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: 2. Eléments conjugués.
DOI: https://doi.org/10.5169/seals-36338

L'ensemble $\mathbf{R}(\theta)$, formé de ce groupe et de l'élément nul, est un **corps**, au sens général de ce terme (ce qui justifie le nom de *corps quadratique*). L'ensemble des éléments rationnels r, de $\mathbf{R}(\theta)$, en est un **sous-corps**, **isomorphe** —ou, par abréviation, égal— *au corps* **R**, des nombres rationnels (inversement $\mathbf{R}(\theta)$ est **sur corps** de **R**).

La construction de l'addition, de la soustraction et de la multiplication et les qualités de ces opérations resteraient valables, même sans l'hypothèse d'irréductibilité de $F(x)$; les inverses n'existeraient alors que pour certains des éléments $r+s\theta$ (ceux pour lesquels $-r:s$ n'annule pas $F(x)$). L'ensemble construit serait seulement un **anneau**, commutatif avec une unité, —ou au sens restreint— .

On peut aussi considérer que $\mathbf{R}(\theta)$ est un *sous-corps* du *corps* des nombres: *réels* si D est positif; *complexes* si D est négatif. Cette conception fournit encore une justification des règles de calcul, y compris la division. Elle sera utilisée ci-dessous pour établir la détermination des cycles d'idéaux semi-réduits, dans un corps réel (**46** et **47**).

2. Eléments conjugués.

Définition. — Dans le corps quadratique $\mathbf{R}(\theta)$, *deux éléments sont appelés* **conjugués**, ou chacun d'eux est le conjugué de l'autre, *lorsqu'ils sont égaux*, respectivement, *à des formes de* 1, θ *et de* 1, θ', *avec les mêmes multiplicateurs* (nombres rationnels). Ils sont désignés par la même lettre, avec et sans accent (comme θ et θ', qui sont des éléments conjugués particuliers):

$$\rho = r+s\theta = (r+Ss)-s\theta' \quad \Leftrightarrow \quad \rho' = r+s\theta' = (r-Ss)-s\theta.$$

Un élément du corps est *égal à son conjugué*, si et seulement si c'est un *élément rationnel* (coefficient de θ nul). Pour le vérifier, il suffit de former la différence de deux conjugués:

$$0 = \rho-\rho' = s\times(\theta-\theta') = -Ss+2s\theta = Ss-2s\theta' \quad \Leftrightarrow \quad s = 0.$$

Les éléments θ et θ' sont conjugués et inégaux.

Deux éléments de $\mathbf{R}(\theta)$, *obtenus en remplacant* x *par* θ *et* θ', *dans un même polynôme* $f(x)$, à coefficients rationnels, *sont conjugués*:

$$f(\theta) = r+s\theta = \rho \quad \Leftrightarrow \quad f(\theta') = r+s\theta' = \rho'.$$

Car les éléments θ et θ', annulant chacun le polynôme fondamental (dans $\mathbf{R}(\theta)$), les valeurs qu'ils donnent à $f(x)$, sont respectivement égales à celles qu'ils donnent au binôme du premier degré:

$$r+sx = f(x) - F(x)\times q(x),$$

reste de la division de $f(x)$ par $F(x)$.

En particulier les éléments conjugués d'une somme, d'un produit (ou, plus généralement, d'une expression entière, à coefficients rationnels), d'éléments de $\mathbf{R}(\theta)$, sont égaux à la somme, au produit (ou à l'expression entière) des éléments respectivement conjugués.

Propriété, caractéristique de la conjugaison. — *Pour que deux éléments*, d'un corps quadratique $\mathbf{R}(\theta)$, *soient conjugués, il faut et il suffit que leur somme et leur produit soient des éléments rationnels* —ou égaux à leurs conjugués— .

Il est équivalent de dire que les deux éléments sont simultanément *zéros d'un même polynôme*, *du second degré*, normé, à coefficients rationnels.

La condition est *nécessaire*: $\rho+\rho'$ et $\rho\times\rho'$ sont respectivement égaux à leurs conjugués, en raison de la commutativité de la somme et du produit; ils sont donc rationnels. D'ailleurs:

$$(r+s\theta)+(r+s\theta') = 2r+Ss; \quad (r+s\theta)\times(r+s\theta') = r^2 - Srs + Ns^2.$$

Les deux éléments conjugués sont zéros du trinôme normé:

$$\mathbf{r}(x) = (x-\rho)\times(x-\rho') = x^2 - (2r+Ss)x + (r^2 - Ss + Ns^2).$$

La condition est *suffisante*: en raison des propriétés de la division des polynômes, un trinôme normé du second degré $\mathbf{r}(x)$, à coefficients rationnels, considéré dans le corps $\mathbf{R}(\theta)$, ne peut avoir plus de deux zéros. Or les valeurs:

$$\mathbf{r}(r+s\theta) = \mathbf{r}(\rho) \qquad \mathbf{r}(r+s\theta') = \mathbf{r}(\rho'),$$

sont conjuguées, quel que soit le trinôme $\mathbf{r}(x)$, à coefficients rationnels.

