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

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 **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 **R**, ou comme une *adjonction* à ce corps **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:

$$1\ \theta, \quad \text{ou} \quad \left\| \begin{matrix} 1 \\ \theta \end{matrix} \right\|; \qquad 1\ \theta', \quad \text{ou} \quad \left\| \begin{matrix} 1 \\ \theta' \end{matrix} \right\|;$$

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

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

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

données: *de* ρ, *relativement à la base utilisée*, et aussi du couple d'éléments conjugués, relativement au couple des bases conjuguées.

Les coordonnées des termes d'une base, relativement à elle-même, sont respectivement 1, 0 et 0, 1. La permutation —ou transposition— des bases conjuguées remplace, ainsi qu'il a été dit r,s par $r+Ss, -s$.

DÉFINITIONS. — On appellera **facteur rationnel**, d'un élément ρ (et du couple d'éléments conjugués ρ,ρ'), *le plus grand commun diviseur positif* q, *de ses coordonnées*, relativement à l'une —ou au couple— des bases canoniques conjuguées.

Le facteur rationnel q est indépendant de la base choisie —ou de l'ordre du couple— , car:

$$\text{p.g.c.d. positif } (r,s) = \text{p.g.c.d. positif } (r+Ss, -s).$$

Un élément —ou un couple d'éléments conjugués— est égal au produit de son facteur rationnel par un élément —ou un couple d'éléments conjugués— dont les coordonnées sont des nombres (entiers rationnels) premiers entre eux a,b:

$$\rho = q\times(a+b\theta), \quad \rho' = q\times(a+b\theta'); \quad \text{p.g.c.d.}(a,b) = 1.$$

DÉFINITIONS. — *On appelle* **entier algébrique d'un corps R**(θ) —ou, en abrégé, **entier du corps**— *tout élément*, du corps, *dont le facteur rationnel* est un nombre entier —ou dont les coordonnées relativement à une base canonique sont des nombres entiers— .

Un entier du corps est qualifié **canonique**, lorsque son facteur rationnel est égal à $+1$ —ou lorsque ses coordonnées sont des (nombres entiers) premiers entre eux— .

Ces définitions et ces propriétés peuvent être rassemblées dans l'énoncé suivant:

deux éléments conjugués du corps sont égaux aux *produits de leur facteur rationnel q par deux éléments conjugués* $\alpha\,\alpha'$ qui sont des *entiers algébriques canoniques*:

$$\rho = q\times\alpha, \quad \rho' = q\times\alpha'; \quad \text{ou} \quad \|\rho\,\rho'\| = q\times\|\alpha\,\alpha'\|$$

Un *élément rationnel* du corps:

$$r+0.\theta = r+0.\theta'; \qquad \text{ou simplement} \quad r;$$

de coordonnées r et 0, est égal à son conjugué; son facteur rationnel est égal à la valeur absolue $|r|$; *c'est un entier algébrique* —ou un entier du corps— *si et seulement si r est un nombre entier*, dans ce cas il est appelé indifféremment: *entier rationnel du corps —ou nombre entier—* .

Les seuls éléments rationnels du corps qui soient des entiers algébriques canoniques sont $+1$ et -1 —l'unité et son opposée—.

THÉORÈMES de la définition axiomatique des entiers algébriques. — 1. Dans un corps quadratique, pour qu'un entier du corps α (et simultanément l'entier conjugué α') *soit un entier canonique, il faut et il suffit que les nombres entiers* $[S(\alpha)]^2$ *et* $N(\alpha)$ *n'aient pas de diviseur carré commun*, sauf l'unité.

2. *Pour qu'un élément* ρ (et, simultanément l'élément conjugué ρ') *soit un entier du corps, il faut et il suffit que sa trace* $S(\rho)$ *et sa norme* $N(\rho)$ *soient des nombres entiers.*

Il est équivalent de dire que ρ (et simultanément le conjugué ρ') doit être zéro d'un trinôme normé du second degré (qui est son polynôme fondamental), dont les coefficients $S(\rho)$ et $N(\rho)$ soient des nombres entiers.

