\begin{matrix}1\\ \theta\end{matrix}\right\| = \overline{B}\times\left\|\begin{matrix}\gamma_1\\ \gamma_2\end{matrix}\right\| \text{ et } \left\|\begin{matrix}\gamma_1\\ \gamma_2\end{matrix}\right\| = \overline{A}\times\left\|\begin{matrix}1\\ \theta\end{matrix}\right\| \Rightarrow \left\|\begin{matrix}1\\ \theta\end{matrix}\right\| = (\overline{B}\times\overline{A})\times\left\|\begin{matrix}1\\ \theta\end{matrix}\right\|.$$

L'implication est une conséquence de l'associativité de la multiplication des matrices —ou de l'élimination de γ_1, γ_2 entre les équations qu'expriment les égalités matricielles— .

Mais, relativement à la base canonique elle-même, 1 et θ ont des coordonnées déterminées qui sont 1, 0 et 0, 1; donc:

$$\overline{B}\times\overline{A} = \left\|\begin{matrix}1\ 0\\ 0\ 1\end{matrix}\right\| \quad \text{ou} \quad [1], \quad \text{matrice unité.}$$

Les déterminants de B et A, qui sont des nombres entiers, dont le produit est égal à $+1$, sont donc égaux à η ($+1$ ou -1). S'il en est ainsi pour la matrice A, elle a une inverse déterminée, à termes entiers:

$$x_1y_2 - x_2y_1 = \eta \quad \Rightarrow \quad \overline{B} = \overline{A}^{-1} = \begin{Vmatrix} \eta y_2 & -\eta y_1 \\ -\eta x_2 & \eta x_1 \end{Vmatrix}$$

Réciproquement, *un couple d'entiers du corps* $\gamma_1\ \gamma_2$, *ainsi construits* par multiplication par une telle matrice $\overline{A}$, *forment une base arithmétique*, qui est *libre.*

Tout élément égal à une forme de ces entiers, avec des multiplicateurs entiers rationnels $z_1\ z_2$, est un entier du corps et on peut calculer ses coordonnées relativement à la base canonique, en appliquant leur détermination:

$$\|x\ y\| \times \begin{Vmatrix} 1 \\ \theta \end{Vmatrix} = \|z_1\ z_2\| \times \overline{A} \times \begin{Vmatrix} 1 \\ \theta \end{Vmatrix} \quad \Rightarrow \quad \|x\ y\| = \|z_1\ z_2\| \times \overline{A}$$

C'est la construction annoncée des coordonnées: à tout couple de nombres entiers $z_1\ z_2$ correspond un, et un seul, couple de nombres entiers $x\ y$. Mais on peut, réciproquement, exprimer $z_1\ z_2$ en fonction de $x\ y$, utilisant la matrice inverse —ou en résolvant les équations linéaires— :

$$\|z_1\ z_2\| = \|x\ y\| \times \overline{A}^{-1};$$

comme la matrice $\overline{A}^{-1}$ est à termes entiers, à tout couple de nombres entiers $x\ y$, correspond un, et un seul, couple de nombres entiers $z_1\ z_2$, qui sont les coordonnées relativement à la nouvelle base, qui est donc *libre.*

On peut aussi bien disposer les éléments des *bases en lignes* et les *coordonnées en colonnes*; les matrices $\overline{A}$ et $\overline{A}^{-1}$ doivent alors être remplacées par leurs *transposées*, notées $\tilde{A}$ et $\tilde{A}^{-1}$ et obtenues en permutant, dans les précédentes, lignes et colonnes de même rang:

$$\tilde{A} = \begin{Vmatrix} x_1 & x_1 \\ y_1 & y_2 \end{Vmatrix} \qquad \tilde{A}^{-1} = \begin{Vmatrix} \eta y_2 & -\eta x_2 \\ -\eta y_1 & \eta x_1 \end{Vmatrix}.$$

On remarquera que la transposée de l'inverse est égale à l'inverse de la transposée et que les déterminants des quatre matrices ainsi considérées ont la même valeur η (+1 ou —1).