Elles ne peuvent être nulles que simultanément; *si* $\mathbf{r}(x)$ *a un zéro, il en a un deuxième qui est le conjugué du premier.*

Si deux éléments ρ, ρ' ont pour somme et pour produit des éléments rationnels: $S(\rho) = S(\rho')$ et $N(\rho) = N(\rho')$, ils sont les deux zéros du trinôme normé

$$\mathbf{r}(x) = x^2 - S(\rho)x + N(\rho) = (x-\rho)\times(x-\rho');$$

donc sont conjugués.

Définitions. — Dans un corps quadratique $\mathbf{R}(\theta)$, pour un couple d'éléments conjugués, ρ et ρ', —ou pour chacun d'eux— , on appelle:

Trace: la somme $\rho+\rho'$, désignée par $S(\rho)$, ou $S(\rho')$;
Norme: le produit $\rho\times\rho'$, désigné par $N(\rho)$, ou $N(\rho')$;
Polynôme fondamental: le trinôme normé, qui a pour zéros ρ et ρ':

$$\mathbf{r}(x) = (x-\rho)\times(x-\rho') = x^2 - S(\rho)\times x + N(\rho);$$

Discriminant: le carré de leur différence, qui est encore un élément rationnel:

$$(\rho-\rho')^2 = [S(\rho)]^2 - 4N(\rho) = s^2\times D; \qquad \text{désigné par } D(\rho).$$

Pour deux éléments conjugués, exprimés avec le générateur θ, ou θ':

$$\rho = r+s\theta = r'+s'\theta'; \qquad \rho' = r+s\theta' = r'+s'\theta;$$

la trace et la norme sont égales indifféremment à:

$$S(\rho) = S(\rho') = 2r+Ss = 2r'+Ss';$$
$$N(\rho) = N(\rho') = r^2+Srs+Ns^2 = r'^2+Sr's'+Ns'^2.$$

On peut encore exprimer la norme en utilisant la décomposition de $4F(x)$:

$$4N(\rho) = 4N(\rho') = (2r+Ss)^2 - Ds^2 = (2r'+Ss')^2 - Ds'^2.$$

Pour le couple d'éléments θ et θ', ces expressions deviennent:

$$S(\theta) = S(\theta') = S; \quad N(\theta) = N(\theta') = N; \quad D(\theta) = D(\theta') = D.$$

Pour un élément rationnel r, ce sont:

$$S(r) = 2r; \quad N(r) = r^2; \quad D(r) = 0.$$

De ces définitions il résulte que: l'*inverse* ρ^{-1}, d'un élément ρ, non nul, *est égal au produit de son conjugué par l'inverse de sa norme*:

$$\rho^{-1} = \rho' \times [N(\rho)]^{-1}, \qquad \rho'^{-1} = \rho \times [N(\rho)]^{-1}$$

La *transformation* —ou l'*autotransformation*— qui, dans un corps quadratique $\mathbf{R}(\theta)$, fait correspondre —ou substitue— à tout élément ρ son conjugué ρ', est *biunivoque* et *involutive* (le conjugué du conjugué est égal à l'élément lui-même). Elle conserve les éléments rationnels —ou laisse invariant le sous-corps $\mathbf{R}$— elle conserve les opérations (addition et multiplication, ainsi que leurs inverses soustraction et division): le conjugué (du résultat) d'une expression rationnelle à coefficients rationnels, d'éléments du corps est égal à (le résultat) de l'expression rationnelle, avec les mêmes coefficients, des conjugués respectifs des éléments de l'expression primitive.

Dans le langage de l'algèbre moderne, la conjugaison est un **automorphisme** du corps $\mathbf{R}(\theta)$, considéré comme une *extension* du corps $\mathbf{R}$, ou comme une *adjonction* à ce corps $\mathbf{R}$, d'un zéro de $F(x)$.

3. Domaine des entiers (algébriques) d'un corps quadratique.

Par anticipation de la définition générale des bases d'un idéal (**9**), on appellera **bases canoniques conjuguées**, d'un corps quadratique $\mathbf{R}(\theta) = \mathbf{R}(\theta')$, les deux couples conjugués d'éléments, éventuellement disposés en colonnes:

$$1\ \theta, \quad \text{ou} \quad \begin{Vmatrix} 1 \\ \theta \end{Vmatrix}; \qquad 1\ \theta', \quad \text{ou} \quad \begin{Vmatrix} 1 \\ \theta' \end{Vmatrix};$$

qui ont permis d'engendrer les couples d'éléments conjugués du corps par des formes, qui peuvent être écrites en produits matriciels:

$$\rho = r + s\theta = \|rs\| \times \begin{Vmatrix} 1 \\ \theta \end{Vmatrix}; \qquad \rho' = r + s\theta' = \|rs\| \times \begin{Vmatrix} 1 \\ \theta' \end{Vmatrix}$$

Les nombres rationnels r,s, multiplicateurs —ou variables—, de la forme qui définit un élément ρ, seront appelés les **coor-**