On établit la *première propriété* par contraposition. La condition est *nécessaire*: si un entier α du corps, de coordonnées a, b n'est pas canonique, il existe (au moins) un diviseur premier p, différent de 1, commun à a et b et son carré p^2 est diviseur commun de:

$$|S(\alpha)|^2 = (2a+Sb)^2 \qquad \text{et} \qquad N(\alpha) = a^2+Sab+Nb^2.$$

La condition est *suffisante*: on peut utiliser l'expression (**2**) de la norme de l'entier algébrique $\alpha = a+b\theta$; (a,b nombres entiers):

$$4N(\alpha) = (2a+Sb)^2-Db^2 = |S(\alpha)|^2-Db^2.$$

Si le carré p^2 d'un *nombre premier impair* p était diviseur commun de $|S(\alpha)|^2$ et de $N(\alpha)$, comme il ne peut diviser D qui n'a pas de facteur carré, le nombre premier p diviserait b et $S(\alpha) = 2a+Sb$, donc a et b, de sorte que l'entier algébrique α ne serait pas canonique.

On peut établir l'impossibilité d'un diviseur 2^2, —ou 4— en

distinguant les deux cas de construction de $\mathbf{R}(\theta)$. Pour $S = 0$, la norme $N(\alpha) = a^2+Nb^2$ ne peut être divisible par 4, car, suivant les parités de a,b (premiers entre eux):

$$\begin{array}{lll} a,b \text{ impairs} & : & \mathrm{N}(\alpha) \equiv 1+N \not\equiv 0, \pmod 4; \\ a \text{ pair, } b \text{ impair:} & & N(\alpha) \equiv \quad N \not\equiv 0, \pmod 4; \\ a \text{ impair, } b \text{ pair:} & & N(\alpha) \equiv 1 \quad \not\equiv 0, \pmod 4. \end{array}$$

Pour $S = -1$, on peut considérer, suivant le cas, la trace ou la norme:

b impair: $\mathrm{S}(\alpha) = 2a-b$ n'est pas divisible par 4;
b pair et a impair: $N(\alpha) = a^2-ab+Nb^2 \equiv 1$ ou $3, \not\equiv 0, \pmod 4$.

On peut alors établir la deuxième propriété; la condition est *nécessaire*: si les coefficients de ρ sont entiers, il en est évidemment de même de $S(\rho)$ et de $N(\rho)$.

La condition est *suffisante*: si le facteur q, de ρ, n'est pas entier, son dénominateur a (au moins) un facteur premier p qui ne divise pas le numérateur (q sous forme irréductible). D'après les expressions de la trace et de la norme:

$$|S(\rho)|^2 = q^2 \times |S(\alpha)|^2, \quad N(\rho) = q^2 \times N(\alpha); \quad \alpha \text{ entier canonique;}$$

p^2 ne peut diviser simultanément $|S(\alpha)|^2$ et $N(\alpha)$; donc $S(\rho)$ et $N(\rho)$ ne peuvent être simultanément des nombres entiers.

L'ensemble des entiers algébriques du corps $\mathbf{R}(\theta)$, qui sera désigné par $\mathbf{E}(\theta)$ est un *domaine d'intégrité*, c'est-à-dire que:

il contient les *sommes*, les *différences* et les *produits mutuels* de ses éléments, ainsi que l'élément unité 1 (donc tous les entiers rationnels du corps); en outre tout élément α, non nul est *régulier*, c'est-à-dire que l'égalité de deux produits par α peut être *simplifiée* et entraîne l'égalité des facteurs:

$$\alpha \times \delta_1 = \alpha \times \delta_2 \quad \Leftrightarrow \quad \alpha \times (\delta_1 - \delta_2) = 0 \quad \Leftrightarrow \quad \delta_1 = \delta_2.$$

Pour vérifier cette régularité, on peut considérer l'égalité dans le corps et en multiplier les deux membres par l'inverse α^{-1}. On pourrait aussi, dans le domaine $\mathbf{E}(\theta)$ considéré seul, multiplier les deux membres par le conjugué de α.

Le domaine $\mathbf{E}(\theta)$ contient tous les entiers rationnels du corps $\mathbf{R}(\theta)$

—ou tous les nombres entiers— ; ils y constituent un **sous-domaine**, qui sera désigné par **E** et qui est *isomorphe* au domaine des nombres entiers (ordinaires, désigné souvent par **Z**).

La conjugaison établit dans $\mathbf{E}(\theta)$ une autocorrespondance (le conjugué d'un entier du corps est un entier), ou, plus exactement un **automorphisme** (**2**), qui conserve les opérations et laisse invariants les entiers rationnels, en sorte que $\mathbf{E}(\theta)$ est une *extension* de **E**.