On peut ainsi noter la construction de la *nouvelle base* et du *nouveau couple de coordonnées*, tous deux *disposés de la même façon*; en colonnes —ou en lignes— :

$$\left\|\begin{matrix}\gamma_1\\ \gamma_2\end{matrix}\right\| = \bar{A} \times \left\|\begin{matrix}1\\ \theta\end{matrix}\right\|; \quad \left\|\begin{matrix}z_1\\ z_2\end{matrix}\right\| = \tilde{A}^{-1} \times \left\|\begin{matrix}x\\ y\end{matrix}\right\| \quad \text{ou} \quad \begin{matrix}\|\gamma_1\ \gamma_2\| = \|1\ \theta\| \times \tilde{A} \\ \|z_1\ z_2\| = \|x\ y\| \times \bar{\tilde{A}}^{-1}\end{matrix}$$

4. 2. *Substitutions linéaires contragrédientes et unimodulaires.*

DÉFINITIONS. — On appelle *substitution linéaire*, définie par une *matrice carrée* $\bar{A}$ (d'ordre 2), le *remplacement d'une colonne* —ou d'une ligne— d'un couple d'éléments (d'un certain domaine) par le produit de sa *multiplication, à gauche* —ou à droite— *par la matrice* $\bar{A}$.

La *substitution inverse*, est celle qui exprime l'ancien couple en fonction du nouveau; elle est définie si le déterminant de $\bar{A}$ a un inverse; elle est alors obtenue par la *multiplication par la matrice inverse* $\bar{A}^{-1}$.

Deux substitutions sont *contragrédientes* lorsqu'elles sont respectivement définies par une matrice et la transposée de son inverse.

Une *matrice carrée* $\bar{A}$ (d'ordre 2), ainsi que la *substitution* linéaire qu'elle définit, *est appelée unimodulaire*, lorsque *ses termes sont des nombres entiers* et que *son déterminant est égal à* +1 *ou à* —1. Il en est alors de même de la matrice inverse $\bar{A}^{-1}$ et des matrices transposées $\tilde{A}$ et $\tilde{A}^{-1}$, ainsi que des substitutions qu'elles définissent.

Avec ce vocabulaire le *remplacement*: d'une *base canonique* par une *base arithmétique* (de 2 termes, donc libre); et des *couples de coordonnées*, d'un entier du corps, relativement à ces bases, sont deux *substitutions* (linéaires) *unimodulaires contragrédientes.*

Le produit et le quotient —ou produit par l'inverse— de deux matrices —ou substitutions— unimodulaires est encore unimodulaire (en raison de la règle de multiplication des déterminants). Comme la

multiplication des matrices est une opération associative, les matrices unimodulaires forment un *groupe* qui contient l'inverse et la transposée de chacune d'elles: $\overline{A}$, $\tilde{A}$ et $\overline{A}^{-1}$, $\tilde{A}^{-1}$.

Il en résulte que *deux bases* arithmétiques (de deux termes, donc libres) et les *deux couples de coordonnées* d'un même entier du corps, relativement à ces bases, sont liés par *deux substitutions unimodulaires contragrédientes.*

4. 3. *Bases conjuguées et base matricielle.*

Deux entiers conjugués ξ et ξ' ont manifestement des coordonnées égales, relativement à une base arithmétique libre et à sa conjuguée, c'est-à-dire formée de termes respectivement conjugués:

$$\xi = \|z_1\ z_2\| \times \left\| \begin{matrix} \gamma_1 \\ \\ \gamma_2 \end{matrix} \right\| \quad \Leftrightarrow \quad \xi' = \|z_1\ z_2\| \times \left\| \begin{matrix} \gamma_1' \\ \\ \gamma_2' \end{matrix} \right\|$$

Les bases canoniques conjuguées $1\ \theta$ et $1\ \theta'$ sont des bases arithmétiques libres conjuguées particulières.

On appellera **base matricielle**, éventuellement canonique, une matrice carrée, d'ordre 2, constituée par deux bases arithmétiques libres, conjuguées, disposées en colonne. On peut utiliser une telle base pour exprimer la construction commune de deux entiers conjugués:

$$\Gamma = \left\| \begin{matrix} \gamma_1\ \gamma_1' \\ \\ \gamma_2\ \gamma_2' \end{matrix} \right\|; \quad \|\xi\ \xi'\| = \|z_1\ z_2\| \times \Gamma.$$

Deux bases matricielles Γ et Δ et les couples de coordonnées (d'un couple d'entiers conjugués $\xi\ \xi'$, du corps) relativement à ces bases: $z_1\ z_2$ et $t_1\ t_2$ se déduisent l'un de l'autre par des substitutions unimodulaires contragrédientes:

$$\Delta = \overline{A} \times \Gamma; \quad \|z_1\ z_2\| = \|t_1\ t_2\| \times \overline{A}.$$

L'étude des *bases arithmétiques*, qui ne sont pas présumées libres, sera faite ci-dessous dans le cas général des bases d'un idéal (9).