DÉFINITION. — On *appelle* **diviseur de l'unité** *un entier algébrique* ε, *dont l'inverse* ε^{-1} *est aussi entier algébrique*, en sorte que cet inverse est aussi diviseur de l'unité.

Un *produit* de diviseurs de l'unité est encore diviseur de l'unité, puisque l'inverse de ce produit, étant égal au produit des inverses des facteurs, est aussi un entier algébrique. Il en résulte que les diviseurs de l'unité d'un corps quadratique $\mathbf{R}(\theta)$, qui appartiennent au domaine $\mathbf{E}(\theta)$ forment un *groupe abélien*, multiplicatif; il est sous-groupe du groupe des éléments non nuls du corps; il sera désigné par $\mathbf{U}(\theta)$.

La construction de l'inverse (**1.— 2**) montre que deux diviseurs inverses de l'unité sont des entiers conjugués, dont la norme commune est égale à $+1$ ou à -1. Les diviseurs de l'unité ε, dans le corps $\mathbf{R}(\theta)$ sont donc obtenus par la résolution (en nombres entiers, x,y; coefficients du diviseur cherché) de l'équation, connue sous le nom de PELL-FERMAT:

$$x^2+Sxy+Ny^2 = +1 \quad \text{ou} \quad -1; \qquad x,y \text{ nombres entiers.}$$

La structure du groupe $\mathbf{U}(\theta)$ dépend de la nature du corps, réel ou imaginaire, c'est-à-dire encore du signe de d, ou D. On voit immédiatement que:

pour toute valeur négative de d, exceptées -1 et -3, il n'y a que *deux diviseurs de l'unité* $+1$ et -1;

pour $d = -1$, il y a *quatre diviseurs de l'unité* $+1, -1, +i, -i$; (i désignant, suivant l'usage, un zéro de x^2+1);

pour $d = -3$, il y a *six diviseurs de l'unité* $+1, -1, +j, +j^2, -j, -j^2$; (zéros de x^2-1, de x^2+x+1, et de x^2-x+1).

On étudie ci-dessous le cas de d positif; le groupe $\mathbf{U}(\theta)$ est alors formé des produits par $+1$ et par -1, des éléments d'un *groupe*

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'.

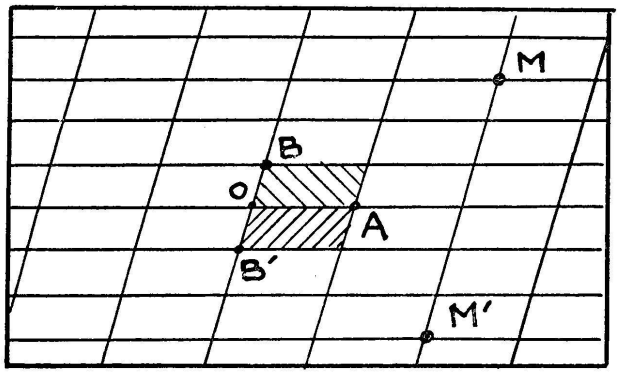
Un entier $\xi = x+y\theta$, de coordonnées x,y, nombres entiers, est égal à la somme de $|x|$ éléments égaux à $+1$, ou à -1 (suivant le signe de x), et de $|y|$ éléments égaux à θ, ou à $-\theta$ (suivant le signe de y). Le conjugué ξ' est obtenu de la même façon en remplaçant θ par θ'. En outre les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

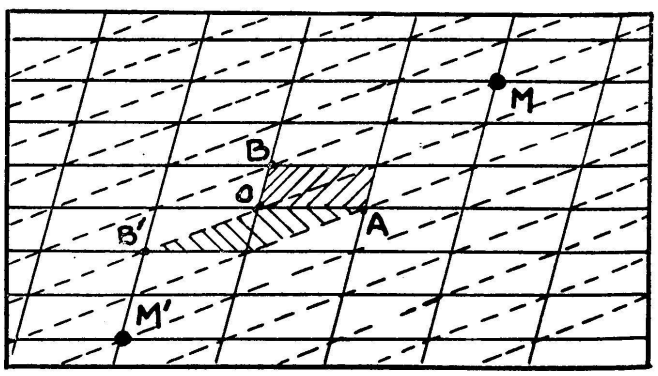
il y a une *correspondance biunivoque* entre les entiers ξ, du corps et les couples x,y de nombres entiers (qui en sont les coordonnées);

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